

به نام خدا

## جزوه کدگذاری ۱

محمد غلامی

دانشیار دانشکده ریاضی دانشگاه شهرکرد- گرایش کدگذاری و رمزنگاری

آنترپی:

منبع (Source): یک منبع، یک زوج مرتب  $(S, P)$  است که در آن  $S = \{x_1, \dots, x_n\}$  یک

مجموعه متناهی است که الفبای منبع نامیده می شود و  $P$  یک توزیع احتمال روی  $S$  است.

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

**ابهام** (*Uncertainty*): قبل از نمونه گیری، نسبت به خروجی مقدار معینی ابهام وجود دارد

و پس از نمونه گیری، مقدار مشخصی اطلاعات (*information*) درباره منبع به دست می -

آوریم. بنابراین، مفاهیم میزان ابهام و اطلاعات با یکدیگر مربوطند.

**مثال:** فرض کنید  $S = \{x_1, \dots, x_n\}$ . اگر  $P(x_1) = 1$  و  $P(x_i) = 0$  برای هر  $i > 1$ ، آنگاه  $x_i$  همواره

انتخاب شده و لذا ابهامی در این حالت نسبت به خروجی نداریم، پس میزان ابهام برابر با

صفر است. در این مثال هیچ نمونه ای 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 می دهد که خروجی دارای توزیع یکنواخت باشد، یعنی

$$\forall 1 \leq i \leq n, P_i = \frac{1}{n}$$

**تعریف.** فرض کنید  $X$  یک متغیر تصادفی با برد  $S = \{x_1, \dots, x_n\}$  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 از مشاهده خروجی و یا متوسط کمترین تعداد بیت

لازم برای توصیف  $X$  می باشد.

**تعریف.** فرض کنید  $X$  و  $Y$  متغیرهای تصادفی با بردهای به ترتیب  $S_1 = \{x_1, \dots, x_n\}$  و

$S_2 = \{y_1, \dots, y_m\}$  باشند. اگر  $p(x_i, y_j) = p(X = x_i, Y = y_j)$  توزیع احتمال رخ دادن همزمان

$X$  و  $Y$  باشد، آنگاه آنتروپی توأم  $Y, X$  به صورت زیر تعریف می شود.

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

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

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

$$p(x_1, \dots, x_n) = p(X_1 = x_1, \dots, X_n = x_n)$$

آنگاه آنتروپی توأم  $X_k, \dots, X_1$  به صورت زیر تعریف می شود:

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

**مثال.** فرض کنید  $X$  یک متغیر تصادفی با توزیع یکنواخت روی  $\{x_1, \dots, x_n\}$  باشد (به عبارت

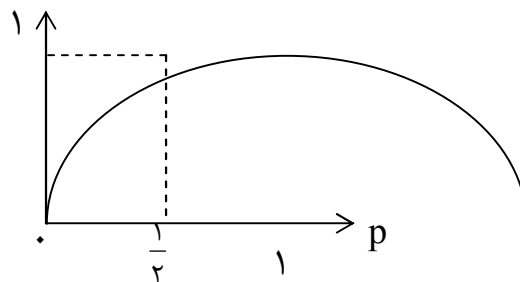
دیگر  $P(X = x_i) = \frac{1}{n}$  برای هر  $1 \leq i \leq n$ )، آنگاه:

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

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



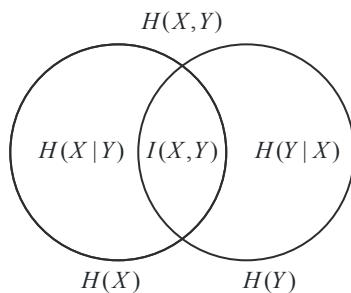
در این صورت اطلاعات متقابل (*mutually information*) بین  $Y, X$  به صورت زیر تعریف می شود:

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

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

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

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



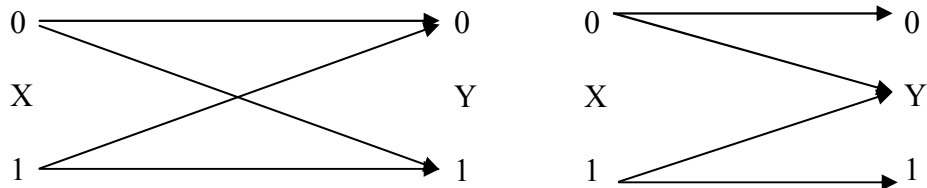
- 1)  $I(X, Y) = I(Y, X)$
- 2)  $H(X, Y) = H(X | Y) + H(Y)$
- 3)  $H(X, Y) \leq H(X) + H(Y)$
- 4)  $I(X, Y) = H(X) + H(Y) - H(X, Y)$

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

**تعریف.** ظرفیت یک کانال، بیشترین اطلاعات متقابل  $I(X, Y)$  روی تمامی توزیع‌های

ورودی  $P(x)$  از  $X$  است؛ به عبارت دیگر  $\zeta = \max_{P(x)} I(X, Y)$ .

