پیک ریاضی

جلد دوم شمارهٔ اول ، بهار ۱۳۶۶

نظریه کدگذاری : مثال نقضی برای تصورهاردی از ریاضیات کاربردی

نوشتهٔ : نورمن لوینسون

ترجمهٔ : رضا کرمی

۱. مقدمه : یکی از درون مایه‌های عمدهٔ کتاب هاردی " دفاعیهٔ یک ریاضیدان " (۱) تمایزی است که او میان دو نوع ریاضیات قائل می‌شود " ریاضیات حقیقی، یعنی کار ریاضیدانان حقیقی، که تقریبا " بتمامی بی فایده است " . و ریاضیات کاربردی که او آن را بیمایه و مبتذل می‌شمارد . برخلاف بی آزاری و معصومیت ریاضیات حقیقی، این " ریاضیات مبتذل کاربردهای بسیاری در جنگ دارد ." هاردی بویژه از بی کاربردی نظریهٔ اعداد دلخوش است ، که اگر ریاضیات حقیقی " به دردی می‌خورد ، همانقدر که باعث خیر می‌شد ، به نیروهای شر نیز فایده می‌رساند . از اینرو " می‌توان شادمانی گاوس و دیگر ریاضیدانان را ، از اینکه هرچه باشد علمی وجود دارد که صرف دور بودنش از فعالیتهای روزمرهٔ بشری متضمن نجابت و پاکیش است ، و از اینکه این علم ، علم آنهاست ، درک کرد ."

هاردی فیزیک نظری را که او شامل نسبیت و مکانیک کوانتم می‌دانست ،

سخت می‌پسندید، چراکه آنها را بکلی بی کاربرد می‌پنداشت. گرچه گذشت زمان نادرستی این پندار را ورا آشکار ساخته است، می‌توان او را به دلیل اینکه در این زمینه‌ها خبره نبوده است، معذور دانست. از این رو آزمون واقعی باورهای هاردی، باید در عرصهٔ ریاضیات محض صورت پذیرد.

در این مقاله نشان خواهیم داد که چگونه نظریهٔ کدگذاری این تصورها ردی را باطل می‌کند. میدانهای متناهی ـ یا همان میدانهای گالوا وقضایایی چند از نظریهٔ اعداد نقشی اساسی در این نظریه ایفا می‌کنند. در بسیاری از زمینه‌های ریاضیات کاربردی، نقش ریاضیات محض در بهترین حالت چیزی است در حد فراهم آوردن یک قضیه وجودی ناساختنی یا یک قضیهٔ یکتایی، و به هر حال به فراشدهای محاسبه‌ای و تحلیلی که به نتایج واقعی می‌انجامند، ربطی ندارد. در عمل فراشدهایی که به کار می‌آیند، بیش از آنکه متکی بر دقت باشند، بر پایهٔ شهود و تجربه بنا می‌شوند. در نظریهٔ کدگذاری چنین نیست. در این نظریه ریاضیدانان محض فراشدهایی ساختنی برای تولید کدها فراهم می‌کنند. این نکته بیش از ریاضیدانان محض، ممکن است ریاضیدانان کاربردی را به شگفتی وادارد. در همگامی با این گروه از خوانندگان، ما در گزارشمان آشنایی با میدانهای متناهی یا نظریهٔ اعداد را پیش دانسته نمی‌انگاریم. به جای آن، از مساله تصحیح خطا در انتقال اطلاعات با استفاده از کدها، آغاز خواهیم کرد، و نشان خواهیم داد که چگونه این مساله به معرفی شیئی ریاضی می‌انجامد، که در واقع یک میدان متناهی است. بسجمله‌های دایره‌بر(2) (سیکلوماتیک)، که از اکتشافات گاوس هستند، نقشی کلیدی ایفا خواهند کرد.

مانده‌های مربعی(3) وقانون تقابل مربعی(4) نیز (که هاردی آن را یکی از زیباترین قضیه‌های ریاضیات می‌شمارد) در نظریهٔ کدگذاری

راه یافته‌اند. ابزارکار را مددیگرقضیه باقیمانده‌ٔ چینی است. هاردی از جنبهٔ زیبایی شناختی " ریاضیات حقیقی " سخن می‌گوید. ریاضیاتی که در آن قضایای برجسته و اثباتهای آنها " حد بالایی از غیرمنتظره بودن، توام با گریزناپذیری و صرفه‌جویی" دارند. همانگونه که خواهیم دید، این در مورد شیوهٔ راهیابی میدانهای متناهی به نظریهٔ کدگذاری نیز صادق است.

همچنانکه دور از انتظار هم نیست، میدانهای متناهی را کسانی وارد نظریهٔ کدگذاری کردند، که به عنوان ریاضیدان آموزش دیده بودند. پاره‌ای از کارهای ابتدایی ظاهراً "منتشرنشده" مانده‌اند. زمینهٔ ویژه‌ای که در اینجا آن را شرح خواهیم داد، یعنی کدهای BCH، مستقلاً "کار بوز (۵) وری ـ چائودری [2] از یک طرف وهوکن هم (۷) [6] از طرف دیگر است. آنچه را که برای سودمندی واقعی روش بیشتر مهم است، یعنی یک فرآیند کارآمد کدگشایی (۸) برای این کدها، مهندسی به نام پیترسن [7] کشف کرده است. کدهای BCH را گورن اشتاین (۹) وتسیرلر (۱۰) بطورقابل ملاحظه‌ای تعمیم داده‌اند [3].

