به نام خدا

جزوه کدگذاری ۱

محمد غلامی

دانشیار دانشکده ریاضی دانشگاه شهرکرد-گرایش کدگذاری و رمزنگاری

آنتروپی:

منبع ($Source$): یک منبع، یک زوج مرتب (S,P) است که در آن $S=\{x_1,...,x_n\}$ یک مجموعه متناهی است که الفبای منبع نامیده می‌شود و P یک توزیع احتمال روی S است.

ما احتمال وقوع x_i را با P_i یا $P(x_i)$ نمایش می‌دهیم.

ابهام ($Uncertaionty$): قبل از نمونه‌گیری، نسبت به خروجی مقدار معینی ابهام وجود دارد و پس از نمونه‌گیری، مقدار مشخصی اطلاعات ($information$) درباره منبع به دست می-آوریم. بنابراین، مفاهیم میزان ابهام و اطلاعات با یکدیگر مربوطند.

مثال: فرض کنید $S=\{x_1,...,x_n\}$. اگر $P(x_1)=۱$ و $P(x_i)=۰$ برای هر $i>1$، آنگاه x_1 همواره انتخاب شده و لذا ابهامی در این حالت نسبت به خروجی نداریم، پس میزان ابهام برابر با صفر است. در این مثال هیچ نمونه‌ای به ما اطلاعات نخواهد داد، زیرا چیزی درباره این منبع به ما نخواهد آموخت.

از طرف دیگر، اگر تنها تعداد کمی از عناصر S دارای احتمال های ناصفر باشند، آنگاه میزان ابهام کم بوده و مقدار اطلاعات در این منبع کوچک است. بیشترین میزان ابهام، زمانی رخ می‌دهد که خروجی دارای توزیع یکنواخت باشد، یعنی $\forall 1\le i\le n,\ P_i=\frac{1}{n}$.

تعریف. فرض کنید X یک متغیر تصادفی با برد $S=\{x_1,...,x_n\}$ باشد و $P(x_i)=P(X=x_i)$. در این حالت آنتروپی X به صورت زیر تعریف می شود:

$$H(X):=\sum_{x=1}^{n}P(x_i)\log_2\frac{1}{p(x_i)}$$

در واقع آنتروپی X معرف متوسط میزان ابهام نسبت به خروجی X قبل از مشاهده خروجی یا متوسط اطلاعات به دست آمده از X پس ازمشاهده خروجی و یا متوسط کمترین تعداد بیت لازم برای توصیف X می باشد.

تعریف. فرض کنیدXوYمتغیرهای تصادفی با بردهای به ترتیب $S_1=\{x_1,...,x_n\}$ و $S_2=\{y_1,...,y_m\}$باشند. اگر $p(x_i,y_j)=p(X=x_i,Y=y_j)$ توزیع احتمال رخ دادن همزمان XوYباشد،آنگاه آنتروپی توأم X,Y به صورت زیر تعریف می‌شود.

$$H(X,Y)=\sum_{i,j}P(x_i,y_j)\log\frac{1}{P(x_i,y_j)}$$

آنتروپی بردار تصادفی $X=(X_1,X_2)$ به صورت $H(X)=H(X_1,X_2)$ تعریف می‌شود.

تعریف. اگر $X_1,...,X_k$ متغیرهای تصادفی بوده و X_i دارای برد S_i باشد و

$$p(x_1,...,x_n)=p(X_1=x_1,...,X_n=x_n)$$

آنگاه آنتروپی توأم $X_1,...,X_k$ به صورت زیر تعریف می‌شود:

$$H(x_1,...,x_n)=\sum_{x_1\in S_1,...,x_n\in S_n}p(x_1,...,x_n)\log_2\frac{1}{p(x_1,...,x_n)}$$

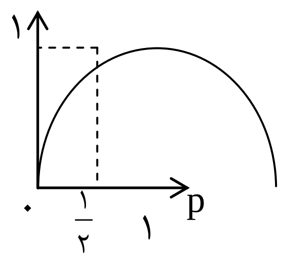
مثال. فرض کنید Xیک متغیر تصادفی با توزیع یکنواخت روی $\{x_1,...,x_n\}$باشد (به عبارت دیگر $P(X=x_i)=\frac{1}{n}$ برای هر $1\le i\le n$)، آنگاه:

$$H(X)=H(\frac{1}{n},...,\frac{1}{n})=\sum_{i=1}^{n}\frac{1}{n}\log_2 n=\log_2 n$$

مثال. اگر X یک توزیع تصادفی روی $\{0,1\}$باشد و $P(1)=1-p,P(0)=p$ آنگاه:

$$H(X)=p\log\frac{1}{p}+(1-p)\log\frac{1}{1-p}=H(p)$$

به شکل زیر است.



نکته. اگر Y,X دو متغیر تصادفی مستقل باشند، یعنی:

$$P(X=x_i,Y=y_j)=P(x=x_i)P(Y=y_j)$$

آنگاه:

$$H(X,Y)=H(X)+H(Y)$$

تعریف. فرض کنید Y,X به ترتیب ورودی و خروجی یک کانال مخابراتی به صورت زیر باشند:

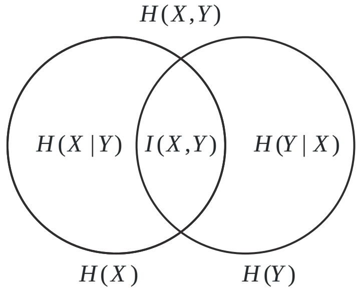
در این صورت اطلاعات متقابل (*mutually information*) بین Y,X به صورت زیر تعریف می شود:

$$I(X,Y)=H(X)-H(X\,|\,Y)=H(Y)-H(Y\,|\,X)$$

در واقع $I(X,Y)$ میزان کاهش در تعداد بیت ها برای توصیفXبه شرط داشتن Y است. در این جا توجه داریم که $H(X\,|\,Y)$ میزان متوسط طول بیت ها برای توصیف Xبه شرط داشتن Yاست که مقدار آن به صورت زیر محاسبه می شود:

$$H(X\,|\,Y)=\sum_{j=1}^{t}p(x_i,y_j)\log_2\frac{1}{p(x_i\,|\,y_j)},\qquad p(x_i\,|\,y_j)=\frac{p(x_i,y_j)}{P(y_j)}$$

نتیجه.رابطه بین آنتروپی های شرطی و اطلاعات متقابل را می توان در شکل زیر خلاصه کرد:



1) $I(X,Y)=I(Y,X)$

2) $H(X,Y)=H(X|Y)+H(Y)$

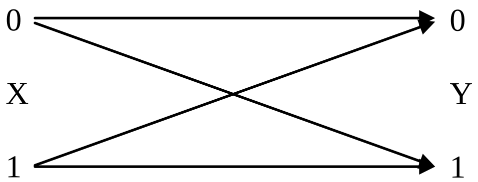
3) $H(X,Y)\le H(X)+H(Y)$

4) $I(X,Y)=H(X)+H(Y)-H(X,Y)$

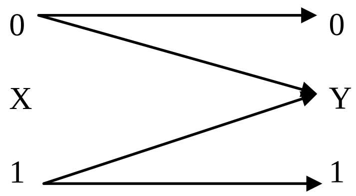
5) $I(X,X)=H(X)$

تعریف. ظرفیت یک کانال، بیشترین اطلاعات متقابل $I(X,Y)$ روی تمامی توزیع‌های ورودی $P(x_i)$ از X است؛ به عبارت دیگر $\varsigma=\max\limits_{P(x_i)} I(X,Y)$.

نتیجه: در مورد کانال BSC داریم $\varsigma=1-H(p)$، و در مورد کانال BEC داریم $\varsigma=1-p$.



کانال BSC



کانال BEC

درس کدگذاری ۱ (همراه با مقدماتی از نظریه اطلاعات)

منابع:

1. Steven Roman, Coding and Information Theory, Springer-Verlag, 1992.
2. Shulin, Daniel J. Costello, Error-Control Coding, Pearson Education, Inc, 2004.

۳. مقدمه ای بر نظریه کدگذاری، ترجمه دکتر محمد غلامی و دکتر رضا سبحانی، انتشارات دانشگاه شهرکرد، ۱۳۹۰.

۴. مقدمه ای بر نظریه اطلاعات و کدگذاری، ترجمه دکتر مرتضی اسماعیلی، انتشارات دانشگاه صنعتی اصفهان.

کدهای بلوکی. فرض کنید $A=\{a_1,a_2,...,a_q\}$ یک مجموعه متناهی باشد که الفبای کد نامیده می‌شود و فرض کنید A^n تمامی رشته‌های به طور n روی A باشد؛ یعنی:

$$A^n=\{a_{i_1}a_{i_2}...a_{i_n} \mid a_{i_1},...,a_{i_n}\in A\}$$

در این صورت هر زیر مجموعه ناتهی C از A^n یک کد بلوکی q–تایی نامیده می‌شود. هر عضو C یک کدکلمه(*codeword*) نامیده می‌شود. اگر $C\subseteq A^n$ دارای M کدکلمه باشد، آنگاه گوییم C دارای طول(*length*) n و اندازه(*size*) M است و آن را یک (n,M)–کد می‌نامیم.

نرخ(*rate*) یک (n,M)–کدq–تایی برابر با $R=\frac{\log_q^M}{n}$ است.

کانال. یک کانال مخابراتی را می‌توان به این صورت فرض نمود که یک کدکلمه $c=c_1...c_n$ از کد C (با طول n روی الفبای کد A) را دریافت نموده و خروجی آن یک رشته خروجی $d=d_1...d_n$ (با همان طول n روی الفبای شامل A) است.

کانال بدون حافظه گسسته (*discrete memoryless channel*).

شامل یک الفبای ورودی $A=\{a_1,...,a_q\}$، یک الفبای خروجی $O=\{b_1,...,b_t\}$ $(A\subseteq O)$ و یک مجموعه از احتمالات کانال یا احتمال‌های انتقال (*transition probabilities*) $p(b_j\mid a_i)$ است که در رابطه زیر صدق می‌کنند.

$$\forall i,\ \sum_{j=1}^{t} p(b_j\mid a_i)=1$$

که در آن $p(b_j\mid a_i)$ احتمال آن است که b_j دریافت شده باشد به شرط آنکه a_i ارسال شده باشد. علاوه بر این، اگر $d=d_1...d_n, c=c_1...c_n$ به ترتیب کلماتی به طول n روی A و O باشند، آنگاه $p(d\mid c)=\prod_{i=1}^{n}P(d_i\mid c_i)$.

مثال. مهم‌ترین کانال بدون حافظه گسسته (DMC)، کانال دوتایی متقارن یا BSC (*binarysymmetric channel*) است که به صورت زیر می‌باشد.

$$p(1\mid 0)=p(0\mid 1)=p, \qquad p(0\mid 0)=p(1\mid 1)=1-p$$

بنابراین احتمال یک خطای بیتی یا احتمال متقاطع (*crossover probability*) برابر با p است.

ماتریس کانال. اگر $\begin{cases} p(b_j\mid a_i) \\ 1\le i\le q, 1\le j\le t\end{cases}$ احتمال‌های انتقال یک کانال باشند، که در آن به $A=\{a_1,...,a_q\}$ و $O=\{b_1,...,b_t\}$ به ترتیب الفبای ورودی و خروجی کانال باشند، آنگاه ماتریس $(P(b_j\mid a_i))_{1\le i\le q,\,1\le j\le t}$ ماتریس کانال نامیده می‌شود.

مثال. در مورد کانال BSC، ماتریس کانال به صورت $\begin{pmatrix} 1-p & p \\ p & 1-p\end{pmatrix}$ است.

توزیع ورودی. می‌توان توزیع ورودی کانال را به صورت یک متغیر تصادفی X در نظر گرفت که در آن $P(X=c)=P(c)$ و توزیع خروجی کانال را به صورت متغیر تصادفی Y در نظر گرفت که $P(Y=d)=P(d)$.

در این‌صورت طبق قاعده بیزداریم:

$$P(d)=\sum_{c\in C}P(d\mid c)P(c)$$

توزیع توأم Y,X به صورت زیر داده می‌شود.

$$P(X=c,Y=d)=P(d|c).P(c)$$

احتمال‌های پیشین کانال (*Backward channel probabilities*) به صورت زیر است:

$$P(X=c|Y=d)=\frac{P(X=c,Y=d)}{P(Y=d)}$$

یا

$$P(c|d)=\frac{p(c,d)}{p(d)}=\frac{p(d|c)p(c)}{p(d)}$$

که در آن از نوشتن Y,X صرف نظر می‌کنیم.

خطای کانال یا خطای سمبل. زمانی رخ می‌دهد که سمبل دریافتی از سمبل ارسال شده متفاوت باشد.

خطاهای گروهی (*Burst errors*):

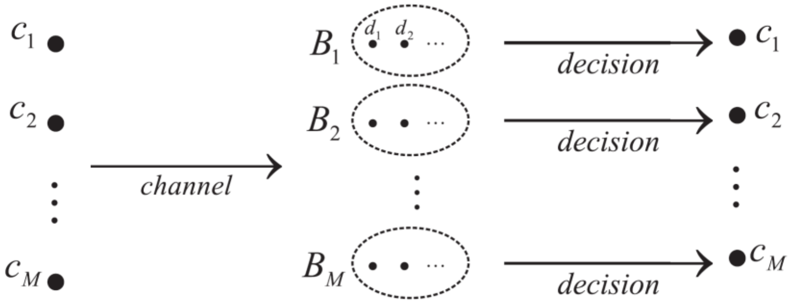
در اکثر کدگذاری‌های کانال، فرض بر این بوده که خطاها در ارسال مستقل هستند. اما این فرض غیر واقعی است. به طور نمونه، برخی از خطاها پشت سر یکدیگر یا به صورت گروهی (*Burst error*) رخ می دهند. در این حالت، طراحی و ساخت کدهایی که به منظور غلبه بر خطاهای گروهی مفید هستند، مورد بحث و بررسی قرار می‌گیرد.

قاعده تصمیم (*Decisien sheme*).

قاعده تصمیم، یک تابع جزیی مانند f از مجموعه رشته‌های خروجی به مجموعه کد کلمات است. کلمه جزیی به این مطلب اشاره دارد که f ممکن است روی تمامی رشته‌های خروجی تعریف نشده باشد. به عبارت دیگر اگر رشته‌ی خروجی d دریافت شده باشد و $f(d)$ قابل تعریف باشد، آنگاه قاعده تصمیم، تصمیم می‌گیرد که $f(d)$ همان کدکلمه‌ای است که ارسال شده است.

در این حالت اگر $f(d)$ همان کدکلمه ارسالی نباشد می‌گوییم خطای تصمیم‌گیری (*decision error*) یا خطای کدگشایی (*decoding error*) رخ داده است.

حال فرض کنید $C=\{c_1,...,c_M\}$ مجموعه تمامی کدکلمات و $B_i = f^{-1}(c_i)=\{d \mid f(d)=c_i\}$ مجموعهٔ تمامی خروجی‌ها باشد که تصمیم مـی‌گیـریم ورودی صـحیح برابـر بـا c_i اسـت، در اینصورت رشته‌های خروجی را می‌توان به مجموعه $\{B_1,...,B_m\}$ افزار نمود.



هدف کدگذاری، طراحی یک قاعده تصمیم مناسب است که تلاش می‌کند تا هـر خطـایی را در انتقال تصحیح نماید.

احتمال تشخیص خطا

اگر کد کلمه C ارسال شده باشد و در کانال، خطا رخ داده باشد، زمانی این خطـا غیـر قابـل تشخیص است که کلمه دریافتی یک کدکلمه دیگر باشد، به عبارت دیگر:

$$P(\text{عدم تشخیص خطا} \mid c \text{ ارسال شده باشد}) = \sum_{\substack{d\in C\\ d\neq c}} p(d\mid c)$$

بنابراین احتمال عدم تشخیص خطا به صورت زیر است:

$$P_{\text{undeterr}} = \sum_{c\in C}\ \sum_{d\in C-\{c\}} p(d\mid c)$$

و احتمال تشخیص خطا $p_{\text{deterr}} = 1 - P_{\text{undeterr}}$ است.

احتمال تصحیح خطا

فرض کنید f یک قاعده تصمیم باشد و کدکلمه c ارسال شده باشد. در این صورت:

$$p(\text{خطا} \mid c) = \sum_{d\notin f^{-1}(c)} p(d\mid c)$$

بنابراین، احتمال (غیر شرطی) p_e خطای تصمیم گیری به صورت زیر است:

$$p_e = \sum_{c\in C} p(error\mid c)\,p(c) = \sum_{c\in C}\ \sum_{d\notin f^{-1}(c)} p(d\mid c)\,p(c)$$

توجه دارید که این احتمال، به توزیع ورودی $p(c)$ و قاعده تصمیم f بستگی دارد.

به منظور تعیین یک قاعده تصمیم مناسب که احتمال خطای تصمیم گیری را کمترین نماید، احتمال خطا را به شرط داشتن یک خروجی، محاسبه می‌کنند (به جای ورودی).

اگر d دریافت شده باشد، آنگاه:

$$p(err \mid d) = 1 - p(f(d) \mid d)$$

زیرا تصمیم درست زمانی صورت می‌گیرد که $f(d)$ ورودی واقعی باشد.

بنابراین با متوسط گیری روی تمامی مقادیر خروجی ممکن داریم:

$$p_e = \sum_d p(err \mid d) p(d) = 1 - \sum_d p(f(d) \mid d) p(d)$$

بنابراین برای مینیمم کردن p_e باید $\sum p(f(d) \mid d) p(d)$ را ماکسیمم کنیم. ولی چون تمامی جملات $p(f(d) \mid d) p(d)$ مثبت بوده و $p(d)$ نیز به f بستگی ندارد، این مقدار ماکسیمم است اگر و تنها اگر $p(f(d) \mid d)$ ماکسیمم باشد. پس تعریف زیر را داریم:

تعریف. به ازای یک توزیع ورودی داده شده، قاعده تصمیم زیرکه در رابطه زیرصدق می‌کند. به ازای هردنباله خروجی مانند d داشته باشیم $p(f(d) \mid d) = \max_c p(c \mid d)$ یک مشاهده‌گر مطلوب (*ideal observer*) نامیده می‌شود. به عبارت دیگر، یک مشاهده‌گر مطلوب، یک قاعده تصمیم است که احتمال خطای تصمیم یا P_e را کمترین می‌کند.

در این حالت توجه داشته باشید که $p(d \mid c)$ احتمال انتقال پسین و $p(c \mid d)$ احتمال پیشین نامیده می شوند.

نکته. مشاهده‌گر مطلوب دارای معایب و مزایایی است. یکی از مهم‌ترین معایب آن، این است که به توزیع ورودی بستگی دارد. یعنی اگر توزیع ورودی تغییر کند، احتمالاً مشاهده-گر مطلوب نیز تغییر می‌کند. برای حذف این وابستگی، به جای مینیمم کردن p_e، می‌توانیم $p_e^{\max}$ را مینیمم کنیم که در آن:

$$p_e^{\max} = \max_c p(err \mid c)$$

دراین حالت $p_e^{\max}$ تنها به fبستگی خواهد داشت (و نه توزیع ورودی)، اما عیب این کار نیز آن است که یافتن قاعده تصمیم f که $p_e^{\max}$ را کمترین کند، ممکن نیست.

روش دیگر برای حذف این وابستگی به توزیع ورودی این است که توزیع ورودی را یکنواخت در نظر بگیریم. یعنی $p(c)=\frac{1}{M}$ (برای هر c) که در آن M اندازه کداست. بنابراین، احتمال خطای تصمیم به صورت زیر است:

$$p_e^{av}=\frac{1}{M}\sum_c p(err\,|\,c)= \text{احتمال متوسط خطا}$$

اما در این حالت:

$$p(c\,|\,d)=\frac{p(d\,|\,c)p(c)}{p(d)}=\frac{1}{mp(d)}p(d\,|\,c)\Rightarrow \max_c p(c\,|\,d)=\frac{1}{mp(d)}\max_c p(d\,|\,c)$$

بنابراین در این حالت، ماکسیمم کردن $p(c\,|\,d)$ معادل با ماکسیمم کردن $p(d\,|\,c)$ است.

تعریف قاعده تصمیم f به طوری که $f(d)$ دارای این خاصیت باشد که به ازای هر خروجی d داشته باشیم $p(d\,|\,f(d))=\max_C p(d\,|\,c)$

قاعده تصمیم بیشترین دستنمایی (*maximum likelihood decision*) نامیده می‌شود.

به عبارت دیگر $f(d)$ یک رشته ورودی با این خاصیت است که هیچ رشته ورودی دیگری احتمال دریافت d را به اندازه آن ماکسیمم نمی‌کند.

قضیه: به ازای توزیع ورودی یکنواخت، قاعده مشاهده‌گر مطلوب همان قاعده تصمیم بیشترین درستنمایی است.

قضیه کانال نویز دار.

کانال بدون حافظهٔ گسسته با ظرفیت ς را در نظر بگیرید. برای هر مقدار مثبت R که در آن $R<\varsigma$، یک دنباله C_n از کدهای $r-$ تایی و قاعده تصمیم متناظر f_n باشرایط زیر وجود دارد:

۱) C_n یک $(n,[r^{nR}])-$ کد است، یعنی C_n دارای طول n و نرخ حداقل R است.

۲) بیشترین احتمال خطای f_n ، زمانی که $n\to\infty$، به صفر می‌کند؛ یعنی:

$p_e^{\max}(n) \to o$

نکته. تمامی اثبات‌های موجود برای قضیه کدگذاری کانال غیرساختاری هستند، به این معنا که این اثبات‌ها در مورد ساخت کدهای وعده داده شده در قضیه، روشی را ارایه نمی‌کنند و تاکنون نیز کسی نتوانسته است به این کدهای وعده داده شده دست یابد. اگر چه کدهایی هستند (مانند کدهای توربو و کدهای خلوت یا $LDPC$) که به نرخ شانون بسیار نزدیک می‌شوند.

از طرف دیگر، دست یافتن به کدهایی که به نرخ شانون دست می‌یابند تمامی آن چیزی نیست که ما دنبالش هستیم. در واقع قاعده تصمیم نیز می‌بایست نسبتاً در کاربرد آسان باشد. از طرف دیگر، قضیه وجود کدهای مناسب را درطول‌های بزرگ وعده می‌دهد که ممکن است از نظر عملی غیر قابل کاربرد باشند. به منظوردست یافتن به قاعده تصمیم مناسب، پژوهشگران به دنبال طراحی و ساخت کدهای جبری و هندسی برآمده‌اند. اولین کاری که باید انجام دهیم، یافتن کمترین فاصله کد با مطرح نمودن یک اندازه (متریک) روی کد C است.

کدگشایی با کمترین فاصله

درحالت کلی یافتن کدهای خوب، بسیار مشکل است. به همین منظور، سعی می‌کنیم، تا با قرار دادن برخی فرض‌های معین در مورد کانال، مسأله را مشهودتر کنیم.

تعریف. فرض کنید y,x دو رشته با طول یکسان روی یک الفبا باشند. در این‌صورت فاصله همینگ $d(x,y)$، بین y,x، تعداد مکان‌هایی است که x با y تفاوت دارد.

مثال. اگر $x=$۱۰۱۱۲ و $y=$۲۰۱۱۰ آنگاه $d(x,y)=2$، زیرا y,x در مکان های اول و پنجم با هم متفاوتند.

تمرین. نشان دهید فاصله همینگ، یک متر است، به عبارت دیگر، قضیه زیر را اثبات کنید.

قضیه. فرض کنید A^n تمامی کلمات به طول n روی الفبای A باشند.، در این‌صورت تابع فاصله همینگ $d: A^n \times A^n \to \mathrm{N} \cup \{0\}$ در خواص زیر صدق می‌کند.

برای هر y،x و z در A^n داریم:

۱- (معین مثبت) $d(x,y)\geq 0,\ \ d(x,y)=\circ \Leftrightarrow x=y$

۲- (تقارن) $d(x,y)=d(y,x)$

۳- (نامساوی مثلثی) $d(x,y)\leq d(x,z)+d(z,y)$

بنابراین زوج (A^n,d) یک فضای متریک است.

اگر کدکلمه c از طریق این کانال ارسال و کلمه d دریافت شده باشد، آنگاه تعداد سمبل های خطا در کانال برابر با $d(c,d)$است. بنابراین: $p(d\,|\,c)=p^{d(c,d)}(1-p)^{n-d(c,d)}$

چون $P<\frac{۱}{۲}$، این احتمال بیشترین است، اگر $d(c,d)$ کمترین باشد. بنابراین کدگشایی MLD(کدگشایی با بیشترین درستنمایی) معادل با انتخاب کدکلمه c است که به کلمه dاز همه کدکلمات دیگر نزدیک تر باشد. به این قاعده، کدگشایی با کمترین فاصله یا قاعده (MDD*minimum distance decoding*) می گوییم.

مثال. $C=\{۰۰۰,۱۱۱\}$ کد تکرار دوتایی به طول ۳ است. با استفاده از قاعده کدگشایی با کمترین فاصله، کدگشا دچار خطا می گردد اگر و تنها اگر حداقل دو خطا رخ دهد، بنابراین:

$$p_{\text{decodeerr}}=3p^2(1-p)+p^3=3p^2-2p^3$$

احتمال خطای کدگشایی

تعریف. اگر در یک کد، بیشتر از یک کدکلمه با کلمه دریافتی دارای فاصله یکسان بود، آنگاه گوییم گره (Tie) رخ داده است. در چنین حالتی کدگشا به طور تصادفی، آن کدکلمه را به یکی از نزدیک ترین کدکلمه‌ها کدگشایی می کند و یا این که اعلام خطا می کند. در حالت اول گوییم کدگشایی کامل (*complete decoding*)بوده و در حالت دوم کدگشایی را غیرکامل(*incomplete decoding*) می گوییم.

نکته. در اثبات قضیه کدگشایی کانال، از کدگشایی غیرکامل بهره می گیریم.

نکته. در تمامی کانال‌هایی که شرط زیر را داشته باشند، قاعده MLD معادل قاعده MDD (کمترین فاصله) است.

"اگر یک خطا در یک سمبل رخ دهد، آنگاه سمبل دریافتی با احتمال یکسان، یکی از سمبل های ممکن دیگر است."

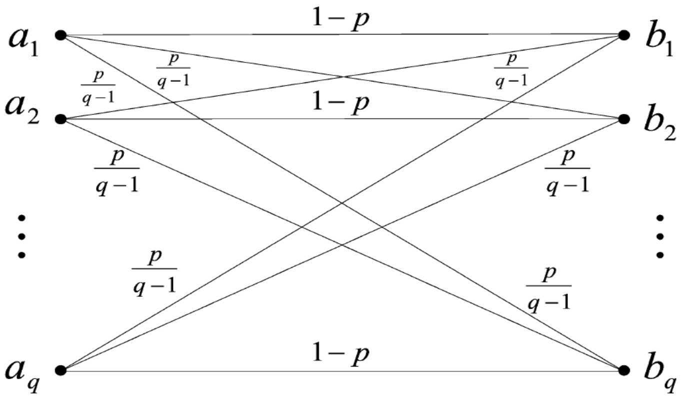
نتیجه. در کانال BEC با ماتریس کانال $\begin{bmatrix}1-p & p & \circ\\ \circ & p & 1-p\end{bmatrix}$، $P<\frac{1}{2}$، MLD معادل قاعده MDD است.

مثال. کانال q- تایی متقارن به صورت زیر است:

$$F_q=\{a_1,\dots,a_q\} \text{ و } p(a_i\,|\,a_j)=1-p,\quad \forall i\neq j,\ p(a_i\,|\,a_j)=\frac{p}{q-1}$$

در این حالت، ماتریس کانال به صورت زیر خواهد بود.

$$\begin{pmatrix}1-p & \frac{p}{q-1} & \dots & \frac{p}{q-1}\\ \frac{p}{q-1} & 1-p & \dots & \frac{p}{q-1}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{p}{q-1} & \frac{p}{q-1} & \dots & 1-p\end{pmatrix}_{q\times q}$$



کدهای تصحیح کننده و تشخیص دهنده t خطا

تعریف. کمترین فاصله یک کد بلوکی مانند C به صورت زیر تعریف می‌شود:

$$d(C)=\min_{c,d\in C,c\neq d} d(c,d)$$

یک (n,M,d)-کد، یک کد بلوکی با طول n، اندازه M و کمترین فاصله d است.

تعریف. کد C، تشخیص دهنده t خطا (*t-error detecting*) نامیده می‌شود، اگر حداکثر t خطا (و حداقل یک خطا) روی هر کدکلمه رخ دهد، آنگاه کلمه دریافتی، یک کدکلمه

نباشد. کد C، تشخیص دهنده دقیقاً t خطا نامیده می‌شود اگر C، تشخیص دهنده t خطا باشد اما تشخیص دهنده $t+1$ خطا نباشد.

قضیه. کد C تشخیص دهنده دقیقاً t خطاست اگر و تنها اگر $d(C)=t+1$.

تعریف. کد C، تصحیح کننده t خطا (*t-error correcting*) است اگر قاعده MDD قادر به تصحیح حداکثر t خطا در هر کدکلمه باشد (با این فرض که تمام گره‌ها (*ties*) به عنوان خطا گزارش شوند). کد C، تصحیح کننده دقیقا t خطاست اگر تصحیح کننده t خطا بوده، اما تصحیح کننده $t+1$ خطا نباشد.

قضیه. کد C تصحیح کننده دقیقا t خطاست اگر و تنها اگر $d(C)=2t+1, 2t+2$.

اثبات: فرض کنید $d(C)=2t+1, 2t+2$. همچنین فرض کنید c ارسال و d دریافت شده باشد، به طوری که $d(c,d)\le t$. در این‌صورت d به c از همه کدکلمات دیگر نزدیک تر است، زیرا اگر وجود داشته باشد $c'\in C$ به طوری که $c'\neq c$ و $d(c',d)\le t$، آنگاه:

$$d(c',c)\le d(c,d)+d(d,c')\le t+t=2t<d(C)$$

که تناقض است. حال نشان می‌دهیم C تصحیح کننده $t+1$ خطا نیست. پس دو حالت زیر را در نظر می گیریم:

الف- $d(C)=2t+1$. پس $c\neq c'\in C$ وجود داردبه طوری که $d(c,c')=2t+1$. حال فرض کنید c ارسال و d دریافت شده باشد به طوری که $d(c',d)=t,\ d(c,d)=t+1$. در واقع d به این صورت ساخته می‌شود که در $t+1$ مکان از ۲t+۱ مکان متفاوت c و c'، با c برابر بوده و درt مکان باقیمانده با c' برابر است. بنابراین طبق قاعده کدگشایی MDD، d به c' کدگشایی می‌شود که اشتباه است. پس C تصحیح کننده t+۱ خطا نیست.

ب- $d(C)=2t+2$. پس $c\neq c'\in C$ وجود دارد به طوری که $d(c,c')=2t+2$. حال d را به گونه‌ای می‌سازیم که $d(c',d)=d(c,d)=t$+۱، آنگاه یک گره رخ داده و کدگشا اعلام خطا می کند.

برعکس، اگر C تصحیح کننده دقیقا t خطا باشد، آنگاه نمی‌توانیم داشته باشیم $d(c,c')\leq ۲t$. زیرا در غیراین‌صورت کلمه d وجود دارد به طوری که $d(c,d)=t$ و $d(c',d)\leq t$. حال اگر c ارسال و d دریافت شده باشد آنگاه d به اشتباه به c' کدگشایی می‌گردد، یا اعلام خطا می‌گردد (در حالت گره). بنابراین $d(C)\geq 2t+1$. اما اگر $d(c)\geq ۲t+۳=۲(t+۱)+۱$ آنگاه طبق قسمت اول، کد C، تصحیح‌کننده $t+۱$ خطا می‌باشد که با فرض در تناقص است؛ پس $d(C)=2t+1,\ 2t+2$.

نتیجه. $d(C)=d$ اگر و تنها اگر C تصحیح کننده دقیقاً $\left\lfloor \frac{d-1}{2} \right\rfloor$ خطا باشد.

مثال. کد تکرار $q-$تایی به طول n به صورت $C=\{۰\cdots۰,11\cdots1,...,(q-1)\cdots(q-1)\}$ است. کمترین فاصله این کد $d(C)=n$ است. بنابراین، این کد، تصحیح‌کننده دقیقاً $\left\lfloor \frac{n-۱}{۲} \right\rfloor$ خطا است. این کد همچنین قادر به تشخیص $d-۱=n-۱$ خطا می باشد.

رابطه بین کمترین فاصله و احتمال خطا.

تعریف. یک (n,M,d)-کد، ماکسیمال نامیده می‌شود اگر مشمول در هیچ $(n,M+1,d)$-کدی نباشد.

مثال. کد $C=\{۰۰۰,۱۱۱,۳۳۳\}$ روی الفبای $A=\{۰,۱,۲,۳\}$ ماکسیمال نیست، زیرا C یک $(۳,۳,۳)$-کد است که می‌توان با اضافه‌کردن کلمه **۲۲۲** مشاهده نمود این کد هنوز یک $(۳,۳,۳)$-کد است؛ ولی $C\cup\{۲۲۲\}$ ماکسیمال است (چرا؟)

نکته. یک (n,M,d)-کد مانند C ماکسیمال است، اگر دارای خاصیت زیر باشد.

برای هر کلمه مانند x، یک کدکلمه $c\in C$ موجود باشد به طوری که $d(x,c)<d$.

بنابراین در چنین کدی، اگر کلمه دریافتی x دارای این خاصیت باشد که $d(x,c)\geq d$، آنگاه x به کدکلمه دیگری نزدیک تر خواهد بود و لذا در این حالت خطا در کدگشایی رخ می‌دهد. بنابراین اگر کانال BSC باشد، داریم:

$$p_{\text{decode error}}\geq\sum_{x=d}^{n}\binom{n}{k}p^k(1-p)^{n-k}=p(d(x,c)\geq d)=p(w(e)\geq d)$$

از طرف دیگر، اگر C یک (n,M,d)-کد تصحیح کننده دقیقاً t خطا باشد، آنگاه داریم:

$$p_{\text{correct}} \ge \sum_{k=0}^{t} \binom{n}{k} p^k (1-p)^{n-k}$$

بنابراین:

$$p_{\text{decodeerr}} = 1 - p_{\text{correct}} \le 1 - \sum_{k=0}^{t} \binom{n}{k} p^k (1-p)^{n-k}$$

که در آن $t = [\frac{d-۱}{۲}]$. حال اگر تعریف کنیم:

$$B_p(n,m) = \sum_{k=\circ}^{m} \binom{n}{k} p^k (۱-p)^{n-k}$$

آنگاه قضیه زیر را داریم:

قضیه. در یک کانال دوتایی متقارن $\text{BSC}(p)$، احتمال خطای کدگشایی برای یک کد (n,M,d) ماکسیمال در رابطه زیر صدق می‌کند:

$$1 - B_p(n, d-1) \le p_{\text{decodeerr}} \le 1 - B_p(n, [\frac{d-1}{2}])$$

شعاع فشردگی (*packing Radii*) و شعاع پوششی (*covering Radii*) یک کد.

تعریف. فرض کنید $x \in A^n$ یک کلمه دلخواه باشد و $|A| = q$. نیز فرض کنید r یک عدد حقیقی نامنفی باشد. گوی به شعاع r حول x به صورت مجموعهٔ زیر تعریف می‌شود:

$$S_q(x,r) = \{y \in A^n \mid d(x,y) \le r\}$$

اگر $V_q(n,r)$ حجم گوی $S_q(x,r)$ باشد، آنگاه:

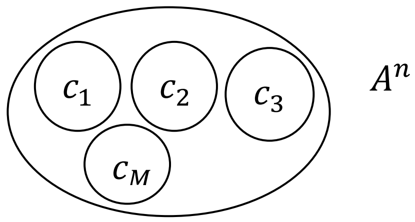
$$V_q(n,r) = \sum_{k=۰}^{r} \binom{n}{k} (q-۱)^k$$

مثال. اگر $A = \{۰,۱\}$ آنگاه A^3 را می‌توان به صورت زیر نمایش داد:

$$S_q(111,1) = \{111, 101, 110, 011\}$$

حال فرض کنید $C_{۱۱}$ یک کد (n,M,d) تصحیح کننده $t-$ خطا باشد. در اینصورت:

$$\forall i \ne j \quad S_q(c_i,t) \cap S_q(c_j,t) = \phi$$



زیرا درغیر اینصورت $x \in S_q(c_i,t) \cap S_q(c_j,t)$ وجود دارد به طوری که:

$$d(x,c_i) \le t, d(x,c_j) \le t \Rightarrow d(c_i,c_j) \le d(x,c_i) + d(x,c_j) \le t + t = 2t < d$$
$$(d = 2t+1 \ \ or \ 2t+2)$$

تعریف. فرض کنید $C \subseteq A^n$. شعاع فشردگی C بزرگترین عدد صحیح r است که در آن گوی‌های $S_q(c,r)$ حول کدکلمات C مجزا باشند. شعاع پوششی C کوچکترین عدد صحیح Sاست به طوری که گوی‌های $S_q(c,s)$ فضای A^nرا احاطه کنند. شعاع فشردگی C را با $\Pr(C)$ و شعاع پوششی C را با $cr(C)$ نمایش می‌دهیم.

قضیه. با فرض این که گره‌ها را همواره به صورت خطا گزارش کنیم، کد C تصحیح کننده t خطاست اگر و تنها اگر گوی‌های $S_q(c,t)$ $(c \in C)$ مجزا باشند.

نتیجه. با فرض اینکه گره‌ها به صورت خطا گزارش شوند، کد C تصحیح کننده دقیقا t خطاست اگر و تنها اگر $\Pr(c) = t$.

کدهای کامل و شبه‌کامل.

تعریف. کد C کامل نامیده می‌شود اگر $cr(C) = pr(C)$. به عبارت دیگر، اگر کد $C \subseteq A^n$ تصحیح کننده دقیقا t خطا باشد، آنگاه C کامل است. اگر گوی‌های به مرکز کدکلمات و شعاع t، تمامی فضای A^n را بپوشانند.

مثال. کدهای همینگ $H_2(3)$ یک کد دوتایی $(7,16,3)$ است.

در واقع:

$$H_2(3) = \{c_1c_2...c_7 \mid c_i \in \{0,1\}, c_1 + c_4 + c_5 + c_7 \overset{2}{\equiv} c_2 + c_4 + c_6 + c_7 \overset{2}{\equiv} c_3 + c_5 + c_6 + c_7 \overset{2}{\equiv} \circ\}$$
$$= \{1101100, 1010100, 0110010, 1110001, 0111100, 1011010, 0011001, 0100101, 1100110,$$
$$1000011, 100001110, 1001101, 0010111, 0101011, 11111111, 0000000\}$$

این کد $t=1$ واضح است که $|S_2(c,1)|=1+\binom{7}{1}=8$ و $|A^7|=2^7=128$ اما ۱۶×۸=۱۲۸، لذا

$A^7=\bigcup_{C\in C}^{\text{مجزا}} S_2(c,1)$، پس این کد، کامل است

قضیه: (شرط گوی- فشردگی یا *sphere packing*):

فرض کنید C یک کد $q-$ تایی (n,m,d) باشد. در این صورت C کامل است اگر و تنها اگر $d=2t+1$ فرد باشد و $M.V_q(n,t)=q^n$، به عبارت دیگر.

$$M=\frac{q^n}{\sum_{k=0}^{t}\binom{n}{k}(q-1)^k}$$

اثبات : اگر C کامل باشد آنگاه واضح است $d\neq 2t+2$. زیرا اگر $d(C)=2t+2$ باشد آنگاه $\Pr(C)=t<cr(C)=t+1$.پس $d=2t+1$ (توجه داریم $t=\left[\frac{d-1}{2}\right]$)

اما اگر C کامل باشد آنگاه $A^n=\bigcup_{i=1}^{M}S_{q(c_i,t)}$ (که در آن $C=\{c_1,c_2,\dots,c_M\}$)

$$\Rightarrow q^n=|A^n|=\sum_{i=1}^{M}\left|S_q(c_i,t)\right|=\sum_{i=1}^{M}\left(\sum_{k=0}^{t}\binom{n}{k}(q-1)^k\right)$$
$$=M\sum_{k=0}^{t}\binom{n}{k}(q-1)^k\Rightarrow M=\frac{q^n}{\sum_{k=0}^{n}\binom{n}{k}(q-1)^k}$$

بنابراین اگر شرط گوی فشردگی برای برخی $(n,M,2t+1)$ کد C برقرار باشد آنگاه چون گوی های به شعاع t حول کد کلمات متمایز هستند و از طرف دیگر طبق شرط گوی فشردگی ، این گوی ها A^n را می پوشانند، بنابراین $\Pr(c)=Cr(c)=t$.

نکته : وجود اعداد n,M,t که در آن شرط گوی فشردگی برقرار باشد به معنای وجود کد کاملی که در این شرط صدق کند، نیست. مسأله تعیین کدهای کامل ، تاکنون حل نشده است، اما در حالتی که اندازه الفبای کد توانی از یک عدد اول باشد، این مسأله تا حدودی حل شده است. به طور نمونه می توان مشاهده کرد که در حالت های زیر شرط گوی فشردگی برقرار است:

(کل فضای $V(n,q)$)　　۱) $(n, M, d) = (n, q^n, 1)$

(کد تنها با یک کد کلمه)　　۲) $(n,M,d) = (n,1, 2n+1)$

(کد تکرار دوتایی)　　۳) $(n,M,d) = (2m+1,2,2m+1)$

(کد همینگ q تایی)　　۴)$(n, M, d) = (\frac{q^r-1}{q-1}, q^{n-r}, 3), r \geq 2$

ون-لینــت (۱۹۶۷) بــا اســتفاده از یــک جســتجوی کــامپیوتری و بــرای $n \leq 1000$ و $d \leq 2001$ ($t \leq 1000$)، $q \leq 100$، نشان داد که شرط گوی فشردگی تنهـا در مـوارد زیر برقرار است:

(کد گلی)　　۱)$(n, M, d) = (23, 2^{11}, 7)$

کدی با چنین پارامترهایی وجود ندارد　　۲)$(n, M, d) = (90, 2^{78}, 5)$

(کد گلی)　　۳)$(n, M, d) = (11, 3^6, 5)$

بنابراین، تعداد کدهای کامل زیاد نیست.

تعریف. کد C شبه کامل(*quasi-perfect*) نامیده می شود، اگر $Cr(C) = Pr(C)+1$. به عبارت دیگر ، کد $C \subseteq A^n$ شبه کامل است، اگر عدد r وجود داشته باشد به طوری که گوی های $S_{q\,(c,r)}$ $(c \in C)$ مجزا باشند و گوی های $S_q(c, r+1)$ با شعاع $r+1$ ، A^n را بپوشانند.

خانواده کدها

۱- کدهای سیستماتیک: یک کد q- تایی (n, q^k)، سیستماتیک نامیده می‌شود اگر k مکـان $i_1,...,i_k$ با این خاصیت وجود داشته باشند که با تحدید نمودن کد کلمـات بـه ایـن مکـان‌هـا، تمامی q^k، آرایه q تایی به طول k را داشته باشیم. مکان‌هـای $\{i_1,...,i_k\}$ مجموعـهٔ اطلاعـات (*information set*) و سـمبل‌هـای کـد کلمـات درایـن مکـان‌هـا سـمبل‌هـای اطلاعـات (*information symbols*) نامیده می‌شوند.

در این حالت، اگر منبع را بتوان به صورت مجموعه تمامی کلمات q– تایی به طول k نمایش داد، آنگاه یک کدسیستماتیک q– تایی از اندازه q^k می‌تواند به منظور کد گذاری چنین منبعی، بدون تغییر کلمات به کار رود.

مثال: کد دوتایی $C=\{0000,0110,1001,1010\}$ روی مکان اول و سوم سیستماتیک است بنابراین اگر منبع $S=\{00,01,10,11\}$ را به کار بریم، می‌توان منبع S را به صورت زیر کد گذاری نمود: $00\rightarrow 0000,\ 01\rightarrow 0110,\ 10\rightarrow 1001,\ 11\rightarrow 1010$ چنین کدگذاری، یک کدگذاری سیستماتیک نامیده می‌شود. واضح است که فرآیند کد گشایی در این صورت، بسیار ساده بوده و کافی است تا کلمات منبع را به طور مستقیم از کد کلمه دریافتی استخراج کنیم.

مثال: کد دوتایی $C=\{000,100,010,001\}$ سیستماتیک نیست. (چرا؟)

میدان‌های متناهی (*finite fields*)

برای این که به کدهای خود، ساختارهای با معنی ببخشیم، فرض می‌کنیم A به عنوان الفبای کد دارای یک ساختار مشخص باشد، مثلاً یک میدان متناهی باشد. قضیه اساسی زیر را داریم:

قضیه: اگر P یک عدد اول باشد و n یک مقدار صحیح مثبت باشد، آنگاه (در حد یکریختی یا *Isomorphism*) دقیقاً یک میدان متناهی از اندازه $q=p^n$ وجود دارد که آن را با $GF(q)$ یا F_q نمایش می‌دهیم.

علاوه بر این، تمامی میدان‌های متناهی دارای اندازه P^n برای مقداری p اول و صحیح مثبت n، هستند.

مجموعه $(F_q)^n$ شامل تمام ی n تایی های مولفه‌های متعلق به F_q، یک فضای برداری روی F_q با بعد n می‌باشد(بحث فضای برداری جبر خطی مطالعه شود) ما $(F_q)^n$ را با $C(n,q)$ نمایش داده و بردار $(x_1,\dots,x_n)$ در این فضا را به صورت $x_1,\dots,x_n$ نمایش می دهیم.

کدهای هم ارز یا هم ارزی کدها (*equivalence of codes*)

خاصیت تصحیح خطای (چنان که قبلا دیدیم) دو کد $C_۲=\{۰۰,۱۰۱\}, C_۱=\{۰۰,۰۱۱\}$ یکسان است و در عمل هیچ تفاوت با یکدیگر ندارند. دلیل آن ، هم ارز بودن $C_۲,C_۱$ که به صورت زیر تعریف می‌شود.

تعریف: دو کد q- تایی (n,M)، $C_۲,C_۱$ هم ارز ($eqviralent$) نامیده می‌شوند. اگر جایگشت σ روی n مکان مختصات و جایگشت‌های $\pi_۱,\pi_۲,...,\pi_n$ روی الفبای کد وجود داشته باشد.

به طوری که $c_1c_2....c_n \in C_1 \Leftrightarrow \pi_1(c_{\sigma(1)})\pi_2(c_{\sigma(r)})...\pi_n(c_{\sigma(n)}) \in C_2$

به عبارت دیگر، دوکد هم ارز هستند اگر بتوان با جایگشت روی مکان‌های هر کد کلمه (از طریق σ) و جایگشت روی سمبل‌های هر مکان از هر کد کلمه (از طریق $\pi_۱,...,\pi_n$)، از یکی به دیگری رسید.

نکته: رابطه هم ارزی بین کدها، یک رابطه هم ارزی است، یعنی در خاصیت بازتابی، تقارنی و ترا گذاری صدق می‌کند. (چرا؟)

لم: اگر $o \in A$، آنگاه هر کد روی A هم ارز با یک کد است که شامل کد کلمه $۰...۰=۰$ باشد.

اثبات: کد کلمه $c_۱c_۲...c_n$ را به طور دلخواه از کد C در نظر بگیرید و جایگشت های زیر را روی مکان‌های آن (به ترتیب)، اعمال کنید.

$$c_i \neq ۰ \Rightarrow \pi_i = \begin{pmatrix} c_i & ۰ & j \\ \downarrow & \downarrow & \downarrow \\ ۰ & c_i & j \end{pmatrix}, j \in A-\{۰,c_i\}$$ روی مکان i.

قضیه: اگر کدهای $C_۱$ و $C_۲$ معادل باشند آنگاه $d(c_۱)=d(c_۲)$، همچنین احتمال تصحیح خطای کد گشایی $C_۲,C_۱$ روی کانال‌های q- تایی متقارن(مانند BSC) با یکدیگر برابر است.

۲) کدهای خطی (*linear codes*):

یکی از مهمترین مزایایی که یک میدان متناهی F_q. به عنوان الفبای کد دارد، در این است که می توان از اعمال فضای برداری روی کد کلمات بهره گرفت. اما به جهت آنکه نیاز داریم تا مجموع دو کد کلمه (یا مضرب اسکالری از یک کد کلمه) از یک کد خود کد کلمه باشند، یک کد خطی را به صورت زیر تعریف می کنیم.

تعریف: کد $L \subseteq V(n,q)$، یک کد خطی (*linear code*) نامیده می‌شود، اگر زیر فضای $V(n,q)$ باشند. در این حالت، اگر L دارای بعد k باشد، آن را به صورت $[n,k]-$ کد نمایش می‌دهیم و اگر $d(L)=d$ کمترین فاصله کد L باشد آنگاه گوئیم L یک (n,k,d) کد است.

نکته: تمامی کدهای خطی، شامل کد کلمه صفر ۰...۰=۰ هستند و نیز نرخ و اندازه یک $[n,k]-$کد -q تایی به صورت زیر تعریف می‌شود $M=q^k, \quad R=\dfrac{k}{n}$.

تعریف: وزن $w(x)$ از یک کلمه $x \in V(n,q)$، تعداد مکان‌های ناصفر X است.

کمترین وزن (*minimum weight*) کد C، کمترین وزن کد کلمات نا صفر C است.

تعریف: اگر $x=x_1...x_n$ و $y=y_1...y_n$ دو کلمه دوتایی باشند، آنگاه اشتراک x را (*intersection*) به صورت زیر تعریف می‌شود:

$$x \cap y=(x_1y_1, x_2y_2, ..., x_ny_n)$$

لم:

۱) برای تمامی $x,y \in V(n,q)$ داریم: $d(x,y)=w(x-y)$

۲) برای تمامی $(q=2)x,y \in V(n,2)$ داریم $d(x,y)=w(x)+w(y)-2w(x \cap y)$

اثبات: (تمرین)

نکته: برای یافتن کمترین فاصله یک (*n,M*) کد در حال کلی به $\binom{m}{2}$محاسبه نیاز است.

اما در مورد یک کد خطی، تنها به $M-1$ محاسبه نیاز داریم (مطابق قضیه زیر)

قضیه: اگر L یک کد خطی باشد آنگاه *d(L)=w(L)*.

اگر $C,d \in L$ آنگاه $c-d \in L$ بنابراین:

$$\begin{array}{llll} d(L)=\min\limits_{C\neq d} d(c,d)=\min\limits_{\substack{C\neq d\in L\\ \circ\neq c-d\in L}} w(c-d)=\min\limits_{\circ\neq C\in L} w(c)=w(L) \end{array}$$

کدهای دوری (*cyclic codes*)

بسیاری از کدهای مهم، بـه طـور قابـل ملاحظـه‌ای، دارای سـاختاری، بیشـتر از یـک فضـای برداری هستند. کد خطی $L\subseteq V(n,q)$ به صورت زیر نسبت داد:

$$\phi: C_\circ C_1 \ldots C_{n-1} \to C_\circ + C_1 x + --- + C_{n-1} x^{n+1}$$

در واقع، ϕ یک یکریختی فضای برداری از L به روی زیر فضای $\phi(L)$ از $F_q[x]$ است. بنابراین، هر کد کلمه از L را می‌توان به صورت یک چند جمله‌ای در نظر گرفت و برعکس مزیت این کار، این است که $F_q[x]$ دارای ساختار بیششتری از فضای برداری است، در واقع $F_q[x]$ یک جبر است به عبارت دیگر، ما می‌توانیم دو کد کلمه را در یکدیگر ضـرب کنـیم (قبلا در فضای برداری نمی‌توانستیم) ولی ممکـن اسـت ضـرب آنهـا دیگـر یـک کـد کلمـه نباشد، برای این منظور ایده خود را ظریف تر می‌کنیم. فرض کنید $P(x)$ یک چنـد جملـه‌ای با درجهٔ n در $F_q[x]$ باشد، در اینصورت:

$p(x)$ ایده‌آل تولید شده توسط $=<P(x)>=\{f(x)P(x) \mid f(x)\in F_q[x]\}$

جبر خارج قسمتی (*quotient algebra*) ، مجموعه تمامی چند جمله‌ای های $F(x)$ با درجه حداکثر n است که به صورت زیر تعریف می‌شود.

$$R=\frac{F_q[x]}{<p(x)>}=\{f(x)\in F_q[x] \mid \deg F(x)<n\}$$

به عبارت دیگر R، مجموعه تمـامی چنـد جملـه‌ای هـا در $F_q[x]$ اسـت کـه در پیمانـه $P(x)$ محاسبه می‌شوند. (مشابه با حلقه Z_m که عناصر در پیمانه m محاسبه می‌شوند). در این حالت حاصل ضرب هر دو چند جمله‌ای در R خواهد بـود. در ایـن حالـت نگاشـت ϕ را مـی‌تـوان یک یکریختی از فضای برداری L به زیر فضـای $\phi(L)$ از R تصـور کـرد کـه در ایـن حالـت $\phi(L)$ یک زیر جبر از R است ولی،می‌توان $\phi(L)$ را به صورت یک ایده‌آل (*Ideal*) از R نیز

تصور کرد، که در این حالت نه تنها $\phi(L)$ یک جبر است، بلکه این خاصیت اضافی وجود دارد که حاصل ضرب هر چند جمله‌ای در هر کد کلمه، یک کد کلمه خواهد بود.

حال فرض کنید $p(x)=x^n-1$ و R_n را جبر خارج قسمتی $R_n=\frac{F_q[x]}{<x^n-1>}$ در نظر بگیرید اگر L یک ایده‌آل از R_n باشد ($L\Delta R_n$)، آنگاه L تحت ضرب هر چند جمله‌ای از R_n بسته است اما این معادل با آن است که L تحت ضرب توسط x بسته باشد، اما (در R_n داریم)

$$x(C_0+C_1x+--+c_{n-1}x^{n-1})=(c_0x+C_1x^2+--+c_{n-1}x^n)\bmod(x^n-1)=$$
$$C_{n-1}+C_0x+C_1x^2+--+C_{n-2}x^{n-1}$$

بنابراین اگر $C_0+C_1x+--+C_{n-1}x^{n-1}\in L$ آنگاه باید

$$C_{n-1}+C_0x+C_1x^2+--+C_{n-2}x^{n-1}\in L$$

به عبارت دیگر $C_0C_1--C_{n-1}\in L\Leftrightarrow C_{n-1}C_0C_1--C_{n-1}\in L$ این مسأله، تعریف زیر را به دنبال دارد.

تعریف کد خطی $L\subseteq C(n,q)$ دوری $(Cyclic)$ است اگر:

$$C_0C_1--C_{n-1}\in L\Rightarrow C_{n-1}C_0C_1--C_{n-2}\in L$$

به عبارت دیگر، L دوری است اگر $L\lhd R_n=\frac{F_q[x]}{<x^n-1>}$

نکته: R_n یک دامنه ایده‌ال اصلی (*Principal ideal domain*) است. به این معنی که هر ایده‌آل از R_n (به عنوان یک کد دوری مانند C)، توسط یک چند جمله‌ای منحصر به فرد $g(x)$ تولید شده است که چند جمله‌ای مولد C (*generator Polynimic*) نامیده می‌شود، به عبارت دیگر $g(x)$ چند جمله‌ای تکین (*Monic*) یکتا با کمترین درجه در C، بنابراین:

$$C=<g(x)>=\{f(x)g(x)\mid F(x)\in R\}$$

در این حالت: $\dim(C=n-\deg g(x)$ (بعد کد C)

علاوه بر این $g(x)\mid x^n-1$، زیرا در غیر اینصورت اگر $r(x)$ باقیمانده ناصفر x^n-1 بر $g(x)$ باشد، داریم $r(m)\in C,\deg\ r(x)<\deg\ g(x)$ که با فرض $g(x)$ در تناقض است بنابراین تمامی ریشه‌های $g(x)$ ریشه‌های x^n-1 هستند (یعنی $x^n=1$ یا ریشه nام واحد) لذا، می-

توانیم یک کد دوری را با تخصیص چند جمله‌ای مولد آن ($g(x)$) یا به طور هم ارز، تعیین ریشه‌های nام واحد (ریشه‌های $x^n - ۱$) که ریشه‌های $g(x)$ هستند، تعیین کرد. بنابراین، بسته به انتخاب این ریشه‌ها، خانواده متفاوتی از کدها را خواهیم داشت.

به طور نمونه، همان گونه که خواهیم دید، ریشه‌های n ام واحد، تشکیل یک گروه دوری تحت عمل ضرب می‌دهند. این ریشه‌ها به صورت $۱, w, w^۲, ..., w^{n-۱}$ هستند که در آن w یک ریشه nام اولیه واحد است. حال با انتخاب یک چند جمله‌ای $g(x)$ با کمترین درجه که ریشه های آن ، شامل ریشه‌های متوالی $۱, w, ..., w^{e-۱}$ باشند، می‌توان یک کد دوری با چند جمله‌ای مولد $g(x)$ را ساخت. البته در این حالت توجه داریم که این ریشه‌های متوالی ممکن است تمام ریشه‌های $g(x)$ نباشد و $g(x)$ ریشه‌های دیگری نیز داشته باشند (که البته همه آنها ریشه $x^{n-۱}$ هستند) چنین کدهایی، کدهای BCH نامیده می‌شوند که دسته مهمی از کدهای دوری هستند.

کدهای غیر خطی

این کد ها به روش های مختلفی ساخته می‌شوند. به طور مثال، برخی از کدهای غیر خطی، از طرح های ترکیباتی ساخته می‌شوند. (مانند مربع‌های لاتین یا طرح‌های بلوکی).

مثال: مجموعه نقاط نمایش داده شده در زیر، به همراه خطوطی که آنها را به هم وصل می‌کنند، تشکیل یک صفحه تصویری (*Projective plane*) از مرتبه ۲ یا صفحه فانو (*Fano plane*) می‌دهند که مثالی از یک طرح ترکیباتی است.

$$B = \{\{1,2,4\},\{2,3,5,\}\{3,4,6\}\{4,5,7\}\{5,6,1\}\{6,4,2\}\{7,1,3\}\}$$

نقاط $V = \{1,2,...,7\}$

ماتریس وقوع این طرح به صورت زیر تعریف می‌شود

$$Q_{ij} = \begin{cases} 1 & j \in l_i \\ ۰ & ... \end{cases} \qquad 1 \le i_j \le 7$$

$$A = (a_{ij})_{7\times7}$$

$$A=\begin{array}{c}l_1\\l_2\\l_3\\l_4\\l_5\\l_6\\l_7\end{array}\begin{pmatrix}1&2&3&4&5&6&7\\1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\\1&0&0&0&1&1&0\\0&1&0&0&0&1&1\end{pmatrix}$$

حال اگر r_1 تا r_7 معرف سطرهای A و S_1 تا S_7 مکمل‌های آنها باشند، آنگاه کد $C=\{0,1,r_1,...,r_7.s_1,...,s_7\}$ یک $(7,16,3)$– کد است. (که در آن ۰ و ۱ بردار 7 تایی صفر و یک هستند) زیرا:

$$d(r_i,r_j)=4=d(s_i,s_j),d(r_i,s_j)=d(r_i,\bar{r}_j)=7-d(r_i,r_j)=7-4=3$$

خانواده کدها

اگر C یک (n,m,d) کد باشد، آنگاه نرخ کد به صورت: $R=R(c)=\dfrac{\log_q^m}{n}$ تعریف می-شود. همچنین تعریف می‌کنیم $\delta=\delta(C)=\dfrac{d}{n}$. برخی کدهای مهم به صورت زیر هستند

۱- کد تکرار q تای: $C=\{\underbrace{0...0}_{n},\underbrace{1...1}_{n},......,\underbrace{(q-1)...(q-1)}_{n}\}$

این کد خطی بوده و به صورت $[n,1,n]$ است.

$$R=\frac{1}{n},\delta=1$$

$\delta,\lim\limits_{n\to\infty}R=0$ بیشترین است

۲- کدهای همینگ: شاید خانواده کد های همینگ $H_q(r)$ مشهورترین کدهای تصحیح خطا باشند. این کد ها در سال ۱۹۴۹ توسط گلی (*Marcel Golay*) و ۱۹۵۰ توسط همینگ (*Richard Hamming*) به طور مستقل مطرح شدند. این کدها خطی و کامل بوده و کد گشای بسیار ساده‌ای دارند.

تمامی کدهای همینگ دوتایی، معادل با کدهای دوری هستند، اما برخی (و نه همه) کدهای همینگ غیره دودویی معادل با کدهای دوری هستند. به طور خاص ...$(r>0)H_q(r)$ یک کد

$[n,k,d]$– خطی q– تایی است جایی که $n=\frac{q^r-۱}{q-۱}$ ،$k=n-r$ و $d=۳$. به طور خاص اگر $q=۲$، آنگاه نرخ کدهای همینگ $\delta=\frac{۳}{n}, R=۱-\frac{r}{n}$ بوده. واضح است که $R \to l$ اما $\delta \to ۰ (n\to\infty)$ این کدها تصحیح کننده دقیقا یک خطا هستند.

کدهای گلی در سال ۱۹۴۸، گلی برخی از کدهای خطی را معرفی نمود، $G_{۱۲}, G_{۱۱}, G_{۲۴}, G_{۲۳}$ معرفی شدند و کدهای گلی نام دارند. کد $G_{۲۴}$ یک کد خطی دوتایی (۲۴,۴۰۹۶/۸)– کد است که توسط فضاپیمای ویاگر (*Coyager*) به منظور انتقال عکس‌های رنگی از مریخ و زحل استفاده شده است. کد $G_{۱۱}$، یک کد دوری سه تایی کامل (۷۲۹/۵و۱۱) است و $G_{۱۲}$ یک کد خطی سه تایی (۷۲۹/۶و۱۲) است. مک ویلیامز والسون (*Sloon*) (۱۹۷۷) به کدهای گلی دوتایی به عنوان مهمترین د ا (چه از دید عملی و چه تئوری) اشاره کرده‌اند.

کدهای رید-مولر

کدهای رید-مولد خانواده‌ای از کدهای خطی دوتایی هستند که ارزش عملی خوبی داشته و دارای خواص کد گشایی مناسبی هستند. برای هر عدد صحیح M و هر عدد صحیح $r,(۰\le r\le m)r$ این کد رید-مولر $R(r,m)$ دارای پارامترهای زیر است. $n=۲^m, k=۱+\binom{m}{۱}+\ldots+\binom{m}{r}$ $d=۲^{m-r}$ کدهای رید- مولر مرتبه اول $R(۱,m)$، دهای $۲^m, ۲^{m+۱}, ۲^{m-۱}$هستند. کد $R(۱/۵)$ توسط فضاپیمای ماریسز ۹، به منظور عکس‌های سیاه و سفید از مریخ در سال ۱۹۷۲، بکارگرفته شد. در مورد کدهای رید-مولر، داریم:

$$R=\frac{۱+\binom{m}{۱}+\ldots+\binom{m}{r}}{۲^m}, \delta=\frac{۱}{۲^r}$$

بنابراین اگر r ثابت باشد، داریم $R\to ۰$ زمانی که $n\to\infty$ و اگر $r\to\infty$ آنگاه $\delta\to ۰$ زمانی که $n\to\infty$

کدهای *BCH* و کدهای رید-سولمن

کدهای BCH (*Bose- chevlehuri-codes Hocqunqhem*) ابتدا در سال ۱۹۵۹ توسط *Hocqunqhem* کشف شده و در سال ۱۹۶۰ توسط *sose* و *Ray-chad huri* نامگذاری شدند. این کدها، تعمیم کدهای همینگ هستند. این کدهای دوری و q– تایی بوده و اهمیت عملی زیادی در تصحیح – خطا دارند.

کدهای *BCH* توسط چند جمله‌ای مولدی که ریشه‌های آن شامل یک لیست e–۱ تایی متوالی $w, w^{2}, ... w^{e}-1$ از ریشه‌های $x^{n}-1$ هستند، تعریف می‌شوند.

در این حالت، به e فاصله مطرح (*designed distance*) کد گفته می‌شود. یک کد *BCH* مانند C با فاصل مطرح e دارای کمترین فاصله $d \geq e$ است. بنابراین اگر چند جمله‌ای مولد $g(x), C$ باشد آنگاه کد C دارای پارامترهای زیر است : $(n, k = n - \deg(g(x)), d \geq e)$

بسیاری از کدهای *BCH* دارای *d=e* هستند و لذا می‌توانیم کدی با کمترین فاصله دلخواه طراحی کنیم. اگر q توانی از یک عدد اول باشد، آنگاه کد رید–سولمن (*Reed-solomon*) q– تایی یک کد *BCH* با طول $n = q-1$ است. بنابراین کدهای رید– سولومن بزرگ (با طول بزرگ) دارای اندازه الفبای بزرگی برای کد هستند که غیر عملی است. اما آنچنان که خواهیم دید می‌توان این کد ها را به کد دو دویی تصویر کرد. همچنین کدهای رید– سولومن در تصحیح خطای گروهی (*Burst error*) دارای اهمیت زیادی هستند.در واقع *NASA* ، از این کدها به طور زیادی در برنامه های فضایی دوردست بهره گرفته . (برای نمونه در مأموریت‌های *MagelanT Galileo* و *Ulysses* به کار گرفته شدند) .

کدهای باقیمانده مربعی

کدهای باقیمانده مربعی، کلاس دیگری از کدهای دوری هستند که دارای طول اول P هستند. (*quadaratic residue codes*) یک عدد صحیح مانند X یک باقیمانده مربعی در پیمانه P نامیده می‌شود.

اگر معادله $x^{2} \overset{p}{\equiv} a$ دارای یک جواب باشد. به عبارت دیگر a ریشه یک عدد در پیمانه P باشد.

در نظریه اعداد، این مطلب اثبات شده است که ۲ یک ریشه مربعی در پیمانه P است اگر و تنها اگر P به شکل $8m\pm1$ باشد. بنابراین کدهای باقیمانده مربعی دارای طول $p=8m\pm1$ (اول) هستند. در این حالت، چند جمله‌ای مولد کد دارای ریشه های زیر است.

$\{W^u \mid$ u یک باقیمانده مربعی در پیمانه P نباشد$\}$ یا

$\{w^r \mid$ r یک باقیمانده مربعی در پیمانه P باشد$\}$

به عبارت دیگر، چند جمله‌ای مولد کد به یکی از دو صورت زیر است

$$g_۱(x)=\prod_{r\in QR}(x-w^r),\; g_۲(x)=\prod_{u\in NQR}(x-w^u)$$

که در آن $QR\subseteq\{۱,۰۰۰,p-۱\}$ باقیمانده های مربعی در پیمانه P و $NQR\subseteq\{۱,...,p-۱\}$ باقیمانده های غیرمربعی در پیمانه P هستند.

می‌توان ثابت کرد $|QR|=|NQR|=\frac{p-۱}{۲}$ ، بنابراین بعد یک کد باقیمانده مربعی به صورت زیر است $K=n-\deg(g(x))=P-\frac{p-۱}{۲}=\frac{p+۱}{۲}$.

متأسفانه، تعیین کمترین فاصله یک کد باقیماندۀ مربعی مشکل است. اما می‌توان ثابت کرد که $\geq\sqrt{P}$ اما این کران، کران خیلی خوبی نیست. توجه داریم که نرخ یک کد باقیمانده مربعی حداقل $R\geq\frac{۱}{۲},۱\frac{۱}{۲}$ خواص کیفی کدهای باقیمانده مربعی در حالت کلی، ناشناخته است. اما برخی از این کدها با طول کم (مانند کدهای کامل گلی $G_{۱۱},G_{۲۳}$) کدهای شناخته شده و خوبی هستند.

کدهای گاپا (*GOppa Codes*)

همانند کدهای دوری که با چند جمله‌ای مولد خود شناخته می‌شود، کدهای گاپا با یک چند جمله‌ای گاپای مخصوص $G(x)$ تعیین می‌شوند که روی یک میدان F_qm به همراه یک مجموعه $L\subseteq F_qm$ از عناصر ناصفر $G(x)$ تشکیل شده است کدهای گاپا، خطی هستند، اما در حالت کلی دوری نیستند یکی از زیباترین وجوه کدهای گاپا در این است که

کمتـــرین فاصـــله کـــد از پـــایین توســـط $1+\deg(G(x))$ کرانـــدار اســـت. در واقـــع اگـــر $g=\deg(G(x))$ ، آنگاه پارامترهای کد گاپا در رابطه زیر صدق می‌کند.

$$n=|L|, \kappa \geq n-mg, \;\; d \geq 1+g$$

(در حالت دودویی، اگر $G(x)$ دارای هیچ ریشه تکراری نباشد، آنگاه می‌توان این کـران را به $d \geq 1+2g$ بهبود بخشید).

کدهای جاستسن (*Justesen Codes*)

توجه دارید که در هر یک از حالتهای قبلی، جـایی کـه نـرخ R و عـدد δ مقـادیر مشخصـی باشند آنگاه زمانی که $n \to \infty$، داریم $R \to 0$ یا $\delta \to 0$. به عبارت دیگر یا نرخ به صـفر میـل می‌کند یا احتمال خطای کد گشایی زمانی که $n \to \infty$ به ۱ میل می‌کند. در ادامه خـانواده‌ای از کدهای خطی را مورد مطالعه قرار می‌دهیم که به کدهای جاستسن معروف هستندو دارای نرخ ثابت $R=\frac{1}{2}$ هستندو در آن:

$$\delta \to H^{-1}(\tfrac{1}{2}) \approx 0/11$$

جایی که $H(\lambda)=-\lambda\log\lambda-(1-\lambda)\log(1-\lambda)$ تابع آنتروپی است. بنابراین کدهای جاستسـن به طور مجانبی خوب هستند (*asym ptotically good*)

کدهای کامل (*Perfect codes*)

برای مدتی، محققین فکر می‌کردند تنها کدهای کامل غیر بدیهی، کد های همینـگ $H_q(r)$ و کدهای گلی G_{13} و G_{11} هستند. کدهای کامل بدیهی، کدهای تکرار دوتایی با طول فـرد، کدهای شامل تنهـا کـد کلمـه صـفر و کـد شـامل همـه عناصـر $V(n,q)$ هسـتند. امـا، وسـیل (*Vasil'ev*) خانواده‌ای از کدهای کامل غیر خطی بـا پـارامترهـای مشـابه بـا کـد همنیـگ را یافت.

قضیه مهم زیر (۱۹۷۳) را درباره کدهای کامـل روی الفبـای بـا انـدازه تـوان یـک عـدد اول، داریم:

قضیه: یک کد کامل q- تایی غیر بدیهی مانند C، جایی که q توانی از یک عدد اول است، دارای پارامترهای مشابه (طول، اندازه و کمترین فاصله) با یکی از کدهای همینگ $H_q(r)$ یا یکی از کدهای گلی $G_{۲۳}$ و $G_{۱۱}$ است علاوه بر این:

۱) اگر C دارای پارامترهای مشابه با یکی از کدهای گلی باشد، آنگاه هم ارز با آن کد گلی است.

۲) اگر C خطی بوده و دارای پارامترهای مشابه با یکی از کدهای همینگ باشد، آنگاه هم ارز با آن کد همینگ است.

به دست آوردن کدهای جدیدی از کدهای قدیمی

در زیر، چندین روش مفید برای به دست آوردن کدهای جدید از کدهای قدیمی را مطرح می‌کنیم.

۱- تعمیم یک کد یا *extending a code*

فرآیند اضافه نمودن یک یا چند مکان مختصات اضافی به کد کلمات یک کد به تعمیم کد معروف است معروف ترین روش برای تعمیم یک کد، با اضافه نمودن یک بیت توازن کلی (*overall parity*) به کد به دست می‌آید. اگر C یک کد (n,m,d) q-تایی باشد، آنگاه کد تعمیم یافته (*extended code*) C به صورت زیر تعریف می‌شود.

$$\hat{C}=\{c_1c_2\dots c_nc_{n+1}\mid c_1,\dots,c_n\in C,\sum_{k=1}^{n+1}C_k=\circ\}$$

اگر $\hat{C}$ یک $(\hat{n},\hat{m},\hat{d})$ - کد باشد، آنگاه

$$\hat{n}=n+1\quad,\quad \hat{m}=m\quad,\quad \hat{d}=d\ \text{ یا }\ d+۱$$

مثال: اگر $C=\{۰۰,۰۱,۱۰,۱۱\}$ آنگاه $\hat{C}=\{۰۰۰,۰۱۱,۱۰۱,۱۱۰\}$ (کد تعمیم یافته C) توجه دارید که C دارای کمترین فاصلهٔ ۱است، اما $\hat{C}$ دارای کمترین فاصله ۲ است.

مثال: کد همینگ $H_۲(r)$ (دوتایی) دارای پارامترهای زیر است:

$$n=۲^r-۱\,,\,M=۲^{(۲^r-۱-r)},d=۳$$

کد همینگ تعمیم یافته $\hat{H}_{۲}(r)$ که با اضافه نمودن یک بیت توازن کلی به $H_{۲}(r)$ بـه دسـت می‌آید، دارای پارامترهای زیر است:

$$\hat{n}=۲^{r},\hat{M}=۲^{(۲^{r}-۱-r)}\ ,\ \hat{d}=۴$$

بنابراین، با وجود این که تعمیم یافته همینگ دارای قدرت تشخیص خطای بیشتری نسبت بـه کد اصلی نیست، اما قدرت تشخیص خطا در آن افزایش می‌یابد.

۲- پنچر نمودن یک کد یا *puncturing acode*

عکس فرآیند تعمیم یک کد، پنچر نمودن کد است. به ایـن صـورت کـه یـک یـا دو مکـان مختصاتی از کد کلمات حذف کی‌شوند. اگر C یک کـد q- تـایی (n,m,d) باشـد و $d\geq ۲$ آنگاه کد C که با پنچر نمودن یک مختص C به دست آمده دارای پارامتر های زیر است:

$n^{*}=n-$ را $M^{*}=M,d^{*}=d$ یا $d-۱$

مثال: کد گلی $G_{۲۳}$ با پارامترهای (۷و۴۰۹۶و۲۳)، با پنچـر نمـودن کـد $G_{۲۴}$ بـا پـارامترهـای (۸و۴۰۹۶و۲۴) بدست آمده است. (توجه دارید که پنچر نمودن $G_{۲۴}$ در هر مکان، یـک کـد معادل با $G_{۲۳}$ می‌دهد).

کد $G_{۲۴}$ در شرط گوی پوششـی (*sphere- paching*) صـدق نمـی‌کنـد. و بنـابراین کامـل نیست. اما کد $G_{۲۳}$ کامل است. بنابراین پنچر نمودن یک کد غیر کامل می‌تواند به یک کـد کامل منجر شود.

قضیه: یک کد $(n,m,۲t+۱)$ دوتایی وجود دارد اگر و تنهـا اگـر یـک کـد$(n+1,M,2t+2)$ دوتایی وجود داشته باشد.

اثبات : فرض کنیم C یک کد $(n,M,2t+1)$ دوتایی باشد و $\hat{C}$ کد تعمیم یافته C باشـد که بـا اضافه نمودن یک بیت توازن کلی به C به دست آمده است. دراین صـورت، چـون وزن هـر کـد کلمـه در $\hat{C}$ زوج اسـت، بنـابراین $d(\hat{C})$ زوج اسـت و لـذا $d(\hat{C})>d(c)=۲t+۱$ پـس $d(\hat{C})=2t+2$. بـرعکس، فـرض کنیـد C یـک کـد دوتـایی $(n+۱,M,۲t+۲)$ باشــد

$d(c,d)=۲t+۲$ و C^* با پنچرنمودن C در یک مکان از مکان‌های متفاوت d,c به دست آمده باشد. بنابراین C^* دارای کمترین فاصله $۲t+۱$ است.

پاک کردن یک کد : Expunging acode

با حذف تعدادی از کد کلمات یک کد، پاک کردن یک کد رخ می‌دهد. (برخی از مولفین از کلمه پیراستن *expurgate* استفاده می‌کنند) . به طور مثال، فرض کنید L یک کد (n,m,d)- خطی دوتایی باشد. اگر L شامل حداقل یک کلمه با وزن فرد باشد، آنگاه دقیقاً نیمی از کد کلمات دارای وزن فرد هستند. (چرا؟)

حال با دور انداختن کد کلمات با وزن فرد یک کد $(n,\frac{m}{2},d')$ به دست می‌آید که در آن $d'\geq d$.

علاوه بر این، چون تمامی کد کلمات باقیمانده دارای وزن زوج هستند، کمترین فاصله کد پاک شده بایدزوج باشد و در این حالت اگر d فرد باشد آنگاه $d'>d$.

افزایش یک کد: Augmenting a code

عکس فرآیند پاک کردن یک کد، افزایش یک کد نامیده می‌شود که با اضافه نمودن تعداد کلمه اضافی به عناصر کد به دست می‌آید. یک روش متداول برای افزایش یک کد دوتایی C، اضافه نمودن مکمل هر کد کلمه به آن است. جایی که C^c(مکمل کد کلمهC) ، با تعویض ۰ و ۱ در C به دست می‌آید.

$$C=0100\Rightarrow C^C=1011$$

لم: اگر $x,y\in V(n,۲)$ آنگاه $d(x,y^c)=n-d(x,y)$.