برله‌کامپ (۱۱) می‌گوید: " محدودیت ذاتی همهٔ طرحهای کدگذاری وکدگشایی ... پیچیدگی (و هزینه) کدگشا بوده است. کارهای مهم رید (۱۲) و سولومون (۱۳) (۱۹۶۰)، بوز و چائودوری (۱۹۶۰)، گورن اشتاین وتسیرلر (۱۹۶۱)، و پیترسن (۱۹۶۱) نوید بخش رهیافت نوینی به این مساله بودند. دانسته شد که می‌توان با متناظر کردن هر رقم در یک کد معین به عضوی در یک میدان متناهی، معادله‌ای جبری یافت که ریشه‌هایش مکان خطاهای کانال را نمایش می‌دهند... در نتیجهٔ این کشف اینک می‌توان کدگشاهایی جبری ساخت که به مراتب ساده‌تر از همهٔ کدگشاهای پیشتر ساخته شده‌اند" [1]

۲. کدگذاری. درآنچه از این پس می‌آید، منظور ما از یک پیام دنباله‌ٔ مرتبی خواهد بود، از دو نماد، که هدف انتقال آن از طریق یک کانال است این کانال ممکن است مثلاً" یک کابل یا یک باند فرکانس رادیویی باشد. محض سهولت این دو نماد را با ۰ و ۱ نمایش می‌دهیم. یک دنباله k تایی از این نمادها را یک k ــ بردار دودویی می‌نامیم، و آن را با $(a_1,a_2,...,a_k)$ نمایش می‌دهیم، که در آن هر a_j، 0 یا 1 است. واضح است که تعداد k بردارهای دودویی 2^k است. اگر کانال انتقال اغتشاش آلود (۱۵) باشد، بردار دریافت شده ممکن است با بردار فرستاده شده فرق کند، به عبارت دیگر فرایند انتقال ممکن است خطا پدید آورد. یک راه افزایش قابلیت اعتماد پیام دریافت شده، تکرار آن به دفعات است. این مثالی از کاربرد **افزونگی** (۱۶) **(حشو)** است، یعنی انتقال بیش از k رقم دودویی که در پیام اصلی وجود دارد، به منظور افزایش قابلیت اعتماد فرآیند انتقال.

اما تکرار ساده کارآمد نیست. در حالت کلی یک m ــ بردار دودویی فرستاده می‌شود که در آن n=k+r، k تعداد ارقام دودویی است که پیام را تشکیل می‌دهند و r تعداد ارقام افزوده است. این ارقام افزوده مطابق با قاعده‌ای معین، برحسب k رقم پیام تعیین می‌شوند. فرایند ساختن n بردار افزوده شده از k بردار اصلی را **کدگذاری** (۱۷) می‌نامند. 2^n تا n ــ بردار دودویی وجود دارد، اما فرآیند کدگذاری زیرمجموعه‌ای شامل 2^k تا از این بردارها را به دست می‌دهد، که آنها را می‌توان **کد ــ بردار** نامید. چون در انتقال خطا پدید می‌آید، n ــ بردارهایی که دریافت می‌شوند لازم نیست همان کد ــ بردارها باشند، فرآیند تصحیح n ــ بردار دریافت شده و درآوردن k ــ بردار اصلی از آن، **کدگشایی** نام دارد. اعمال حسابی در کدگذاری وکدگشایی به پیمانه‌ٔ ۲ انجام می‌شوند، یعنی با ملاحظهٔ اینکه 1+1=0. این

مطلب با جمع دودویی بدون ذوبریک معادل است، و از اینرو فرآیندی است که به سادگی می‌توان آن را در یک کامپیوتر الکترونیک طراحی کرد. این حساب دودویی تنها شامل 0 و 1 است و از قواعد زیر پیروی می‌کند:

$$0+0=0\ ,\ 0+1=1+0=1,\ 1+1=0\ ,\ 0.0=0.1=1.0=0\ ,\ 1.1=1$$

0 و 1 با این قواعد تشکیل میدانی با دو عنصر می‌دهند، که به میدان گالوا با دو عنصر، GF(2) مشهور است. (این همان جایی نیست که در آن میدانهای متناهی، نقشی اساسی در نظریه کدگذاری می‌یابند، زیرا GF(2) به تنهایی چیز بسیار پیش پا افتاده‌ای است) در آنچه که از این پس می‌آید، همه اعمال حسابی که در مورد بردارها، ماتریسها و بسجمله‌ها انجام می‌شود، در GF(2) فرض می‌شود. یادآور می‌شویم که، به پیمانهٔ ۲، همهٔ اعداد زوج با صفر و همه اعداد فرد با یک نمایش داده می‌شوند.

۳. **کد تصحیح کنندهٔ یک خطایی همینگ**[۱۸]. فرض کنید کانالی به اندازه‌ای مطمئن باشد که بتوان چنین انگاشت که به هنگام انتقال یک n- بردار دودویی بردار دریافت شده تنها شامل حداکثر یک خطا در یکی از درایه‌های خود است. با چند افزونگی می‌توان مکان خطا را مشخص کرد؟ فرض کنید m عدد صحیح مثبتی باشد و قرار دهید $n=2^m-1$. (این فرض در مورد n که از این پس آن را رعایت خواهیم کرد، بیش از حد لزوم محدود کننده است، اما برای نمایاندن ایده‌های اصلی کفایت می‌کند.) برای آنکه یک عدد دودویی b بتواند رقم خطا را در میان n رقم دودویی دریافت شده مشخص کند، باید نمایش عددی بین صفر و 2^m-1 باشد، و از اینرو خود می‌بایست m رقم داشته باشد. می‌توان قرار داد کرد که صفر بودن همهٔ این m رقم، نمایشگر آن است که هیچ خطایی اتفاق نیفتاده است. مثلاً" فرض کنیم m=4 و در نتیجه

$n=15$. دراین صورت اعداد دودویی چهار رقمی از 0001 تا 1111 همه اعداد صحیح از ۱ تا ۱۵ را نمایش می‌دهند. از ملاحظات بالا چنین به نظر می‌آید که شاید بتوان یک خطای تنها را در انتقال یک n ـ بردار ($n=2^m-1$)، با $r=m$ و درنتیجه $k=n-m$، تصحیح کرد. همینگ یک روش ممکن انجام چنین تصحیحی را کشف کرد [4]. از نو فرض کنیم $m=4$ چنان که $n=15$ و $r=4$، ودرنتیجه $k=11$. از این پس همهٔ بردارهایی که درنظر خواهیم گرفت، بردارهای ستونی خواهند بود، که آنها را (بنا بر ملاحظات چاپی) به شکل سطری هم خواهیم نوشت. کد ـ بردارها را با $C=(c_1, c_2, \ldots, c_{15})$ نشان خواهیم داد، که در آن c_jها ارقام دودویی هستند. فرض کنید H ماتریسی با ۱۵ ستون باشد، که در آن هرستون برداری دودویی است با چهار درایه، همهٔ ستونها از هم متمایزند، وهیچیک از آنها برابر بردار صفر نیستند:

$$H=\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & \ldots & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & \ldots & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & \ldots & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & \ldots & 1 \end{bmatrix}$$

(اگرستونی از H به صورت سطری نوشته شود و به عنوان نمایش دودویی یک عدد محسوب شود، شمارهٔ ستون را نشان خواهد داد. این نکته به لحاظ سادگی نمایش رعایت شده است، گرچه چندان اساسی نیست).

فرض کنیم یازده درایهٔ $c_{15}, \ldots, c_{10}, c_9, c_7, c_6, c_5, c_3$ بردار C، درایه‌های k ـ بردار پیام باشند. c_8, c_4, c_2, c_1 را چنان تعیین کنید که:

$$HC = 0 \qquad (۳۰۱)$$

این عمل امکان‌پذیر است زیرا ماتریس مربعی که از هشتمین، چهارمین،

دومین و اولین ستون H تشکیل میشود، تا تکین است (درواقع این ماتریس همان ماتریس یکه میباشد.) از (۳۰۱) نتیجه میشود که همهٔ کد- بردارهای C بر سطرهای H متعامد هستند. از آنجا که اعمال حسابی به پیمانهٔ ۲ انجام میشوند، C_8, C_4, C_2, C_1 همه ارقام دودویی خواهند بود. تعیین این چهار رقم، فرایند کدگذاری را تکمیل میکند

حال فرض کنیم که در انتقال C، چندین خطا رخ داده باشد، چنانکه n- بردار دودویی R که دریافت شده است، با C یکی نباشد. n- بردار دودویی E را چنین تعریف میکنیم.

$$E = R - C = R + C \qquad (۳۰۲)$$

(اعمال حسابی بین این بردارها، مولفه به مولفه و به پیمانهٔ ۲ انجام میشود.) اگر درایههای j ام R و C یعنی R_j و C_j با هم برابر باشند، آنگاه $E_j=0$ اما اگر $R_j \neq C_j$، آنگاه $E_j=1$. پس درایههای ناصفر بردار E دقیقا" در آن محلهایی هستند که در آنها خطایی در انتقال رخ داده است.

حال از (۳۰۱) داریم:

$$HR = HC + HE = HE$$

اگر خطایی در انتقال رخ نداده باشد، آنگاه $E = 0$ و در نتیجه $HR = 0$. اگر دقیقا" یک خطا، و آن هم در محل j ام رخ داده باشد، آنگاه $E_j = 1$ و در نتیجه:

$$HR = H^{(j)}$$

که در آن $H^{(j)}$ نمایشگر j مین ستون H است. واضح است که دانستن بردار $H^{(j)}$، j را مشخص میکند. (درواقع انتخاب ماتریس H به گونهای بود که آرایش سطری $H^{(j)}$ نمایش دودویی j را به دست میداد) پس اگر حداکثر یک خطا رخ داده باشد، HR محل این رخداد را تعیین خواهد کرد. پس با تعیین

E، چون داریم $C = R+E$، بردار C را اینک می‌توان به‌دست آورد. اگر از درایه‌های C_8, C_4, C_2, C_1 صرف‌نظر کنیم، آنچه می‌ماند همان k-بردار دودویی پیام اصلی است. این فرآیند بازسازی پیام از R، فرآیند کدگشایی است. پرواضح است که اگر بیش از یک خطا رخ داده باشد، یعنی E دارای بیش از یک درایهٔ ناصفر باشد، این فراشد دیگر معتبر نیست. برای تصحیح بیش از یک خطا در R، شاید به‌نظر برسد که باید تعداد ارقام افزوده r را افزایش دهیم، و درنتیجه k را کاهش دهیم. علاوه‌براین تغییر، برای آنکه HR محلهای خطا را در R نشان دهد، H باید سطرهای بیشتری داشته باشد. می‌توان انتظار داشت که اگر H دارای الگویی ساختمانی براساس یک الگوریتم نسبتاً "سادهٔ ریاضی" باشد، فرایند کدگشایی کمترین پیچیدگی را داشته باشد. یک طرح نسبتاً "سادهٔ ریاضی" برای یافتن محل خطاها، که حداقل از نظر اصولی تا حد تعیین تعدادی از پیش دانسته خطا کار می‌کند، در کدهای BCH که پس از این بررسی خواهند شد، به‌کار رفته است. کدهای BCH از میدانهای متناهی استفاده می‌کنند.