اثبات: $d(x,y^c)$ = تعداد مکان‌هایی که x با y^c متفاوت است= تعداد مکان‌هایی که X با y یکسان است= $n-d(x,y)$.

قضیه: فرض کنید C یک کد دوتایی (n,m,d) باشد. در این صورت

$$d(C\cup C^c)=\min\{d,n-d_{\max}\}$$

که در آن $d_{\max}$ بیشترین فاصله بین کد کلمات در C است.

اثبات: داریم $d(C \cup C^c) = \min\{d(C), d(C^c), \min d(c,d)$ که $c \in C, d \in C^c\}$

اما $d(C) = d(C^c) = d$ و بنابراین لم قبل:

$$\min_{\substack{C \in C_c \\ d \in C}} d(c,d) = \min_{C,d \in C} d(c,d^c) = \min_{C,d \in C} (n - d(c,d)) =$$

$$n - \max_{c,d \in C}(d(c,d)) = n - d\max$$

اگر L کد خطی دوتایی باشد و $L\in 1...11=1$ آنگاه $L = L^C$ اما اگر $L \notin ۱$ آنگاه $L \cap L^C = \phi$. در واقع قضیع زیر را داریم:

قضیه: اگر L یک کد دوتایی خطی (n,m,d) باشد که شامل کد کلمه ۱۱...۱=۱ نباشد، آنگاه $L \cup L^C$ یک کد خطی دوتایی $(n,۲m.d')$ است که در آن:

$$d' = \min\{d, n - W_{\max}\}$$

جایی که $W_{\max}$ ، بیشترین وزن کد کلمات در L است.

کوتاه کردن یک کد *Shortening acode*

کوتاه کردن یک کد، فرآیند حفظ کد کلماتی است که در یک مکان مفروض دارای یک سمبل مشخص باشد (به طور مثال در مکان اول دارای سمبل صفر باشند) و سپس حذف آن موقعیت. اگر C یک (n,m,d)- کد باشد، آنگاه کوتاه شده آن کد دارای طول ***n-1*** و کمترین فاصله d خواهد بود. کوتاه کردن یک کد در مکان ***i***ام با در نظر گرفتن تمامی کد کلماتی که در آن مکان دارای مقدار S باشند به بخش متقاطع (*dross- section*) $X_i = S$ معروف است.

قضیه: اگر C یک کد خطی دودویی (n,m,d) باشد، آنگاه بخش متقاطع $x_i = o$ یک کد خطی دوتایی $(n-۱, \frac{۱}{۲}m, d)$ است.

ساختار جمع مستقیم (*Direct sum Constroction*)

اگر C_1 یک کد q- تایی (n_1,m_1,d_1) و C_2 یک کد q- تایی (n_2,m_2,d_2)باشند، آنگاه جمع مستقیم C_3، کد زیر است.

$$C_3=\{cd \mid c\in C_1, d\in C_2\}$$

به وضوح C_3 دارای پارامترهای زیر است:

$$n=n_1+n_2, M=M_1M_2, d=\min\{d_1,d_2\}$$

ساختار $(u,u+V)$

این ساختار، نسبت به ساختار جمع مستقیم، بسیار مفید تر است. اگر C_1 یک کد (n,m_1,d_1) و C_2 یک کد (n,m_2,d_2) باشد، که هر دو روی الفبای F_q تعریف شده‌اند. آنگاه کد $C_1\oplus C_2$ به صورت زیر ساخته می‌شود:

$$C_1\oplus C_2=\{c(c+d)\mid C+C_1, d\in C_2\}$$

به وضوح طول $C_1\oplus C_2$ ، $2n$ بوده و اندازه آن M_1M_2 است. حال نشان می‌دهیم $d(C_1\oplus C_2)\geq \min\{2d_1,d_2\}$. زیرا فرض کنید $u_2=c_2(c_2+d_2), u_1=c_1(c_1+d_1)$دو کد کلمهٔ متمایز در $C_1\oplus C_2$باشند آنگاه اگر $d_1=d_2$ داریم: $d(u_1,u_2)=2d(c_1,c_2)\geq 2d_1$

و از طرف دیگر، اگر $d_1\neq d_2$ آنگاه :

$$d(u_1,u_2)=w(u_1-u_2)=w(c_1-c_2)+w(c_1-c_2+d_1-d_2)\geq w(d_1-d_2)=d(d_1,d_2)\geq d_2$$
$$(w(a+b)\geq w(a)-w(b))$$

اما می توان مشاهده نمود که در تمامی حالات، تساوی رخ می‌دهد یعنی:

$$d(C_1\oplus C_2)=\min\{2d_1,d_2\}$$

مثال: فرض کنید $R(1,m)$ کد رید- مولد مرتبه اول باشد که کد دوتایی $(2^m,2^{m+1},2^{m-1})$ است. و فرض کنید $\operatorname{Re}p(2^m)$ کد تکرار دوتایی به طول 2^m باشد که یک کد $(2^m,2,2^m)$ است. در این حالت $R(1,m)\oplus \operatorname{Re}p(2^m)$ یک کد دوتایی $(2^{m+1},2^{m+2},2^m)$ است که دیده می‌شود همان کد $R(1,M+1)$ است.

گروه خودریختی یک کد

متناظر با هر کد روی F_q ، یک گروه مشخص وجود دارد که گروه خودریختی آن کد نامیده می‌شود. این گروه در مطالعه ساختار کد، مانند کد گشایی می-تواند مفید باشد.

تعریف: فرض کنید C یک (n,m)- کد روی F_q باشد. گروه خودریختی $Aot(C)$ از C، مجموعهٔ تمامی تبدیل های تک جمله ای M با درجه n است، به طوری که $M(C) \subseteq C$.

زمانی که $q=۲$، یک تبدیل تک جمله‌ای، چیزی جز یک جایگشت π روی مکان‌های مختصات کد نیست. یعنی $\pi C = C_{\pi(۱)} C_{\pi(۲)} .... C_{\pi(n)}$

بنابراین، در مورد کدهای دودویی، تعریف زیر را داریم.

تعریف: فرض کنید یک کد دو دویی (n,k) باشد گروه خودریختی ($automorphism$ C($group$ به صورت زیر است:

$$Aut(C) = \{\pi \in S_n \mid \pi c \in C, \forall c \in C\}$$

یادآوری می‌کنیم که اگر μ یک تبدیل تک جمله‌ای باشد، در این صورت کد $\mu(C) = \{\pi c \mid c \in C\}$ با استفاده از تعریف، معادل ضرب اسکالر بر روی کد C است.

قضیه: مجموعه $Aut(C)$ یک گروه است. در مورد کد دوتایی C، گروه $Aut(C)$ ی زیر گروه از گروه متقارن S_n است.

مثال: گروه خودریختی کد $C = \{۰۰۰۰, ۱۱۰۰, ۰۰۱۱, ۱۱۱۱\}$ ، زیر گروهی از $S_۴$ با اندازه 8 به صورت زیر است.

$$Aut(C) = \{id, (۱۲), (۳۴), (۱۲)(۳۴), (۱۳)(۲۴), (۱۴)(۲۳), (۱۳۲۴), (۱۴۲۳)\}$$

مسأله اساسی کد گذاری

یک کد (n,m,d) خوب می‌بایست از یک طرف داریا اندازه بزرگ (M بزرگ) باشد تا بتواند تعداد بیشتری از پیام‌های منبع را کد نماید و از طرف دیگر باید دارای کمترین فاصله (d) بزرگ باشد تا بتواند خطاهای بیشتری را تصحیح کند. در اینجا تعریف می کنیم.

$Aq(n,d)$:= بزرگترین اندازه M ممکن به طوری که یک کد (n,m,d) q- تایی موجود باشد. اعداد $Aq(n,d)$ در کدگذاری یک نقش اساسی ایفا می‌نند و تلاش‌های زیادی به منظور تعیین مقادیر آنها صورت گرفته است. در واقع مسأله تعیین $Aq(n,d)$ به مسأله اساسی کد گذاری تعبیر شده است بیشتر نتایج در این قسمت به تعیین $Aq(n,d)$ برای مقادیر کوچک n,q و d یا تعیین کران‌های بالایی روی $Aq(n,d)$ پرداخته شده است. کارهای قابل ملاحظه‌ای به منظور تعیین رفتار مجانبی $Aq(n,d)$ به عنوان تابعی از $\delta=\frac{d}{n}$ ، زمانی که $n\to\infty$، صورت گرفته است. یک (n,m,d) کد که در آن $M=Aq(n,d)$، کد بهینه (*Oplimal*) نامیده می‌شود.

قضیه: بار هر $n\geq ۱$ داریم.

۱) $Aq(n,1)=q^n$ ۲) $A_q(n,n)=q$

قضیه: برای هر $n\geq ۲$ داریم: $A_q(n,d)\leq q\ A_q(n-۱,d)$

قضیه: در مورد کدهای دوتایی $(q=۲)$ داریم: $A_2(n,2t+1)=A_2(n+1,2t+2)$

این قضیه را به این صورت نیز می‌توان بیان کرد که اگر d زوج باشد آنگاه

$$A_۲(n,d)=A_۲(n-۱,d-۱)$$

بنابراین، در مورد کدهای دوتایی، کافی است تا $A_۲(n,d)$ را برای تمامی مقادیر فرد d (یا برای تمام مقادیر زوج) تعیین کنیم.

قضیه: کران پائینی روی $Aq(n,d)$ کران گیلبرت- ورشامو $Gilbert-vershamov$

$$A_q(n,d)\geq\frac{q^n}{\sum_{k=\circ}^{d-1}\binom{n}{k}(q-1)^k}$$

قضیه: زمانی که q توانی از یک عدد اول باشد، آنگاه یک کد $[n,k]$ خطی q- تایی با کمترین فاصله d وجود دارد به شرط آن که:

$$q^k \prec \frac{q^n}{\sum_{i=0}^{d-2}\binom{n-1}{i}(q-1)^i}$$

بنابراین، اگر K بزرگترین عدد صحیح باشد که در شرط فوق صدق می‌کند. آنگاه $A_q(n,d) \geq k$.

کران بالایی روی $A_q(n,d)$

قضیه: کران سینگتون $A_q(n,d) \leq q^{n-d+1}$.

توجه: کران سینگلتون، کران خیلی خوبی نیست. اما حالت‌هایی وجود دارد که تساوی در کران سینگلتون رخ می‌دهد.

قضیه: (کران بسته کروی یا کران همینگ)

$$A_q(n,d) \leq \frac{q^n}{\sum_{k=0}^{t}\binom{n}{k}(q-1)^k}, t=[\frac{d-1}{2}]$$

توجه دارید که کدی که تساوی در کران بسته کروی برقرار باشد، کد کامل است.

قضیه: کران پلاتکین، فرض کنید $\theta = \frac{q-1}{q}$ اگر $d > \theta n$، آنگاه:

$$A_q(n,d) \leq \frac{d}{d-\theta n}$$

توجه دارید که کران پلاتکین زمانی که d نسبتاً بزرگ باشد، برقرار است.

قضیه: برای هر $n \geq 2$، داریم $A_q(n,d) \leq q\ A_q(n-1,d)$

اثبات: فرض کنید C یک کد (n,m,d) q- تایی بهینه باشد. بنابراین $m = A_q(n,d)$ اما یک i وجود دارد به طوری که تعداد کد کلماتی از C که در آن $x_1 = i$، حداقل برابر $\frac{M}{q}$ است (چرا؟)، بنابراین اگر این کد کلمات را در نظر گرفته و مکان $X_1 = i$ را از آنها حذف کنیم آنگاه داریم:

$$A_q(n-1,d) \geq \frac{M}{q} = \frac{A_q(n,d)}{q}$$

مقادیر کوچک $A_q(n,d)$ اگر $q=۲$، $A_۲(n,d)$:

جدول مقابل توسط هیل ($Hill$) سال ۱۹۸۶ معرفی شد که تعمیمی از کاری است که اسلون ($Sloon$) (سال ۱۹۸۲) ارائه نمود.

بسیاری از کران های پایینی در این جدول، با استفاده از کدهایی که قبلاً معرفی کردیم، مانند کدهای همینگ، کد تکرار به همراه کوتاه کردن این کد ها به دست آمده‌اند.

n	d=۳	d=۵	d=۷
۵	۴	۲	–
۶	۸	۲	––
۷	۱۶	۲	۲
۸	۲۰	۴	۲
۹	۴۰	۶	۲
۱۰	۷۲–۷۹	۱۲	۲
۱۱	۱۴۴–۱۵۸	۲۶	۴
۱۲	۲۵۶	۳۲	۴
۱۳	۵۱۲	۶۴	۸
۱۴	۱۰۲۴	۱۲۸	۱۶
۱۵	۲۰۴۸	۲۵۶	۳۲
۱۶	۱۵۶۰–۳۲۷۶	–۳۴۰ ۲۵۶	۳۶–۳۷

قضیه: (کران سینگلتون) $A_q(n,d)\le q^{n-d+1}$

اثبات: فرض کنید C یک (n,m,d)- کد q- تایی باشد اگر $d-1$ مکان آخر را از تمامی کد کلمات C حذف کنیم، آنگاه M کلمه حاصل متمایز هستند (چرا؟)، اما در این حالت طول تمامی کلمات $n-d+1$ است، پس $M\le q^{n-d+1}$.

گرچه کران سینگلتون، کران خوبی نیست، اما در مثال زیر، تساوی برقرار است.

مثال:

$$C=\{000,10a,boa,ba1,01a,abo,1ob,111,oab,b10,1ba,aaa,ob1,a01,a1b,bbb\}$$

یک کد (۲و۱۶و۳) روی $F_4=\{0,1,a,b\}$ است، بنابراین $A_4(3,2)\ge 16$

اما کران سینگلتون داریم ************* $A_4(3,2)\le 4$، سپس $A_4(3,2)=16$.

نتیجه: اگر C یک $[n,k,d]$ که باشد، آنگاه با توجه به کران سینگلتون داریم:

$$q^k\le A_q(n,d)\le q^{n-d+1}\Rightarrow k\le n-d+1 \text{ یا } d\le n-k+1$$

تعریف: در یک کد خطی $d=n-k+1$ یک کد با بیشترین فاصله قابل تفکیک (*maximum distance separable code*) یا *MDS* نامیده می‌شود. به عبارت دیگر d دارای بیشترین مقدار ممکن است. (بنابراین یک کد *MDS*، یک کد($n,n-d+1,d$) یا به طور هم ارز($n,k,n-k+1$) است.

نکته: در یک کد *MDS*، اگر هر مجموعه $n-k=d-1$ از مکان‌های مختصات کد را حذف کنیم. q^k رشته مجزا به طول k را داریم که همان $V(k,q)$ است. بنابراین C روی هر k مکان، سیستماتیک است.

ترکیب یا *interleaving*

فرض کنید $C_2=<c_{21},c_{22},...,c_{2M_2}>, C_1=<c_{11},c_{12},...,c_{1M1}>$ دو کد به ترتیب $(n_2,m_2,d_2),(n_1,m_1,d_1)$ باشند. در این صورت می‌توان کد کلمات C_1,C_2 را ترکیب (*Interleave*) نمود و کد جدید $C_1\Theta C_2$ را به دست آورد که در آن:

$$C_1 \Theta C_2 = \begin{cases} \{C_{11}C_{21}, C_{12}C_{22}, ..., C_{1m_1}C_{2m_1}\} M_1 \le M_2 \\ \{C_{11}C_{21}, ..., C_{1m_2 C_{2m_2}}\} M_1 \succ M_2 \end{cases}$$

مـی‌تـوان نشـان داد کـه $C_۱\Theta C_۲$ ، یـک $(n_1+n_2, \min\{M_1, M_2\}, d)$ کـد اسـت کـه در آن $d \ge d_۱ + d_۲$. اگر تعریف کنیم:

$$uC = \{uc \mid c \in C\}$$
$$(u \in Z - \{\circ\})$$

آنگاه قضیه زیر را داریم:

قضیه: فـرض کنیـد $C_۲, C_۱$ بـه ترتیـب $(n_۱, M_۱, d_۱)$ و $(m_۲, m_۲, d_۲)$ کـه مرتـب باشـند آنگـاه $uC_1\Theta \sim vC_2$ دارای پارامترهای زیر است:

$$(un_1 + vn_2, \min\{M_1, M_2\}, d)$$

جایی که : $D \ge ud_1 + vd_2$

کدهای هادمارد

در اینجا، دسته ای از کدها به نام کدهای هادامارد را تعریف و مورد بررسـی قـرار مـی‌دهـیم که در کران پلاتکین رابطه تساوی در مورد آنها صدق می کند.

تعریف: یک ماتریس هادمارد H_n از مرتبه n یک ماتریس و $n \times n$ با درایه‌های ± ۱ است که در شرط $H_n H_n^t = nI_n$ صدق کند. اگر در سطر اول و ستون اور H_n، تمامی عناصـر ۱ باشـد، آنگاه H_n را نرمال می گوئیم.

برای مثال، ماتریس هادامارد زیر نرمال است:

$$H_۴ = \begin{bmatrix} ۱ & ۱ & ۱ & ۱ \\ ۱ & -۱ & ۱ & -۱ \\ ۱ & ۱ & -۱ & -۱ \\ ۱ & -۱ & -۱ & ۱ \end{bmatrix}$$

ثابت شده است که شرط لازم برای وجود یک ماتریس هادامارد H_n ایـن اسـت کـه $n = ۱,۲$ یا $4|n$، اما مشخص نیست که آیا شرط کافی نیز می‌باشد. بـه سـادگی مـی‌تـوان ایـده وجـود ماتریس هادامـارد H_n ، مـاتریس هادامـارد نرمـال شـده بـا همـان انـدازه را نتیجـه مـی‌دهـد.

یادآوری می‌کنیم که $C^c=\{C^c \mid c\in C\}$ که در آن C^c با تعویض نقش صفر و یک در کد کلمه دوتایی C به دست می‌آید.

قضیه: فرض کنید H_n یک ماترس هادامارد نرمال باشد، با تعویض تمامی ۱ ها با صفر و تمامی ۱- ها با ۱ در ماتریس H_n، ماتریس A_n را داریم که ماتریس هادامارد دوتایی نامیده می‌شود. حال با توجه به A_n، می‌توانیم کد های هادامارد زیر را بسازیم.

۱) سطرهای A_n (با حذف ستون اول) یک $(n-۱,n,\frac{۱}{۲}n)$ کد تشکیل می‌دهند که $Had۱_n$ نامیده می‌شود .

۲) با کوتاه کردن کد هادامارد $Had۱_n$ در مکان اول $(x_۱=o)$ کد هادامارد کوتاه شده $S\ Had۱_n$ به دست می‌آید که یک $(n-۲,\frac{۱}{۲}n,\frac{۱}{۲}n)$ کد است.

۳) مجموعه $Had1_n\cup(Had\ 1_n)^c$ یک کد $(n-۱,۲n,\frac{۱}{۲}n-۱)$ است که با $Had۲_n$ نمایش داده می‌شود.

۴) سطرهای A_n به همراه مکمل‌های این سطرها یک کد $(n,۲n,\frac{۱}{۲}n)$ تشکیل می‌دهند که با $Had۳_n$ نمایش داده می‌شود.

اثبات: ۱) چون سطرهای A_n متعامدند، تعداد مکان‌هایی که در آن هر دو سطر برابرند، با تعداد مکان های که در آن، این سطرها متمایزند، برابر است. بنابراین فاصله بین هر دو سطح متمایز A_n برابر با $\frac{۱}{۲}n$است.

۲) این مطلب، نتیجه‌ای از این واقعیت است که تمامی ستون‌های H_n، بجز ستون اول دارای تعداد برابر ۱ و ۱- هستند.

۳) این مطلب با توجه به قضیه‌ای که ثابت نمودیم.

$$d(C\cup C^c)=\min\{d,n-d\max\}$$

بدیهی است زیرا:

$$d=\min\{\frac{1}{2}n,(n-1)-\frac{1}{2}n\}=\frac{1}{2}n-1$$

۴) مشابه با۳ داریم: $d(C)=\min\{\frac{1}{2}n, n-\frac{1}{2}n\}=\frac{1}{2}n$

کدهای خطی و دوگان آن‌ها

در این فصل، جزئیات بیشتری از مهمترین کلاس از کدها، یعنی کدهای خطی می‌پردایم:

تعریف: یک کد $L\subseteq V(n,q)$ خطی است، اگر L زیر فضای $V(n,q)$ باشد. در این حالت اگر بعد L برابر با K باشد، آنگاه L را یک $[n,k]$ - کد نامیده و اگر $d=d(L)$ کمترین فاصله L باشد، آنگاه L را یک $[n,k,d]$- کد می‌نامیم.

قضیه: اگر L یک کد خطی باشد آنگاه $d(L)=w(L)$.

ماتریس مولد یک کد خطی

از آنجایی که یک کد خطی، یک زیر فضای برداری است، توسط یک پایه تعریف می-شود.

تعریف: فرض کنید L یک $[n,k]$- کد باشد. ماتریس $G, k\times n$ که سطرهای آن تشکیل یک پایه برای L می‌دهند، یک ماتریس مودل برای L نامیده می‌شود. دراین حالت، کد کلمات موجود در L، دقیقا ترکیبات خطی سطرهای G هستند. به عبارت دیگر:

$$L=\{xG \mid x\in V(K,q)\}$$

این رابطه روش ساده تری برای کد گذاری معرفی می‌کند. به عبارت دیگر، اگر اعضای یک منبع (*Source*) را بتوان مجموعه تمامی کلمات q- تایی به طول k در نظر گرفت، آنگاه می‌توانیم کلمه منبع $x\in V(k,q)$ را به کد کلمه xG کد نمائیم.

مثال: کد دودویی با ماتریس مولد زیر را در نظر بگیرید:

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

این کد، می‌تواند به منظور کدگذاری سمبل‌های منبع $V(۳,۲)$ به کار رود. به عبارت دیگر اگر $x=(x_1,x_2,x_3)\in v(3,2)$ آنگاه کدکلمه متناظر با آن به صورت زیر است.

$$[x_1 \ \ x_2 \ \ x_3] \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} = (x_1 + x_3, x_1 + x_2, x_2 + x_3,, x_2)$$

نکته: از آنجایی که اعمال سطری روی ماتریس G (جابجایی سطرها ضرب یک سطر در یک اسکالر ناصفر اضافه نمودن مضرب اسکالری از یک سطر به سطر دیگر)، فضای تولید شده توسط سطرها راتغییر نمی‌دهد، لذا ماتریسی که با استفاده از اعمال سطری روی ماتریس مولد به دست آمده باشد، نیز یک ماتریس مولد برای کد است.

حال با استفاده از این مطلب، قضیه زیر را داریم:

قضیه: فرض کنید L یک $[n,k]-$ کد خطی باشد. به ازای هر k مکان دلخواه یک کد هم ارز با کد L وجود دارد که در این مکان‌ها، سیستماتیک است.

شکل استاندارد: ماتریس مولد به شکل $G=(I_k \mid A)$ ، که در آن I_k ماتریس همانی از مرتبه k است، شکل استاندارد نامیده می‌شود.

نکته: یک کد خطی روی k مکان اول سیستماتیک است اگر و تنها اگر ماتریس مولد آن به شکل استاندارد باشد.

مثال: بعدا مشاهده می‌کنیم که ماتریس زیر یک ماتریس مولد برای کد همینگ $H_2(3)$ است.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

توجه دارید که G در این حالت، به شکل استاندارد است. پس کد همینگ $H_2(3)$ می‌تواند کلمات منبع از $V(4,2)$را به صورت زیر کد کند:

$$xG = (x_1, x_2, x_3, x_4)G = (x_1, x_2, x_3, x_4, x_2 + x_3 + x_4, x_1 + x_3 + x_4, x_1 + x_2 + x_4)$$

چون G دارای شکل استاندارد است، پیام منبع اصلی درk مکان اول کد کلمات ظاهر می‌-شود.

قضیه: دو کد خطی $L_۲,L_۱$ ، با ماتریس های مولد $G_۲,G_۱$، هم ارز هستند اگر و تنها اگر با اعمال سطری و ضرب یک ستون در یک اسکالر ناصفر، بتوان از $G_2 \sim G_1$رسید.

دوگان یک کد خطی

فضای برداری $V(n,q)$ دارای یک ضرب داخلی طبیعی است، به خصوص، اگر $x = x_1....x_n$, $y = y_1....y_n$ در $V(n,q)$ باشند، آنگاه ضرب داخلی y,x با می‌توان به صورت زیر تعریف کرد:

$$\underset{or<x,y>}{x,y} = x_1 y_1 + ... + x_n y_n$$

مفهوم زیر، یک نقش کلیدی در کدهای خطی دارد.

تعریف: فرض کنید L یک $[n,k]$- کد باشد. مجموعه:

$$L^{\perp} = \{x \in V(n,q) | x.c = 0 \quad \forall c \in C\}$$

کد دوگان L نامیده می‌شود.

قضیه ۱) اگر G ماتریس مولد L باشد آنگاه:

$$L^{\perp} = \{x \in V(n,q) \mid xG^t = \circ\}$$

۲) اگر L یک کد $[n,k]$- خطی باشد آنگاه $L^{\perp}$ یک $[n,n\text{-}k]$- کد خطی است.

۳) برای هر کد خطی L داریم، $(L^{\perp})^{\perp} = L$:

اثبات: ۱) این مطلب، از این واقعیت نتیجه می‌شود که x به هر کد کلمه در L عمود است اگر و تنها اگر x بر هر یک از عناصر پایه در L عمود باشد.

۲) از قسمت (۱) نتیجه می‌شود که بیان می‌کند $L^{\perp}$ فضای جواب یک دستگاه با k معادله و n متغیر است که دارای رتبه k می‌باشد.

۳) $L \subseteq L^{\perp\perp}$ و $\dim L = \dim L^{\perp\perp}$، پس حکم واضح است.

توجه: خواص فضای دوگان یک کد روی یک میدان متناهی، می‌توان از خواص فضای دوگان یک فضای بردرای روی اعداد حقیقی کاملاً متمایز باشد. به طور مثال، اگر W یک

زیرفضا از یک فضای برداری حقیقی متناهی البعد V باشد، آنگاه $W \cap W^{\perp} = \{0\}$ ، زیرا هیچ برداری بر خودش عمود نیست.

اما این مطلب، هموره در مورد کدهای خطی درست نیست. در واقع، همان طور که مثال بعد نشان می‌دهد، حتی می‌توانیم داشته باشیم $L^{\perp} = L$.

مثال: برای کد دوتایی [۲و۴]، $L = \{0000, 1100, 0011, 1111\}$ داریم $L \subseteq L^{\perp}$. و از آنجایی که $L^{\perp}$ نیز یک [۲و۴]- کد دوتایی است، داریم $L = L^{\perp}$.

تعریف: کد خطی L، به طوری که $L = L^{\perp}$، خوددوگان ($self$ - $dual$) نامیده می‌شود.

نکته: با وجود این که $L \cap L^{\perp}$ لزوماً کد صفر نیست داریم:

(با توجه به قضیه قبل) $\dim(L) + \dim(L^{\perp}) = n$

فرض کنید L یک کد خطی با ماتریس مولد $k \times n$ $G = (I_k \mid A)$ (به شکل استاندارد) باشد.

همچنین فرض کنید $H = (-A^t \mid I_{n-k})$ ، در این صورت:

$$GH^t = (I_k \mid A)\begin{pmatrix} -A \\ I_{n-k} \end{pmatrix} = -A + A = 0$$

بنابراین، سطرهای H بر سطرهای G عمود هستند و از آنجایی که $rank(H) = n - k = \dim(L^{\perp})$ می‌توان نتیجه گرفت H ماتریس مولدی برای کددوگان $L^{\perp}$ است.

ماتریس H، همچنین ماتریس بررسی توازن کد L نامیده می‌شود. دلیل این نامگذاری این است که : $x \in L \Leftrightarrow xH^t = 0$

اما اگر $x = (x_1, \dots, x_n)$, $H = (h_{ij})$, $xH^t = 0$ معادل با معادلات زیر است.

$$\text{معادلات بررسی توازن}\begin{cases} h_{11}x_1 + h_{12}x_2 + \dots + h_{1n}x_n = 0 \\ h_{21}x_1 + h_{22}x_2 + \dots + h_{2n}x_n = 0 \\ \dots\dots \quad \dots\dots\dots \quad \dots\dots \\ h_{n-k,1}x_1 \mid + h_{n-k,2}x_2 + \dots + h_{n-k,n}x_n = 0 \end{cases}$$

بنابراین، سطرهای H ضرایب دستگاه معادلات فوق است که در آن جواب‌ها همان کد کلمات موجود در L هستند. این معادلات خطی، همچنین، معادلات بررسی توازن نامیده می‌شوند. ماتریس بررسی به شکل $(B|I_m)$، فرم استاندارد نامیده می‌شود.

مثال: در مثال قبل، ماتریس زیر یک ماتریس مولد استاندارد برای کد $H_۲(۳)$ معرفی شد.

$$G=(I_۴\mid A) \quad , \quad A=\begin{pmatrix} ۰ & ۱ & ۱ \\ ۱ & ۰ & ۰ \\ ۱ & ۱ & ۱ \\ ۱ & ۱ & ۱ \end{pmatrix}$$

در این حالت، شکل استاندارد ماتریس بررسی توازن کد به صورت زیر است:

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

معادلات بررسی توازن
$$\begin{cases} x_۲+x_۳+x_۴+x_۵=۰ \\ x_۱+x_۳+x_۴+x_۶=۰ \\ x_۱+x_۲+x_۴+x_۷=۰ \end{cases}$$

در این حالت، معادلات بررسی توازن به صورت زیر هستند:

$$\begin{cases} x_۲+x_۳+x_۴+x_۵=۰ \\ x_۱+x_۳+x_۴+x_۶=۰ \\ x_۱+x_۲+x_۴+x_۷=۰ \end{cases}$$

روش کارایی برای تعیین کمترین فاصله که از روی ماتریس مولد (به طور مستقیم) وجود ندارد. اما می‌توان از روی ماتریس بررسی توازن H از کد L، این کار ار انجام داد. به خصوص، فرض کنید ستون‌های H $k_1, k_2, \dots, k_n$ باشد و انتخاب خاصی از w ستون H وابستهٔ خطی باشند. در این حالت ضرایب $C_۱,\dots,C_n$ وجود دارند که دقیقاً W تا از آنها ناصفر بوده و داریم:

$$c_1k_1+\dots+c_nk_n=۰$$

این معادل با $CH^t=۰$ است، جایی که $C=c_1..c_n$ و لذا $C\in L$. علاوه بر این چون C یک کد کلمه با وزن W است، داریم: $d(L)=W(L)\le W$

از طرف دیگر، اگر C یک کد کلمه با وزن W باشد، آنگاه داریم $CH^t=۰$ و لذا W ستون H وابسته خطی هستند. این مطلب، قضیه بسیار مفید زیر را ثابت می‌کند.

قضیه: فرض کنید L یک $[n,k,d]$- کد با ماتریس بررسی توازن H باشد. در اینصورت d کوچکترین عدد صحیح r است که در آن r ستون وابسته خطی در H وجود دارند.

(بنابراین، H دارای d ستون وابسته خطی است و هر d-1 ستون H- مستقل خطی هستند).

کدگشایی سیندروم

با استفاده از ماتریس بررسی توازن یک کد خطی، می‌توان یک الگوریتم کد گشایی کارا برای آن طراحی می‌نمود.

تعریف: فرض کنید L یک $[n,k]$- کد با ماتریس بررسی توازن H باشد. برای هر $x \in V(n,q)$ کلمه xH^t، سیندروم X نامیده می‌شود.

نتیجه: $x \in L \Leftrightarrow$، سیندروم X برابر با صفر باشد.

حال می‌خواهیم درباره فضاهای خارج قسمتی (*quotient spaces*) مطالبی را یادآوری کنیم.

اگر $L \subseteq V(n,q)$ یک کد خطی (یا زیر فضای ناتهی) باشد، آنگاه فضای خارج قسمتی $V(n,q)$ درپیمانه L به صورت زیر تعریف می‌شود:

$$\frac{V(n,q)}{L} = \{x + L \mid x \in V(n,q)\}$$

مجموعه $x + L = \{x + c \mid C \in L\}$ هم دسته $L(coset)$ نامیده می‌شود.

با استفاده از جمع بردرای و ضرب اسکالر زیر را می‌توان دیده فضای خارج قسمتی روی F_q خود یک فضای برداری است.

$$a(x+L) = ax + L, \quad (x+L)+(y+L) = (x+y)+L$$

یادآوری می‌کنیم که $x + L = y + L$ اگر و تنها اگر $x - y \in L$.

با توجه به مطالب فوق، قضیه زیر را داریم:

قضیه: فرض کنید L یک $[n,k]$- کد با ماتریس بررسی توان H باشد. در این صورت y,x در $V(n,q)$ دارای سیندروم یکسانی هستند اگر و تنها اگر y,x در هم دسته یکسانی از فضای $V(n,q)/L$ قرار بگیرند.

اثبات:

$$xH^t = yH^t \Leftrightarrow (x-y)H^t = \circ \Leftrightarrow x-y \in L \Leftrightarrow x+L = y+L$$

کدگشایی سیندروم

حال فرض کنید کد کلمه x ارسال و کلمه c دریافت شده باشد. قاعده کمترین فاصله ایجاب می‌کند که x را به کد کلمه c که در آن $e=x-c$ دارای کمترین وزن باشد کدگشایی کنیم. اما چون $c \in L$ پس e در هم دسته $x+L$ است. بنابراین، قاعده کمترین فاصله ایجاب می‌کند که x را به کد کلمه $c = x- e$ کدگشایی کنیم که $e \in x+L$ دارای کمترین وزن باشد، یعنی به کلمه با کمترین وزن در میان تمامی کلماتی که با x دارای سیندروم یکسان هستند.

آرایه استاندارد: فرض کنید $L=\{0,C_1,...,C_m\}$ ، در این صورت جدول زیر یک آرایه استاندارد برای L است:

$$\begin{array}{ccccc}
\circ & c_1 & c_2 & \dots & c_m \\
e_1 & c_1+e_1 & c_2+e_1 & \dots & c_m+e_1 \\
e_2 & c_1+e_2 & c_2+e_2 & \dots & c_m+e_2 \\
 & & & \vdots & \\
e_s & c_1+e_s & c_2+e_s & \dots & c_m+e_s
\end{array}$$

در حقیقت، اولین سطر این آرایه، عناصر کد است. برای تشکیل دومین سطر، کلمه e_1 با کمترین وزن را طوری انتخاب می‌کنیم به طوری که e_1 در سطر اول نیامده باشد و این کار را به همین منوال ادامه می‌دهیم تا جایی که دیگر چنین کلمه‌ای یافت نشود. حال از جمع e_i ها با عناصر C، سطرهای L را می‌سازیم. سطرهای آرایه استاندارد، طبق مطالب بیان شده با هم اشتراکی نداشته و تمام فضای $V(n,q)$ را تولید می‌کنند.

در این حالت اگر کلمه x دریافت شده باشد، $x = e_i + C_i$ (برای برخی $\circ \le j \le m, 1 \le i \le s$)، آنگاه X را به c_j (سرستون x) کدگشایی می‌کنیم. در این حالت e_i دارای سیندروم یکسان با X بوده و در ابتدای سطری خواهد بود که X قرار دارد.

مثال: فرض کنید L کد [۲و۴] دوتایی با ماتریس مولد زیر باشد.

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

هم دسته‌های مجزای L به صورت زیر هستند.

$$\circ + C = \{0000, 0100, 1101, 1001\}$$
$$1000 + C = \{1000, 1100, 0101, 0001\}$$
$$0010 + C = \{0010, 0110, 1111, 1011\}$$
$$1010 + C = \{1010, 1110, 0111, 0011\}$$

چون، سردسته ها دارای کمترین وزن در هم دستهٔ خود هستند، آرایه استاندارد به صورت زیر است.

۰۰۰۰	۰۱۰۰	۱۱۰۱	۱۰۰۱
۱۰۰۰	۱۱۰۰	۰۱۰۱	۰۰۰۱
۰۰۱۰	۰۱۱۰	۱۱۱۱	۱۰۱۱
۱۰۱۰	۱۱۱۰	۰۱۱۱	۰۰۱۱

بااضافه نمودن سطر دوم G به سطر اول، ماتریس مولد در شکل استاندارد را داریم:

$$G' = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \to H = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

ماتریس بررسی توازن

در این حالت جدول سردسته ها با مقادیر سیندروم آنها به صورت زیر است.

سر دسته e_i	مقدار سیندروم $s_i = s(e_i) \leftarrow$
۰۰۰۰	۰۰
۱۰۰۰	۰۱
۰۰۱۰	۱۰
۱۰۱۰	۱۱

حال برای کدگشایی کلمه دریافتی $x=$۱۱۱۰، کافی است سیندروم آن را حساب کنیم.

$s(x)=۱۱۱۰\times H^t=۱۱=S(۱۰۱۰)$

پس کدگشایی به صورت $C=x-e=۱۱۱۰-۱۰۱۰=۰۱۰۰$ خواهد بود.

توجه: در کد گشایی سیندروم، خطا به درستی تصحیح می‌گردد اگر و تنها اگر آن خطا متعلق به یکی از سردسته ها باشد.

اثبات: فرض کنید کد کلمه C ارسال و کلمه $x=c+e$ دریافت شده باشد؛ که در آن e بردار خطاست اگر e یکی از سردسته ها باشد، آنگاه کد گشایی سیندروم، آن را به $(c+e)-e=c$ کدگشایی می‌کند که درست است در غیر این صورت، اگر e از سردسته ها نباشد و سردسته $e_i\neq e,\ x$ باشد، آنگاه کد گشایی سیندروم، x را به $(c+e)-e_j(\neq c)$ کد گشایی می‌کند که در نتیجه کدگشایی اشتباه کرده است.

نکته: اگر L دارای کمترین فاصله d باشد، آنگاه تمامی کلمات موجود در $V(n,q)$ با وزن حداکثر $t=[\frac{d-۱}{۲}]$ متعلق به یکی از سردسته ها هستند. زیرا اگر y,x دو کلمه با وزن حداکثر t باشند و در یک سردسته واقع باشند، آنگاه $x-y$ یک کد کلمه با وزن حداکثر $۲t$ $(2t\leq d-1)$ است که تناقض است.

نکته: کد L کامل است اگر و تنها اگر تمامی سردسته‌ها، کلمات باوزن حداکثر $t=[\frac{d-۱}{۲}]$ باشند.