۴. میدانهای $GF(2^m)$. (خوانندهٔ آشنا با میدانهای متناهی، می‌تواند به مروری سطحی براین بخش بسنده کند.) یک ستون ماتریس m سطری H را می‌توان به‌عنوان یک m-بردار دودویی به‌حساب آورد (که البته در آن $m > 1$). اگر x مجهولی باشد و a_jها همگی در $GF(2)$ باشند، آنگاه می‌توان از بسجملهٔ $\sum_{j=0}^{m-1} a_j x^j$ برای نمایش یک m-بردار دودویی با درایه‌های a_j به‌کار برد (راحت‌تر است که اندیس‌نویسی j را از ۰ آغاز کنیم). چون به‌ازای هر $0 < j < m-1$، درایهٔ a_j می‌تواند صفر یا یک باشد، درکل 2^m تا از این بسجمله‌های از درجهٔ نابیشتر از $m-1$ وجود دارد. جمع این بسجمله‌ها معادل

است با جمع بردارها در $GF(2)$ ،وبا زیکی از این 2^m بسجمله را نتیجه می‌دهد

اگر بخواهیم حاصلضرب دو بسجمله‌ٔ از این نوع بازهم بسجمله‌ای از این نوع باشد ،قضیه جدی‌تر می‌شود .چون درجهٔ حاصلضرب دو بسجمله ،برابر برمجموع درجه‌های آنها ست ،برآورده کردن این شرط که درجهٔ حاصلضرب حداکثر $m-1$ باشد ،محتاج افزودن قراردادهایی است .یک راه ممکن محاسبه بسجمله‌ها به پیمانهٔ یک بسجمله معین از درجه m است ،که آن را $f(x)$ می‌نامیم .پس بسجملهٔ $P(x)$ با $P_1(x)$ یعنی با قیماندهٔ تقسیم $P(x)$ بر $f(x)$ هم ارز است ،به عبارت دیگر

$$P(x) = P_1(x) \pmod f$$

اگر

$$P(x) = J(x)f(x)+P_1(x)$$

که در آن $J(x)$ بسجمله‌ای است مناسب ،ودرجهٔ $P_1(x)$ حداکثر $m-1$ است .
البته اعمال حسابی در این تقسیم با زهم در $GF(2)$ انجام می‌شود .بویژه ، $P(x)=0 \pmod f$ اگر وتنها اگر $f(x)$ یک شمارندهٔ (مقسوم‌علیه) $P(x)$ باشد .

همانگونه که پیشتر گفته شد ،دقیقا" 2^m بسجمله با ضرایب در $GF(2)$ وجود دارند که ضرایبشان از $m-1$ بیشتر نیست .در این چند بسجملهٔ پوچ را که در آن همهٔ ضرایب صفر هستند ،در نظر نمی‌گیریم .پس $n=2^m-1$ بسجمله می‌ماند .کار کردن با m ـ بردارهایی که توسط این بسجمله‌ها نمایش داده می‌شوند ،اگر دنبالهٔ

$$(۴.۱) \qquad \{x^j\} \ , \ 0 \leqslant j \leqslant n-1 \ , \ \pmod f$$

همهٔ n بسجملهٔ ناپوچ را تولید کنند ،بسیار ساده‌تر می‌شود .

مثال : $m=2$, $f(x)=x^2+x+1$ پس $n=3$ ، در این صورت دنبالهٔ $1,x,x^2$, $\pmod f$ برابر است با $1+x$ و x و 1 که سه بسجملهٔ ناپوچ با درجهٔ نابیشتر از $m-1=1$ وبا ضرایب در $GF(2)$ ، هستند .

نشان خواهیم داد که دنباله‌ٔ (۴۰۱) همهٔ n بسجمله‌ٔ ناپوچ را تولید می‌کند، اگر

$$x^n=1 \pmod f \quad \text{و} \quad x^k \neq 1 \pmod f,\ 1\leq k<n \qquad (۴۰۲)$$

به ازای

(این درواقع بیان این مطلب است که بسجمله‌های (۴۰۱) گروهی دوری از مرتبهٔ n تشکیل می‌دهند) بسجمله‌های x^j $(0\leq j\leq n-1)$ به پیمانهٔ f متمایزهستند. فرض کنیم

$$x^j = x^k \pmod f \qquad 0\leq j<k\leq n-1$$

با ضرب دوطرف این معادله در x^{n-k} واستفاده از آخرین معادلهٔ (۴۰۲) حاصل می‌شود:

$$x^{n-(k-j)} = 1 \pmod f$$

چون $j<k$ این نتیجه با (۴۰۲) متناقض است. بعلاوه هیچ x^j یی به پیمانهٔ f برابر صفر نیست، زیرا اگر $x^j=0 \pmod f$ با ضرب دوطرف در x^{n-j} به دست می‌آوریم $1=0 \pmod f$، یعنی $f(x)$ بسجملهٔ 1 را می‌شمارد، که می‌دانیم ناممکن است، زیرا درجه f بزرگتر یا مساوی با 1 است. بنابراین هر n عضو دنبالهٔ (۴۰۱) به پیمانهٔ f، متمایزهستند، وهیچکدام از آنها بسجملهٔ پوچ نیست. پس اگر شرایط (۴۰۲) برآورده شده باشند، دنبالهٔ (۴۰۱) همهٔ n بسجملهٔ ناپوچ را تولید می‌کند.

اگر به ازای عدد ثابت $i\geq 1$، داشته باشیم $y=x^i$، آنگاه کوچکترین عدد صحیح ℓ که به ازای آن $y^\ell=1 \pmod f$، مرتبهٔ y نامیده می‌شود.

اگر به ازای $k\geq 1$ داشته باشیم $y^k=1 \pmod f$، آنگاه k مضربی از ℓ است. درواقع، فرض کنیم $k=q\ell+s$ که در آن $q\geq 0$ و $0\leq s<\ell$

دراین صورت $1=y^k=y^{\ell s+s}=y^s \pmod f$. چون $s<\ell$ از تعریف ℓ

نتیجه می‌شود که $s=0$ و این حالت خاصی از قضیه‌ای کلاسیک ثابت می‌شود:

لم ۴۰۱. فرض کنیم y توانی از x باشد و مرتبهٔ y برابر ℓ باشد. اگر $y^k=1 \pmod f$ آنگاه k مضربی از ℓ است.