احتمال کدگشایی صحیح

فرض کنید L یک کد خطی باشد و α_i تعداد سردسته های با وزن $۰\leq i\leq n,i$، در جدول استاندارد باشند. در این صورت زمانی احتمال کد گشایی صحیح برابر با احتمال آن است که خطاها، یکی از این سردسته ها باشند، بنابراین:

$$P_{corr\ decode}\text{کدگشایی صحیح}=\sum_{i=۰}^{n}\alpha_i P^i(1-p)^{n-i}$$

احتمال تشخیص خطا

فرض کنید کد کلمه c ارسال و کلمهٔ d دریافت شده باشد، کدگشا، در صورتی متوجه وجود خطا نمی‌شود که d یک کد کلمه متمایز با c باشد، بنابراین:

$$0 \neq c-d \in C$$

$$P_{\text{عدم تشخیص خطا}} = \sum_{k=1}^{n} A_k p^k (1-p)^{n-k} \qquad (= p(0 \neq c \in C))$$

که در آن A_k تعداد کد کلمات با وزن $1 \leq K \leq n, k$ می‌باشد.

کدگشایی با منطقه اکثریت (*Mojority Logic decoding*)

برای تشریح این قاعده کد گشایی، آن را با یک مثال تبیین می‌کنیم.

فرض کنید $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$ ماتریس مولد کد همینگ $H_2(3)$ باشد. G همچنین ماتریس بررسی توازن کد دوگان همینگ $H_2(3)$ نیز هست که آن را به C نمایش می‌دهیم.

در این حالت، با انجام اعمال سطری روی G، ماتریس حاصل باز ماتریس بررسی توازن C باقی می‌ماند.

$$G \xrightarrow[2 \leq i \leq 4]{r_1 + r_i \to r_i} G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$ اضافه نمودن سطر اول به مابقی سطر ها

$$\xrightarrow{r_1 + r_2 + r_3 \to r_3} G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$ اضافه نمودن سطر اول و دوم به سطر سوم

معادلات بررسی توازن متناظر به سطرهای ۴،۳ و ۱ به ترتیب به صورت زیر می‌باشد:

$$\begin{aligned} x_1 + x_2 + x_3 \qquad\qquad &= 0 \\ x_1 \qquad + x_4 + x_5 \qquad &= 0 \\ x_1 \qquad\qquad + x_6 + x_7 &= 0 \end{aligned}$$

در این معادلات توجه دارید که ضریب $x_۱$ در تمامی معادلات برابر با ۱ و ضریب سایر متغیرها، تنها در یکی از معادلات برابر با ۱است.

با توجه به این مثال، تعریف زیر را داریم:

تعریف: یک دستگاه از معادلات بررسی توازن یک کد خطی، نسبت به متغیر x_i متعامد نامیده می‌شود هرگاه x_i در هریک از معادلات این دستگاه دارای ضریب ۱ و هر متغیر دیگر، تنها در یکی از معادلات دارای مضرب ۱ باشد. به طور نمونه، معادلات بالا نسبت به $x_۱$ متعامد هستند. حال فرض کنید در اولین مکان یک خطا رخ داده باشد، آنگاه تمامی معادلات (*) نادرست خواهند بود. بنابراین (با فرض وجود یک خطا) تعداد معادلات نادرست (*) نشان می دهد که خطا در مکان اول رخ داده یا در مکانی بجز اول، همچنین اگر دقیقاً ۲ معادله از معادلات فوق نادرست باشند، نتیجه می‌گیریم که حداقل ۲ خطا رخ داده است. به این قاعده، کدگشایی با منطق اکثریت (*Mojority logic decoding*) می‌گویند.

به عنوان تمرین، می‌توان نشان داد که با انتخاب حریصانه اعمال سطری، می‌توان کدگشایی با منطق اکثریت را روی تمامی ۷ مکان C مشاهده کرد.

در حالت کلی، فرض کنید در یک کد خطی $[n,k]$، L . r معادله بررسی توازن داریم. فرض کنید این معادلات نسبت به متغیر x_i متعامد باشند. در این حالت فرض کنید $t \leq \frac{r}{۲}$ خطا در انتقال رخ داده باشد.

اگر یکی از این خطاها در مکان i ام رخ داده باشد، آنگاه حداکثر t-1 معادله برقرار هستند و لذا حداقل $r-(t-۱) \geq \frac{r}{۲}+۱$ معادله، برقرار نیستند. از طرف دیگر، اگر در i امین مکان، خطا رخ نداده باشد، آنگاه حداکثر $t \leq \frac{r}{۲}$ معادله، برقرار نیستند. بنابراین i امین مکان از کلمهٔ دریافتی دچار خطا شده است اگر و تنها اگر اکثر معادلات برقرار نباشند.

کدهای خود دوگان

یک کد خطی مانند L، خود متعامد (*self-orthogonal*) نامیده می‌شود اگر $L \subseteq L^{\perp}$. قضیه زیر را داریم (اثبات به عنوان تمرین)

قضیه: فرض کنید G ماتریس مولد یک کد خطی q- تایی مانند L باشد. در این صورت L خودمتعامد است اگر و تنها اگر سطرهای G بریکدیگر عمود بوده و دارای وزن بخش پذیربر q باشند.

قضیه: اگر سطرهای متمایز ماتریس مولد یک کد خطی دوتایی مانند L بوده و دارای وزن بخش پذیر بر ۴ باشند، آنگاه L خود متعامد بوده و وزن تمام یکد کلمات L بر ۴ بخش پذیراست.

اثبات: خود متعامد بودن L از قضیه قبل نتیجه می‌شود. از طرف دیگر داریم.

$$W(u+v)=W(u)+W(v)-2W(u\cap v)$$

اما v,u متعامدند، بنابراین $W(u\cap v)$ زوج است و لذا چون $۴|W(v),۴|w(u)$ پس $4|w(v+u)$

مثال: کد دوتایی $[۷و۳]$-L با ماتریس مولد زیر را در نظر بگیرید:

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

این کد، خود متعامد بوده و وزن تمامی کد کلمات بر ۴ بخش پذیر است. بنابراین L دارای ۷ کد کلمه با وزن بخش پذیر بر ۴ می‌باشد. و لذا وزن آنها، دقیقاً ۴ است. (چرا؟)

علاوه بر این $L^{\perp}$ یک $[۴و۷]$- کد شامل L است. از طرفدیگر $۱\in L^{\perp}$ (چرا؟)

بنابراین ماتریس $\begin{pmatrix} ۱ \\ G \end{pmatrix}$ یک ماتریس مولد برای $L^{\perp}$ است.

تعریف: کد L خود متعامد (*relf-dual*) نامیده می‌شود اگر $L=L^{\perp}$. در این حالت L می‌بایست یک $[n,\frac{n}{۲}]$- کد باشد. (اگر n زوج باشد). در واقع یک $[n,k]$- کد خطی L خوددوگان است اگر و تنها اگر خودمتعامد باشد و $K=\frac{n}{۲}$.

مثال: اگر یک بیت توازن کلی به کد موجود در مثال قبل اضافه کنیم آنگاه کد $\acute{L}$ با ماتریس مولد زیر به دست می‌آید:

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

$L^{\acute{}}$ یک کد خود دوگان است، زیرا خود متعامد بوده و [۴و۸]-کد است.

نکته: یکی از دلایلی که کدهای خوددوگان، مهم هستند، این است که کد های خوددوگان با طول دلخواه وجود دارند که به کران پائین گیلبرت- ورشامو دست می‌یابند. بنابراین، این کدها کدهای خود دوگان به طور قابل قبول خوب (*reasanably good*) هستند.

نکته: اگر کد L خود دوگان باشد، آنگاه هر ماتریس بررسی توازن برای L، یک ماتریس مولد نیز هست و برعکس، هر ماتریس مولد یک ماتریس بررسی توازن است. بنابراین اگر $G=(I_{\frac{n}{2}}\mid A)$ یک ماتریس مولد برای L باشد. $H=(-A^{t}\mid I_{\frac{n}{۲}})$ نیز یک ماتریس مولد است.

قضیه: یک کد خود دوگان $\left[n,\frac{n}{۲}\right]$ موجود است اگر و تنها اگر یکی از شرایط زیر برقرار باشد.

۱) qو n هر دو زوج باشند ۲) $q\overset{۴}{\equiv}۱$ و n زوج باشد **۳** $q\overset{۴}{\equiv}۳$ و n بر۴ بخش پذیر باشد.

نتیجه: همواره به ازای تمامی اعداد صحیح زوج n، یک کد دوتایی خوددگان $\left[n,\frac{n}{۲}\right]$ موجود است. و یک کد خود دوگان سه تایی $\left[n,\frac{n}{۲}\right]$ وجود دارد اگر و تنها اگر n بر ۴ بخش پذیر باشد.

نکته: یک کد خود دوگان L دارای این خاصیت است که تمامی وزن کد کلمات زوج می‌باشند. در این حالت، اگر وزن تمامی کد کلمات بر ۴ بخش پذیر باشد، یک کد دوبار زوج (*doubly even*) نامیده می‌شود.

قضیه: یک کد دو بار زوج $\left[n,\frac{n}{۲}\right]$ وجود دارد اگر و تنها اگر n بر ۸ بخش پذیر باشد.

تشخیص و تصحیح خطای گروهی (*burst error detection and correctia*)

در انتقال برخی اوقات، خطاها به صورت گروهی یا خوشه‌ای رخ می‌دهند. برای مثال، تداخل های الکتریکی، برخی اوقات بیشر از یک واحد زمانی طول می‌کشد و معمولاً روی یک دیسک یا نوار مغناطیسی، بیشتر از فضای مورد نیاز برای ذخیره یک سمبل از کد تأثیر می‌گذارد.

تعریف: یک خطای گروهی (*burst*) در $V(n,q)$ به طول b یک رشته در $V(n,q)$است که مکانهای ناصفر آن را می‌توان به b مکان متوالی محدود کرد به طوری که اولین و آخرین مکان آن ناصفر است.

لم: فرض کنید L یک $[n,k]$- کد خطی باشد. اگر L شامل خطاهای گروهی به طول b یا کمتر نباشد، آنگاه باید داشته باشیم $k \leq n-b$.

اثبات: مجموعه S شامل تمامی رشته‌ها در $V(n,q)$ با صفر های موجود در n-b مکان آخر را در نظر بگیرید. (توجه داشته باشید که b مکان اول می‌توانند شامل هر مقدار، از جمله صفر، باشند).

در این حالت، اگر دو رشته از S در یک هم دسته از L قرار گیرند. آنگاه تفاضل آنها یک خطای گروهی به طول b خواهد بود که غیر ممکن است. بنابراین تعداد هم دسته های L، که برابر با q^{n-k} است می‌بایست از اندازه S که q^b است، بزگرت باشد. یعنی $q^{n-k} \geq q^b \Leftarrow n-k \geq b$.

قضیه: اگر یک $[n,k]$- کد خطی مانند L بتواند تمامی خطاهای گروهی، طول b را تشخیص دهد آنگاه می‌بایست داشته باشیم $k \leq n-b$. علاوه بر این، یک $[n,n$-$b]$- کد خطی وجود دارد به طوری که تمام خطاهای گروهی با طول b یا کمتر را تشخیص دهد.

اثبات: برای این که کد L بتواند خطاهای گروهی با طول b یا کمتر را تشخیص دهد. نباید L شامل خطاهای گروهی با طول b یا کمتر باشد. بنابراین داریم $k \le n-b$.

برای اثبات قسمت دوم قضیه، ماتریس بررسی توازن H با اندازه $b\times n$ را در نظر بگیرید که سطر اول آن به صورت زیر باشد.

$$\underbrace{10\ldots.0}_{\text{سمبل } b} \qquad \underbrace{10\ldots.0}_{\text{سمبل } b} \qquad \ldots. \qquad \underbrace{10\ldots0}_{\text{سمبل } b} \qquad \underbrace{10\ldots0}_{\text{سمبل } b}$$

و مابقی سطرهای H، با شیفت سطر اول به اندازه یک واحد به سمت راست از سطر قبلی به دست آمده باشد (به عبارت دیگر بااضافه نمودن یک صفر به اول سطر قبلی). برای مثال، برای $b=3$ و $n=11$ داریم:

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

حال فرض کنید e یک خطای گروهی به طول b یا کمتر در $V(n,q)$ باشد. از آنجایی که هر b ستون متوالی H، تشکیل یک ماتریس جایگشتی $b\times b$ می‌دهند. سیندروم eH^t ، دقیقاً یک جایگشت روی مکانهای e است که ناصفر است. پس $eH^t \neq 0$ و کدگشا قادر به تشخیص e است.

قضیه: اگر یک $[n,k]$- کد خطی مانند L، بتواند تمامی خطاهای گروهی با طول b یا کمتر را (با استفاده از قاعده کمترین فاصله) تصحیح کند، آنگاه باید داشته باشیم $k \le n-2b$.

اثبات: اگر $2 \le l \le 2b$، انگاه هر خطای گروهی با طول l را می‌توان به صورت تفاضل e_1-e_2 از دو خطای گروهی e_2,e_1 با طول b نوشت. از آنجایی که L می تواند e_1وe_2 را تصحیح کند e_1وe_2 نمی توانند در یک همدسته از L قرار بگیرند و لذا $e=e_1-e_2$ نمی تواند یک کدکلمه باشد. چون یک خطای گروهی با طول l نمی‌تواند یک کدکلمه باشد، می‌توان با جایگذاری b با $2b$ در لم قبل به دست آوریم $k \le n-2b$ زیرا در این حالت می‌توان نشان داد خطاهای گروهی با اندازهٔ $2b$ (در $2b$ مکان اول) که تعداد آنها a^{2b} است، نمی‌توانند در

هم دستهٔ یکسانی باشند، زیرا تفاضل آنها کدکلمه خواهد بودکه تناقض است. پس $q^{2b} \le q^{n-k}$ و حکم ثابت است.

نکته: در اثبات قضیه فوق، مشاهده کردیم که اگر L بتواند هر خطای گروهی به طول b یا کمتر را تصحیح کند، آنگاه هیچ دو خطای گروهی در یک هم دسته یکسان از L قرار نمی-گیرند. با شمارش خطاهای گروهی با اندازه b یا کمتر، یک کران پائین برای تعداد هم دسته‌های L می‌یابیم که یک کران بالا روی بعد L را نتیجه می‌دهد. یعنی داریم:

قضیه: اگر L یک $[n,k]$- کد خطی باشد که تمام خطاهای گروهی با طول b یا کمتر را تصحیح کند آنگاه داریم:

$$A_1 : \underbrace{\times \ldots \times}_{b} \; \underbrace{\circ \ldots \circ}_{n-b} \qquad k \le n-b+1-\log_q((q-1)(n-b+1)+1)$$

اثبات: تمرین

زیرا اگر $\{b$ مکان iام خطای گروهی اند$\} = 1 \le i \le n-b+1, A_i$ $\quad A_2 : \circ \underbrace{\times \ldots \times}_{b} \; \underbrace{\circ \ldots \circ}_{n-b-1}$

زیرا مکان اول در هر A_i (بجز A_i آخر) یک عضو، ناصفر

از F_q است و بقیه دلخواهند) $\quad A_{n-b+1} : \underbrace{\circ \ldots \circ}_{n-b-1} \; \underbrace{\times \ldots \times}_{b}$

$$\sum_{i=1}^{n-b+1} |A_i| = q^{b-1}((q-1)(n-b+1)+1)$$

$$|A_i| = \begin{cases} (q-1)q^{b-1} & i < n-b+1 \\ q^b & i = n-b+1 \end{cases}$$

کدهای تفکیک پذیر با بیشترین فاصله (*maximum dirtance seperable codes*) یا *MDS*

مسأله اصلی کدگذاری در مورد کدهای خطی می‌تواند به صورت زیر بیان شود.

با فرض داشتن طول n و کمترین فاصله d، بزرگترین بعد k را بیابید که برای آن یک $[n,k,d]$- کد وجود داشته باشد. همچنان که دیده‌ایم، این مسأله در حالت کلی کاملاً سخت است.

از طرف دیگر، مامی‌توانیم n و k را ثابت نگاه داشته و بیشترین فاصله d را در میان تمامی کدهای با طول n و بعد k بیابیم. این مسأله، دارای پاسخ بسیار ساده تری است و به برخی از قضایای جالب منجر می‌شود از کران سینگلتون، داریم: $A_q(n,d) \le q^{n-d+1}$، با توجه به این کران، در مورد کدهای خطی داریم:

قضیه: برای یک کد $[n,k]$- خطی، داریم: $d \le n-k+1$.

تعریف: یک $[n,k,n-k+1]$- کد، یعنی یک $[n,k]$- با بیشترین فاصله ممکن، یک کد تفکیک پذیر با بیشترین فاصله یا کد MDS نامیده می‌شود.

کدهای MDS بدیهی به آسان می‌توان دید که کدهای q- تایی MDS با پارامتر های $[n,n,1]$، $[n,1,n]$ و $[n,n-1,2]$ وجود دارند. این کدها به کدهای MDS بدیهی معروف هستند. بنابراین هر $[n,k]$- کد MDS غیر بدیهی در رابطه $2 \le k \le n-2$ صدق می کند.

مشخصه کدهای *MDS*

کدهای MDS می توانند به چندین روش زیبا، مشخص شوند. در ابتدا با ماتریس بررسی توازن آنها شروع می کنیم یادآوری می کنیم که یک کد خطی دارای کمترین فاصله d است اگر و تنها اگر هر $d-1$ ستون ماتریس بررسی توازن H مستقل خطی باشند، اما d ستون وجود داشته باشند که وابسته خطی هستند. بنابراین قضیه زیر را داریم.

قضیه: فرض کنید L یک $[n,k]$- کد با ماتریس بررسی توازن H باشد. در این صورت L یک کد MDS است اگر و تنها اگر هر $n-k$ ستون H مستقل خطی باشند.

قضیه: اگر L، یک کد MDS باشد، آنگاه $L^{\perp}$ نیز MDS است.

اثبات: فرض کنید L، یک $[n,k]$- کد با ماتریس بررسی توازن H باشد. بنابراین H ماتریس مولد کد $L^{\perp}$ است. چون هر $(n-k)\times(n-k)$ زیر ماتریس H، وارون پذیر است. تمام ترکیبات خطی سطرهای H، دارای حداکثر $n-k-1$ درایه صفر هستند. بنابراین، تمامی ترکیبات خطی غیربدیهی سطرهای H دارای وزن حداقل $n-(n-k-1)=k+1$ می باشد. به عبارت دیگر،

کمترین فاصله $L^{\perp}$ برابر با $k+1=n-(n-k)+1$ است، که بیان می‌کند $L^{\perp}$ یک کد MDS است.

نکته: با استفاده از قضایای فوق، می‌توان کدهای MDS را بر حسب ماتریس مولد آنها، مشخص نمود که L یک $[n,k]$- کد MDS است اگر و تنها اگر $L^{\perp}$ یک $[n,n\text{-}k]$- کد MDS باشد، که در این صورت هر k ستون ماتریس بررسی توازن $L^{\perp}$ (یعنی ماتریس مولد L) مستقل خطی هستند. پس قضیه زیر را داریم:

قضیه: فرض کنید L یک $[n,k]$- کد با ماتریس مولد G باشد.در این صورت L، MDS است اگر و تنها اگر هر k ستون G مستقل خطی باشند.

توجه: قضیه فوق بیان می‌کند که هر k مکان از یک $[n,k]$- کد MDS، اطلاعات هستند. و بنابراین یک کد MDS، روی هر k مکان سیستماتیک است.

در اینجا، مشخصه زیبای دیگری از کدهای MDS را بیان می‌کنیم.

قضیه: فرض کنید L یک $[n,k]$- کد با ماتریس مولد $G=(I_k\,|\,A)$ به شکل استاندارد باشد. در این صورت، L یک کد MDS است اگر و تنها اگر هر زیر ماتریس مربعی A، نا منفرد باشد.

اثبات: فرض کنید L یک کد MDS باشد و B_u یک زیر ماتریس $u\times u$ از A باشند.

با تعویض سطرها و ستون‌های G، می‌توانیم فرض کنیم B_u در گوشه چپ بالایی A واقع است. حال ماتریس M، متشکل از $k\text{-}u$ ستون آخر I_k به همراه، ستون های شامل B را به صورت زیر، در نظر بگیرید. بنابراین، M به صورت زیر است:

$$M=\begin{pmatrix} O_{u,k-u} & B_u \\ I_{k-u} & * \end{pmatrix}$$

چون L، MDS است. داریم $\det(M)\neq 0$ و چون $\det(B_u)=\pm\det(M)$، نتیجه حاصل می‌شود.

اثبات عکس قضیه به عنوان تمرین واگذار می‌شود.

تعریف: محمل $(suppport)$ بردار $x\in V(n,q)$، مجموعه تمامی مکان‌های ناصفر x است.

نتیجه زیر، کدهای MDS را به روش دیگر مشخص می کند.

قضیه: یک $[n,k,d]$- کد L، یک کد MDS است اگر و تنها اگر بـه ازای هـر d مفـروض از آن، یک کد کلمه (با کمترین وزن) وجودداشته باشد به طـوری کـه محمـل ایـن کـد کلمـه دقیقا در این مکان ها باشد.

اثبات: فرض کنید L یک $[n,k]$ – کد MDS باشد. $d=n-k+1$ مـاکن از آن، مـثلا $i_1,...i_d$، را انتخاب کنید. مکان i_1، به همراه $k-1$ مکان انتخاب نشده $j_1,...,j_{k-1}$ را در نظر بگیرید. چون k مکان $i_1, j_1,..., j_{k-1}$ ، سمبل‌هـای اطلاعـات هسـتند، بنـابراین کـد کلمـه C وجـود دارد کـه دارای سمبل ۱ در مکان i_1 و سمبل صفر در سایر مکان‌های $j_1,..., j_{k-1}$ است. بنابرین، محمـل C، همان $i_1,...i_d$ می‌باشد (زیرا کمترین فاصله کد برابر با d است). برای عکس قضیه

n-d+1 سطر از ماتریس $M=(I_{n-d+1} | i_{d-1})$ را در نظر بگیرید کـه I_{n-d+1} یـک مـاتریس همانی و 1_{d-1} یک $(d-1)\times(d-1)$ ماتریس با درایه‌های تماماً ۱ است.

این سطرها، مستقل خطـی هسـتند و دارای وزن d مـی‌باشـند. چـون یـک کـد کلمـه $C_i \in L$ وجود دارد که داری محمل یکسان با سطر I ام M است، نتیجه می گیریم $k \geq n-d+1$ ، که این مطلب MDS بودن L را نشان می‌دهد.

مطالب فوق را می‌توان در قضیه زیر، خلاصه کرد:

قضیه فرض کنید L یک $[n,k,d]$- کد روی F_q باشد. شرایط زیر هم ارزند.

۱) L یک کد MDS است ۲) هر k ستون ماتریس مولد L، مستقل خطی هستند.

۳) هر n-k ستون ماتریس بررسی توازن L، مستقل خطی هستند. ۴) $L^{\perp}$ یک کد MDS اسـت.

۵) اگر $G=(I | A)$ ، یک شکل استاندارد از ماتریس مولد L باشد، آنگـاه هـر زیـر مـاتریس مربعی A، نامنفرد است.

۶) به ازای هر d مکان مفروض، یک کد کلمـه(با کمتـرین وزن) وجـود دارد کـه محمـل آن دقیقاً این مکان هاست.

کدهای MDS ساخته شده از ماتریس واندرموند (*Vandermonde*)

ساخت خانواده‌ای از کدهای MDS، سخت نیست برای این منظور، فرض کنید $\alpha_1,...,\alpha_u$ عناصر ناصفر از یک میدان باشند. ماتریس واندرمون بر پایه این عناصر به صورت زیر است.

$$V(\alpha_1,...\alpha_u)=\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_u \\ \alpha_2 & \alpha_2^2 & \dots & \alpha_u^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{u-1} & \alpha_2^{u-1} & \dots & \alpha_u^{u-1} \end{pmatrix}$$

لم: دترمینان ماتریس واندرموند به صورت زیر است:

$$\det(V(\alpha_1,...,\alpha_u))=\prod_{1\le i<j\le u}(\alpha_j-\alpha_i)$$

به خصوص اگر α_iها متمایز باشند، آنگاه $V(\alpha_i,...,\alpha_u)$ نامنفرد است.

اثبات: فرض کنید $p(x)=\det(V(\alpha_1,...,\alpha_{u-1},x))$ دراین صورت $P(x)$ یک چند جمله‌ای با درجه u-1 بر حسب X است. چون هر یک از $\alpha_1,...,\alpha_{u-1}$ ها، یک ریشه از $p(x)$ هستند، بنابراین $p(x)=\beta\prod_{i=1}^{u-1}(x-\alpha_i)$ ، جایی که β (نسبت به X) ثابت است.

اما β ضریب $x^{u-۱}$ در $p(x)$ است که همان $det(V(\alpha_1,...,\alpha_{u-1}))$ است. بنابرین، با فرض $x=\alpha_u$، داریم:

$$\det[V(\alpha_1,...,\alpha_u)]=\det[V(\alpha_1,...,\alpha_{u-1})]\prod_{i=1}^{u-1}(\alpha_u-\alpha_i)$$

حال، فرض کنید $f_q=\{۰,\alpha_1,...,\alpha_{q-1}\}$ و ماتریس $(q-k+۱)\times(q+۱)$ زیر، حاصل از یک ماتریس واندرموند با اضافه نمودن دو ستون اضافی زیر را در نظر بگیرید.

$$H_1=\begin{pmatrix} 1 & \cdots & 1 & 1\,0 \\ \alpha_1 & \cdots & \alpha_{q-1} & 0\,0 \\ \alpha_1^2 & \cdots & \alpha_{q-1}^2 & 0\,0 \\ \vdots & \vdots & \ddots & \vdots\,\vdots \\ \alpha_1^{q-k} & \cdots & \alpha_{q-1}^{q-k} & 0\,1 \end{pmatrix}$$

جایی که $1\le k \le q$ (به ازای $k=q$، ماتریس $H_۱$ ماتریس سطری شامل تمامی درایه‌ها است).

این مطلب به خواننده واگذار می‌شود که هر $q-k+۱$ ستون $H_۱$ یک ماتریس نامنفرد تشکیل می‌دهد بنابراین، قضیه زیر را داریم:

قضیه: برای $۱\le k \le q$، ماتریس H_1، ماتریس بررسی توازن یک $[q+1,k]$- کد MS q- تایی

است .

تذکر: توجه کنید که در حالت کلی، نمی‌توانیم ستون‌های اضافی به ماتریس $H_۱$ را اضافه کنیم و یک ماتریس بررسی توازن برای یک کد MDS بسازی برای نمونه، ماتریس زیر را در نظر بگیرید.

$$H_2 = \begin{pmatrix} 1 & \dots & 1 & 1 & 0 & 0 \\ \alpha_1 & \dots & \alpha_{q-1} & 0 & 1 & 0 \\ \alpha_1^2 & \dots & {\alpha^2}_{q-1} & 0 & 0 & 1 \end{pmatrix}$$

حال بیایید، دو ستون H_2 از میان q–۱ ستون اول را به همراه q+۱امین ستون در نظر بگیرید.

$\begin{pmatrix} 1 & 1 & 0 \\ \alpha_i & \alpha_j & 1 \\ \alpha_i^2 & \alpha_j^2 & 0 \end{pmatrix}$. این ماتریس، دارای دترمینان $\alpha_i^2-\alpha_i^2$است.

به ازای هر انتخاب ناصفر α_i,α_j، میدان F_q باید در رابطه $x\ne y \Rightarrow x^۲ \ne y^۲$ صدق کند. به عنوان تمرین می توان نشان داد که این رابطه برقرار است اگر و تنها اگر مشخصه F_q، ۲ باشد، یعنی اگر و تنها اگر q توانی از ۲ باشد.

بنابراین، تنها در حالتی که $H_۲, q=۲^m$ ماتریس بررسی توازن یک کد MDS است. قضیهٔ زیر نتیجه ای از مطالب فوق است.

قضیه : برای $q = 2^m$ H_2 ، ماتریس بررسی توازن یک [q–۱وq+۲]- کد MDS qتایی است. با در نظر گرفتن کدهای دوگان و مطالب فوق نتیجه زیر را داریم.

نتیجــه: بـه ازای $1 \le K \le q$ کـدهای MDS $[q+1,k]$ $[q+1q-k+1]$ وجـود دارنـد. بـه ازای $q=2^m$ ، کدهای MDS و $[q+2و q-1]$ و $[q+2و 3]$ وجود دارند.

برخی کدهای خطی

در این فصل، نگاهی به سه دسته از معروف ترین خانواده از کـدهای خطی مـی‌پـردازیم،

کدهای همنیگ

کدهای همینگ $H_q(r)$ شاید معروف ترین کدهای تصحیح –خطا باشند.

این کد ها، به طور مستقل توسط گلی در سال ۱۹۴۹ و همیگ سال ۱۹۵۰ کشف شـدند ایـن کدها خطی و کامل بوده و به روش بسیار جالبی کدگشایی می‌شوند. عـلاوه بـرا یـن، تمـامی کدهای همینگ دوتایی هم ارز با کدهای دوری بوده و برخی (نه همه) کدهای همینگ غیر دودویی هم ارز با کدهای دوری هستند.

قبلاً مشاهده کردیم که کمترین فاصله یک $[n,k]$- کد خطی بـا مـاتریس بررسـی تـوازن H، کوچکترین عـدد صـحیح d اسـت کـه بـرای آن d سـتون وابسـته خطـی از H وجـود دارنـد. بنابراین، ماتریس بررسی توازن یک $[n,k,3]$- کد دارای این خاصـیت اسـت هـیچ دو سـتون آن وابسته خطی نیستند، یعنی هیچ ستونی مضرب اسکالر ستون دیگر نیست، اما برخی از سـه ستونی‌ها وابسته خطی‌اند بـه ازای یـک الفبـای کـد مفـروض F_q، مـی‌تـوانیم یـک مـاتریس بررسی توازن با این خصوصیات بسازیم که دارای بیشترین تعداد ستون ممکن به صورت زیر باشد.

در ابتدا، یک ستون ناصفر C_1 در $V_1=V(r,q)$ را بردارید. سپس یک ستون ناصفر C_2 در

$V_2=V_1=\{\alpha c_i \mid \alpha \neq 0\}$

را انتخاب کنید. برداشـتن سـتون‌هـای ناصـفر و سـپس دورانـداختن تمـامی مضـارب اسـکالر ستون‌های انتخاب شده تا زمانی که دیگر انتخابی نداشته باشیم را ادامه مـی‌دهـیم. از آنجـایی که

$\left|\{\alpha c_i \mid \alpha \neq 0\}\right| = q-1$

نتیجه: یک ماتریس بررسی توازن با $\frac{q^r-۱}{q-۱}$ ستون خواهد بود، به طوری که در آن هیچ دو ستونی وابسته نیستند،اما برخی از سه ستون ها وابسته اند. ماتریس حاصل، یک ماتریس همینگ از مرتبه r خواهد بد که ماتریس بررسی توازن یک $[n,k,۳]$- کد q- تایی خطی با پارامتر های زیر است.

$$n=\frac{q^r-1}{q-1}, k=n-r, d=3$$

که به کد همینگ q- تایی از مرتبه r معروف است و با $H_q(r)$ نمایش داده می‌شود. توجه دارید که زمانی که اندازه کد همینگ کاملاً بزرگ باشد، و نرخ کد، به سمت ۱ میل کند (وقتی $r\to\infty$)، آنگاه این کدها تنها کدهای تصحیح کننده یک خطا هستند.

همچنین توجه دارید که انتخاب ستون‌ها، یکتانیست. و بنابراین ماتریس های همینگ متفاوتی دارند و در نتیجه کدهای همینگ متفاوتی با پارامترهای یکسان وجود دارند. اما، هر کد همینگ می‌تواند از دیگری (با پارامتر های یکسان) با استفاده از جایگشت ستون‌ها و ضرب هر ستون در مقادیر ناصفر به دست آید.

در اینجا از هر دو کد همینگ با اندازه یکسان، هم ارز (تحت ضرب اسکالر) هستند. درواقع، تحت هم ارزی (با ضرب اسکالر) کدهای همینگ با استفاده از پارامترا و این که خطی هستند، یکتا می‌باشد.

حالت دوتایی کدهای همینگ، بیسار معروف است. جایی که $H_۲(r)$ یک $[n,k,۳]$- کد دو دویی خطی، با پارامتر های زیر است.

$$n=2^r-1, k=2^r-1-r, d=3$$

در این حالت، ستون‌های ماتریس همینگ از مرتبه r، نمایش‌های دودویی $۲^r-۱$ عددس صحیح متوالی است. به سادگی می‌توان دیدکدهای همینگ کامل هستند.

کدگشایی کد همینگ

برخی اشکال ماتریس همینگ H، نسبت به سایر اشکال آن دارای شکل زیباتری هستند.

در حالت دودویی، ستونهای H را به ترتیب صعودی (نمایش دودویی اعداد از کوچک به بزرگ) انتخاب می کنیم. بنابراین به طور مثال، ماتریس بررسی توازن کد همینگ $H_2(3)$ به صورت زیر است:

$$H_۱=\begin{pmatrix} ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \end{pmatrix}$$

حال، اگر در انتقال یک کدکلمه، در مکان i ام یک خطا رخ دهد و بردار خطای e_i حاصل شود، آنگاه سیندروم کلمه دریافتی برابر با e_iH^t خواهد بود که دقیقا همان ستون i ام H است که به صورت سطری نوشته شده است. علاوه بر، این می‌توان تصور کرد که سیندروم، دراین حالت، همان نمایش دودویی مکان خطاست.

مثال: ماتریس $H_۱=\begin{pmatrix} ۰ & ۰ & ۰ & ۱ & ۱ & ۱ & ۱ \\ ۰ & ۱ & ۱ & ۰ & ۰ & ۱ & ۱ \\ ۱ & ۰ & ۱ & ۰ & ۱ & ۰ & ۱ \end{pmatrix}$ را در نظر بگیرید، اگر خطا به صورت $e_۳=۰۰۱۰۰۰۰$ باشد، آنگاه مقدار سیندروم به صورت زیر است.

$$e_۳H_۱^t=(۰۰۱۰۰۰۰)\begin{pmatrix} ۰ & ۰ & ۱ \\ ۰ & ۱ & ۰ \\ ۰ & ۱ & ۱ \\ ۱ & ۰ & ۰ \\ ۱ & ۰ & ۱ \\ ۱ & ۱ & ۰ \\ ۱ & ۱ & ۱ \end{pmatrix}=(۰۱۱)=(۰۱۱)_۲=(۳)_{۱۰}.$$

یعنی مکان خطا، مکان سوم بوده و

$$e=e_۳=۰۰۱۰۰۰۰$$

توجه: در حالت غیر دودویی، به طور مشابه می‌توانیم ستون های ماتریس بررسی توازن کد را به ترتیب صعودی (نمایش سه تایی اعداد از کوچک به بزرگ) انتخاب کنیم. اما اولین درایه ناصفر در این نمایش‌های سه تایی، برابر با ۱باشد.

مثال: ماتریس بررسی توازن $H_2(3)$ به صورت زیر است:

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

توجه: حال اگر یک خطا در iامین مکان رخ دهد، آنگاه بردار خطا به شکل αe_i، برای اسکالر ناصفر α ، خواهد بود. بنابراین، مقدار سیندروم به صورت $\alpha e_i H^t$ می‌باشد. که در آن این مقدار α برابر ستون i ام H است که به صورت سطری مرتب شده است. بنابراین باتوجه به ساختار H، می‌توان مشاهده کرد که α اولین مقدار ناصفر در سیندروم است. علاوه برا ین، با ضرب سیندروم در i,α^{-1} امین ستون H را داریم که مکان خطا را به ما نشان می‌دهد.

مثال: اگر ماتریس $H_{۲}$ در مثال قبل را به کار بریم، آنگاه سیندروم کلمه دریافتی $y=۱۱۰۱۱۱۲۲۱۳۰۱$ به صورت زیر است:

$$yH_{۲}^{t}=[۲ \circ ۱]=۲[۱ \circ ۲]=۲\times$$ (۷ امین ستون $H_{۲}$)

بنابراین، با کم نمودن ۲ از ۷امین مکان y کد کلمه زیر بدست می‌آید:

$$C=۱۱۰۱۱۱۰۲۱۳۰۱$$

میدان های متناهی و کدهای دوری

میدان‌های متناهی، دارای یک نقش اساسی در نظریه کدگذاری است و بنابراین به دست آوردن یک فهم عمیق از ساختار این میدان‌ها مهم است. همچنین، فهم ساختار چند جمله-ای‌هایی که ضرایب آنها متعلق به یک میدان متناهی است، دارای اهمیت است. به طور مثال، این که چند جمله‌ای مینیمال یک عضو را روی مدان متناهی بیابیم که نیاز است تا چند جمله ای x^n-1 را روی یک میدان متناهی تجزیه کنیم.

فرض کنید F,K میدان باشد. اگر k توسیع F باشد (یعنی $F \subseteq K$) می‌نویسیم $F < K$.

در این حالت K روی F یک فضای برداری خواهد بود. اگر بعد k روی F متناهی باشد، آنگاه گوئیم k یک توسیع متناهی F است و بعد آن را با $[F:k]$ نمایش می‌دهیم.

لم: فرض کنیم F یک میدان متناهی بوده و k توسیع F با $d=[k:F]$ باشد. در این صورت $|k|=|F|^d$.

اثبات: فرض کنید $\{\alpha_1,...,\alpha_d\}$ یک پایه برای k روی F باشد. دراین صورت هر عضو k دارای نمایش یکتای به صورت $a_1\alpha_1+...+a_d\alpha_d$ خواهد بود که در آن $a_i \in F$.

چون $|F|$ حالت ممکن برای هر ضریب a_i وجود دارد و به ازای بردارهای متفاوت $(a_1,...,a_d)$ ترکیب خطی $a_1\alpha_1+...+a_d\alpha_d$ نیز متفاوت خواهند بود، بنابراین $|k|=|F|^d$.

قضیه: اگر F یک میدان متناهی باشد، آنگاه F دارای یک مشخصه اول می‌باشد. علاوه بر این اگر $Char(F)=P$، آنگاه F دارای P^n عضو می‌باشد (برای یک مقدار صحیح مثبت n).

اثبات: در یک میدان با مشخصه صفر تمامی اعضای ... ، ۲ ، ۱ متمایز هستند. بنابراین، یک میدان متناهی دارای یک مشخصهٔ ناصفر است. بنابراین ، مشخصه F، کوچکترین عدد صحیح مثبت n است که در آن $n1=0$ حال فرض کنید $char(F)=n$. اگر $n=pq$ جایی که $P,q<n$ آنگاه $pq1=0$ بنابراین $(p1)(q1)=0$ که ایجاب می‌کند $p1=0$ یا $q1=0$. در هر حالت، با این که n کوچکترین عدد صحیح مثبت است که در آن $n1=0$ در تناقض است. پس n باید اول باشد. پس $Char(F)=P$ یک عدد اول است،در این حال، می‌توان نشان داد Z_P یک زیر میدان F است و لذا اگر $n=[F:Z_P]$ آنگاه:

$$|F|=|Z_p|^n=P^n$$

قرارداد: از اینجا به بعد P را معرف یک عدد اول و q را توانی از یک عدد اول فرض می-کنیم.

لم: اگر F یک میدان متناهی با مشخصه p باشد، آنگاه:

$$(\alpha \pm \beta)^{P^n} = \alpha^{p^n} \pm \beta^{p^n}$$

(برای هر عدد صحیح n و تمامی $\alpha, \beta \in F$)

یک مشخصه از میدان‌های متناهی

مطابق با تعریف، مجموعه F^* متشکل از عناصر ناصفر میدان F، تشکیل یک گروه تحت ضرب می‌دهند. اگر $|F| = q$، آنگاه $|F^*| = q-1$ و چون مرتبه هر عضو در یک گروه، مرتبه آن گروه را عاد می کند، بنابراین داریم: $\alpha \in F^* \Rightarrow \alpha^{q-1} = 1$ یا به طور هم ارز $x \in F \Rightarrow \alpha^q = \alpha$ از طرف دیگر، هر عضو F یک ریشه از چند جمله‌ای $f_q(x) = x^q - x$ است. اما چون این چند جمله‌ای دارای q ریشه است، می‌بینیم که F مجموعه تمامی ریشه-های $f_q(x)$ است و بنابراین F میدان شکافنده $f_q(x)$ است.

قضیه: اگر $|F| = q$، آنگاه F هم مجموعه تمامی ریشه‌های چند جمله‌ای $f_q(x) = x^q - x$ است و هم میدان شکافنده $f_q(x)$.

نکته: قضیه فوق، این مطلب را بیان می کند که هر میدان متناهی از اندازه q، میدان شکافنده $f_q(x)$ است و چون هر دو میدان شکافنده برای یک چند جمله‌ای، یکریخت هستند، نتیجه می گیریم که میدان‌های متناهی با اندازه یکسان، یکریخت هستند.

توجه: این مطلب که آیا به ازای هر q (توانی از یک عدد اول)، یک میدان متناهی با q عضو وجود دارد یا خیر، باقی مانده که وجود آن را به صورت زیر اثبات می کنیم.

فرض کنید $k, q = p^n$ میدان شکافنده $f_q(x) = x^q - x$ و R مجموعه تمامی ریشه‌های $f_q(x)$ باشد. اگر $\alpha, \beta \in R$، آنگاه $\alpha^q = \alpha, \beta^q = \beta$ ؛ بنابراین:

$$(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta(\alpha\beta^{-1})^q = \alpha^q(\beta^q)^{-1} = \alpha\beta^{-1}$$

که در نتیجه: $\alpha \pm \beta, \alpha\beta^{-1} \in R$، بنابراین R زیر میدانی از k است که در نتیجه $R = k$ علاوه بر این، چون(در Z_p)

$$Df_q(x) = qx^{q-۱} - ۱ = -۱$$

پس $DF_q(x)$ با $F_q(x)$ دارای هیچ ریشه مشترکی نیست. بنابراین $F_q(x)$ دارای هیچ ریشه تکراری نمی‌باشد. ولذا R دقیقا یک میدان با اندازه q است. با توجه به مطالب بیان شده، قضیه زیر را داریم:

قضیه: ۱) تمام میدان های متناهی دارای اندازه $q = P^n$ (برای یک عدد اول P) هستند.

۲) برای هر $q = p^n$، دقیقاً یک میدان یکتا (در حد یکریختی) از اندازه q وجوددارد که هم مجموعه ریشه‌های چند جمله‌ای $F_q(x) - x^q - x$ است و هم میدان شکافنده $F_q(x)$.

توجه: میدان متناهی با اندازه q را معمولا با F_q یا $GF(q)$ نمایش می‌دهیم.(نماد GF معرف میدان گالوا یا *FieldGalois* به افتخار اورست گالوا (*Evariste Galois*) نامگذاری شده است.

زیر میدان های یک میدان متناهی

هدف ما، در اینجا، تبیین زیر میدان‌های یک میدان متناهی است. به خصوص نشان خواهیم داد که هر میدان از اندازه P^n دقیقاً دارای یک زیر میدان از اندازه P^d (برای هر $d|n$) است و لذا میدان های ساخته شده ، تمامی زیرمیدان های F می باشند.

قضیه: فرض کنید k یک میدان متناهی با اندازه $|K|=P^n$ باشد و F یک زیر میدان K باشد. در این صورت $|F|=P^d$ که در آن $d|n$.

توجه: اگر $d|n$ آنگاه k دارای یک زیرمیدان یکتا از اندازه P^d می‌باشد.

برای مشاهدهٔ این مطلب، فرض کنید k یک میدان یکتا از اندازه P^n باشد و $d|n$ می دانیم k میدان شکافندهٔ چندجمله ای اما $fp^n(x)=x^{p^n}-x$ است حال به سادگی دیده می شود :

$$d|n \to p^d-1|p^n-1 \to x^{p^d}-x|x^{p^n}-x \to f_pd(x)|f_{p^n}(x)$$

اما $f_{p^n}(x)$ روی میدان k را می توان به عوامل خطی تجزیه کرد. بنابراین $f_{p^d}(x)$نیز حاصل ضربی از برخی از این عوامل خطی است. به بیان دیگر، k شامل یک میدان شکافنده $f_{p^d}(x)$است. یعنی k شامل یک زیر میدان با اندازهٔ p^d است. به وضوح، چنین زیر میدانی با اندازه P^d یکتاست، زیرا درغیر اینصورت $F_pd(x)$ دارای بیشتر از P^d ریشه است که تناقض است (زیرا $\deg\ F_Pd(x)=P^d$) با توجه به مطالب فوق، قضیه زیر را اثبات کرده‌ایم.

قضیه: فرض کنید k یک میدان متناهی با اندازه P^n باشد. در این صورت به ازای هر d (که در آن $d|n$)، دقیقا یک زیر میدان از اندازه P^d وجود دارد. علاوه بر این تمامی زیر میدان-های k، به این صورت می‌باشد.

ساختار ضربی یک میدان متناهی

مجموعه F^*، شامل تمامی عناصر ناصفر میدان F، تحت ضرب تشکیل یک گروه متناهی می دهند. این گروه نمی تواند ساختار ساده تری در مقایسه با دوری بودن داشته باشد. هدف ما،اثبات این مطلب، با نشان دادن این گزاره است که اگر $|F^*|=q-۱$ آنگاه F^* دقیقاً دارای $\phi(d)$ عضو از مرتبه d است (برای هر $d|q-۱$) جایی که در آن ϕ، تابع اویلر است. به

خصوص، F^* باید حداقل یک عضو از مرتبه $q-۱$ را شامل باشد و در نتیجه F^* دوری خواهد بود.

بیایید درباره گروه‌های دوری مطلبی را یاد آوری کنیم. اگر G یک گروه دوری از مرتبه n باشد آنگاه G شامل دقیقا $\phi(d)$ عضو از مرتبه d است (که n را عاد می‌کند). بنابراین:

$$\sum_{d|n}\phi(d)=n$$

حال فرض کنید $|F^*|=q-۱$ و $\propto$ یک عضو F^* از مرتبه d باشد. در این صورت $d\,|\,q-۱$.

زیر گروه دوری تولید شده $\propto$ را در نظر بگیرید.

$$<\propto>=\{۱,\propto,\propto^{۲},\ldots,\propto^{d-۱}\}$$

مرتبه هر عضو $<\propto>$ بر d بخش پذیر است، بنابراین هر عضو $<\propto>$، یک ریشه از $x^d-۱$ است اما چند جمله‌ای $x^d-۱$ در F دارای حداکثر d ریشه مجزا است (این در جایی است که ما از این واقعیت بهره می‌گیریم که Fیک میدان است)، بنابراین $<\propto>$، مجموعه تمامی ریشه‌های $x^d-۱$ است به خصوص تمامی عناصر F زا مرتبه d می‌بایست در $<\propto>$ باشند.

اما گروه دوری $<\propto>$ دارای دقیقا $\phi(d)$ عضو از مرتبه D است و لذا دقیقا $\phi(d)$ عضو از F دارای مرتبه d هستند. بنابراین، اگر F دارای یک عضو از مرتبه $d\,|\,q-۱,d$ ، باشد آنگاه دقیقاً $\phi(d)$ عضو به این صورت وجود دارند، حال فرض کنید $\psi(d)$، تعداد عناصری از F باشد که دارای مرتبه d هستند، آنگاه $\phi(d)$ یا $\psi(d)=۰$ اما داریم:

$$q-۱=\sum_{d|q-۱}\psi(d)\le\sum_{d|n}\phi(d)=q-۱$$

لذا $\psi(d)=\phi(d)$ (برای تمامی $d\,|\,q-۱$)، پس قضیه زیر را اثبات کرده‌ایم.

قضیه اگر F یک میدان متناهی با q عضو باشد، آنگاه F دارای دقیقا $\phi(d)$ عضـو از مرتبـه d می‌باشد، که در آن $d \mid q-1$.

نتیجه: گروه F^* شامل عناصر ناصفر، F دوری است.

تعریف: هر عضو F_q که گروه دوری F_q^* را تولید کند، یـک عضـو اولیـه $(Primitive)$ F_q نامیده می‌شود.

توصیف عناصر یک میدان متناهی

در حالت کلی، چندین روش وجود دارد که در آن مـی‌تـوان عناصـر یـک میـدان متنـاهی را توصیف کرد. یک روش، استفاده از حلقـه تجزیـه بـه صـورت $\frac{F_q[x]}{<p(x)>}$ اسـت، جـایی کـه $P(x)$ یک چند جمله‌ای تحویل ناپذیر می‌باشد. روش دیگر، استفاده از این واقعیت می‌باشـد که F_q^* دوری می‌باشد و بنابراین عناصر آن تمامی توان‌های یک عضو اولیه هستند. آنچنـان که خواهیم دید، اولین نمایش مناسب بازمانی است که بخواهیم عملیات جمع بین عناصـر F_q را انجام دهیم و نمایش دوم، مناسب عملیات ضرب است. اما، خوشبختانه مـی‌تـوانیم ایـن دو روش را با یکدیگر ترکیب کنیم.

می‌دانیم اگر $P(x)$ یک چنـد جملـه‌ای تحویـل ناپـذیر روی F_q باشـد، آنگـاه حلقـه تجزیـه $K = \frac{F_q[x]}{<p(x)>}$ یک میدان اسـت در واقـع، اگـر $\deg(p(x) = d)$ ، آنگـاه k دارای درجـه‌ی d روی F_q می‌باشد، بنابراین $k = F_q d$ این نمایش، روشی برای توصـیف عناصـر یـک میـدان نشان می‌دهد.

چون:
$$F_q d = \frac{F_q[x]}{<p(x)>} = \{r(x) + <p(x)> \mid \deg(r(x) < d\}$$

پس $F_q d$ را می‌توان با تمام چند جمله‌ای‌های با درجـه حـداکثر $d-1$ بـه همـراه عمـل جمـع و ضرب پیمانه‌ای (در پیمانه $p(x)$) یکسان در نظر گرفت.

اگر $\propto$ یک ریشه از $P(x)$ در یک میدان شکافنده باشد، آنگاه می‌توانیم میدان $F_q d$ را مجموعه تمام چند جمله‌ای ها بر حسب $\propto$ با درجه حداکثر d-۱ در نظر بگیریم که جمع و ضرب در پیمانه $p(x)$ صورت می گیرد. این مطلب، بیان غیر رسمی آن است که بگوییم $\frac{F_q[x]}{< p(x) >}$ با $F_q(\alpha)$ یکریخت است.

مثال چند جمله‌ای $p(x) = x^۴ + x^۳ + x^۲ + x + ۱$ روی $F_۲$ تحویل ناپذیر است.

زیرا در غیر اینصورت $p(x)$ دارای یک عامل خطی یا درجه **۲** می باشد .اما $P(۱) \neq ۰, p(۰) \neq ۰$ ، بنابراین $p(x)$ شامل عامل خطی نیست. برای این که نشان دهیم $p(x)$ شامل هیچ عانمل درجه دومی نیست، تمامی عوامل درجه دوم روی $F_۲$ به صورت زیر هستند.

$$x^2, x^2 + 1, x^2 + x, x^2 + x + 1$$

اما به آسانی می‌توان دید $p(x)$ شامل حاصل ضرب هیچ دوتا از این عوامل نیست. حال $q = ۲$ و $d = ۴$، پس

$$\frac{F_2[x]}{< x^4 + x^3 + x^2 + x + 1 >} = F_{16} =$$

بنابراین، با این که $\propto$ ریشه‌ای از $p(x)$ باش، می‌توانیم عناصر $F_{۱۶}$ را به صورت چند جمله-ای های با درجه **۳** یا کمتر، بر حسب $\propto$ بنویسیم.

۰,۱: مقادیر ثابت

$\propto, \propto + ۱$:خطی

۲ درجه: $\propto^۲, \propto^۲ + ۱, \propto^۲ + \propto, \propto^۲ + \propto + ۱$

۳ درجه: $\propto^۳, \propto^۳ + ۱, \propto^۳ + \propto, \propto^۳ + \propto^۲, \propto^۳ + \propto + ۱, \propto^۳ + \propto^۲ + ۱,$
$\propto^۳ + \propto^۲ + \propto, \propto^۳ + \propto^۲ + \propto + ۱$

هر چند جمله‌ای $F(\propto) \in F_۲[\propto]$ را می‌توان در پیمانه $p(x)$ کاهش داد؛ برای این کار کافی است قرار دهیم $p(\alpha) = ۰$ پس در این مثال:

$$\propto^{4}=\propto^{3}+\propto^{2}+\propto+1$$

در این حالت، محاسبات تا حدودی با توجه به این واقعیت که $\propto$ دارای مرتبه نسبتاً کوچکی خواهد بود، ساده تر به نظر می‌رسد.

$$\propto^{5}=\propto.\propto^{4}=\propto(\propto^{3}+\propto^{2}+\propto+1)=\propto^{4}+\propto^{3}+\propto^{2}+\propto+1$$

بنابراین، $\propto^{7}=\propto^{2},\propto^{6}=\propto$ و به همین ترتیب ادامه دارد.

با استفاده از این نمایش، جمع کاملاً ساده به نظر می‌آید. کافی است چندجمله‌ای های با درجه حداکثر ۳ را به یکدیگر جمع کنید، برای مثال؛ در F_{2}داریم $2=0$؛ پس

$$(\propto^{3}+\propto+1)+(x^{3}+\propto^{2}+1)=\propto^{2}+\propto$$

اما، ضرب کردن ساده نیست، زیرا باید حاصل ضرب را در پیمانه $p(\propto)$ کاهش دهیم. به عنوان نمونه، دراین مثال:

$$(\propto^{3}+\propto+1)(\propto^{3}+\propto^{2}+1)=\propto^{6}+\propto^{5}+\propto^{3}+\propto^{4}+\propto^{3}+\propto+\propto^{3}+\propto^{2}+1=$$
$$\propto^{6}+\propto^{5}+\propto^{4}+\propto^{3}+1=\propto H+\propto^{4}+\propto^{3}+1=\propto^{4}+\propto^{3}+\propto$$

در مورد میدان‌های بزرگتر، حاصل ضرب چند جمله‌ای غیر عملی است، به خصوص در نمایش تناوبی بعداً در نظر می گیریم.

اگر β یک عضو اولیه از F_qباشد، آنگاه: $F_q=\{0,1,\beta...,\beta^{q-2}\}$

در این نمایش، ضرب به سادگی صورت می گیرد. $\beta^{i}.\beta^{i}=\beta^{(i+j)\bmod(q-1)}$

اما در این نمایش جمع کردن اصلاً واضح نیست. از طرف دیگر، اگر چند جمله‌ای مینیمال $P(x)$ برای βرا داشته باشیم، آنگاه می‌توانیم عناصر F_{16}را به صورت چند جمله‌ای هایی بر حسب β در نظر گرفته و از آنها به منظور جمع بهره‌گیریم. بیایید مثال زیرا در نظر بگیرید.

مثال: چند جمله‌ای $q(x)=x^{4}+x+1$ تحویل ناپذیر است (روی F_{2}) فرض کنید βیک ریشه از این، چند جمله‌ای باشد. بنابراین. مانند مثال قبل، می‌توانیم عناصر F_{16} را به صورت مجموعه چند جمله‌ای های با درجه حداکثر ۳ برحسب β در نظر بگیریم، که در آن

$$\beta^{4}=\beta+1$$

از طرف دیگر:

$$\beta^{15}=(\beta^{5})^{3}=(\beta.\beta^{4})^{3}=(\beta(\beta+1))^{3}=\beta^{3}(\beta+1)^{3}=$$
$$\beta^{3}(\beta^{3}+\beta^{2}+\beta+1)=\beta^{6}+\beta^{5}+\beta^{4}+\beta^{3}(\beta^{3}+\beta^{2})+(\beta^{2}+\beta)+$$
$$(\beta+1)+\beta^{3}=1$$

این رابطه نشان می‌دهد که مرتبه β باید ۱۵ را عاد کند. ولی $\beta^{5}\neq 1,\beta^{3}\neq 1$، پس $ord(\beta)=15$ و لذا β اولیه است. چون β یک عضو اولیه F_{16} است، پس عناصر ناصفر F_{16} را می‌توان به صورت توان‌های β، $\beta^k, k=0,1,...,14$، در نظر گرفت. حال می‌توانیم بین این دو نمایش (ضرب و جمع) یک ارتباط برقرار کنیم، برای این کار می‌توان هر عضو β^k را به صورت یک چند جمله بر حسب β با درجه حداکثر ۳ نمایش داد. با استفاده از این واقعیت که $\beta^{4}=\beta+1$ داریم:

$$\beta^{4}=\beta+1\Rightarrow\beta^{5}=\beta.\beta^{4}=\beta(\beta+1)=\beta^{2}+\beta,\beta^{6}=\beta.\beta^{5}=\beta^{3}+\beta^{2}$$
$$\beta^{7}=\beta.\beta^{6}=\beta^{4}+\beta^{3}=\beta^{3}+\beta+1$$

و به همین ترتیب. لیست کامل، در جدول زیر نمایش داده شده است.

در این جدول به جای β^k، تنها k را نوشته‌ایم و به جای چندجمله‌ای $a_3\beta^{3}+a_2\beta^{3}+a_1\beta+a_0$ (به منظور سادگی)، رشته $a_3a_2a_1a_0$ را نوشته‌ایم.

محاسبات، در این جدول، کاملاً سرراست است.

به عنوان مثال، داریم:

$$\begin{aligned}&(\beta^{8}+\beta^{4}+1)(\beta^{3}+\beta)=\beta^{11}+\beta^{9}+\beta^{7}+\\&\beta^{5}+\beta^{3}+\beta=1110+1010+1011+\\&0110+1000+0010+0011=\beta^{4}=\beta+1\end{aligned}$$

$k;\beta k$	$a_3a_2a_1a_0; a_0+a_1\beta+a_2\beta^2+a_3\beta^3$
۰	۰۰۰۱
۱	۰۰۱۰
۲	۰۱۰۰
۳	۱۰۰۰
۴	۰۰۱۱
۵	۰۱۱۰
۶	۱۱۰۰
۷	۱۰۱۱
۸	۰۱۰۱
۹	۱۰۱۰
۱۰	۰۱۱۱
۱۱	۱۱۱۰
۱۲	۱۱۱۱
۱۳	۱۱۰۱
۱۴	۱۰۰۱

در این مثال، می‌بینیم که نقطه کلیدی برای انجام محاسبات در یک میدان متناهی، داشتن یک عضو اولیه است. (که به همراه چند جمله‌ای مینیمال آن آمده است). این نکته، انگیزه‌ای برای تعریف زیر می‌باشد:

تعریف: فرض کنید β یک عضو اولیه از میدان F_qn باشد. چندجمله‌ای مینیمال β روی F_q یک چند جمله‌ای اولیه (*Primitive polynomial*) برای F_qn نامیده می‌شود.

در ادامه خواهیم دید که تمام ریشه‌های چند جمله‌ای تحویل ناپذیر روی یک میدان متناهی، دارای مرتبه یکسان هستند. بنابراین یک چند جمله‌ای اولیه برای F_qn یک چند جمله‌ای تکین تحویل ناپذیر روی F_q است که تمامی ریشه‌های آن، عناصر اولیه F_qn می‌باشند. همچنین، خواهیم دید که تمامی چند جمله‌ای های اولیه برای F_qn روی F_q دارای درجه هستند.

در حالت کلی، یافتن چند جمله‌ای های اولیه کارآسانی نیست. روش‌های متفاوتی وجود دارند که در حالت‌های خاصی، تا حدی موفق بوده‌اند، اما در اینجا به آنها نمی‌پردازیم. خوشبختانه، جدول‌های گسترده‌ای از چند جمله‌ای های اولیه و میدان‌ها، داده شده اند. برای این کار، می‌توان کار لیدل (*Lidl*) و نیدریتر (*Niederriter*) (۱۹۸۶) مراجعه کرد.

هر دو نمایش یک میدان متناهی که در بالا گفتیم، به یک نمایش ماتریسی منجر می‌شود. برای مشاهده این مطلب، با ایده‌ای از جبر خطی کار را شروع می‌کنیم. ماتریس همراه (*Companion Matrix*) یک چند جمله‌ای تکین $P(x)=a_0+a_1x+\dots+a_{n-1}x^{n-1}+x^n$، ماتریسی به صورت زیر است.

$$C=\begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 1 & -a_{n-1} \end{pmatrix}$$

می‌توان نشان داد که ماتریس همراه یک چند جمله‌ای، در آن چند جمله‌ای صدق می‌کند، یعنی $P(C)=0$.بنابراین، می‌توان C را به عنوان ریشه‌ای از $P(x)$ در نظر گرفت.

بنابراین اگر $P(x)$ یک چند جمله‌ای تکین تحویل ناپذیر روی F_q با درجه d و ماتریس همراه C باشد، آنگاه، میدان F_{qd} را می‌توان به صورت مجموعه چند جمله‌ای ها بر حسب C با درجه کمتر از d نمایش داد، جایی که جمع و ضرب در پیمانه $P(C)$ هستند. اما چند جمله‌ای های برحسب C، فقط ماتریس هستند؛ بنابراین می‌توانیم نمایشی از عناصر F_q را به صورت ماتریس های روی F_q در نظر بگیریم.

مثال: چندجمله‌ای تحویل ناپذیر $P(x)=x^2+1$ روی F_3 را در نظر بگیرید عناصر F_9 می‌توانند به صورت چند جمله‌ای های با درجه کمتر از ۲ با ماتریس همراه $C\,P(x)$ نمایش داده شوند. به خصوص، عناصر $F9$

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

به صورت زیر هستند:

$$0=\begin{pmatrix}0&0\\0&0\end{pmatrix}, I=\begin{pmatrix}1&0\\0&1\end{pmatrix}, 2I\begin{pmatrix}2&0\\0&2\end{pmatrix}, C\begin{pmatrix}0&2\\1&0\end{pmatrix}, I+C=\begin{pmatrix}1&2\\1&1\end{pmatrix}$$

$$2I+C=\begin{pmatrix}2&2\\1&2\end{pmatrix}, 2C=\begin{pmatrix}0&1\\2&0\end{pmatrix}, I+2C=\begin{pmatrix}1&1\\2&1\end{pmatrix}, 2I+2C=\begin{pmatrix}2&1\\2&2\end{pmatrix}$$

در روشی دیگر، اگر ماتریس A، ماتریس همراه چند جمله‌ای اولیه $q(x)=x^2+x+2$ روی F_3 باشد، آنگاه می‌دانیم که تمام عناصر F_q توان های یک ریشه از $q(x)$ هستند. بنابراین:

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

و عناصر F_9 به صورت زیر هستند:

$$0=\begin{bmatrix}0&0\\0&0\end{bmatrix}. A\begin{pmatrix}0&1\\1&2\end{pmatrix}, A^2=\begin{pmatrix}1&2\\2&2\end{pmatrix}, A^3=\begin{pmatrix}2&2\\2&0\end{pmatrix},$$

$$A^4=\begin{pmatrix}2&0\\0&2\end{pmatrix}, A^5=\begin{pmatrix}0&2\\2&0\end{pmatrix}, A^6=\begin{pmatrix}2&1\\1&1\end{pmatrix}, A^7=\begin{pmatrix}1&1\\1&0\end{pmatrix},$$

$$A^8=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

در هر حالت، جمع و ضرب با استفاده قواعد جبر ماتریس‌ها به دست می‌آید. مزیت این نمایش‌ها این است که محاسبات به صورت خودکار صورت می‌گیرد، برای نمونه،

$$(I+C)(I+2C)=\begin{pmatrix}1&2\\1&1\end{pmatrix}\begin{pmatrix}1&1\\2&1\end{pmatrix}=\begin{pmatrix}2&0\\0&2\end{pmatrix}=2I$$

از طرف دیگر، اگر $deg\ (p(x))$ بزرگ باشد، آنگاه ماتریس‌ها بزرگ خواهند شد و لذا محاسبات پیچیده می‌گردد.

چند جمله‌ای‌های تحویل ناپذیر میدان‌های متناهی

در این بخش، درباره خواص اصلی چند جمله‌ای‌های تحویل ناپذیر روی میدان‌های متناهی بحث می‌کنیم. فرض کنیم میدان شکافنده یک چند جمله‌ای $f(x)$ را با $split\ (f(x))$ یا $split(f)$ نمایش دهیم، لم زیر بسیار مفید است.

لم: فرض کنید $f(x)$ یک چند جمله‌ای تحویل ناپذیر روی F_q باشد و $\propto$ یک ریشه از $f(x)$ در میدان تعمیم یافته باشد. بنابراین، اگر $g(x) \in F_q[x]$ آنگاه $g(x) = \circ$ اگر و تنها اگر $f(x) \mid g(x)$.

اثبات: اثبات با توجه به این واقعیت که $f(x)$ مضرب اسکالر و ناصفری از چند جمله‌ای مینیمال $\propto$ روی F_q است، نتیجه می‌شود. بحث اصل خود را باطرح اساسی ترین سوال در این باره، یعنی وجود چنین میدانی آغاز می کنیم.

قضیه: برای هر میدان متناهی F_qو هر عدد صحیح مثبت d. یک چند جمله‌ای تحویل ناپذیر $f(x)$ با درجه d روی F_qموجود است.

اثبات: فرض کنید β یک عضو اولیه از $F_q d$ باشد؛ در این صورت $F_q(\beta) = F_q d$ و چون $[F_q(\beta) : F_q] = [F_q d : F_q] = d$، بنابراین چند جمله‌ای تحویل ناپذیر β روی F_q می‌بایست دارای درجه d باشد.

میدان شکافنده یک چند جمله‌ای تحویل ناپذیر

در یک میدان نامتناهی مانند F، اگر α یک ریشه چند جمله‌ای تحویل ناپذیر $f(x) \in F[x]$ باشد، آنگاه میدان $F(\alpha)$، حاصل از الحاق α به F، در حالت کلی میدان شکافنده $F(x)$ نمی باشد.به بیان دیگر ، الحاق یک ریشه αاز $f(x)$ در حالت کلی ، ریشه های دیگر $f(x)$ را در بر نمی‌گیرد. در واقع، کلی ترین مطلبی که درباره بعد میدان شکافنده یک چند جمله‌ای تحویل ناپذیر با درجه d می‌توان گفت، این است که بعد آن بین d و $d!$ است.

اما، در مورد میدان‌های متناهی، الحاق یک ریشه چند جمله‌ای تحویل ناپذیر، همواره میدان شکافنده آن چند جمله‌ای را نتیجه می‌دهد. بنابراین، میدان شکافنده در این حالت، دارای درجه‌ای مساوی با درجه خود چند جمله‌ای است. برای مشاهده دلیل این مطلب، فرض کنید $F(x)$با درجه d روی F_q تحویل ناپذیر باشد. فرض کنید α ریشه‌ای از $F(x)$ در $split(f)$ باشد. میدان‌های زیر را در نظر بگیرید: $F_q < F_q(\alpha) < split(f)$ چون $[F_q(x) = F_q] = d$، پس

$|F_q(x)|=q^d$ و لذا $F_q(\alpha)$ مجموعه تمامی ریشه‌های چند جمله‌ای $f_q d(x)=x^{q^d}-x$ است.
به خصوص، $\propto$ریشه‌ای از $f_q d(x)$ نیز هستند و بنابراین، این ریشه‌ها متعلق به $F_q(\alpha)$ می‌باشند.لذا $\mathrm{split}(f)<F_q(\alpha)$. لذا $F_q(\propto)=split(f)$، این مطلب، به اثبات قضیه زیر منجر می‌شود.

قضیه: فرض کنید $f(x)\in f_q[x]$ یک چند جمله‌ای تحویل ناپذیر با درجه d باشد.و α ریشه دلخواهی از $F(x)$ باشد. در این صورت، میدان شکافنده $F(x)$ به صورت زیر است:

$$split(f)=F_q(\alpha)=F_q d$$

به خصوص، میدان شکافنده $F(x)$ روی F_q دارای درجه d است.

نتیجه: فرض کنید $f(x)\in F_q[x]$ چندجمله‌ای تحویل ناپذیر با درجه d باشد صورت $f(x)|x^{q^n}-x$ اگر و تنها اگر $d|n$.

اثبات: در ابتدا توجه داریم که $split(f)=F_q d, split(x^{q^n}-x)=F_q n$ بنابراین طبق قضیه ای از از قبل،

$$split(f)<split(x^{q^n}-x)\Leftrightarrow d\mid n$$

حال، اگر $f(x)|x^{q^n}-x$ آنگاه هر ریشه $f(x)$، ریشه‌ای از $x^{q^n}-x$ است. در نتیجه، $split(f)<split(x^{q^n}-x)$ و لذا $d|n$. برعکس، اگر $d|n$ آنگاه $split(f)<split(x^{q^n}-x)$ و لذا هر ریشهٔ $\propto$ از $f(x)$، در $split(x^{q^n}-x)$ قرار می‌گیرد. اما، $split(x^{q^n}-x)$ مجموعه تمامی ریشه‌های $(x^{q^n}-x)$ است و لذا α می‌بایست ریشه‌ای از $(x^{q^n}-x)$ باشد. بنابراین $f(x)|x^{q^n}-x$.

ماهیت ریشه‌های یک چند جمله‌ای تحویل ناپذیر

حال بیایید به ماهیت ریشه‌های یک چند جمله‌ای تحویل ناپذیر مانند f،روی F_q نگاه دقیق تری بیندازیم می‌دانیم ریشه‌های $f(x)$ متعلق به $f_q d$ هستند که در آن: $d=\deg(f(x))$.
فرض کنید $f(x)=a_0+a_1x+\ldots+a_d x^d$ که در آن $a_i\in F_q$. اگر αیک ریشه از $f(x)$ باشد، آنگاه:

$$f(x)=a_{\circ}+a_{1}\alpha+...+a_{d}\alpha^{d}=\circ$$

حال از این مزیت که با یک میدان با مشخصه p کار می کنیم، به صورت زیر بهره می گیـریم.

چون $a_i \in F_q$، می‌دانیم $a_i{}^q=a_i$ و نیز:

$$f(x^q)=a_{\circ}+a_1\alpha^q+...+a_d\alpha^{qd}=a_{\circ}{}^q+a_1^q\alpha^q+...+a_d^q\alpha^{qd}=$$
$$a_{\circ}{}^q+(a_1\alpha)^q+...+(a_d\alpha^d)^q=(a_{\circ}+a_1\alpha+...+a_d\alpha^d)^q=$$
$$(f(\alpha))^q=\circ$$

بنابراین اگر α ریشه‌ای از $f(x)$ باشد، α^q نیز ریشه‌ای از $f(x)$ خواهد بود. به همین ترتیب، می‌بینیم که $\alpha,\alpha^q,\alpha^{q^2},...,\alpha^{q^{d-1}}$ نیز ریشـه‌هـایی از $f(x)$ هسـتند. حـال اگـر نشـان دهـیم ایـن ریشه‌ها متمایز هستند، آنگاه اینها، تمامی ریشه‌های $f(x)$ خواهند بود. اگـر $\underset{(i<j)}{\alpha^{qi}=\alpha^{qj}}$ آنگـاه دوطرف را به توان q^{d-j} می‌رسانیم، پس داریم:

$$\alpha^{q^{d+i-j}}=\alpha^{q^d}=\alpha$$

و لذا α یک ریشه از چند جمله‌ای $x^{q^{d+i-j}}-x$ است، بنابراین:

$$f(x)\,|\,x^{q^{d+i-j}}-x$$

که، با نتیجه قبل در تناقض است .بنابراین، این ریشه‌ها متمایز هستند.

همچنین، توجه داریم که d کوچکترین عدد صحیح مثبتی است که در آن $\alpha^{q^d}=\alpha$

با توجه به مطالب فوق، قضیه زیر را اثبات کرده‌ایم.

قضیه: فرض کنید $f(x)\in f_q[x]$ یک چند جمله‌ای تحویل ناپذیر با درجـه d باشـد. اگـر α یک ریشه از $f(x)$ در $split(f)=F_q d$ باشد، انگاه، تمامی ریشه‌های $f(x)$ بـه صـورت زیـر می‌باشند.

$$\alpha,\alpha^q,\alpha^{q^2},...,\alpha^{q^{d-1}}$$

علاوه بر این، d کوچکترین عدد صحیح مثبتی است که در ان $\alpha^{q^d}=\alpha$.

نتیجه: فرض کنید $f(x)\in F_q[x]$ تحویـل ناپـذیر باشـد. درایـن صـورت، تمـامی ریشـه‌هـای $f(x)$ در $split(f)$ دارای مرتبه یکسانی می‌باشند.

اثبات: این مطلب با توجه به این که (*split(f)*) دارای مرتبه $qd-1$ است و q^i, q^{d-1} (برای هر i) نسبت به هم اول هستند، نتیجه می‌شود.

تعریف: مرتبه هر ریشه از یک چند جمله‌ای تحویل ناپذیر مانند $f(x) \in F_q[x]$ در میدان شکافنده آن، مرتبه $f(x)$ نامیده می‌شود و با $o(f(x))$ یا $o(f)$ نمایش داده می‌شود.

توجه: با نگاهی به این واقعیت که هر عضو F_q ریشه دقیقاً یک چند جمله‌ای تحویل ناپذیر روی F_q (یعنی چند جمله‌ای مینیمال آن) است، تعریف زیر نتیجه می‌شود.

تعریف: عناصر $\alpha, \beta \in F_q n$ ، روی F_q مزدوج (*conjulate*) نامیده می‌شوند اگر آنها ریشه-های چند جمله‌ای تحویل ناپذیر تکین یکسانی روی F_q باشند؛ یعنی دارای چند جمله‌ای مینیمال یکسانی روی F_q باشند.

نتیجه: مزدوج های $\alpha \in F_q n$ روی F_q به صورت زیر هستند.

$$\alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{d-1}}$$

جایی که d کوچکترین عدد صحیح مثبت است که در آن $\alpha^{q^d} = \alpha$.

محاسبه چند جمله‌ای های مینیمال

می‌توان از قضایا و مطالب گفته شده در بالا استفاده کرد و چندجمله‌ای مینیمال هر عضو $\alpha \in F_q$ را یافت.

نتیجه: فرض کنید $\alpha \in F_q n$. در این صورت چند جمله‌ای مینیمال αبه صورت زیر است:

$$irr(\alpha, F_q) = (x-\alpha)(x-\alpha^q)....(x-\alpha^{q^{d-1}})$$

جایی که d کوچک ترین عدد صحیح مثبت است که در آن $\propto^{q^d} = \propto$ به خصوص، چند جمله‌ای طرف راست (زمانی که عوامل در یکدیگر ضرب شده و ساده شوند) می‌بایست دارای ضرایبی در F_qباشد.

مثال: قبلا دیدیم چند جمله‌ای $P(x)=x^۴+x+۱$ برای $F_{۱۶}$ روی $F_۲$، اولیه می‌باشد. بنابراین، هر ریشه β از $p(x)$، $F^*{}_{16}$ را تولید می‌کند. حال بیایید، چندجمله‌ای مینیمال عناصر $F_{۱۶}$ را بیابیم.

با محاسبه مزدوج‌ها، شروع می‌کنیم: (توجه داریم که $\beta^{۱۵}=۱$)

β مزدوج‌های: $\beta,\beta^۲,\beta^۴,\beta^۸ \qquad (\beta^{۱۶}=\beta)$

$\beta^۳$ مزدوج‌های: $\beta^۳,\beta^۶,\beta^{۱۲},\beta^{۲۴}=\beta^۹ \qquad (\beta^{۴۸}=\beta^۳)$

$\beta^۵$ مزدوج‌های: $\beta^۵,\beta^{۱۰}$

$\beta^۷$ مزدوج‌های: $\beta^۷,\beta^{۱۴},\beta^{۲۸},\beta^{۱۳},\beta^{۵۶},\beta^{۱۱}, \qquad (\beta^{۱۱۲}=\beta^۷)$

حال فرض کنید $m_k(x)$ چندجمله‌ای مینیمال β^k باشد، در اینصورت به طور نمونه داریم:

$$m_۵(x)=m_{۱۰}(x)=(x-\beta^۵)(x-\beta^{۱۰})=x^۲-(\beta^۵+\beta^{۱۰})x+\beta^{۱۵}$$

اما طبق جدول قبل داریم: $\beta^۵+\beta^{۱۰}=۰۱۱۰+۰۱۱۱=۰۰۰۱=\beta^۰=۱$

و چون $\beta^{۱۵}=۱$، داریم $m_۵(x)=m_{۱۰}(x)=x^۲+x+۱$

سایر چند جمله‌ای های مینیمال نیز به طور مشابه، محاسبه می‌شوند. لیست کامل به صورت زیر است.

$$m_۰(x)=x+۱$$
$$m_۱(x)=m_۲(x)=m_۴(x)=m_۸(x)=x^۴+x+۱$$
$$m_۳(x)=m_۶(x)=m_۹(x)=m_{۱۲}(x)=x^۴+x^۳+x^۲+x++۱$$
$$m_۵(x)=m_{۱۰}(x)=x^۲+x+۱$$
$$m_۷(x)=m_{۱۱}(x)=m_{۱۳}(x)=m_{۱۴}(x)=x^۴+x^۳+۱$$

گروه خودریختی $F_q n$

حال می‌خواهیم، گروه خودریختی‌های یک میدان تعمیم یافته را مشخص کنیم.