از (۴۰۲) چنین برمی‌آید که $f(x)$ باید یک سازهٔ x^n-1 باشد. باز به حالت $m=4$ (و در نتیجه $n=15$) برمی‌گردیم و چند سازهٔ $x^{15}-1$ را محاسبه می‌کنیم. به حساب معمولی باز می‌گردیم و توجه می‌کنیم که اگر $x^3=1$ و $x^5=1$، آنگاه $x^{15}=1$. پس x^5-1 و x^3-1 سازه‌های $x^{15}-1$ هستند. البته $x-1$ یک سازهٔ همهٔ این بسجمله‌هاست. حال اتحادیه‌ی زیر را در نظر می‌گیریم:

$$x^{15}-1 = (x-1)\ \frac{x^3-1}{x-1}\ \frac{x^5-1}{x-1}\ \left(\frac{(x^{15}-1)(x-1)}{(x^3-1)\ (x^5-1)}\right)$$

$$= Q^{(1)}(x)Q^{(3)}(x)Q^{(5)}(x)Q^{(15)}(x)$$

که در آن

$$Q^{(1)}(x)=x-1 \quad , \quad Q^{(3)}(x)= x^2+x+1 \quad , \quad Q^{(5)}(x)= x^4+x^3+x^2+x+1$$

و (همانگونه که می‌توان تحقیق کرد) $Q^{(15)}(x)=x^8-x^7+x^5-x^4+x^3-x+1$

تذکر: بسجمله‌های $Q^{(j)}(x)$ در بالا مثالهایی از بسجمله‌های دایره بر گاوس، آیزنشتاین [۱۹] و دیگران هستند. یکی از ریشه‌های واحد مانند p از مرتبهٔ $j\geq 1$ نامیده می‌شود، درصورتی که j کوچکترین توانی باشد که به ازای آن $p^j=1$. همانگونه که از لم ۴۰۱ نتیجه می‌شود، مرتبهٔ ریشه‌های $x^{15}-1$ باید همگی سازه‌های ۱۵ باشند. تجزیهٔ (۴۰۳) در بالا شامل ریشه‌هایی

از مرتبهٔ 5,3,1 و 15 است و این ریشه‌ها دقیقاً" در $Q^{(1)}$، $Q^{(3)}$ ، $Q^{(5)}$ و $Q^{(15)}$ قرار دارند. همه ریشه‌های بسجمله $Q^{(i)}(x)$ از مرتبهٔ j هستند.

تذکر: گزینش m=4 کاملاً" تصادفی نبوده است. توجه کنید که حالتهای m=3 و m=5 نمی‌توانند چندان مثالهای روشن کننده‌ای باشند، زیر ۷ و ۳۱ — اعداد اول هستند و به همین دلیل در این حالتها تجزیه (۴.۳) بیش از حدی که بتواند جالب باشد، ساده می‌شود. حالت m=6 نیز از نظر محاسباتی چندان طولانی است، که مثال مناسبی به نظر نمی‌رسد.

با زبه GF(2) برگردیم، $Q^{(1)}$ ، $Q^{(3)}$ و $Q^{(5)}$ مشابه (۴.۳) باقی می‌مانند. اما همچنانکه می‌توان بسادگی تحقیق کرد،

$$Q^{(15)}(x) = (x^4+x^3+1)(x^4+x+1)$$

حال f(x) را برابر یکی از سازه‌های درجهٔ چهار $Q^{(15)}$ می‌گیریم، مثلاً"

$$f(x)=x^4+x^3+1 \qquad (۴.۴)$$

در این صورت چون f(x) یک سازهٔ $Q^{(15)}(x)$ است، سازه‌ای از $x^{15}-1$ نیز خواهد بود، و در نتیجه $x^{15}=1 \pmod f$. بنا به لم ۴.۱، مرتبهٔ x باید یک شمارندهٔ ۱۵ باشد، پس برابر 1، 3، 5 یا 15 است. اما f(x) بوضوح x-1 یا x^3-1 را نمی‌شمارد، و می‌توان ثابت کرد که شمارندهٔ x^5-1 نیز نیست. پس مرتبهٔ x، 1، 3 یا 5 نیست و در نتیجه باید ۱۵ باشد (این در واقع مصداقی خاص از یک ویژگی کلی بسجمله‌های دایره‌بر است، که بسادگی می‌توان آن را ثابت کرد). بنابراین شرایط (۴.۲) برآورده می‌شود و از اینرو $x^{14},\ldots,x^2,x,1$ (به پیمانهٔ f) پانزده بسجملهٔ درجه سهٔ با ضرایب در GF(2) هستند، که هیچیک از آنها بسجملهٔ پوچ نیست. به ازای هر $x^{15-j}, 1\leqslant j\leqslant 14$ بوضوح وارون x^j به پیمانهٔ f است. پس این

بسجمله‌ها تحت عمل ضرب به پیمانهٔ f ،گروهی دوری تشکیل می‌دهند . اگر بسجملهٔ پوچ را نیز به اینها بیفزاییم ،۱۶ بسجملهٔ حاصل تحت عمل جمع هم تشکیل گروهی می‌دهند .آشکارا نتیجه می‌شود که این ۱۶ بسجملهٔ درجهٔ ۳ با ضرایب در GF (2) میدانی با ۱۶ عضو تشکیل می‌دهند .این میدان را GF (16) می‌نامند .

تذکر : بسجملهٔ (۴.۴) تحویل ناپذیراست ،یعنی آن را نمی‌توان به صورت حاصلضرب دو بسجمله از درجهٔ کمتر نوشت (با اعمال حسابی در GF (2)) درواقع اگر می‌شد چنین کرد ،باید می‌داشتیم

$$f_1(x)f_2(x) = f(x)$$

اما خود $f_1(x)$ عضوی از GF (16) است ،پس باید وارونی داشته باشد .درمورد $f_2(x)$ هم همین مطلب صادق است .اگر دو طرف را در این وارونها ضرب کنیم ، برابری $1=0 \pmod{f}$ به دست می‌آید که ناممکن است .

تذکر : اصولاً" کل فراشد بالا را می‌توان برای اثبات وجود $GF(2^m)$ ،به ازای هر m ،و نیز برای مشخص کردن f (x) مناسب از درجهٔ m ،به کار برد .درواقع برای آنکه به آن حالت کلی بپردازیم ،نخست باید بحث نظری بیشتری را حول $Q^{(j)}(x)$ ها و بسجمله‌های تحویل ناپذیر با ضرایب در GF (2) بپرورانیم . [1]

یک روش ساده‌تر برای مشخص کردن اینکه به پیمانهٔ f (x) کار می‌کنیم چنین است : فرض کنیم α یک ریشهٔ f (x) باشد .پس $\alpha^4+\alpha^3+1=0$ و درنتیجه هر بسجمله‌ای برحسب α به خودی خود با بسجملهٔ دودویی درجه سه‌ای هم‌ارز خواهد بود .این بسجملهٔ درجهٔ سه همانی است که از محاسبه به پیمانهٔ f به دست می‌آید ،زیرا تنها ویژگی α که به کار می‌آید این است که $f(\alpha)=0$ ، پس عناصر GF (16) را می‌توان چونان بسجمله‌های دودویی درجهٔ سه برحسب α به حساب آورد .

جمعبندی: فرض کنیم α چنان باشد که $\alpha^4+\alpha^3+1=0$ (تنها از همین معادله استفاده می‌شود و نه از مقدار عددی α) در این صورت هر بسجمله برحسب α با ضرایب در $GF(2)$ با یک بسجمله‌ٔ دودویی درجهٔ سه برحسب α برابر است. $2^4=16$ تا بسجمله‌ٔ از این نوع وجود دارند که میدان $GF(16)$ را تشکیل می‌دهند. افزون بر این، دنباله‌ٔ $\{\alpha^j\}$ که در آن $0 \leqslant j \leqslant 14$ همهٔ ۱۵ بسجمله‌ٔ دودویی درجهٔ سه ناپوچ را تولید می‌کند، که همراه با بسجمله‌ٔ پوچ $GF(16)$ را می‌سازند. یک بسجمله‌ٔ دودویی درجه سه را می‌توان به صورت یک ۴ـ بردار دودویی در نظر گرفت.

۵. یک کد تصحیح کننده‌ٔ چندخطایی. برای آنکه نشان دهیم چگونه میدانهای متناهی وارد نظریهٔ کدگذاری می‌شوند، بررسی حالت $m=4$ و $2^m=16$ را ادامه می‌دهیم. در این مرحله فرض کنیم هدف تصحیح تا ۳ خطا در انتقال بردار کدگذاری شدهٔ C با $n=15$ درایه باشد. همانگونه که پیشتر دیدیم برای تصحیح یک خطا در انتقال برداری با $n=15$ درایه به ماتریسی ۴ سطری نیاز است. از اینرو شاید تصور اینکه بتوان ۳ خطا را با ماتریس ۱۲ سطری تصحیح کرد، موجه باشد. با ضرب این ماتریس در R به یک ۱۲ـ بردار دست می‌یابیم، که می‌توان آن را مرکب از سه ۴ـ بردار به شمار آورد. از همین رو این بردار حاوی اطلاعات لازم برای نمایش سه عدد صحیح بین ۱ و ۱۵ است، و در نتیجه می‌توان در صورت امکان تا سه خطا را در R مشخص کند. یک شیوهٔ بقاعده ساختن H این است که دوازده سطر آن را در سه بلوک چهار سطری، به گونهٔ زیر قرار دهیم:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \dots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \dots & \alpha^{42} \\ 1 & \alpha^5 & \alpha^{10} & \alpha^{15} & \dots & \alpha^{70} \end{bmatrix}$$

روشن است که هرتوانی از α نمایشگریک ۴ـ بردار دودویی متعلق به $GF(16)$ است. علت این را که چرا بلوکهای سطری α^{2j} , α^{4j} ($0 \leq j \leq 14$) را می‌توان حذف کرد، بزودی درخواهیم یافت (چون در $GF(2)$ داریم $\alpha^4=\alpha^3+1$ ، اولین بلوک چهارسطری را می توان از روی $1\,\alpha\alpha^2 \ldots \alpha^{14}$ محاسبه کرد این بلوک برابراست با

0	0	0	1	1	1	1	0	1	0	1	1	0	0	1
0	0	1	0	0	0	1	1	1	1	0	1	0	1	1
0	1	0	0	0	1	1	1	1	0	1	0	1	1	0
1	0	0	0	1	1	1	1	0	1	0	1	1	0	0

دومین بلوک چهارسطری H، یعنی $1, \alpha^3\alpha^6 \ldots \alpha^{42}$، ازاولین ،چهارمین ، هفتمین ،دهمین وسیزدهمین ستونهای ماتریس بالاتشکیل یافته است ، که هریک سه بارتکرارشده اندسومین بلوک شامل اولین ،ششمین ویازدهمین ستونهای ماتریس بالاست ، که هریک پنج بارتکرارشده اند)

نمایش بسجمله ای ۱۵ـ بردار دودویی دریافت شده R ،بادرایه های R_j, $0 \leq j \leq 14$ چنین است :

$$R(x) = \sum_{j=0}^{14} R_j x^j$$

(توجه کنید که دراینجا $R(x)$ به پیمانهٔ f محاسبه نمی‌شود) حاصلضرب ماتریس H در R یعنی HR یک بردارستونی با ۱۲ درایه زیراست :

$$R(\alpha), R(\alpha^3), R(\alpha^5)$$

که هریک درنمایش سطری خودبه‌عنوان سه ۴ـ بردار محسوب می‌شود ،وهر ۴ـ بردار نمایش یک عضو $GF(16)$ است .