تعریف: یک خودریختی (*automorphism*) از $f_q n$ روی f_q، یک نگاشت دوسویی $\sigma: F_q n\to F_{q^n}$ است که در آن:

۱) $\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$ ۲) $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$

۳) اگر $a \in F_q$ آنگاه $\sigma(a)=a$

شرط آخر، بیان می کند که σ روی F_q را ثابت نگه می دارد.

قضیه: مجموعهٔ خودریختی های F_{q^n} روی F_q یک گروه دوری از مرتبه n تشکیل می‌دهند (تحت ترکیب توابع) که توسط نگاشت $\sigma_q(\alpha)=\alpha^q$ تولید شده است.

اثبات: فرض کنید β یک عضو اولیه از F_qn باشد. در این صورت β دارای مرتبه $q^n-۱$ است و لذا چند جمله‌ای مینیمال آن $m(x)$، دارای ریشه‌های زیر است.

$$\beta, \beta^q, \beta^{q^۲}, ..., \beta^{q^{n-۱}}$$

حال، فرض کنید $f(x)$ یک چندجمله‌ای روی F_q باشد. چون یک خودریختی τ از F_qn روی F_q ، ضرایب $f(x)$ را ثابت نگه می‌دارد، می‌بینیم که $f(\alpha)=۰$ ، اگر و تنها اگر $f(\tau(\alpha))=۰$. به بیان دیگر، τ ریشه‌های $f(x)$ را که در F_qn هستند،جایگشت می‌دهد. به خصوص τ می‌بایست β (ریشه $m(x)$) را به ریشه‌دیگری تصویر کند، یعنی $\tau(\beta)=\beta^{q^i}$ (برای مقداری i). اما چون β یک عضو اولیه از F_qn است، τ کاملاً توسط مقادیر آن روی β تعیین می‌شود و چون:

$$\sigma_q{}^i(\beta)=\beta^{q^i}=\tau(\beta)$$

نتیجه می گیریم که $\tau=\sigma_q^i$. بنابراین، تمامی خودریختی‌های F_qn روی F_q به شکل σ_q^i هستند (برای مقداری i).

ریشه‌های واحد (*The roots of unity*)

در این بخش با این سوال که چگونه می‌توانیم چند جمله‌ای $x^n-۱$ را روی یک میدان متناهی مانند F_q تجزیه کنیم، پاسخ می‌دهیم. این سوال، ما را به بحث کدهای دوری راهنمای می کند. اگر q,n نسبت به هم اول نباشند، آنگاه می توانیم بنویسیم $n=mp^k$ که در آن $(m,q)=۱$ و P مشخصه F_q است. در این حالت:

$x^n - ۱ = x^{mpk} - ۱ = (x^m - ۱)^{pk}$

بنابراین، از اینجا به بعد فرض خواهیم کرد q,n نسبت به هم اول هستند.

توجه: فرض کنید $F_q s$، میدان شکافنده $x^n - ۱$ روی F_q باشد. در این صورت چند جمله‌ی $x^n - ۱$ دارای ریشه تکراری در هیچ یک از توسیع های F_q نیست، زیرا

$d(x^n - 1) = nx^{n-1}$

دارای هیچ ریشه مشترکی با $x^n - ۱$ نیست. بنابراین $x^n - ۱$ دارای n ریشه متمایز در میدان شکافنده $F_q s$ است. (توجه دارید که این مستلزم آن است که $(n,q) = ۱$).

تعریف: ریشه‌های $x^n - ۱$ در میدان شکافنده $F_q s$، ریشه‌های nام واحد در F_q نامیده می-شوند. مجموعه ریشه‌های nام واحد با $E^{(n)}$ نمایش داده می‌شوند.

نکته: توجه دارید که ریشه‌های nام واحد، حتی زمانی که a,n نسبت به هم اول نباشند تعریف شده هستند. اما در این حالت، تعداد ریشه‌های متمایز، کمتراز n خواهد بود.

زمانی که $(n,q) = ۱$، مجموعه $E^{(n)}$ دارای ساختار خاص و جالبی خواهد بود.

قضیه: مجموعه $E^{(n)}$ شامل ریشه‌های nام واحد، یک زیر گروه دوری از اندازه n از گروه ضربی $F_q s^*$ است.

اثبات: از قبل می‌دانیم که $|E^{(n)}| = n$. فرض کنید. $\alpha, \beta \in E^{(n)}$، در اینصورت:

$(\alpha\beta^{-1})^n = \alpha^n(\beta^n)^{-1} = 1 \Rightarrow \alpha\beta^{-1} \in E^{(n)}$

بنابراین $E^{(n)}$ یک زیر گروه دوری از $F_q s^*$ است و لذا دوری است.

تعریف : یک ریشه nام واحد روی F_q که گروه دوری E^n را تولید کند، یعنی یک ریشهٔ n ام واحد از مرتبهٔ n باشد. ریشه اولیه nام واحد روی F_q نامیده می‌شود از اینجا به بعد قرارداد می‌کنیم W یک ریشه اولیه واحد است.

از آنجایی که $E^{(n)}$ دوری است، نتیجه زیر را داریم.

نتیجه: دقیقا $\phi(n)$ریشه n ام اولیه واحد روی F_q وجود دارند. به خصوص، چون $\phi(n) > ۰$، یک ریشه اولیه nام واحد روی F_q، برای هر عدد صحیح مثبت n که نسبت به q اول باشد، وجود دارد.

توجه: نتیجه فوق، به ما این اجازه را می‌دهد تا یک فرمول ساده برای s (که در آن F_qs یک میدان شکافنده است) برحسب n بیابیم. در این حالت، اگر w ریشه nام اولیه واحد باشد، آنگاه w از مرتبه n بوده و چون $w \neq ۰$ داریم:

$$w \in F_q r \Leftrightarrow w^{q^r} = w \Leftrightarrow w^{q^r - 1} = 1 \Leftrightarrow n \mid q^r - 1$$

چون s کوچکترین عدد r است که در آن $w \in F_q r$، نتیجه زیر را اثبات کرده‌ایم.

نتیجه: اگر F_qs میدان شکافنده $x^n - ۱$ روی F_q باشد، آنگاه s کوچکترین عدد صحیح مثبت است که در آن $n \mid q^s - ۱$، یعنی S کوچکترین عدد صحیح مثبت است. که در $q^s \overset{n}{\equiv} ۱$.
به بیان دیگر، s مرتبه q در پیمانه n است که با $on\ (q)$ نمایش داده می‌شود.

عناصر اولیه میدان و ریشه‌های اولیه واحد

تفاوت بین یک عضو اولیه میدان شکافنده F_qs از $x^n - ۱$ و یک ریشه اولیه nام واحد بسیار حائز اهمیت است. با استفاده از تعریف، β یک عضو اولیه میدان F_qs است.
اگر β گروه دوری F_qs^* را تولید کند. از طرف دیگر، با استفاده از تعریف، w یک ریشه nام اولیه واحد است، اگر آن زیر گروه دوری $E^{(n)}$ را تولید کند. بنابراین

$\beta \Leftrightarrow F_qs^* = \{۱, \beta, \beta^۲, \ldots\}$ عضو اولیه F_qs است

$w \Leftrightarrow E^{(n)} = \{1, w, w^2, \ldots\}$ یک ریشه n ام اولیه واحد است.

اما، توجه دارید که یک ریشه اولیه n ام واحد w، F_qs را روی F_q (به عنوان یک عضو میدان که ضرب و جمع را اجازه می‌دهد) تولید می کند. یعنی $F_q(w) = F_qs$.

این مطلب، از این واقعیت نتیجه می‌شود:

$$F_q(w) = F_q(E^{(n)}) = F_qs$$

اگر β یک عضو اولیه $F_q s$ باشد، آنگاه β دارای مرتبه $q^{۶}-۱$است. چون $n|q^{۶}-۱$ پس $q^n-۱=nr$ (برای یک $r\in Z$)، بنابراین:

$$O(\beta^k)=\frac{q^{۶}-۱}{(k,q^{۶}-۱)}=\frac{nr}{(k,nr)}$$

بنابراین، β^k یک ریشه nام اولیه واحد است اگروتنهااگر:

$$\frac{nr}{(k,nr)}=n$$

یا به طورهم ارز $(k,nr)=r$، اما این، رابطه برقرار است اگروتنها اگر $K=ra$، جایی که $(u,n)=۱$ چون $\phi(n)$ ریشهnام اولیه دقیقاً وجود دارند، بنابراین قضیه زیر را اثبات کرده‌ایم.

قضیه: فرض کنید β یک عضو اولیه میدان شکافنده $F_q s$ از $x^n-۱$ باشد در این صورت $\phi(n)$ ریشه اولیه nام واحد روی F_q، دقیقا به صورت زیر هستند.

$$\{\beta^k \mid k=\frac{q^s-۱}{n}u, u<n, (u,n)=۱\}$$

به خصوص، $\beta^{\frac{q^s-۱}{n}}$ یک ریشه nام اولیه واحد است.

اثبات: قضیه زیر به عنوان تمرین واگذاری می‌شود.

قضیه: فرض کنید F_q یک میدان متناهی باشد. همچنین فرض کنید Ωمجموعهٔ ریشه‌های nام اولیه روی F_q باشد و F مجموعهٔ عناصر اولیه میدان شکافنده $F_q s$ از $x^n-۱$ باشد. در این صورت، یا $\Omega\cap F=\phi$ یا در غیراینصورت $\Omega=F$؛ همچنین حالت دوم در زمانی رخ می‌دهد که $n=q^s-۱$.

روشی برای تجزیه $x^{n-۱}$

برای $(n,q)=۱$، می‌توانیم چندجمله‌ای $x^n-۱$ را روی F_q، با استفاده از این واقعیت که $x^n-۱$ دارای n ریشه، متمایز است که، تجزیه کنیم. بنابراین $x^n-۱$ حاصل ضرب چند جمله‌ای های مینیمال متمایز این ریشه‌هاست. این چندجمله‌ای های مینیمال می‌توانند با استفاده از روش های موجود در بخش قبل، محاسبه شوند. اشکال اصلی این روش این است

که ما باید در میدان شکافندهٔ F_{q^s}: (که یک میدان بزرگتر است) کار کنیم. فرض کنیم β یک عوض اولیه F_{q^s} باشد که در آن $S = o_n(q)$. با استفاده از مطالب قبل، می‌توانیم یک ریشه nام اولیه واحد w را به صورت زیر بدست آوریم.

$$w = \beta \frac{q^s - ۱}{n}$$

بنابراین، ریشه‌های $x^n - ۱$ به صورت زیر هستند.

$$۱, w, w^۲, \ldots, w^{n-۱}$$

حال، تنها چیزی که نیاز داریم محاسبه چند جمله‌ای های مینیمال این ریشه‌ها و سپس ضرب نمودن این چندجمله‌ای های متمایز است. برای $i = ۰, \ldots, n-۱$، مزدوج‌های w^i به صورت زیر می‌باشند.

$$w^i, w^{qi}, w^{iq^۲}$$

جایی که d کوچکترین عدد صحیح مثبت است که در آن $w^{iq^d} = w^i$. اما

$$w^{iq^d} = w^i \Leftrightarrow w^{iq^{d-1}} = 1 \Leftrightarrow n \mid iq^{d-1} \Leftrightarrow iq^d \overset{n}{\equiv} i$$

بنابراین، می‌توانیم شرط $iq^d \overset{n}{\equiv} i$ را برای تعیین تمامی مزدوج‌ها به کار بریم.

لذا، چند جمله‌ای مینیمال ریشه‌های $x^n - ۱$ به صورت زیر است:

$$m_i(x) = \left(x - w^i\right)\left(x - w^{iq}\right)\left(x - w^{iq^2}\right) \ldots \left(x - w^{iq^{d-1}}\right)$$

جایی که d کوچکترین مقدار صحیح مثبت است که در آن $iq^d \overset{n}{\equiv} i$.

تعریف: مجموعه $C_i = \{i, iq, \ldots, iq^{d-۱}\}$، جایی که d کوچکترین عدد صحیح مثبت باشد که در آن $iq^d \overset{n}{\equiv} i$، iامین هم دسته دوری (*i-Th cyclotomic coset*) برای q در پیمانه n نامیده می‌شود. این مجموعه ها می‌توانند بدون مراجعه خاص به یک دسته nام اولیه واحد تعریف شوند. حال در اینجا، مثالی برای روشن شدن بحث می‌آوریم.

مثال: چند جمله‌ای $h_{۱۵}(x) = x^{۱۵} - ۱$ روی $F_۲$ را در نظر بگیرید.

در اینجا $q=۲, n=۱۵$. چون $S=O_{15}(2)=4$، میدان شکافنده $h_n(x)$ به صورت $F_q s=F_{۱۶}$ است. از طرف دیگر چندجمله‌ای $x^۴+x+۱$ یک چند جمله‌ای اولیه روی $F_۲$ می‌باشد، بنابراین اگر β ریشه این چند جمله‌ای باشد، β یک عضو اولیه از میدان $F_{۱۶}$ می‌باشد. با استفاده از β، می‌توانیم w را به عنوان ۱۵ امین ریشه اولیه واحد بیابیم:

$$w=\beta^{\frac{q^6-1}{n}}$$

در این حالت، β هم یک عضو اولی و هم یک ریشه اولیه خواهد بود. بنابراین، $x^{۱۵}-۱$ به صورت زیر هستند:

$$۱,\beta,\beta^۲,....\beta^{۱۴}$$

چندجمله‌ای مینیمال این ریشه‌ها، قبلا محاسبه شده اند (دریک مثال). بنابراین:

$$x^{۱۵}-۱=(x+۱)(x^۴+x+۱)(x^۴+x^۳+x^۲+x+۱)(x^۲+x+۱)(x^۴+x^۳+۱)$$

مثال: برخی اوقات، اطلاع از هم دسته‌های دوری می‌تواند تجزیه خاصی از $x^n-۱$ را به ما نشان دهد (یعنی همان تجزیه و چند جمله‌ای های تحویل ناپذیر). برای نمونه، چندجمله‌ای $x^۹-۱$ روی $F_۲$ را در نظر بگیرید. چون $q=۲$ و $n=۹$، هم دسته های دوری به صورت زیر می‌باشند.

$$C_۰=\{۰\},C_۱=\{۱,۲,۴,۸,۷,۵\},C_۳=\{۳,۶\}$$

بنابراین $x^۹-۱$ را می‌توان به عوامل خطی تحویل ناپذیر، یک عامل درجه دو تحویل ناپذیر و یک عامل تحویل ناپذیر از درجه ۶ تجزیه کرد. اما، به آسانی می‌توان دید که روی $F_۲$ داریم:

$$x^۹-۱=(x^۳)^۳-۱=(x^۳-۱)(x^۶+x^۳+۱)=(x-۱)(x^۲+x+۱)(x^۶+x^۳+۱)$$

و بنابراین، تجزیه خواسته شده، حاصل می گردد.

مرتبه چند جمله‌ای تحویل ناپذیر

یادآوری می کنیم که مرتبه $o(f)$ از یک چند جمله‌ای تحویل ناپذیر $f(x)$ با مرتبه هر یک از ریشه‌های آن در میدان شکافنده $F_q d$ از $f(x)$ برابر است.

قضیه: فرض کنید $f(x)$ یک چند جمله‌ای تحویل ناپذیر روی F_q باشد.

۱) اگر $\deg(f(x))=d$ آنگاه $o(f)\,|\,q^d-1$

۲) $f(x)\,|\,x^n-1 \Leftrightarrow o(f(x))\,|\,n$

۳) $o(f)$ کوچکترین عدد صحیح مثبت e است به طوری که $f(x)\,|\,x^e-1$

اثبات:

۱) چون $split(f)=F_{q^d}$، پس هر ریشه $f(x)$ یک ریشه از $x^{q^d-1}-1$ نیز هست و لذا مرتبه آن ریشه، q^d-1 را عاد می‌کند. لذا $o(f)\,|\,q^d-1$.

۲) هر ریشه $f(x)$ متعلق به $split(f)$، دارای مرتبه $o(f)$ است و لذا یک ریشه از چند جمله‌ای $x^{o(f)}-1$ است. لذا $f(x)\,|\,x^{o(f)}-1$.

۳) اگر $f(x)\,|\,x^n-1$ آنگاه هر ریشه $f(x)$ یک ریشه از چند جمله‌ای x^n-1 است و لذا مرتبه آن، مقسوم علیه‌ای از n است. یعنی، $o(f)\,|\,n$. برعکس، اگر $n=ko(f)$ آنگاه $x^{o(f)}-1\,|\,x^{ko(f)}-1=x^{n=1}$ و مابقی اثبات، با توجه به قسمت (۲) بدیهی است.

۴) این قسمت، با توجه به قسمت (۳) نتیجه می‌شود.

نکته می‌توانیم درجه d یک چند جمله‌ای تحویل ناپذیر از مرتبه E را به صورت زیر بیابیم.

اگر $\propto$ ریشه‌ای از $f(x)$ رد F_{q^d} باشد، آنگاه طبق قضیه‌ای از قبل داریم:

$$F_q\propto = F_q(\propto)$$

اما $\propto$، eامین ریشه اولیه واحد است و لذا:

$$F_q(\propto)=F_q(E^{(n)})=split(x^e-1)=F_{q^s}$$

جایی که $s=o_e(q)$. بنابراین $d=s=o_e(q)$.

قضیه فرض کنید $f(x)$ یک چند جمله‌ای تحویل ناپذیر روی F_q با مرتبه $o(f)$ باشد. در این صورت درجه $f(x)$، همان مرتبه q در پیمانه $o(f)$ است. به عبارت دیگر.

$$\deg(f(x))=o_{o(f)}(q)$$

نتیجه اگر $f(x)$ یک چند جمله‌ای اولیه برای $F_q n$ روی F_a باشد، آنگاه $\deg(f(x))=n$.

نکته: با توجه به قضیه قبل، توجه داریم که مرتبه یک چند جمله‌ای تحویل ناپذیر، درجه آن چند جمله‌ای را تعیین یم‌کند. (به طور یکتا)؛ اما عکس آن همواره بر قرار نیست. به طور مثال چند جمله‌ای $f(x)=x^۴+x+۱$ و $p(x)=x^۴+x^۳+x^۲+x+۱$ ، هر دو دارای درجه ۴ هستند. اما $o(f(x))=۱۵$, $o(p(x))=۵$. اما قضیه زیر، در حالت خاص، زمانی که چند جمله‌ای تحویل ناپذیر $f(x)$ روی F_q ، در میدان گسترش یافته $F_q n$ تحویل ناپذیر باشد، می‌توان مرتبه آن چند جمله‌ای را از روی درجه آن بیابد.

قضیه فرض کنید $f(x)$ یک چند جمله ای تحویل ناپذیر روی F_q باشد. در این صورت چند جمله‌ای $f(x)$ را می‌توان در میدان گسترش یافته $F_q n$ به (n,d) چند جمله‌ای تحویل ناپذیر، هر یک با درجه $\frac{d}{(n,d)}$ تجزیه کرد و بخ خصوص f روی $F_q n$ تحویل ناپذیر است اگر و تنها اگر $(n,d)=۱$.

محاسبه مرتبه یک چند جمله‌ای تحویل ناپذیر

فرض کنید $f(x)$ یک چند جمله‌ای تحویل ناپذیر با درجه d باشد. می‌خواهیم مرتبه f را بیابیم. ابتدا $q^d-۱$ را به عوامل اول آن تجزیه می‌کنیم.

$$q^d-۱=\prod_i p_i^{r_i}$$

حال، چون $o(f)\mid q^d-۱$، داریم:

$$p^{ri}\mid o(f)\Leftrightarrow o(f)\nmid\frac{q^d-۱}{p_i}\Leftrightarrow f(x)\nmid\frac{(q^d-۱)}{p^i}-۱\Leftrightarrow_x\frac{q^d-۱}{p_i}\overset{f(x)}{\not\equiv}۱$$

بنابراین، با محاسبه باقی مانده‌های $x^{\frac{q^d-۱}{p_i}}$ (درپیمانه $f(x)$)، می‌توانی بیشترین توان هر p_i که $o(f)$ را عاد می‌کند. بیابیم.

مثال: چند جمله‌ای تحویل ناپذیر $f(x)=x^6+x+1$ روی F_2 را در نر بگیرید. چون $q=2$، داریم $q^6-1=63=3^2\times 7$. حال می‌بینیم که 3^2، مرتبه f یا $o(f)$ را عاد می‌کند یا خیر.

چون $\frac{63}{3}=21$، درایم: $3^3\,|\,o(f) \Leftrightarrow x^{21}\not\equiv 1 \bmod(x^6+x+1)$

اما به سادگی می‌توان دید: $x^{21}\underline{\underline{\underline{x^6+x+1}}}\ x^2+x\not\equiv 1$ و لذا $3^2\,|\,o(f)$ حال

عدد اول ۷ را بررسی می‌کنیم. داریم: $V\,|\,o(f) \Leftrightarrow x^9 \not\equiv (moc(x^6+x+1))$

اما $x^9 \bmod(x^6+x+1)$، لذا $v\,|\,o(f)$. بنابراین $o(f)=63$. لذا f یک چندجمله‌ای اولیه روی F_2 است.

مثال

چندجمله‌ای تحویل ناپذیر $g(x)=x^6+x^4+x^2+x+1$ را در نظر بگیرید. در این حالت داریم:

$$3^2 lo(g) \Leftrightarrow x^{21}\not\equiv 1 \bmod(x^6+x^4+x^2+x+1)$$

اما $x^{21} \bmod(x^6+s^4+x^2+x+1)=1$ و لذا $3^2 \nmid o(f)$ بنابراین بایدمقسوم علیه **۳** را بررسی کنیم.

$$3^2 lo(g) \Leftrightarrow x^7\not\equiv 1 \bmod(x^6+x^4+x^2+x+1)$$

اما $x^7 \bmod(x^6+x^4+x^2+x+1)=x^5+x^3+x^2+x\neq 1$؛ لذا $3lo(g)$. سرانجام،بایدعامل را بررسی کنیم.

$$7lo(g) \Leftrightarrow x^9\not\equiv 1 \bmod(x^6+x^4+x^2+x+1)$$

چون $x^9 \bmod(x^6+x^4+x^2+x+1)=x^4+x^2+1\neq 1$؛ لذا $7lo(g)$.پس $lo(g)=21$

کدهای دوری یا (*Cylcic codes*)

کدهای دوری، به دلایل بسیاری مهم هسند. جدا از این که این کد ها دارای ساختار ریاضی بسیار غنی هستند این کد ها از دیدگاه عملی نیز حائز اهمیت هسند؛ زیرا کد گذاری و کدگشایی این کد ها با استفاده از مدارهای سوئیچ کننده خطی به روش کاملاً کارایی صورت می‌گیرد.

در سراسر بح خود درباره کدهای دوری، فرض بر این است که q,n نسبت به هم اول هستند. به خصوص، اگر $q=۲$ آنگاه n باید فرد باشد. حال بیایید تعریف کد های دوری را مرور کنیم اگر L یک کد خطی q- تایی باشد، آنگاه به هر کد کلمه $C = C_{\circ}C_{۱}$ در L، یک چند جمله‌ای از $F_q[x]$ به صورت زیر را نسبت می‌دهیم.

$$\phi : c_{\circ}c_{۱}...c_{n-۱} \rightarrow c_{\circ} + c_{۱}x + ... + c_{n-۱}x^{n-۱}$$

نگاشت ϕ یک یکریختی فضای برداری از L به زیر فضای $\phi(L)$ از $F_q[x]$ است. به طور معمول، از این نگاشت صرف نظر کرده و کد کلمات در L را به صورت چند جمله‌ای در نظر می گیریم و ****

تعریف: یک کد خطی $L \subseteq V(n,q)$ خطی است، اگر:

$$c_{\circ}c_{۱}....c_{n-۱} \in L \Rightarrow c_{n-۱}c_{\circ}c_{۱}...c_{n-۲} \in L$$

در این حالت، اگر کد کلمات را به صورت جند جمله‌ای در نظر بگیریم، کد L خطی است اگر ایده‌الی از حلقه $R_n = \dfrac{Fa[x]}{< x^n - ۱ >}$ باشد.

یادآوری می کنیم که R_n مجموعه تمای چند جمله‌ای های روی F_q با درجه کمتر از n است جمع و ضرب در R_n، مانندجمع و ضرب چند جمله‌ای ها در $F_q[x]$ است، با این تفاوت که به جای x^n، قرار می‌دهیم ۱، (یعنی $x^n = ۱$)، چون تمامی چند جمله‌ای ها در پیمانه $x^n = ۱$ هستند، این نماد را به کار می گیریم که $f(x) \equiv q(x)$ معرف هم نهشتی در پیمانه $x^n = ۱$ باشد.

توجه داریم که مطابقه با تعریف، کد خطی C دوری است اگر تحت شیفت دوری زیر بسته باشد.

$$c_{\circ}c_{۱}...c_{n-۱} \rightarrow c_{n-۱}c_{\circ}c_{۱}...v_{n-۲}$$

در این حالت، می‌توان دید که C تحت جایگشت‌های دوری نیز پایاست.

$$c_{\circ}c_{۱}...c_{n-۱} \rightarrow c_{n-۱}c_{\circ}c_{۱}...v_{n-۲}$$

اگر $p(x) \in R_n$ ، آنگاه ایده‌هال تولید شده توسط $p(x)$ که با $< p(x) >$ نمایش داده می‌شود، کوچکترین ایده‌ال در R_n شامل $p(x)$ است، به عنوان تمرین، می‌توان دید:

$$< p(x) >= \{ f(x)p(x) \mid f(x) \in R_n \}$$

جایی که تمامی چند جمله‌ای هادر پیمانه $x^n - ۱$ حساب شده‌اند.

چندجمله‌ای مولد یک کد دوری

قضیه زیر شامل برخی واقعیت های اساسی درباره کدهای دوری است. در واقع این قضیه مبین این مطلب است که R_n یک حلقه ایده‌ال های اصلی است.

۱) یک چند جمله‌ای تکین یکتا با کمترین درجه در C وجود دارد. این چند جمله‌ای، کد C را تولید می‌کند. یعنی $C =< g(x) >$؛ $g(x)$ چند جمله‌ای مولد نامیده می‌شود. (توجه داریم که چندجمله‌ای مولد یکتانیست، یعنی تنها چند جمله‌ای نیست که کد C را تولید می‌کند.)

۲) $g(x) \mid x^n - ۱$

۳) اگر $\deg(g(x)) = r$ آنگاه C دارای بعد n-r است. در واقع

$$C =< g(x) >= \{ r(x)g(x) \mid \deg r(x) < n - r \}$$

۴) اگر $g(x) = g_۰ + g_۱x + ... + g_rx^r$ آنگاه $C, g_۰ \neq ۰$ دارای ماتریس مولد زیر است.

$$G = \begin{pmatrix} g_۰ & g_۱ & g_۲ & \cdots & g_r & ۰ & ۰ & \cdots & ۰ \\ ۰ & g_۰ & g_۱ & g_۲ & \cdots & g_r & ۰ & \cdots & ۰ \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ ۰ & ۰ & g_۰ & g_۱ & g_۲ & \cdots & ۰ & \cdots & g_۲ \end{pmatrix}$$

جایی که هر سطر G، شیفت دوری سطر قبلی است.

اثبات: ۱) فرض کنید C شامل دو چند جمله‌ای تکین متمایز $g_۲(x), g_۱(x)$ با کمترین درجه r باشد. آنگاه $g_۱(x) - g_۲(x)$ یک چند جمله‌ای ناصفر در C با درجه کمتر از r است که تناقض است بنابراین تنها یک چند جمله‌ای تکین با درجه r در C وجود دارد.

چون $g(x) \in C$ و C یک ایده‌آل است، داریم $< g(x) > \subseteq C$. از طرف دیگر، فرض کنید $p(x) \in C$ و قرار دهید، $p(x) = q(x)g(x) + r(m)$ جایی که $\deg r(x) < r$.

در این صورت $r(x)=p(x)-q(x)g(x)\in C$ دارای درجه کمتر از r است که متناقض است. پس $r(x)=0$، و لذا $p(x)=q(x)g(x)\in <g(x)>$. بنابراین $C\subseteq <g(x)>$ و؛ در نتیجه $C=<g(x)>$.

۳) ایده‌آل تولید شده توسط $g(x)$ به صورت زیر است.

$$<g(x)>=\{f(x)p(x) \mid f(x)\in R_n\}$$

که در پیمانه x^n-1 محاسبه شده است، باید نشان دهیم که کافی است $f(x)$ را به چند جمله‌ای های با درجه کمتر از n-r تحدید کنیم. می‌دانیم $g(x)\mid x^n-1$ و $x^n-1=h(x)g(x)$، برای یک چند جمله‌ای $h(x)$ با درجه n-r. حال اگر $f(x)$ را بر $h(x)$ تقسیم کنیم، داریم:

$$f(x)=q(x)h(x)+r(x)$$

جایی که $\deg(r(x))<n-r$. در این صورت:

$$f(x)g(x\cdot)=q(x)h(x)g(x)+r(x)g(x)=q(x)(x^n-1)+r(x)g(x)$$

و لذا در R_n، داریم $f(x)g(x)=r(x)g(x)$ که همان است که می‌بایست نشان می‌دادیم.

همچنین می‌توان نشان داد که مجموعه $C,\{g(x),x(x),...,x^{n-r-1}g(x)\}$ را تولید می‌کند و چون این مجموعه، مستقل خطی نیز می‌باشد، یک پایه برای C است. بنابراین $\dim(C)=n-r$.

۴) اگر $g_0=0$، انگاه $g(x)=xg_1(x)$ جایی که $\deg(g_1(x)<r$. اما در این صورت داریم: $g_1(x)=\log_1(x)\equiv x^n.g_1(x)=x^{n-1}g(n)$، بنابراین $g_1(x)\in C$ که با این واقعیت که هیچ چند جمله‌ای در C دارای درجه کمتر r است، در تناقض می‌باشد. بنابراین $g_0\neq 0$. سرانجام، G یک ماتریس مولد C است، زیرا $\{g(x),xg(x),...,x^{n-r-1}g(x)\}$ یک پایه برای C است.

توجه یک کد دوری می‌تواند توسط چند جمله‌ای بجز چند جمله‌ای مولد، تولید شود.

مثال کدو دوری $C=<1+x>$ در $R_3=\dfrac{F_2[x]}{<x^3-1>}$ را در نظر بگیرید. با توجه به قضیه قبل می‌دانیم: $\dim(C)=3-1=2$ و C شامل کد کلمات زیر است:

$$\circ, 1+x, x(1+x)=x+x^2, (1+x)(1+x)=1+x^2$$

بنابراین:

$$C=\{\circ, 1+x, 1+x^2, x+x^2\}=\{000, 110, 101, 011\}$$

خواننده می‌تواند نشان دهد که:

$$<1+x^2>=\{f(x)(1+x^2)\mid f(x)\in R_3\}=C$$

و لذا C توسط چند جمله‌ای $1+x^2$ نیز تولید شده است.

نکته: در مثال قبل، دیدیم $C=<1+x>=<1+x^2>$. می‌توانیم نماد $C=<<p(x)>>$ را قرار داد کنیم که در آن C توسط $p(x)$ تولید شده و $p(x)$ یک چند جمله‌ای مولد برای C است.

یک چند جمله‌ای با کمترین درجه و تکین در C. فرض کنید $p(x)$ یک چند جمله‌ای تکین در R_n باشد و $C=<p(x)>$ کد دوری تولید شده توسط $p(x)$ باشد. اگر $x^n-1, p(x)$ را عاد نکند، آنگاه مطابق قضیه قبل، $p(x)$ نمی‌تواند یک چند جمله‌ای مولد برای یک کد دروی است اگر و تنها اگر $p(x)\mid x^n-1$.

اثبات: یک طرف آن را ثابت کنیم. برای اثبات عکس آن، فرض کنید $p(x)\mid x^n-1$ و نیز فرض کنید $g(x)$ چند جمله مولد کد $C=<p(x)>$ باشد. فرض کنید $p(x)\neq g(x)$، چون $p(x)$ و $g(x)$ هر دو تکین هستند، داریم $\deg(p(x))>\deg(g(x))$.

با استفاده از فرض، $x^n-1=p(x)f(x)$ برای یک چند جمله‌ای $f(x)$. علاوه بر این چون $g(x)\in<p(x)>$، داریم $g(x)\equiv a(x)p(x)$، برای یک $a(x)\in R_n$.

حال با ضرب طرفین در $f(x)$ داریم:

$$g(x)f(x)=a(x)p(x)f(x)\equiv a(x)(x^n-1)\equiv \circ$$

اما $\deg(g(x)f(x))<\deg p)x(f(x))=n$ و لذا $g(x)f(x)=\circ$ که غیر ممکن است بنابراین $p(x)=g(x)$.

نکته: قضیه فوق مبین این مطلب است که نگاشت $\phi: g(x) \to << g(x) >>$ که هر چند جمله‌ای تکین $g(x)$، که در آن $g(x) | x^n - ۱$، را به کد دوری $<< g(x) >>$ می‌برد. یک تناظر یک به یک بین مجموعه $x^n - ۱$ و مجموعه I_n شامل تمامی کدهای دوری در R_n است. این مطلب نشان می‌دهد که چرا می‌توانیم $x^n - ۱$ را روی یک میدان متناهی تجزیه کنیم.

مثال: از قبل دیدیم که چند جمله‌ای $x^n - ۱$روی $F_۲$ را می‌تواند به عوامل تحویل ناپذیر به صورت زیر تجزیه کرد:

$$x^۹ - ۱ = (x-۱)(x^۲ + x + ۱)(x^۶ + x^۳ + ۱)$$

بنابراین $۸ = ۲^۳$ کد دوری در R_q وجود دارد. برای نمونه، کد دوری $C_۱ = << x^۶ + x^۳ + ۱ >>$ دارای بعد $۹-۶=۳$ و ماتریس مولد زیر است.

$$G_۱ = \begin{pmatrix} ۱ & ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۰ \\ ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ \\ ۰ & ۰ & ۱ & ۰ & ۰ & ۱ & ۰ & ۰ & ۱ \end{pmatrix}$$

مثال: $x^{۲۳} - ۱$ روی $F_۲$ را می‌توان به عوامل تحویل ناپذیر به صورت زیر تجزیه کرد:

$$x^{۲۳} - ۱ = (x+۱)(x^{۱۱} + x^۹ + x^۷ + x^۶ + x^۵ + x + ۱)(x^{۱۱} + x^{۱۰} + x^۶ + x^۵ + x^۴ + x^۲ + ۱)$$

نیز، می‌توان نشان داد که کد دوری دوتایی $C_۱ = << x^{۱۱} + x^{۱۰} + x^۶ + x^۵ + x^۴ + x^۲ + ۱ >>$ دارای پارامترهای مشابه با کد گلی $G_{۲۳}$ است. جزئیات آن تقریبا واضح است. بنابراین با توجه به قضیه یکتایی برای کدهای گلی $G_{۲۳}$ هم ارز با کد دوری $C_۱$ است.

به روش مشابه، روی $F_۳$ داریم:

$$x^{۱۱} - ۱ = (x-۱)(x^۵ + x^۴ - x^۳ + x^۲ - ۱)(x^۵ - x^۳ + x^۲ - x - ۱)$$

و کد دوتایی سه تایی $C_۲ = << x^۵ + x^۴ + x^۳ + x^۲ - ۱ >>$دارای پارامترهای مشابه با کد گلی $G_{۱۱}$ است. بنابراین $G_{۱۱}$هم ارز با کد دوری $C_۲$ است.

نکته: نگاشت $\phi: g(x) \rightarrow << g(x) >>$ با توجه به ترتیب جزئی روی P_n و I_n دارای خواص مشابهی است توجه کنید اگر $C_۲,C_۱$ در R_n دوری باشند، آنگاه مجموع:

$$C_۱ + C_۲ = \{c_۱ + c_۲ \mid c_۱ \in c_۱, C_۲ \in C_۲\}$$

کوچکترین کد دوری شامل $C_۲,C_۱$ در R_n است. کسانی با اصطلاح شبکه (*lattice*) آشنا باشند، متوجه می‌شوند که ϕ یک پاد یکریختی (*onti-isomorphism*) از شبکه $(Q_n,۱)$ به شبکه $(I_n,۱)$است. اثبات قیه زیر را به عنوان یک تمرین به خواننده واگذاری می‌کنیم.

قضیه: فرض کنید $C_۲ << g_۲(x) >>, C_۱ = << g_۱(x) >>$ کدهای دوری در R_n باشند. در این صورت.

۱) $C_۱ \subset C_۲$ ارگ و تنها اگر $g_۲(x) \mid g_۱(x)$.

۲) $C_۱ \cap C_۲ = << lcm(g_۱(x), g(x)) >>$ ($lcm(a,b)$، کوچکترین مضرب مشترک b,a است)

۳) $C_۱ + C_۲ = << \gcd(g_۱(x), g(x)) >>$

چندجمله‌ای توازن یک کد دوری

از آنجایی که چند جمله‌ای مولد $g(x)$ از یک کد دوری $[n, n-r]$ در $x^n - ۱, R_n$ را عاد می‌کند، داریم.

$$x^n - ۱ = g(x)h(x)$$

جایی که $h(x)$ یک چند جمله‌ای از درجه *n-r* است. چند جمله‌ای توازن (*chack polynomial*)C نامیده می‌شود. این مطلب، در قضیه بعد آمده است.