همچنان که در (۳.۲) بود ،فرض کنیم $R=C+E$. اگر $E = 0$,T آنگاه می‌خواهیم

$HR=0$ وبنابراین باید داشته باشیم $HC = 0$. فرض کنیم

$$C(x)= \sum_{j=0}^{14} c_j x^j$$

HC برحسب α برابر است با ۱۲- بردار دودویی $C(\alpha), C(\alpha^3), C(\alpha^5)$. برای اینکه این ۱۲- بردار صفر شود، بسجمله‌ء درجه‌ء چهارده‌ء $C(x)$ باید به‌ازای $x=\alpha, x=\alpha^3, x=\alpha^5$ صفر باشد. برای اینکه $C(x)$ به‌ازای $x=\alpha$ صفر شود، کافی است $f(x)$ در $GF(2)$، سازه‌ای از $C(x)$ باشد. راحت‌تر است که اینجا $f(x)$ را با $M_1(x)$ نشان دهیم. برای آنکه بسجمله‌ای چون $M_3(x)$ بیابیم، که α^3 ریشه‌اش باشد، توجه می‌کنیم که مرتبه‌ء α^3 پنج است وبنابراین ریشه‌ای است از $Q^{(5)}(x)$، یعنی ریشه‌ای از

$$Q^{(5)}(x)= 1+x+x^2+x^3+x^4$$

$Q^{(5)}(x)$ را با $M_3(x)$ نشان می‌دهیم. بدگونه‌ء مشابه، α^5 از درجه‌ء سه است وبنابراین ریشه‌ای است از $Q^{(3)}(x) = 1+x+x^2$، که آن را با $M_5(x)$ نشان می‌دهیم. (بسجمله‌های M_1, M_3 و M_5 بسجمله‌های مینیموم هستند، به‌این معنی که هیچ بسجمله‌های دیگری ازدرجه‌های پایینتر با ضرایب در $GF(2)$ وجود ندارد که α, α^3 و α^5 بترتیب ریشه‌هایشان باشند) فرض کنیم

$$g(x)=M_1(x)M_3(x)M_5(x)$$

دراین صورت، چون M_1 و M_3 ازدرجه‌ء چهارهستند و M_5 ازدرجه‌ء ۲ است، $g(x)$ ازدرجه‌ء ۱۰ خواهد بود. علاوه‌براین $g(x)$ به‌ازای $x=\alpha$, $x=\alpha^3$ و $x=\alpha^5$ صفرخواهد شد، زیرا $M_1(\alpha), M_3(\alpha^3)$ و $M_5(\alpha^5)$ همگی صفرند. حال برای آنکه α، α^3 و α^5 ریشه‌های $C(x)$ باشند، لازم است که $g(x)$ سازه‌ای از $C(x)$ باشد. به‌یادآورید که C برداری است با ۱۵ درایه. فرض کنیم c_{12} و c_{11} و c_{10} و c_{13} یک بردارپیام با $k=5$ رقم دودویی باشد. $\sum_0^9 c_j x^j$

را برابر باقیمانده ٔ تقسیم

$$\frac{c_{14}x^{14}+c_{13}x^{13}+\ldots+c_{10}x^{10}}{g(x)}$$

بگیریم، چنانکه بواقع $g(x)$ سازه‌ای از $c(x)$ و α، α^3 و α^5 ریشه‌های آن باشند. البته با درنظرگرفتن این مطلب که اعمال حسابی در $GF(2)$ انجام می‌شوند. این همان فرایندکدگذاری با $n=15$، $k=15$ و $r=10$ است. بسجمله ٔ دودویی $g(x)$ را بسجمله ٔ پدیدآورنده ٔ کد می‌نامند. درواقع یک کد ــ بردار c کاملاً" با این مطلب که $c(x)$ بر $g(x)$ بخش پذیر است، مشخص می‌شود.

حال نشان می‌دهیم که دست کم از نظر اصولی می‌توان از ۱۲ــ بردار HR برای تصحیح تا حداکثر ۳ خطا در انتقال استفاده کرد. چون $HC=0$، داریم $HR=HE$ و ۱۲ــ بردار HE به عنوان سه ۴ــ بردار، $E(\alpha)$، $E(\alpha^3)$، $E(\alpha^5)$ را معین می‌کند. به یاد داشته باشید که ۱ بودن درایه‌های E به معنی رخ دادن خطا و صفر بودن آنها به معنی رخ ندادن خطاست. فرض کنیم ۳ خطا، مثلاً" در درایه‌های i_1، i_2 و i_3 بردار E رخ داده باشد. دراین صورت

$$E(\alpha)=\alpha^{i_1}+\alpha^{i_2}+\alpha^{i_3}$$

$$E(\alpha^3)=\alpha^{3i_1}+\alpha^{3i_2}+\alpha^{3i_3}$$

$$E(\alpha^5)=\alpha^{5i_1}+\alpha^{5i_2}+\alpha^{5i_3}$$

ازسوی دیگر، اگر a_j ها عناصر $GF(2)$ باشند، داریم:

$$\left(\sum a_j\alpha^j\right)^2=\sum a_j^2\,\alpha^{2j}=\sum a_j\alpha^{2j} \qquad (۵.۱)$$