قضیه: فرض کنید $h(x)$ یک چند جمله‌ای توازن یک کد دوری C در R_n باشد. در این صورت:

۱) کد C می‌تواند به صورت زیر توصیف شود:

$$C = \{p(x) \in R_n \mid P(x)h(x) \equiv ۰\}$$

۲) اگر $h(x)=h_0+h_1x+....+h_{n-r}x^{n-r}$، آنگاه یک ماتریس بررسی توازن کد C به صورت زیر است.

$$H=\begin{pmatrix} h_{n-r} & 0 & h_0 & 0 & 0 & 0 \\ 0 & h_{n-r} & \cdots & h_0 & 0 & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \\ 0 & \dots & 0 & h_{n-r} & \cdots & h_0 \end{pmatrix}_{r\times n}$$

۳) کددوگان یا $C^{\perp}$، کد دوری با بعد r و ماتریس مولد زیر است:

$$h^{\perp}(x)=h_0^{-1}x^{n-r}h(x^{-1})=h_0^{-1}(h_0x^{n-r}+h_1x^{n-r-1}+...+h_{n-r})$$

جایی که چندجمله‌ای آخر در پرانتز، چند جمله‌ای معکوس (*reverse polynomial*)، چند جمله‌ای توازن $h(x)$ است (توجه کنید $C^{\perp}$، توسط $h(x)$ تولید نشده است)

اثبات: ۱- فرض کنید $g(x)$، چند جمله‌ای مولد C باشد اگر $p(x)\in C$، آنگاه $p(x)=t(x)g(x)$ برای یک $f(x)\in R_n$ بنابراین

$$p(x)h(x)=f(x)g(x)h(x)=f(x)(x^n-1)\equiv 0$$

از طرف دیگر، اگر $p(x)h(x)\equiv 0,\ p(x)\in R_n$، آنگاه می‌نویسیم.

$$p(x)=q(x)g(x)+r(x)$$

جایی که $\deg(r(x))<r$. با ضرب طرفین در $h(x)$ داریم:

$$p(x)h(x)=q(x)g(x)h(x)+r(x)+r(x)h(x)$$

با توجه به این رابطه داریم $r(x)h(x)\equiv 0$ اما $\deg(r(x)h(x))<r+(n-r)=n$

در نتیجه $r(x)h(x)=0$. بنابراین $r(x)=0$ و $p(x)=q(x)g(x)\in C$.

۲) اگر $c(x)\in C$، انگاه $c(x)h(x)\equiv 0$ حال $\deg(C(x)h(x))<2n-r$ و با توجه به این مطلب نتیجه می‌گیری که ضرایب $x^{n-r},x^{n-r+1},...,x^{n-1}$ در حاصل ضرب $C(x)h(x)$ باید صفر باشد، یعنی.

$$\begin{cases} C_0 h_{n-r} + C_1 h_{n-r-1} + \ldots + c_{n-r} h_0 = 0 \\ C_1 h_{n-r} + C_2 h_{n-r-1} + \ldots + c_{n-r+1} h_0 = 0 \\ \ldots \\ C_{r-1} h_{n-r} + C_r h_{n-r-1} + \ldots + c_{n-r} h_0 = 0 \end{cases}$$

اما این معادلات، هم ارز با این است که $(C_0 C_1 \ldots C_{n-1})H^t = 0$ و لذا H، کد C' را که بر C عمود است تولید می‌کند، یعنی $C' \subset C^\perp$. اما، چون $h_{n-r} \neq 0$، نتیجه می‌شود $\dim(C') = r$ و لذا $C' \subset C^\perp$.

۳) اگر نشان دهیم $h^\perp(x)$، $x^n - 1$ را عاد می‌کند، آنگاه $h^\perp(x)$ چند جمله‌ای مودر کد دوری $< h^\perp(x) >$ خواهد بود که دارای ماتریس مولد H است؛ بنابراین $< h^\perp(x) > = C^\perp$ اما:

$$h(x)g(x) = x^n - 1$$

ایجاب می‌کند $h(x^{-1})g(x^{-1}) = x^{-n} - 1$ یا $x^{n-r}h(x^{-1})x^r g(x^{-1} = 1 - x^n)$

که نشان می‌دهد: $h^\perp(x) \mid x^n - 1$

مثال کد $C_1 = << x^6 + x^3 + 1 >>$ دارای چند جمله‌ای توازن زیر است:

$(n=9)$ $$h(x) = (x-1)(x^2 + x + 1) = x^3 - 1$$

و چون $h^\perp(x) = x^3(x^{-3} - 1) = x^3 + 1$، کد C_1 دارای ماتریس بررسی توازن زیر است:

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

قضیه: زیر مثالی از آنچه ما می‌توانیم از کدهای دوری با توجه به چندجمله‌ای مولد آن به دست آوریم، معرفی می‌کند.

قضقیه فرض کنید E_n کد زوج دوتایی با طول n باشد. یعنی کد شامل تمامی کد کلمات با وزن زوج در $V(n,2)$. فرض کنید C یک کد دوتایی با طول n باشد. در این صورت:

۱) $E_n = << x - 1 >>$ $\qquad$ $c = << g(x) >> \subset E_n$ اگر و تنها اگر $x - 1 \mid g(x)$

اثبات برای اثبات قسمت ۱) که می‌بینیم که در کد دوری $<<x-1>>$

داریم: $h(x)=\frac{x^n-1}{x-1}=x^{n-1}+x^{n-2}+...+1=h^{\perp}(x)$

و لذا: $<<x-1>>^{\perp}=<<x^{n-1}+x^{n-2}+...+1>>=\{0,1\}$

بنابراین: $<<x-1>>=<<x-1>>^{\perp\perp}=\{0,1\}^{\perp}=E_n$

قسمت ۲) از قسمت (۱) نتیجه می‌شود و این که اگر $<<g_1(x)>>\subseteq<<g_2(x)>>$ انگاه $g_2(x)\,|\,g_1(x)$.

مثال: کد $C_1=<<x^6+x^3+1>>$, $(n=q)$ ، دارای کد کلات با وزن فرد است. زیرا $x-1\nmid x^6+x^3+1$. اما کد $c_2=<<(x-1)(x^6+x^3+1)>>$، زیر کدی از C_1است ه تنها دارای کد کلمات با وزن زوج است.

صفرهای یک کد دوری (*The zeros of a cyclic code*)

اگر بتوانیم ریشه‌های چند جمله‌ای x^n-1 (یعین ریشه‌های nام واحد) را بیابیم، آنگاه قادر خواهمی بود تا کدهای دوری در R_n را مشخص کنیم(با استفاده ازمعرفی چند جمله‌ای مولد آنها).

فرض کنید $x^n-1=\prod_i m_i(x)$ یک تجزیه از x^n-1 به عوامل تحویل ناپذیر تکین روی F_q باشد اگر $\propto$ یک ریشه از $m_i(x)$ (در میدان گسترش یافته ای از F_q) باشد آنگاه $m_i(x)$ چند جمله‌ای کمین (*m.himal*)، $\propto$ روی F_q است. بنابراین برای هر چند جمله‌ای $f(x)\in F_q[x]$ ، داریم $f(x)=0$ ارگ و تنها اگر $f(x)=a(x)m_i(x)$ ، برای یک چند جمله‌ای $a(x)$. به خصوص، اگر $f(x)\in R_n$ آنگاه $f(x)=0$ اگر و تنها اگر $f(x)\in<<m_i(x)>>$.

قضیه فرض کنید $g(x)=q_1(x)....q_t(x)$، حاصلضرب عوامل تحویل ناپذیر x^n-1 باشد و فرض کنید $\{\propto_1,...,\propto_u\}$ ریشه‌های $g(x)$ در میدان شکافنده x^n-1 روی F_q باشد.

در این صورت: $<<g(x)>>=\{f(x)\in R_n\,|\,f(x_1)f(x_2)=...=F(x_u)=0\}$

علاوه بر این، می‌توانیم تنها یک ریشه از هر عامل تحویل ناپذیر $g(x)$ را در نظر بگیریم. یعنی، اگر β_i یک ریشه از $q_i(x)$ (برای $1 \le i \le t$)باشد. آنگاه:

$$<< g(x) >>=\{v(x) \in R_n \mid f(\beta_i) = ... = f(\beta_t) = 0\}$$

تعریف: ریشه‌های چند جمله‌ای مولد یک کد دوری، صفرهای کد نامیه می‌شود. تمامی ریشه‌های دیگر $x^n - 1$، عناصر ناصفر کد نامیده می‌شوند.

تذکر: توجه داشته باشید که اگر $\{\propto_1 ,...,\propto_u\}$ یک مجموعه از ریشه‌های $x^n - 1$ باشند، آنگاه چند جمله‌ای .

مولد کد:

$$C = \{ f(x) \in R_n \mid f(\propto_1) = ... = f(\propto_u) = 0\}$$

کوچکترین مضرب مشترک چندجمله‌ای های مینیمال ریشه‌های $\propto_1 ,...,\propto_u$ می‌باشد.

تذکر نمایش یک کد دوری از طریق صفرهای آن، می‌تواند برای به دست آوردن یک ماتریس بررسی توازن برای کد به کار رود. فرض کنید $\{\propto_1 ,...,\propto_u\}$ مجموعه ای از ریشه‌های $x^n - 1$باشد که متعلق به میدان گسترش یافته $f_q d$ هستند. اگر $f(x) = \sum f_j x^j$ یک چند جمله‌ای در R_n باشد، آنگاه $(x_i) = 0$ اگر و تنها $\sum_1 f_j \propto_i^j = 0$. چون $f_q d$ همچنین می‌تواند به صورت فضای بردای $f_q d$ یا بعد d روی F_q تصور شود، می‌توانیم هر یک از توانهای $\propto_i^j$ را به صورت یک بردار ستونی $[\propto_i^j]$ با طول d روی F_q در نظر بگیریم. علاوه بر این چون $f_j \in F_q$ داریم:

$$[f_j \propto_i^j] = f_j [x_i^j]$$

بنابراین:

$$\sum_i f_j [x_i^j] = [\sum_i f_j \propto_i^j] = 0$$

و قرار دهیم $f = (f_0 ,..., f_{n-1})$ = آنگاه:

$$f(x_i) = (\forall 1 \le i \le u) \Leftrightarrow f\ H^t = 0$$

البته سطرهای H ممکن است مستقل خطی نباشند که در این حالت، با حذف سطرهای وابسته، یک ماتریس بررسی توازن برای کد با صفرهای آن، می‌توان نشان داد که کدهای همینگ دوری هستند. حالت دوتایی همینگ ساده تر بوده و لذا ابتدا آن رادر نظر می‌یگریم.

قضیه: کد همینگ $H_۲(r)$ هم ارز با یک کد دوری است.

اثبات: یادآوری می‌کنیم که کد همینگ دوتایی $H_۲(r)$ داریا پارامتر های $[۲^r-۱,۲^r-۱-r,۳]$ است و ستون‌های ماتریس بررسی توازن آن، تمامی $۲^r-۱$ بردار دوتایی ناصفر است.

حال فرض کنید $n=۲^r-۱$ و w یک ریشه nام اولیه واحد روی $F_۲$ باشد. چون $o_n(۲)=r$ ، سپس میدان شکافنده $x^n-۱$ برابر با $F_۲r$ است و چون w دارای مرتبه $n=۲^r-۱$ است، پس w یک عضو اولیه میدان $F_۲r$ می‌باشد. در نیتجه، توان‌های w، تمامی عناصر ناصفر میدان $F_۲r$ و در نتیجه ستون‌های ماتریس H را تشکیل می‌دهند. پس:

$$H=[[w^۰],[w^۱],...,[w^{n-۱}]]$$

شامل تمامی برداراهای دوتایی ناصفر به طول r است. این مطلب، نشان می‌دهد که کد همینگ $H_۲(r)$ با این ماتریس بررسی توازن یک کد دوری است که تنها صفرهای آن، یک ریشه اولیه واحد w است (w ریشه $x^{۲^r}-۱$ است) و تمامی صفرهای دیگر آن، ریشه‌های چند جمله‌ای مینیمال W هستند.

مثال: کد همینگ $H_۲(r)$را در نظر بگیرید. در این حالت، $n=۲-۱=۱۵$ و میدان شکافنده $x^n-۱$ برابر با $F_{۱۶}$ است. اگر β یک عضو اولیه از $F_{۱۶}$ باشد، آنگاه β همچنین ۱۵امین ریشه‌اولیه واحد نیز هست. مزدوج های β به صورت زیر می‌باشند.

$$\beta,\beta^۲,\beta^۴,\beta^۸$$

چون $\beta^{۱۶}=\beta$. بنابراین، چند جمله‌ای مینیمال β به صورت زیر است.

$$(x-B)(x-\beta^۲)(x-\beta^۴)(x-\beta^۸)$$

که با در نظر گـرفتن چنـد جملـه‌ای اولیـه x^4+x+1 (یعنـی $f_{16}=\frac{F_2[x]}{<x^4 9x+1>}$)بـرای F_{16} ، $H_2(4)$ کد دوری تولید شده توسط $f(x)=x^4+x+1$ در (R_{15}) خواهد بود.

برای حالت غیر دودویی نیز می‌توان نشان داد، کد همینگ دوری سات. در واقع قضیه زیر را داریم.

قضیه: فرض کنید $n=\frac{q^r-1}{q-1}$ و نیز فرض کنید $(r,q-1)=1$. در این صورت کد همینـگ q-تایی $H_q(r)$ هم ارزی با یک کد دوری خواهد بود.

مولد خود توان یک کد دوری

از قبل لیست کاملی از تمامی کدهای دوری در R_n را کـه مـی‌تواننـد از تجزیـه x^n-1 بـه عوامل تحویل ناپذیر روی F_q به دست آیند، مشاهده کردیم. اما، تجزیه x^n+1 کار سـاده‌ای نیست. یک روش برای انجام این کار، این است که در ابتدا یک ریشه nام واحد را به دسـت آوریم که برای این کار، باید بـا میـدان شـکافنده $F_q s$از x^n-1 کـار کنـیم. در اینجـا، روش دیگری برای توصیف کدهای دوری به دست می‌آوریـم کـه بـه جـای چنـد جملـه‌ای مولـد (*generator polynomial*) بــا نــوع دیگــری از چنــد جملــه‌ای هــای تولیــد کننــده (*generationg polynomial*) کار می‌کنیم.

تعریف یک چند جمله‌ای $e(x)\in R_n$، خود توان (*idempotent*) در R_n نامیده می‌شـود اگـر $e^2(x)\equiv e(x)$.

مثال چند جمله‌ای $x^3+x^5+x^6$ در R_n باشد (با چنـد جملـه‌ای مولـد $g(x)$ و چنـد جملـه‌ای توازن $h(x)$).

در یان صورت $g(x)$ و $h(x)$ نسـبت بـه هـم اول بـوده و لـذا چنـد جملـه‌ای هـای $b(x),a(x)$ وجود دارند به طوری که:

$$a(x)g(x)+b(x)h(x)=1$$

چند جمله‌ای $e(x)=a(x)g(x) \bmod (x^n-1)$ دارای خواص زیر است.

۱) $e(x)$، تنها عضویکه C است، یعنی برای تمام $p(x)\in C$ داریم $p(x)e(x)\equiv p(x)$.

۲) $e(x)$ تنها چند جمله‌ای در C است که هم خود توان و هم مولد می‌باشد، یعنی $C=<e(x)>$.

اثبات: اگر e_1,e_2 هر دو در C یکه باشند آنگاه $e_1(x)\equiv e_1(x)e_2(x)\equiv e_2(x)$، بنابراین $e_1(x)=e_2(x)$ پس اگر یک یکه وجود داشته باشد آنگاه یکتاست چون $g(x)h(x)=x^n-1$ دارای هیچ ریشه تکراری در هر میدان گسترش یافته نیست، $h(x),g(x)$ نسبت به هم اول هستند.

اگر $P(x)\in C$ آنگاه $p(x)h(x)$، لذا $a(x)g(x)\equiv p(x)$ که بیان می‌کند.

$e(x)=a(x)g(x) \bmod (x-1)$ یک عضو یکه در C می‌باشند و لذا $e(x)$، C را تولید می‌کند زیرا هر چند جمله در C یک مضرب $e(x)$ است. حال اگر رابطه $a(x)g(x)+b(x)h(x)=1$

را در $a(x)g(x)$ ضرب کنیم، داریم $[a(x)g(x)]^2+a(x)b(x)g(x)h(x)=a(x)h(x)$

و لذا $(a(x)g(x))^2=a(x)g(x)$، در نتیجه $e(x)$ خود توان است.

باری کامل کردن اثبات، تنها نیاز داریم نشان دهیم یک عضو خود توان $f(x)$ که C را تولید می‌کند می‌بایست برابر با $e(x)$. چون $f(x)$ ، C را تولید می‌کند، لذا $q(x)\in R_n$ وجود دارد که در ان $e(x)\equiv q(x)f(x)$. بنابراین.

که در نتیجه $f(x)=e(x)$ و اثبات کامل می‌شود.

تذکر به چند جمله‌ای $e(x)$ در قضیه بالا، خود توان تولید کننده (*generating idempotent*) C گفته می‌شود، و می‌نویسیم $C=[e(x)]$. همچنین در قضیه فوق، با استفاده

از الگوریتم اقلیدسی، می‌توانیم $e(w)$را از $g(x)$به دست آوریم. قضیه بعد، نحوه این کار را تشریح می‌کند:

قضیه: چندجمله‌ای مولد که $[[e(x)]]$ به صورت زیر است:

$$g(x) = \gcd(e(x), x^n - ۱)$$

اثبات: می‌دانیم $x^n - ۱ = g(x)\ h(x)$ و نیز $e(x) = a(x)g(x)$. لذا داریم:

$$\gcd(e(x), x^n - ۱) = \gcd(a(x)g(x), h(x)g(x)) = g(x)$$

زیرا $a(x)$ و $h(x)$، نسبت به هم اول هستند

قضیه فرض کنید $c_۲ = [[e_۲(x)]], C_۱ = [[e_۱(x)]]$، کدهای دوری در R_n باشند.

در این صورت: ۱) $C_۱ \subset C_۲$ اگر و تنها اگر $e_۱(x)e_۲(x) \equiv e_۱(x)$

۲) $C_۱ \cap C_۲ = [[e_۱(x)e_۲(x)]]$

۳) $C_۱ + C_۲ = [[e_۱(x) + e_۲(x) - e_۱(x)e_۲(x)]]$

که در آن تمامی چند جمله‌ای ها در پیمانه $x^n - ۱$ بدست آمده اند.

تذکر: قضیه زیر یک رابطه جالب بین چند جمله‌ای مولد و خودتوان تولید کننده یک کد دوری مطرح می‌کند.

قضیه: فرض کنید Cیک کد دوری در R_n با چند جمله‌ای مولد $g(x)$و خود توان تولید کننده $g(x)$ باشد. در این صورت $e(x), g(x)$ دقیقا دارای ریش‌های یکسانی در میدان شکافنده $x^n - ۱$، درمیان ریشه‌های nام واحد، هستند.

علاوه بر این اگر $f(x)$ در R_nخودتوان باشد و در میان ریش‌های nام واحد، دارای ریشه-های یکسانی با $g(x)$ باشد، آنگاه $f(x)$ خود توان تولید کننده $<<g(x)>>$ خواهد بود.

اثبات: فرض کنید w یک ریشهnام اولیه واحد باشد. چون $e(x) \equiv a(x)g(x)$، در نتیجه $g(x^i) = ۰$ ایجاب می‌کند $e(w^i)$اگر و تنها اگر $h(w^i) \neq ۰$، بنابراین $e(w^i) = ۰$ ایجاب می-کند $h(w^i) \neq ۰$ که در نتیجه $g(w^i)$. در مورد قسمت دوم قضیه، مشاهده می‌کنیم که چون

هر ریشه $g(x)$، یک ریشه $f(x)$ نیز می‌باشد و $g(x)$ هیچ ریشه تکراری در یک میدان گسترش یافته نیست. لذا داریم $g(x)\,|\,f(x)$ علاوه بر این، چون ریشه‌های چند جمله‌ای توازن $h(x)$ دقیقاً ناریشه‌های $g(x)$، در میان ریشه‌های nام واحد، هستند.، می‌بینیم که $h(x)$و $f(x)$ دارای هیچ ریشه مشترکی در یک میدان گسترش یافته نیستند. بنابراین، آنها نسبت به هم اول هستند. اما، اگر D یک کد دوری در R_n با خود توان تولید کننده $f(x)$ باشد، آنگاه چند جمله‌ای مولد D به صورت زیر است:

$$\gcd(f(x), x^n - ۱) = \gcd(f(x), h(x)g(x)) = g(x)$$

لذا $D=C$. بنابراین، $f(x)$ خود توان تولید کننده C می‌باشند.

در مورد خود توان های دوگان یک کد، قضیه زیر را داریم.

قضیه: فرض کنید $C=[[e(x)]]$ یک کد دوری با چندجمله‌ای توازن $h(x)$ باشد.در این صورت کد دوری $<<h(x)>>$ دارای خود توان تولید کننده $۱-e(x)$است و $C^{\perp} = <<h^{\perp}(x)>>$ دارای خود توان تولید کننده $(۱-e(x^{n-۱}))\bmod(x^n-۱)$ می‌باشد.

اثبات: چون $h(x)(۱-e(x)) \equiv h(x)(۱-a(x)g(x)) \equiv h(x)$

می‌بینیم که $۱-e(x)$ در $<<h(x)>>$ یکه است به طور مشابه چون:

$$h^{\perp}(x) = h_{\circ}^{-۱}x^k h(x-۱) \equiv h^{\perp}(x) - h_{\circ}^{-۱}x^k h x^{n-۱})e(x^{n-۱}) \equiv$$
$$h^{\perp}(x) - h_{\circ}^{\perp}x^k h(x^{n-۱})a(a^{n-۱})g(z^{n-۱}) \equiv h^{\perp}(x)$$

بنابراین $(۱-e(x^{n-۱}))\bmod(x^{-}-۱)$ در $C^{\perp} = <<h^{\perp}(x)>>$ یکه است.

یافتن خودتوان های تولید کننده

حال به دنبال جواب این سوال هستیم که بدون داشتن تجزیه $x^n-۱$، چگونه می‌توانیم خودتوان‌ها را بیابیم.در اینجا، توجه خود را روی حالت $q=۲$ معطوف می کنیم.

در $F_۲[x]$، داریم $f(x^۲) = f^۲(x)$ و لذا یک چند جمله‌ای $e(x) = e_{\circ} + e_۱ + \dots + e_{n-۱}x^{n-۱}$ در R_n خود توان است اگر و تنها اگر $e(x^۲) \equiv e(x)$. اما این رابطه در R_n، برقرار است اگر و

تنها اگر زمانی که $e_i \neq ۰$، داشته باشیم $e_{۲i(\text{mod } n)} \neq ۰$، در نتیجه $e(x)$ می‌بایست مجموعه چندجمله‌ای هایی به صورت زیر باشد:

$$x^i + x^{۲i} + ... + x^{۲^{d-۱}i}$$

جایی که توان‌ها، تشکیل یک هم دسته‌ی دوری می‌دهند. لذا قضیه زیر را اثبات کرده‌ایم.

قضیه: فرض کنید $q = ۲$، خود توانهای موجود در R_n دقیقا مجموع چندجمله‌ای های به صورت $x^i + x^{۲i} + ... + x^{۲^{d-۱}i}$ هستند، جایی که $C_i = \{i, ۲i, ..., ۲^{d-۱}i\}$ یک هم دسته‌ی دوری برای ۲ پیمانه n می‌باشد.

مثال: فرض کنید $n = ۹$ هم دسته‌های دوری برای ۲ پیمانه ۹ به صورت زیر می‌باشند،

$$C_۰ = \{۰\}, C_۱ = \{۱,۲,۴,۸,۷,۵\}, C_۳ = \{۳,۶\}$$

و لذا $۸ = ۲^۳$ خودتوان به صورت زیر وجود دارند.

$$\begin{array}{ll} e_۲(x) = x^۰ = ۱ & e_۱(x) = ۰ \\ e_۴(x) = x^۳ + x^۶ & e_۳(x) = x + x^۲ + x^۴ + x^۵ + x^۷ + x^۸ \\ e_۶(x) = e_۲(x) + e_۴(x) & e_۵(x) = e_۲(x) + e_۳(x) \\ e_۸(x) = e_۲(x) + e_۳(x) + e_۴(x) & e_۷(x) = e_۳(x) + e_۴(x) \end{array}$$

چندجمله‌ای های مولد متناظر نیز با استفاده از قضایای قبل، قابل حصول هستند. برای نمونه، از الگوریتم اقلیدسی داریم: $q_۳(x) = (\gcd(e_۳(x), x^۹ - ۱) = x + ۱$

کدهای BCH

کران BCH: ابتدا بر مطالب قبل یک مرور مختصر می کنیم. از قبل می‌دانیم که یک کد دوری توسط صفرهای آن تعریف می‌شود. به خصوص، اگر $\propto_1,\ldots,\propto_u$ ریشه‌های nام واحد در F_qباشد، آنگاه $C=\{p(x)\in R_n \mid p(\propto_1)=\ldots=p(x_u)=0\}$

یک کد دوری است که چندجمله‌ای مولد $g(x)$، حاصل ضرب چندجمله‌ای های مینیمال $\propto_1,\ldots,\propto_u$روی F_qاست. این رویکرد، این مطلب را پیشنهاد می کند که ما می‌توانیم برخی کدهای جالب را با تخصیص مجموعه ریشه‌های nام واحد به عنوان صفرهای $g(x)$بیابیم. یادآوری می کنیم که اگر $x^n-1=\prod_i m_i(x)$ ، تجزیه x^n-1 به عوامل تحویل ناپذیر روی F_q باشد، آنگاه ریشه‌های چندجمله‌ای $m_i(x)$مزدوج هستند، یعنی این ریشه‌ها به صورت $\{w^i, w^{iq},\ldots, w^{iq^{d-1}}\}$هستند، جایی که d کوچک ترین عدد صحیح مثبت است به طوری که $i_q d \overset{n}{\equiv} i$. نیز، یادآوری می کنیم که مجموعهٔ

$$C_i(x)=\{i, q_i,\ldots, q^{d-1}i\}$$

I امین هم دسته‌ی دوری q در پیمانه n نامیه می‌شود. بنابراین:

$$m_i(x)=\prod_{j\in c_i}(x-w^j)$$

قضیه (کران BCH): فرض کنید w یک ریشه اولیه nام واحد روی F_q باشد. فرض کنید C یک کد دوری در R_n با چند جمله مولد $g(x)$ باشد که در آن $g(x)$ چند جمله‌ای تکین با کمترین درجه روی F_q است که $\delta-1$ عدد زیر ریشه‌هایی از آن هستند.

$$w^b, w^{b+1},\ldots, w^{b+\delta-2} \qquad (b\geq 0)$$

در این صورت، C دارای کمترین فاصله حداقل δ خواهد بود.

نکته: این قضیه، این مطلب را به ما می‌گوید که ما می‌توانیم یک کد با کمترین، فاصله حداقل δ رابا تخصیص چندجمله‌ای مولد کد با $\delta-1$ ریشه متوالی آن مشخص کنیم (یعنی توان‌ها متوالی باشند).

قضیه: فرض کنید n,w امین ریشه واحد باشد. فرض کنید C یک کد دوری در R_n با ماتریس مولد $g(x)$ باشد به طوری که $g(x)$ چند جمله‌ای تکین با کمترین درجه در C است که دارای $\delta-1$ ریشه متوالی: $w^b, w^{b+r},..., w^{b+(\delta-2)r}$ درمیان صفرهای آن کد است، جایی که n,r نسبت به هم اول بوده و $b \geq 0$. در این صورت C دارای کمترین فاصله حداقل δ است.

کدهای BCH

حال آماده هستیم تا کدهای BCH را تعریف کنیم. این کدها، به طور مستقیم توسط بوس ($R.C.Bose$). چادهوری ($D.K.Ray\ chavdhuri$) (۱۹۶۰) و هنگهام ($A.Hocquenghem$) (۱۹۵۹) کشف شدند. به چندین دلیل این کدها جزو دسته ها بسیار مهم هستند. برای نمونه، این کدها دارای قدرت تصحیح خطای خوبی هستند، جایی که طول آنها زیادبزرگ نباشد. همچنین آنها می‌توانند به آسانی کدگذاری و کدگشایی شوند و نسبت به خانواده کدهای دیگر، دارای خواص خوبی هستند.

تعریف: فرض کنید W یک ریشه nام واحد روی F_q باشد و $q(x)$ چندجمله‌ای تکین روی F_q با کمترین درجه باشد به طوری که $\delta-1$ مقادیر زیر:

$$w^b, w^{b+1},..., w^{b+s-2}$$

در میان صفرهای $g(x)$ باشند، جایی که $\delta \geq 1, b \geq 0$ بنابراین:

$g(x)=lcm\{m_b(x),m_{b+1}(x),...,m_{b+s-2}(x)\}$

کد دوری q- تایی $B_q(n,\delta,w,b)$ با طول n و چندجمله‌ای مولد $g(x)$، یک کد BCH با فاصله مطرح (*designed dist*) δ است (توجه کنید که فاصله مطرح از تعداد صفرهای یکی بیشتر است).

اگر $b=1$، آنگاه کد $B_p(n,\delta,w)=B_p(n,\delta,w,1)$، یک کد BCH به معنای باریک (*narrow sense*) نامیده می‌شود. زمانی که w یک عضو اولیه میدان باشد و $n=q^s-1$ (برای مقداری $s\geq 1$) آنگاه $B_a(n,\delta,w,b)$ یک کد BCH اولیه نامیده می‌شود.

نکته: کد های BCH بامعنی باریک، تعمیمی از کدهای همینگ هستند. به خصوص، قبلاً مشاهده کردیم که کدهای همینگ دوتایی می توانند به صورت دسته ای از کدهای دوری با چندجمله ای مولد *g(x)* تعریف شوند که در آن $g(x)$ یک چندجمله ای تکین با کمترین درجه روی F_2 است که ریشهٔ n ام اولیه واحد w ریشه *g(x)* است. بنابراین، کدهای دوری، کدهای BCH با معنی ضعیف با فاصله مطرح $\delta=2$، هستند.

با استفاده از کران BCH، می‌توان دید که کد BCH، $B_q(n,\delta,w,b)$ دارای کمترین فاصله حداقل برای فاصله مطرح آن (یعنی δ)است. علاوه براین، چون میدان شکافنده x^n-1 روی F_q دارای درجه q^s روی F_q است (جایی که $s=o_n(q)$)، در نتیجه داریم:

$\deg(m_{b+i}(x))\leq s$ و لذا $\dim(B_q(n,\delta,w,b))=n-\deg(g(x))\geq n-s(s-1)$

بنابراین:

قضیه :کد BCH، q-تایی $B_a(n,\delta,w,b)$ با طول n و فاصله مطرح δ دارای پارامتر های زیر است:

$$\begin{cases}\dim(B_a(n,\delta,w,b))\geq n-(\delta-1)o_n(q)\\ d(B_a(n,\delta,w,b)\geq \delta\end{cases}$$

جایی که $o_n(q)$، مرتبه q در پیمانه n است.

نکته: با توجه به تعریف کد BCH، می‌بینیم که:

$$B_q(n,\delta,w,b)=\{p(x)\in R_n \mid p(w^b)=p(w^{b+1})=...=p(w^{b+s-2})=0\}$$

و لذا اگر $[w^i]$معرف بـردار سـتونی w^i $(w^i \in F_a^s)$در میـدان شـکافنده $F_q s$از x^n-1 باشـد، آنگاه $s(\delta-1)$ سطر ماتریس:

$$H=\begin{pmatrix} 1 & [w^b] & [w^{2b}] & \dots & [w^{(n-1)b}] \\ 1 & [w^{b+1}] & [w^{2(b+1)}] & \dots & [w^{(n-1)(b+1)}] \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & [w^{b+\delta-2}] & [w^{2(b+\delta-2)}] & \dots & [w^{(n-1)(b+\delta-2)}] \end{pmatrix}$$

تشکیل یک مجموعه کامل از معادلات بررسی توازن می‌دهند و همین کـه سـطرهای وابسـته حذف شوند، ماتریس حاصل، ماتریس بررسی توازن $B_a(n,\delta,w,b)$ خواهد شد.

کدهای BCH دوتایی

در حالت دوتایی، اگر C_k نمایش یک هم دسته دوری (*cyclotomic coset*) باشـد، آنگـاه $u\in C_k$ اگر و تنها اگر $2u(\bmod n)\in c_k$. بنابراین $M_i(x)=m_{2i}(x)$. این مطلـب، ایجـاب مـی-کند که چندجمله‌ای های:

$$g_1(x)=lcm\{m_1(x)m_2(x),...,m_{2E}(x)\}$$
$$g_2(x)=lcm\{m_1(x)m_2(x),...,m_{2E-1}(x)\}$$
$$g_3(x)=lcm\{m_1(x)m_3(x),...,m_{2E-1}(x)\}$$

یکی باشند. توجه دارید که مجموعه چندجمله‌ای های آخر $m_i(x)$ تنهـا دارای انـدیس هـای فرد هستند). چون $g_2(x)=g_1(x)$، داریم: $B_2(n,2\varepsilon+1,w)=B_2(n,2\varepsilon,w)$

بنابراین می‌توانیم توجه خود را معطوف کدهای BCH بـا معنـی باریـک بـا طـول n و فاصـله مطرح $\delta=2\varepsilon+1$کنیم در این حالـت بعـد حـداقل $n\text{-}\varepsilon O_n(2)$ اسـت، جـایی کـه $o_n(2)$ مرتبه ۲ در پیمانه n است به بیان دیگر:

$$\dim(b_2(n,24+1,w))\geq n-4o_n(2)$$

مثال: فرض کنید $q=2$، $n=2^5-1-31, q=2$ برای تعیین کـدهای BCH بـا معنـای باریـک (اولیه) $B_2(31,\delta,w)$ با فاصله‌های مطرح متفاوت ابتدا هـم دسـته هـای دوری را محاسـبه مـی-کنیم.

$C_{۰}=\{۰\}, C_{۱}=\{۱,۲,۴,۸,۱۶\}, C_{۳}=\{۳,۶,۱۲,۲۴,۱۷\}, C_{۵}=\{۵,۱۰,۲۰,۹,۱۸\}$
$C_{۷}=\{۷,۱۴,۲۸,۲۵,۱۹\}, C_{۱۱}\{۱۱,۲۲,۱۳,۲۶,۲۱\}, C_{۱۵}\{۱۵,۳۰,۲۹,۲۷,۲۳\}$

چندجمله‌ای مولد کد BCH با معنای باریک $B_{۲}(۳۱,۹,w)$ با فاصله مطرح $\delta=۹$، برای نمونه به صورت زیر است:

$$g(x)=lcm\{m_{۱}(x),...,m_{۸}(x)\}=m_{۱}(x)m_{۵}(x)m_{۷}(x)$$

بنابراین، بعد $B_{۲}(۳۱,۹,w)$ برابر با $n-\deg(g(x))=۳۱-۲۰=۱۱$ است.

توجه دارید که این کران پایین، با کران BCH مطابقت دارد.

نیز توجه دارید که چون $۹\in C_{۵}$، داریم $x_{۹}(x)=m_{۵}(x)$ و لذا:

$$B_{۲}(۳۱,۱۱,w)=B_{۲}(۳۱,۹,w)$$

بنابراین، دراین حالت، کران پائین BCH برابر با $۳۱-۲۵=۶$ است که به طور اکید از بعد واقعی کمتراست. جدول زیر، شامل لیست کاملی از تمام کدهای BCH دوتایی به معنای باریک با طول ۳۱ است. در این جدول، نماد زیرا قرار داد کرده‌ایم.

$$m_{i_{۱}i_{۲},...,i_{k}}(x)=m_{i_{۱}}(x)...m_{i_{k}}(x)$$

فاصلهٔ واقعی	بعد	چند جمله‌ای مولد	فاصله مطرح
۱	۳۱	۱	۱
۳	۲۶	$m_{۱}(x)$	۳
۵	۲۱	$m_{۱,۳}(x)$	۵
۷	۱۶	$m_{۱,۳,۵}(x)$	۷
۱۱	۱۱	$m_{۱,۳,۵,۷}(x)$	۱۱ یا ۹
۱۵	۶	$m_{۱,۳,۵,۷,۹}(x)$	۱۵ یا ۱۳
۳۱	۱	$x^{۳۱}-۱$	۱۹,۱۷,...,۳۱

نکته: مثال قبل، نشان می‌دهد که یک کد BCH با فاصله مطرح فرد δ ممکن است با یک کد BCH با فاصله مطرح فرد $\delta' > \delta$ مطابقت داشته باشد.این مطلب، تعریف زیر را به دنبال دارد.

تعریف: فرض کنید B یک کد BCH باشد. بزرگترین فاصله مطرح δ که در آن B یک کد BCH با فاصله مطرح δ باشد، یک فاصله بوز (Bose) از کد نامیده می‌شود.

مثال: فرض کنید $n=۲۳, q=۲$. چون $s=o_{۲۳}(۲)=۱۱$، لذا میدان شکافنده ۱-$۲^{۲۳}$، برابر با $F_{۲^{۱۱}}$ است. هم دسته‌های دوری ۲ در پیمانه ۲۳ به صورت زیر هستند.

$C_{۰}=\{۰\},\ C_{۱}=\{۱,۲,۴,۸,۱۶,۹,۱۸,۱۳,۳,۶,۱۲\},$
$C_{۵}=\{۵,۱۰,۲۰,۱۷,۱۱,۲۲,۲۱,۱۹,۱۵,۷,۱۴\}$

لذا کد BCH با معنای باریک $B_{۲}(۲۳,۵,w)$ با فاصله مطرح $\delta=۵$ دارای ماتریس مولد:

$g(x)=lcm\{m_{۱}(x),m_{۲}(x),m_{۴}(x)\}=m_{۱}(x)$

است به خصوص، $B_{۲}(۲۳,۵,w)$ یک کد[23,12] دودویی است. به آسانی می‌توان دید که $B_2(23,5,W)$ هم ارز با کد گلی G_{23}، با کمترین فاصلهٔ ۷ است. بنابراین در این حالت کمترین فاصله واقعی کد بزرگتر از فاصلهٔ مطرح آن است.

کد رید- سولومن (Reed-Soloman)

در اینجا، دسته خاصی از کدهای BCH، معروف به کدهای رید- سولومن را معرفی می-کنیم.

این، کدها، در عمل به ندرت مورد استفاده قرار می‌گیرند. در واقع ، به کارگیری این کدها، در ترکیب با کدهای غیربلوکی، روش استانداردی در NASA، از زمان پرواز فضاپیمای ویاگر در سال ۱۹۷۷، بوده است. این کدها، همچنین در مأموریت های فضایی یولیس، مگلان و گالیلو به کار رفته‌اند.این کدها، دارای بیشترین فاصله ممکن هستند (یعنی MDS می‌باشند). همچنین این کدها در تصحیح خطاهای گروهی بسیار مفید هستند.

تعریف: فرض کنید $a \geq ۳$. یک کد رید- سولومن (RS) $R=R(n,\delta,w,b)$ یک کد BCH q- تایی، $B_q(q-۱,\delta,w,b)$ با طول $n=q-۱$ است.

نکته: طول یک کد رید- سولومن q- تایی با تعداد عناصر ناصفر در میدان پایه F_q برابر است چون $n=q-1$ و چون ریشه‌های چندجمله‌ای $x^{q-1}-1$، دقیقا، عناصر ناصفر F_q هستند.

لذا داریم: $$x^n-1=x^{q-1}-1=\prod_{\propto\in F_q}(x-\propto)$$

بنابراین، اگر w یک $(q-1)$امین ریشه اولیه واحد روی F_qباشد (یعنی یک عضو اولیه F_q) در این صورت، $m_i(x)=x-w^i$. در نتیجه، یک کد رید- سولومن با فاصله مطرح δ دارای ماتریس مولد زیر است.

$$g(x)=(x-w^b)(x-w^{b+1})....(x-w^{b+s-1}) \qquad (b\geq o)$$

مثال: فرض کنید $q=8$ و لذا $n=7$. یک ریشه w از چند جمله‌ای اولیه x^3+x+1 روی F_2، یک عضو اولیه F_8 را به ما می‌دهد. برای به دست آوردن یک کد RS با بعد ۵، می‌خواهیم $\deg(g(x))=7-5=2$ در این حالت، داریم:

$$g(x)=(x-w)(x-w^2)=x^2-(w+w^2)x+w^3=x^2+w^4x+w^3$$

خواص کدهای رید- سولومن

۱-کدهای رید سولومن، MDS هستند.

ماتریس مولد یک کد رید- سولومن با فاصله مطرح $\deg(g(x))=\delta-1$ است.

لذا: $$k=\dim(R(n,\delta,w,b))=n-\deg(g(x))=n-\delta+1$$

بنابراین، با توجه به کران BCH، کمترین فاصله این کد در رابطه زیر صدق می‌کند.

$$d\geq\delta=n-k+1$$

اما کران سینگلتون، به صورت $d\leq n-k+1$ است؛ لذا

$$d=\delta=n-k+1$$

که به ما می‌گوید $R(n,\delta,w,b)$یک کد MDS است و همچنین فاصله مطرح با کمترین فاصله برابر است.

قضیه: کدهای رید- سولومن، کدهای با بیشترین. فاصله مطرح (MDS) هستند، علاوه براین، کمترین فاصله یک کد رید- سولومن برابر با کمترین فاصله آن است.

لذا، کدهای RS دارای بیشترین فاصله ممکن درمیان تمامی کدهای q-تایی با طول n=q−۱ و بعد $k=n-\delta+۱$ هستند.

۲- دوگان یک کد رید سولومن:

در حالت کلی دوگان یک کد BCH ممکن است یک کد BCH دیگر نشود. برای نمونه، فرض کنید $q=۲, n=۲۵$. هم دسته های دوری q در پیمانه n به صورت زیر هستند.

$$C_۰=\{۰\},\ C_۱=\{۱,۲,۴,۸,۱۶,۷,۱۴,۳,۶,۱۲,۲۴,۲۳,۲۱,۱۷,۹,۱۱۸,۱۱,۲۲,۱۹,۱۳\}$$
$$C_۵=\{۵,۱۰,۲۰,۱۵\}$$

فرض کنید $B=B_۲(۲۵,۱,w)$، کد BCH با یک صفر تعریف شده w باشد، کد دوگان $B^{\perp}$ دارای صفرهایی یکسان باعناصر متقابل (reciprpcals) عناصر ناصفر B است و لذا $B^{\perp}$ دارای صفر های زیر است.

$$\{w^{۰},w^{-۵},w^{-۱۰},w^{-۲۰},w^{-۱۵}\}=\{w^{۰},w^{۲۰},w^{۱۵},w^{۵},w^{۱۰}\}$$

لذا $B^{\perp}$ یک کد BCH نیست. از طرف دیگر، برای کدهای رید- سولومن قضیه زیر را داریم: (اثبات به صورت تمرین).

قضیه: دوگان یک کد رید- سولومن، یک کد رید- سولومن است.

گسترش یک کد رید سولومن

با توجه به مطالب قبل، یادآوری می‌کنیم که اگر Cیک $(n,m,d)-$ کد q- تایی باشد، آنگاه کد گسترش یافته $\hat{C}$با اضافه کردن یک بیت توازن کلی C_nبه هر کد کلمه، $C=C_۰...C_{n-۱}$ که رابطه زیر صدق کند، حاصل می‌شود. $\sum_{k=۰}^{n} C_k=۰$

اگر $\hat{C}$ یک $(\hat{n},\hat{m},\hat{d})-$ کد باشد، آنگاه:

$\hat{n}=n+۱, \hat{M}=m, \hat{d}=d$ یا $d+۱$

از طرف دیگر، در موردکدهای رید- سولومن، کمترین فاصله کدگسترش یافته از کمترین فاصله کد اصلی بیشتر است.

قضیه: فرض کنید C یک کد رید سولومن $[n,k,d]$ با چند جمله‌ای مولد زیر باشد.

$$g(x)=(x-w)(x-w^{۲})...(x-w^{d-۱})$$

در این صورت، کد گسترش یافته $\hat{C}$، یک $[n+۱,k,d+۱]-$ کد است.

اثبات: فرض کنید $c(x)=c_{0}+c_{1}x+\ldots+c_{n-1}x^{n-1}$ یک کد کلمه در C با وزن d باشد. با گسترش $c(x)$، داریم $\hat{C}(x)=c_{0}+c_{1}x+\ldots+C_{n-1}x^{n-1}+c_{n}x^{n}$، جایی که:

$$c=-\sum_{i=0}^{n-1}c_i=-(1)$$

حال می‌خواهیم نشان دهیم وزن $\hat{C}(x)$ برابر با $d+1$ است که این رابطه درست است اگر و تنها اگر $c(1)\neq 0$ چون $g(x)$ چند جمله‌ای مولد C است داریم $C(x)=p(x)g(x)$ به ازای یک چندجمله‌ای $p(x)$، بنابراین $C(1)=p(1)g(1)$به وضوح، $g(1)\neq 0$، زیرا $w^i\neq 1$ برای $i=1,2,\ldots,d-1$ ، اگر $P(1)=0$ آنگاه چندجمله‌ای $C(x), g_1(x)=(x-1)g(x)$ را عاد می‌کند. بنابراین، $C(x)$ در کد دوری تولید شده توسط $g_1(x)=(x-1)(x-w)(x-w^2)\ldots(x-w^{d-1})$ که شامل d صفر متوالی، $w^{0},\ldots,w^{d-1}$ است، قرار می‌گیرد و لذا با استفاده از کران BCH، $c(x)$ دارای وزن حداقل $d+1$ خواهد بود. اما این مطلب، با این واقعیت که $c(x)$ دارای وزن d است، در تناقض است. لذا $p(1)\neq 0$ و اثبات در اینجا کامل می‌شود.

به دست آوردن یک کد دوتایی کد 2^m- تایی

یک کد q- تایی با q بزرگ در برخی مواقع ممکن است قابل پیاده سازی نباشد. اما، اگر $q=2^m$ (برای مقداری m)، آنگاه یک $[n,k]$- کد q- تایی را می‌توان به یک $[mn,mk]$- کد دوتایی، با یک روش قابل فهم، تبدیل کرد.

فرض کنید $\{\alpha_1,\ldots,\alpha_m\}$ یک پایه مرتب برای f_{2^m} روی F_2 باشد. برای هر عضو F_{2^m} مانند a، داریم: $a=a_1\alpha_1+\ldots+a_m\alpha_m$ و لذا می‌توان به a رشته $a_1\ldots a_m$ را نسبت داد. این تخصیص را می‌توان به صورت:

$a\to a_1a_2\ldots a_m$

نشان داد. حال اگر C یک $[n,k]$کد 2^m تایی باشد آنگاه هر کد کلمه در C دارای شکلی به صورت $c=c_0c_1\ldots c_{n-1}$ است که در آن $c_i\in F_{2^m}$. بنابراین اگر:

$C_i\to C_{i1}\ldots C_{im}$

آنگاه، می‌توان به هر $C \in C$، رشته $C \to (C_{11}...C_{1m})(C_{21}...C_{2m})...(C_{n1}...C_{nm})$ با طول mn را نسبت داد. (پرانتزها، تنها به منظور سادگی در خواندن گذاشته شده اند) کد $C^{\to}$ شامل چنین رشته‌هایی، یک کد دوتایی با طول mn خواهد بود.

علاوه بر این، $C^{\to}$ یک فضای برداری روی F_2 با اندازه $|C^{\to}|=|C|=(2^m)^k=2^{mk}$ است.

بنابراین، $C^{\to}$ روی F_2 دارای بعد mk است. سرانجام اگر $a \neq b$ و

$$a \to a_1...a_m \quad , \quad b \to b_1...b_m$$

آنگاه، برای حداقل یک i، داریم $a_i \neq b_i$ و لذا کمترین، فاصله $C^{\to}$، حداقل برابر با d است. مطالب فوق، در قضیه زیر خلاصه شده اند.

قضیه: فرض کنید C یک $[n,k,d]$-کد 2^m- تایی باشد، فرض کنید $\{\propto_1,...,\propto_m\}$ یک پایه مرتب برای F_2m روی F_2 باشد. که $C^{\to}$، تولید شده به وسیله جایگذاری هر سبمل کد $a=\sum a_i \propto_i$ در هر کد کلمه از C با رشته m- تایی متناظر با آن $a_i,...a_m$، یک $[n^{\to},k^{\to},d^{\to}]$- کد دوتایی است، جایی که:

$$n^{\to}=,mn,k^{\to}=mk,d^{\to}\geq d$$

علاوه بر این با جایگذاری هر سمبل کدکلمه درC با رشته m تایی متناظر با آن، می- توانیم یک سمبل بررسی توازن به هر کدکلمه از این رشته mتایی به صورت زیر اضافه کنیم:

$$C \to (C_{11},...C_1ms_1)(c_{21}...C_{2m}x_2)...(c_{n1}...c_{nm}x_n)$$

جایی که $C_{i1}+...C_{im}+x_i=0$ (برای $1\leq i\leq n$)

که $C^{\uparrow}$ حاصل دارای پارامترهای زیر خواهد بود:

$$n^{\uparrow}=(m+1)n,k^{\uparrow}=mk,d^{\uparrow}\geq 2d$$

برای مشاهده این مطلب که $d^{\uparrow}\geq 2d$، می‌بینیم که حداقل d تا از رشته‌های mتایی اصلی در هر کد کلمه از $C^{\to}$ باید ناصفر باشند. اما اگر یکی از این رشته‌ها دارای وزن ۱ باشد. آنگاه اضافه نمودن یک بیت توازن، وزن آن را به ۲ افزایش می‌دهد. به عبارت دیگر، وزن

هر رشته $m+1$ - تایی ناصفر حداقل برابر با ۲ است و لذا وزن هر کد کلمه از $C^{\uparrow}$ حداقل ۲dاست. توجه دارید که نرخ $C^{\uparrow}$ به صورت زیر است:

$$R(C^{\uparrow})=\frac{mk}{(m+1)n}=\frac{m}{m+1}R(C)$$

که برای mهای به اندازه کافی بزرگ، نسبت به نرخ اصلی کدC، زیاد کوچک نیست. از طرف دیگر کمترین فاصله کد جدید، حداقل دوبار از کمترین فاصله C بیشتر است. بنابراین، با بکارگیری یک روش نسبتاً ساده، می‌توانیم به قدرت تصحیح کد مهمی دست یابیم. باید این نکته را ذکر کنیم که اگر C یک کد دوری باشد، آنگاه کد های $C^{\rightarrow}$و $C^{\uparrow}$ لزوما دوری نیستند. همچنین کمترین فاصله کد $C^{\rightarrow}$ می‌تواند به انتخاب پایه‌های F_2m روی F_2 وابسته باشد.

مثال: فرض کنید $k=2,n=3,q=4$، چندجمله‌ای x^2+x+1، یک چند جمله‌ای اولیه برای F_4 روی F_2 است. بنابراین، اگر w یک ریشه از این چندجمله‌ای باشد، آنگاه داریم:

$$F_4=\{0,1,w,w^2\}$$

یک کد $[3,2,2]$ - رید سولومن ۴ تایی C دارای چند جمله‌ای مولد با درجه ۱ است.

بیایید، فرض کنیم $g(x)=x-w$. دراین صورت، کد C به صورت زیراست.

$$C=\{p(x)(x-w)\,|\,\deg(p(x))\le 1\}$$

برای نمونه، یک کد کلمه در C به صورت $(x+w)(x-w)=x^2-w^2$ است که به صورت رشته $w^2 01$ می‌توان آن را نشان داد. می‌توان دید که تمامی ۱۶ کد کلمه موجود درC به صورت رشته‌های زیر هستند.

$000\ ,\ w10\ ,\ w^2w0\ ,\ 1w^20$

$0w1\ ,\ 0w^2w\ ,\ 01w^2\ ,\ ww^21$

$w^201\ ,\ 111\ ,\ www\ ,\ w^21w$

$10w\ ,\ www^2\ ,\ w^2w^2w^2\ ,\ 1ww^2$

که در آن $\{1,w\}$ یک پایه مرتب برای F_4 روی F_2 است. تحت این پایه، داریم

$0\rightarrow 00 \qquad 1\rightarrow 10 \qquad w\rightarrow 01 \qquad w^2\rightarrow 11$

و لذا کد [۶,۴] دوتایی $C^{\to}$ به صرت زیر می‌باشد.

۰۰۰۰۰۰ , ۰۱۱۰۰۰ , ۱۱۰۱۰۰ , ۱۰۱۱۰۰
۰۰۰۱۱۰ , ۰۰۱۱۰۱ , ۰۰۱۰۱۱ , ۰۱۱۱۰۰
۱۱۰۰۱۰ , ۱۰۱۰۱۰ , ۰۱۰۱۰۱ , ۱۱۱۰۰۱
۱۰۰۰۰۱ , ۰۱۰۱۱۱ , ۱۱۱۱۱۱ , ۱۰۰۱۱۱

به طریق مشابه، می‌توان کد $C^{\uparrow}$ را مشخص کرد.

تصحیح خطای گروهی (Brst error Corretion)

کد دوتایی گسترش یافته $C^{\to}$ می‌تواند خواص تصحیح خطای گروهی بسیار خوبی داشته باشد اگر کد اصلی C، تصحیح کننده t خطا باشد، آنگاه کد گسترش یافته $C^{\to}$ می‌تواند خطاهای گروهی با طول حداکثر $b=(t-۱)m+۱$ را تصحیح کند. زیرا هر خطای گروهی با طول b بیت یا کمتر می‌تواند حداکثر روی t رشته به طول m، تأثیر بگذارد.

مثال: فرض کنید می‌خواهیم یک کد دوتایی، بر پایه یک کد رید سولومن، بیابیم که بتواند خطاهای گروهی با طول b=۱۳ یا کمتر را تصحیح کند. دراین صورت می‌خواهیم:

$(T+۱)m+۱=۱۳ \Rightarrow (t-۱)m=۱۲$

حال اگر فرض کنیم $d=۲t+۱$ (کمترین فاصله فرد باشد)، آنگاه رابطه فوق معادل با رابطه زیر است: $(d-۳)m=۲۴$.

حال، چون $d \le n=۲^m-۱$، می‌توانیم m=۴ و d=۹ را اختیار کنیم.

در این حالت، کد رید- سولومن C دارای پارامترهای [۹و۷و۱۵] خواهد بود (روی $F۶$).

کد دوتایی گسترش یافته $C^{\to}$ نیز دارای پارامترهای [۶۰,۲۸,≥۹]است و می‌توانیم خطاهای گروهی با طول ۱۳ یا کمتر را توسط آن تصحیح کنیم.

کدگذاری کدهای رید- سولومن

فرض کنید C یک [n,k,d]- کد رید- سولومن باشد، جایی که $n=q-۱$. فرض کنید.

$a_۰ \ldots a_{k-۱}$ یک رشته پیام است، قرار می‌دهیم: $a(x)=\sum_{i=۰}^{k-۱} a_i x^i$

و پیام $a(x)$ را به چند جمله ای $C(x)=\sum_{j=۰}^{n-۱} a(w^j)x^j$ کد می‌کنیم. البته باید نشان دهیم $C(x)$ یک کدکلمه درC است، یا به عبارت دیگر باید نشان دهیم: $C(w)=\ldots C(w^{d-۱})$

برای این منظور، فرض می‌کنیم $a(x)=\sum_{i=0}^{n-1}a_i x^i$ ، که در آن به ضرایب اضافی $(0 \geq k)a_i$

برابر با صفر در نظر گرفته شده‌اند، در نتیجه داریم:

$$a_j=\frac{1}{n}\sum_{j=0}^{n-1}a(w^i)w^{-ij}=\frac{1}{n}C(w^{-1})=\frac{1}{n}C(w^{n*i})$$

و لذا $C(w^{n-i})=n^a j$ به خصوص برای $0 \leq j \leq d-1=n-k$، داریم:

(زیرا $n-j\geq k$ و لذا $a_{n-j}=0$) $\qquad C(w^i)=na_{n-j}=0$

که نشان می دهیم $C(x)$ یک کد کلمه از C است.

کد گشایی کدهای رید-سولومن

از آنجایی که کدهای رید- سولومن، زیر کلامی از کدهای BCH هستند، لذا می‌توان آنها را با استفاده از کدهای BCH، کدگشایی کرد. در اینجا، روشی برای کدگشایی کدهای رید سولومن بر پایه منطق اکثریت می‌آوریم. متأسفانه، این روش، زمانی که $\binom{n}{k}$ در $[n,k,d]-$ کدها، افزایش می‌یابد خیلی عملی نیست. فرض کنید، پیام اصلی به صورت $a(x)=\sum_{i=0}^{k-1}a_i x^i$ باشد و کد کلمه متناظر با آن $c(x)=\sum_{i=0}^{n-1}a(w^i)x^i$ روی کانال ارسال شود.

در این حالت a را می‌توان به صورت رشته $a=a_0a_1...a_{k-1}$ و کد کلمه C را به صورت:

$$C=C_0C_1...C_{n-1}=a(1)a(w)...a(w^{n-1})$$

در نظر گرفت، حال فرض کنید $u=u_0u_1...u_{n-1}$ کلمه دریافتی و $e=e_0...e_{n-1}$ بردار خطا باشد.دراین صورت، $u_i=e_i+c_i=e_i+a(w^i)$ معلوم است. و داریم.

$$u_0=e_0+a_0+a_1+...+a_{k-1}$$
$$u_1=e_1+a_0+wa_1+...+w^{k-1}a_{k-1}$$
$$u_2=e_2+a_0+w^2a_1+...+w^{2(k-1)}a_{k-1}$$
$$e_{n-1}=e_{n-1}+a_0+w^{n-1}a_1+...+w^{(k-1)(n-1)}a_{k-1}$$

اگر هیچ خطایی در هنگام انتقال رخ ندهد آنگاه تمامی e_i ها برابر با صفر هستند و هر k تا از این معادلات می‌توانند برای تعیین k مقدار نا مشخص $a_0,...,a_{k-1}$ به کار روند. این مطلب، با توجه به این که ماتریس ضرایب هر k معادله، یک ماتریس واندرموند است نتیجه می‌شود.

از طرف دیگر،فرض کنید t خطا رخ دهد. بیایید معادلاتی را که در آن $e_i \neq ۰$ به معادلاتی را که $e_i = ۰$، به معادلات خوب تعبیر کنیم. بنابراین، t معادله بد و n-t معادله خوب داریم. اگر ما تمامیk معادله ها از $\binom{n}{k}$ زیر دستگاه از معادلات فوق را شامل تمامی معادلات خوب را حل کنیم، آنگاه می‌توانیم a_iهای درست را به دست آوریم. علاوه بر این، یک جواب نادرست نمی‌تواند در هیچ مجموعه ای از k معادله خوب صدق کند و لذا این جواب می‌تواند حداکثر در $t+k-۱$معادله صدق کند. یعنی حداکثر در $\binom{t+k-۱}{k}$ زیر دستگاه از دستگاه فوق، بنابراین، اگر $\binom{t+k-۱}{k} > \binom{n-۱}{k}$آنگاه جواب حداکثر (magrity solution) در میان $\binom{n}{k}$ جواب مقادیر صحیح a_iها را مشخص خواهد کرد. اما این رابطه برقرار است اگر و تنها اگر $t+k-۱ > t-۱$ یعنی، اگر و تنها اگر $d = n-k+۱ > ۲t$.

مطالب فوق را می‌توان در قضیه زیر خلاصه کرد.

قضیه: *فرض کنید C یک کد رید-سولومن $[n,k,d]$باشد. روش کدگشایی با منطق اکثریت می‌تواند حداکثر $t < \frac{۱}{۲}d$ خطا را در انتقال با هزینه، داشتن حل $\binom{n}{k}$ دستگاه از معادلات با اندازه $k \times k$، تصحیح کند.*

کدهای باقمانده مربعی (Quadratic Residue codes)

فرض کنید w یک ریشه n ام واحد روی F_q باشد وقرار دهید.

$$x^n - ۱ = \prod_i m_i(x)$$

جایی که چند جمله‌ای های مینیمال $m_i(x)$ به صورت زیر داده شده‌اند.

$$m_i(x) = \prod_{j \in c_i} (x - w^j), C_i = \{i, iq, \dots iq^{d-۱}\}$$

و C_i، i امین هم دسته دوری در پیمانه q باشد.

قبلاً مشاهده کردیم که یک کد دوری می‌تواند توسط صفرهای آن، Z، کاملاً مشخص شود، جایی که:

$$Z = \{w^i : i \in z\}$$

و z یک اجتماع از هم دسته‌های دوری در پیمانه q است. در مورد کدهای BCH، ما زیر مجموعه‌ای از صفرها را اختیار کردیم که در آن توان‌ها اعداد صحیح متوالی به صورت زیر بودند:

$$S = \{w^{i} = b, b+1, \ldots b+\delta-2\}$$

و سپس، مجموعه صفرها را با در نظر گرفتن اجتماع تمامی هم دسته‌های دوری که اعداد $b, b+1, \ldots, b+\delta-2,1$ را شامل شوند، به دست آوردیم. در مورد کدهای ریدسولومن، هم دسته‌های دوری تک عضو هستند و لذا S تمای ریشه‌های آن کد خواهد بود. نکته ای که در ادامه خواهیم به آن اشاره کنیم، نحوه ساخت دسته‌ای از کدهای دوری است که صفرهای آنها به روش خاصی، ساخته می‌شود.

این کد، ها به کدهای باقیمانده مربعی معروفند.

تعریف: فرض کنید p یک عدد اول باشد. اگر $(a,p)=1$ آنگاه a یک باقیمانده مربعی در پیمانه P نامیده می‌شود، اگر یک X وجود داشته باشد به طوری که در آن:

$$x^{2} \equiv a (\bmod p)$$

اگر چنین X وجود نداشته باشد، آنگاه a را یک غیرباقیمانده مربعی در پیمانهP می‌نامیم. به عبارت دیگر، a یک باقیمانده مربعی است (در پیمانهP)اگر پیمانه P، دارای ریشه باشد. مجموعه باقیمانده های مربعی در پیمانه P را که متعلق به مجموعه $Z_r{}^* = \{1,2,\ldots,p-1\}$ باشند، با QR نمایش داده می‌شوند. به همین منوال، مجموعه غیر باقیمانده‌های مربعی که در $Z_p{}^*$ باشند را با NQR نمایش می‌دهیم. به آسانی دیده می‌شود که هر باقیمانده مربعی در پیمانه P با یک عضو QR هم نهشت است.

قضیه: $QR, |QR| = \frac{P-1}{2}$ به صورت زیر است.

$$QR = \{1^{2}, 2^{2}, \ldots, (\frac{p-1}{2})^{2}\}$$

جایی که اعداد در پیمانه P محاسبه شده‌اند،همچنین :

$$NQR = Z_p^{*} - QR \text{ و} |NQR| = \frac{p-1}{2}$$

مثال: مجموعهٔ باقیمانده های مربعی در پیمانهٔ ۱۱ به صورت زیر هستند:

$$QR = \{1^{2}, 2^{2}, 3^{2}, 4^{2}, 5^{2}\} = \{1, 4, 9, 5, 3\}$$

تعریف: فرض کنید P یک عدد اول باشد و $(a,p)=۱$. نماد لژاندر $\left(\frac{a}{\gamma}\right)$ به صورت زیر تعریف شده است:

$$\left(\frac{a}{\gamma}\right)=\begin{cases}۱ & a\in QR\\ -۱ & a\in NQE\end{cases}\qquad \text{اگر}$$

قضیه (خواص نماد لژاندر): اگر q,p اعداد اول متمایزی باشند و $(a,p)=(b,p)=۱$ آنگاه:

$$۱)\ \left(\frac{۱}{p}\right)=\left(\frac{a^۲}{p}\right)=۱ \qquad ۲)\ a\overset{p}{\equiv}b\Rightarrow(\frac{a}{۲})=\left(\frac{b}{p}\right)$$

$$۳)\ (\text{محک اویلر})\left(\frac{a}{p}\right)\overset{p}{\equiv}a^{\frac{p-۱}{۲}} \qquad ۴)\ \left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

$$۵)\ \left(\frac{-۱}{p}\right)\overset{p}{\equiv}\Leftrightarrow p\overset{۴}{\equiv}۱ \qquad ۶)\ \left(\frac{۲}{p}\right)=۱\Leftrightarrow p\overset{۸}{\equiv}\pm۱$$

$$۷)\ \left(\frac{۳}{p}\right)=۱\Leftrightarrow p\overset{۱۲}{\equiv}\pm۱$$

نتیجه: حاصل‌ضرب دومانده مربعی (همان باقیمانده مربعی) در پیمانه p، یک مانده مربعی دیگر در پیمانه p خواهد بود. حاصل ضرب دو نامانده مربعی (همان باقیمانده مربعی)، در پیمانه P، غیر یک مانده مربعی در پیمانه P است. حاصل ضرب یک مانده مربعی و یک نامانده مربعی در پیمانه P، یک نامانده مربعی در پیمانه خواهد بود.

نتیجه: اگر $S\in QR$، آنگاه $QR=\{sR(\bmod p)\mid r\in Qr\}$

مثال: چون $(\frac{-a^۲}{p})=(\frac{-۱}{p})(\frac{a^۲}{p})=(\frac{-۱}{p})=(-۱)^{\frac{p-۱}{۲}}$ می‌بینیم $x^۲\overset{p}{\equiv}-a^۲$ دارای یک جواب است اگر و تنها اگر $P\overset{p}{\equiv}-a^۲$ دارای یک جواب است و تنها اگر $P\overset{p}{\equiv}۱$.

مثال: هم نهشتی $x^۲\overset{p}{\equiv}۱۵$ را در نظر بگیرید. داریم:

$$(\frac{۱۵}{۱۹})=(\frac{-۴}{۱۹})=(\frac{-۱}{۱۹})(\frac{۲}{۱۹})^۲=(\frac{-۱}{۱۹})=-۱$$

زیرا$19\underset{\neq}{\overset{4}{1}}$. بنابراین، این همنشهشتی دارای جوابی نیست.

کدهای باقیمانده مربعی

در اینجا، تنها روی حالت دوتایی تأکید می‌کنیم. اما، به آسانی می‌توان تعریف را برای حالت غیر دودویی نیز تعمیم داد. می‌دانیم $|QR|=|NQR|=\frac{p-۱}{۲}$ و لذا NQR,QR یک افزار $\{۱,۲,...,p-۱\}$ به بلوک‌های با اندازه یکسان هستند. حال، فرض کنید w یک ریشه اولیه Pام واحد روی F_q باشد.

بنابراین، ریشه‌های Pام واحد به صورت مجموعه $\{۱,w,w^۲,...,w^{p-۱}\}$ هستند.

در اینجا می‌توان دید $Z=\{w^i \mid i\in QR\}$ یک مجموعه کامل از ریشه‌های یک کد دوری q-تایی هستند (برای یک عدد اولq). برای مشاهده این مطلب، کافی است نشان دهیم QR اجتماعی ازهمدسته‌های دوری در پیمانه q است. یعنی باید داشته باشیم.

$$i\in QR \Rightarrow C_i=\{i,iq,...,iq^{d-۱}\}\subseteq QR$$

اما طبق قضایای قبل $i\in QR$، اگر و تنها اگر $iq\in QR$، اگر و تنها اگر $q\in QR$. بنابراین q باید یک عدد اول باقیمانده مربعی در پیمانه P باشد. در این حالت.

$$q(x)\prod_{r\in QR}(x-w^r),n(x)=\prod_{u\in NQR}(x-w^u)$$

دارای ضرایبی در F_q خواهند بود و لذا:

$$x^p-۱=(x-۱)q(x)n(x)$$

حال، می‌توانیم کدهای باقیمانده مربعی را تعریف کنیم.

تعریف: فرض کنید P یک عدد فرد اول باشد و q یک عدد اول باقیانده مربعی در پیمانه p باشد.

کدهای دوری q- تایی

$$Q(p)=<<q(x)>>,\overline{Q(p\cdot}=<<(x-۱)q(x)>>$$
$$N(p)=<<n(x)>>\ \overline{N(p)}=<<(x-۱)n(x)>>$$

با طول p، در $R_p=\frac{F_q[x]}{<x^p-۱>}$ ، کد های باقیمانده مربعی نامیده می‌شود.

چون ما تنها با کدهای باقیمانده مربعی دودویی کار خواهیم کرد، نیاز داریم تا q=۲ یک مانده مربعی در پیمانه P باشد و لذا از این جا به بعد، فرض می‌کنیم P یک عدد اول به شکل $۸m\pm۱$ باشد. واضح است که:

$$\overline{Q(p)} \subseteq Q(p) \quad , \quad \overline{N(p)} \subseteq N(p)$$

در واقع، $\overline{Q(p)}$ زیر مجموعه‌ای از $Q(p)$شامل تمامی کدکلمات با وزن زوج در $Q(p)$ است؛ به طور مشابه، این مطلب را در مورد $N(p),\overline{N(p)}$ داریم. از طرف دیگر داریم:

$$\dim(Q(p)) = p - \deg(q(x)) = p - |QR| = \frac{P+۱}{۲}$$

$$\dim(N(p)) = p - \deg(n(x)) = p\,|NQR| = \frac{p+۱}{۲}$$

کدهای G(p) و N(p) هم ارز هستند. برای مشاهده این مطلب، فرض کنید $N \in NQR$ و جایگشت مکان‌های مختصات کد به صورت $\prod_{۷}(i) = V_i (\bmod p)$ را در نظر بگیرید.

توجه دارید که $\Pi_۷$ می‌تواند با جایگذاری $x^۷$ به جای v و سپس کاهش در پیمانه $x^p - ۱$ به دست آید؛ جایی که علاوه بر آن: $\Pi_۷(f(x)g(x)) = \Pi_v(f(x))\Pi_v(g(x))$

برای مشاهده این مطلب که $\Pi_۷$، Q(p) را به N(p) تصویر می‌کند، قرار می‌دهیم $p(x) = \Pi_۷(q(x))$ در این صورت $p(x) = \Pi_۷(q(x)) \equiv q(x^۷) \equiv \prod_{r \in QR} (x^۷ - w^r) kod(x^p - ۱)$

و لذا یک چند جمله‌ای a(x) وجود دارد که در آن:

$$p(x) = \prod_{r \in QR} (x^۷ - w^r) + a(x)(x^p - ۱)$$

از آنجایی که حاصل ضرب دو نامانده مربعی، یک مانده مربعی است، نتیجه می‌گیریم که برای هر uv در QR است. لذا:

$$P(w^u) = \prod_{r \in QR} (w^{uv} - w^r) + a(w^u)(w^{up} - ۱) = ۰$$

در نتیجه، $p(x), x - w^u$ را عاد می‌کند. (برای تمامی $u \in NQR$)و لذا $n(x) \mid p(x)$. بنابراین $n(x)$ نیز $p(x)$را در پیمانه $x^p - ۱$ عاد می‌کند؛ که در نتیجه:

$$\Pi_۷(Q(p)) = < q(x^۷) \bmod (x^p - ۱) > \subseteq < n(x) > = n(p)$$

اما، چون $\Pi_۷$ یک به یک بوده و $N(p)$, $Q(p)$ دارای اندازه یکسان هستند، داریم $\Pi_۷(q(p)) = N(p)$ و لذا $Q(p), N(p)$ هم ارز هستند. مطالب فوق ار می‌توان در قضیه زیر خلاصه کرد.

قضیه: برای کدهای باقیمانده مربعی به طول p، داریم.

$$\dim(Q(p)) = \dim(N(P)) = \frac{p+۱}{۲}$$

$$\dim(q(p)) = \dim(N(p)) = \frac{p-۱}{۲}$$

علاوه بر این، کدهای $N(p)\,,Q(p)$ هم ارز هستند. همچنین کدهای $\overline{N(p)}\,,\overline{Q(p)}$ هم ارز می‌باشند.

مثال بعد، نشان می‌دهد که کدهای $N(p)\,,Q(p)$ می‌توانند با جایگزینی یک ریشه p–ام اولیه واحد w با ریشه دیگر به دست آینده

مثال: فرض کنید $p=۷$. در این صورت: $QR=\{۱,۴,۲\}, NQR=\{۳,۵,۶\}$

بنابراین، اگر w یک ریشه هفتم اولیه، واحد روی $F_۲$ باشد، آنگاه.

$$Q(x) = (x-w)(x-w^۲)(x-w^۴) = x^۳ x + ۱$$

$$n(x) = (x-w^۳)(x-w^۵)(x-w^۶) = x^۳ + x^۲ + ۱$$

بنابراین، $Q(۷) = << x^۳ + x + ۱ >>$، کد همینگ $[۷,۴,۳]((H_۲(۳))$ است. توجه داشته باشید که $H_۲(۳)$ می‌تواند به صورت یک کد دوری با صفر w مشخص شود.

به طور مشابه، کد $N(۷) = << x^۳ + x^۲ + ۱ >>$، کد دوری با صفر $w^۳$ است (که $w^۳$ نیز یک ریشه ۷ام اولیه واحد است) و لذا کد همینگ $H_۲(۳)$ نیز دوری است.

و کدهای گلی به عنوان کد های باقیمانده مربعی

قبلا مشاهده کردیم که چگونه می‌توان $x^n - ۱$ را تجزیه کرد. (به عوامل تحویل ناپذیر روی $F_q[x]$). با به کارگیری این روشن.

$$x^{۲۳} - ۱ = (x+۱)(x^{۱۱} + x^۹ + x^۷ + x^۶ + x^۵ + x + ۱)(x^{۱۱} + x^{۱۰} + x^۶ + x^۵ + x^۴ + x^۲ + ۱)$$

تجزیه $x^{۲۳} - ۱$ به عوامل تحویل ناپذیری روی $F_۲$ است. حال چون ۲ یک مانده مربعی در پیمانه است، لذا: $x^{۲۳} - ۱ = (x-۱)q(x)n(x)$

بنابراین، کد گلی $G_{۲۳}$ هم ارز با کد باقیمانده مربعی $Q(۲۳)$ خواهد بود.

به روش مشابه، روی $F_۳$ داریم:

$$x^{۱۱} - ۱ = (x-۱)(x^۵ + x^۴ - x^۳ + x^۲ - ۱)(x^۵ - x^۳ + x^۲ + x - ۱)$$

جایی که عوامل فوق، تحویل ناپذیر بوده و چون ۳ یک مانده مربعی در پیمانه ۱۱ است، نتیجه می‌گیریم که $G_{۱۱}$ هم ارز با یک کد باقیمانده مربع سه تایی $Q(۱۱)$ است.

کران ریشه مربعی (The Square root bound)

حال، می‌خواهیم درباره کمترین فاصله یک کد باقیمانده مربعی مطالبی را بدانیم. به نظر می‌رسد که با توجه به مطالب قبل، کمترین فاصله یک کد باقیمانده مربعی، فرد است. در اینجا، نتیجه زیر را داریم که به کران ریشه مربعی معروف است. متأسفانه، این کران اغلب خیلی خوب نیست.

قضیه: (کران ریشه مربعی)، مترین فاصله d از کدهای دوتایی $N(p),Q(p)$ در رابطه $d^۲ \geq p$ صدق می‌کند. علاوه بر این اگر. $p=۸m-۱$ آنگاه:

$$d^۲-d+۱\geq p$$

می‌توان دید که اگر $u\in NQR$ آنگاه $C(x)=c(x^u)\operatorname{mod}(x^p-۱)$ یک کلمه با وزن مینیمم d در $N(P)$ است. بنابراین، چند جمله‌ای

$$P(x)=[c(x)\overline{c(x)}]\operatorname{mod}(x^p-۱)=[c(x)c(x^u)]\operatorname{mod}(x^p-۱)$$

****

$$q(x)n(x)=\frac{x^p-۱}{x-۱}=۱+x+x^۲+...+x^{p-۱}$$

در واقع، ازاین که $Q(p)$ دارای کمترین وزن فرد است؛ نتیجه می‌شود:

$p(x)\neq o$ به طور خلاصه p(x) ناصفر است، بر $q(x)n(x)$ بخش پذیر است و دارای درجه حداکثر P-۱ است و لذا p(x) باید مضرب اسکالر ناصفری از $q(x)n(x)$ باشد.

در نتیجه، $C(x)C(x^u)$ دارای وزن حداقل p است. اما $c(x^u),c(x)$ دارای d جمله ناصفر هستند و لذا این حاصل ضرب نمی‌تواند دارای بیشتر از $d^۲$ جمله ناصفر باشد. لذا $d^۲\geq p$.

اگر $p=۸m-۱$، آنگاه $C(x)C(x-۱)$ دارای حداکثر $d^۲$ جمله ناصفر است که d جمله آن به صورت $a_ix^ix^{-i}=a_i$ است که ثابت می‌باشد. بنابراین همه این جملات به یک جمله تبدیل شده و $C(x)c(x^{-۱})$ دارای وزن حداکثر $d^۲-d+۱$ خواهد بود که در نتیجه:

$$d^۲-d+۱\geq p$$

مثال: کدهای باقیمانده مربعی دوتایی با طول $p=۷$ دارای کمترین فاصله d هستند که در رابطه $d^۲-d+۱\geq ۷$ صدق می‌کند. لذا $d\geq ۳$ آنچنان که قبلا مشاهده کردیم، کد باقیمانده مربعی [۷,۴] دارای کمترین فاصله d=۳ است.

توجه جدول زیر، برخی پارامترهای مربوط به کدهای مانده دوتایی را به همراه کران های پائینی کمترین فاصله (از قضیه قبل) لیست کرده است.

کران پایین روی d	d	k	p
۳	۳	۴	۷
۴	۵	۹	۱۷
۶	۷	۱۲	۲۳
۶	۷	۱۶	۳۱
۶	۹	۲۱	۴۱
۸	۱۱	۲۴	۴۷
۹	۱۱	۳۶	۷۱
۹	۱۳	۳۷	۷۳
۱۰	۱۵	۴۰	۷۹
۹	۱۷	۴۵	۸۹
۹	۱۵	۴۹	۹۷
۱۱	۱۹	۵۲	۱۰۳
۱۲	۱۹	۶۷	۱۲۷
۱۳	۱۹	۷۶	۱۵۱