زیرا تمام جمله‌های به صورت $a_j a_k \alpha^{j+k}$ (که در آن $j\neq k$) ضریب

$2=1+1$ دارند. حال فرض کنیم سه خطا در درایه‌های i_4، i_5، i_6 که همگی متمایز از i_2, i_1 و i_3 هستند، رخ داده باشد، به‌گونه‌ای که این سه خطا نیز همان مقادیری را برای $E(\alpha^5), E(\alpha^3), E(\alpha)$ نتیجه دهند، که i_3, i_2, i_1 به‌دست داده بودند. بنابراین،

$$\alpha^{ji_1} + \alpha^{ji_2} + \alpha^{ji_3} = \alpha^{ji_4} + \alpha^{ji_5} + \alpha^{ji_6} \qquad (j=1,3,5)$$

ویا،

$$(۵.۲) \qquad \sum_{d=1}^{6} \alpha^{ji_d} = 0 \qquad (j=1,3,5)$$

اما کاربست (۵.۱) درحالت $j=1$، (۵.۲) را درحالت $j=2$ نتیجه می‌دهد به‌همین ترتیب کاربست (۵.۱) درحالت $j=2$ ودرحالت $j=3$، (۵.۲) را به‌ترتیب درحالتهای $j=4$ و $j=6$ نتیجه می‌دهد. (به‌همین دلیل بودکه ما توانهای زوج را ازسطرهای H حذف کردیم) پس

$$(۵.۳) \qquad \sum_{d=1}^{6} \alpha^{ji_d} = 0 \qquad (j=1,2,3,4,5,6)$$

دترمینان دستگاه بالا یک دترمینان واندرموند [۲۰] است که برابر است با

$$(۵.۴) \qquad \alpha^{i_1+i_2+\cdots+i_6} \prod_{1\leqslant e<d\leqslant 6} (\alpha^{i_d} - \alpha^{i_e})$$

هرسازهٔ (۵.۴) چنین است:

$$\alpha^{i_d} - \alpha^{i_e} = \alpha^{i_e}(\alpha^{i_d - i_e} - 1)$$

چون $0 \leqslant i_d \leqslant 14$ پس $0 < |i_d - i_e| \leqslant 14$. پس ازآنجاکه مرتبهٔ α برابر ۱۵ است، هیچ یک ازسازه‌های (۵.۴) صفرنیستند، ودرنتیجه خوددترمینان

تا صفر است . پس دستگاه همگن (۵۰۳) جواب ندارد .اگرحالتهای دیگر را هم در نظر بگیریم مثلا" حالتی که در آن با زهم دو مجموعه از ۳ خطا وجود داشته باشد ،اما اشتراک این دومجموعه تهی باشد ،یا حالتهایی که یکی یا هردومجموعه شامل کمتر از ۳ خطا باشند .دستگاه (۵۰۳) ستونهای کمتری خواهد داشت ،واز اینرو چندسطر را می‌توان حذف کرد ،که از نو به یک دترمینان واندرموند ختم می‌شود .پس اگرحداکثر ۳ خطا وجود داشته باشد ، HR مکان آنها را به طوریگانه مشخص می‌کند .

البته برای یک کدگذاری موفق ،این نتیجهٔ یگانگی که به دست آمد ،گرچه از حیث نظری کاملا" قانع کننده است ،اما عملا" چندان کارامد نیست .به جای آن ،باید فراشدی سازنده و بالنسبه ساده برای تعیین مکان احتمالی درایه‌های یک در E فراهم آید .ساختار تماما" مرتب H برحسب توانهای α است که فراهم آوردن چندین فراشد ماشین کدگذاری را ممکن می‌سازد [I ،فصل ۷] .

کدهای BCH که برپایه مفاهیم ریاضیات محض بنا شده‌اند ،تنها بخشی از نظریهٔ کدگذاری نیست که از زمینه‌های دور از انتظاری از ریاضیات محض استفاده می‌کنند .کدهای هندسهٔ اقلیدسی [I ،صفحهٔ ۳۷۵] ،کدهای هندسهٔ تصویری [I ،صفحهٔ ۳۷۶] ،کدهای ضرب تانسوری [I ،صفحهٔ ۳۴۶] و کدهای ماندهٔ مجذوری [I ،صفحهٔ ۳۵۴] نیز از کدهایی هستند که در نظریهٔ کدگذاری از آنها استفاده می‌شود .

این مقاله برگردان فارسی مقاله زیر است :

Norman Levinson

Coding Theory: A Counterexample to 6.H.Hardy's conception of applied Mathematics;

American Mathematical Monthly, March 1970.

توضیحات :

1. A Mathematician's Apology

2. Cyclomatic Polynomials

3. quadratic residues

4. law of quadratic reciprocity

5. Bose

6. Ray-Chauduri

7. Hocquenhen

8. decoding

9. Gorenstein

10. Zierler

11. Berlekamp

12. Reed

13. Solomon

14. message

15. noisy

16. redundancy

17. decoding

18. Hamming

19. Eisenstein

20. Vandermonde

منابع :

1. Elwyn R.Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

2. R.C.Bose and D.K.Ray-Chaudhuri, On a class of error correcting binary group codes, Information and Control, 3 (1960) 68-79 and 279-290.

3. D.C.Gorenstein and N.Zierler, A class of error-correcting codes in P^m symbols, J.Soc. Indust.Appl.Math., 9 (1961) 207-214.

4. R.W.Hamming,Error detecting and error correcting codes,Bell System Tech. J.,29 (1950)147-160.

5. G.H.Hardy,A Mathematician's Apology,Cambridge University Press,1967 Edition.

6. A.Hocquenhem,Codes correcteurs d'erreurs,Chiffres,2 (1959) 147-156.

7. W.W.Peterson,Error-correcting Codes,M.I.T.Press,1961.

8. I.A.Reed and G.Solomon,Polynomial codes over certain finite fields,J.Soc.Indust.Appl.Math.,8(1960)300-304.