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



کانال  $BEC$  کانال  $BSC$

## 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  $A = \{a_1, a_2, \dots, a_q\}$  یک مجموعه متناهی باشد که الفبای کد

نامیده می شود و فرض کنید  $A^n$  تمامی رشته های به طور  $n$  روی  $A$  باشد؛ یعنی:

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

در این صورت هر زیر مجموعه ناتهی  $C$  از  $A^n$  یک کد بلوکی  $q$ -تایی نامیده می شود. هر عضو

$C$  یک کد کلمه نامیده می شود. اگر  $C \subseteq A^n$  دارای  $M$  کد کلمه باشد، آنگاه گوییم  $C$  دارای

طول  $n$  و اندازه  $M$  است و آن را یک  $(n, M)$ -کد می نامیم. نرخ (rate) یک  $(n, M)$ -کد  $q$ -

$$\text{تایی برابر با } R = \frac{\log_q M}{n} \text{ است.}$$

**کانال.** یک کانال مخابراتی را می‌توان به این صورت فرض نمود که یک کد کلمه

از  $c = c_1 \dots c_n$  (با طول  $n$  روی الفبای کد  $A$ ) را دریافت نموده و خروجی آن یک

رشته خروجی  $d = d_1 \dots d_n$  (با همان طول  $n$  روی الفبای شامل  $A$ ) است.

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

شامل یک الفبای ورودی  $A = \{a_1, \dots, a_q\}$ ، یک الفبای خروجی  $O = \{b_1, \dots, b_t\}$  ( $A \subseteq O$ ) و

یک مجموعه از احتمالات کانال یا احتمال‌های انتقال (*transition probabilities*)

$p(b_j | a_i)$  است که در رابطه زیر صدق می‌کنند.

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

که در آن  $p(b_j | a_i)$  احتمال آن است که  $b_j$  دریافت شده باشد به شرط آنکه  $a_i$  ارسال شده

باشد. علاوه بر این، اگر  $d = d_1 \dots d_n, c = c_1 \dots c_n$  به ترتیب کلماتی به طول  $n$  روی  $A$  و  $O$

$$. p(d | c) = \prod_{i=1}^n P(d_i | c_i)$$
 باشند، آنگاه

**مثال.** مهم‌ترین کانال بدون حافظه گسسته (*DMC*)، کانال دوتایی متقارن *BSC*

(*binary symmetric channel*) است که به صورت زیر می‌باشد.

$$p(1 | 0) = p(0 | 1) = p, \quad p(0 | 0) = p(1 | 1) = 1 - p$$

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

**ماتریس کانال.** اگر  $\left\{ \begin{array}{l} p(b_j | a_i) \\ 1 \leq i \leq q, 1 \leq j \leq t \end{array} \right.$  احتمال‌های انتقال یک کانال باشند، که در آن به

$A = \{a_1, \dots, a_q\}$  و  $O = \{b_1, \dots, b_t\}$  به ترتیب الفبای ورودی و خروجی کانال باشند، آنگاه

ماتریس  $(P(b_j | a_i))_{1 \leq i \leq q, 1 \leq j \leq t}$  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 این صورت طبق قاعده بیزداریم:

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

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 می‌دهند. در این حالت، طراحی و ساخت کدهایی که به منظور غلبه بر خطاهای گروهی مفید هستند، مورد بحث و بررسی قرار می‌گیرد.

### **قاعده تصمیم (*Decision scheme*):**

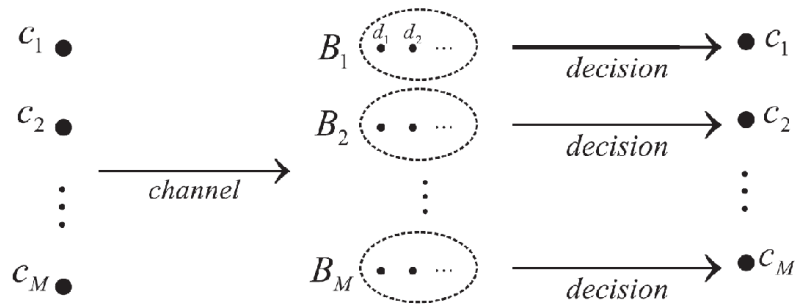
قاعده تصمیم، یک تابع جزئی مانند  $f$  از مجموعه رشته‌های خروجی به مجموعه کد کلمات است. کلمه جزئی به این مطلب اشاره دارد که  $f$  ممکن است روی تمامی رشته‌های خروجی تعریف نشده باشد. به عبارت دیگر اگر رشته‌ی خروجی  $d$  دریافت شده باشد و  $f(d)$  قابل تعریف باشد، آنگاه قاعده تصمیم، تصمیم می‌گیرد که  $f(d)$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

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

حال فرض کنید  $C = \{c_1, \dots, c_M\}$  مجموعه تمامی کلمات و  $B_i = f^{-1}(c_i) = \{d \mid f(d) = c_i\}$

مجموعه تمامی خروجی‌ها باشد که تصمیم می‌گیریم ورودی صحیح برابر با  $c_i$  است، در

اینصورت رشته‌های خروجی را می‌توان به مجموعه  $\{B_1, \dots, B_m\}$  افزار نمود.



هدف کدگذاری، طراحی یک قاعده تصمیم مناسب است که تلاش می‌کند تا هر خطایی

را در انتقال تصحیح نماید.

## احتمال تشخیص خطا

اگر کد کلمه  $C$  ارسال شده باشد و در کانال، خطا رخ داده باشد، زمانی این خطا غیر قابل

تشخیص است که کلمه دریافتی یک کد کلمه دیگر باشد، به عبارت دیگر:

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

بنابراین احتمال عدم تشخیص خطا به صورت زیر است:

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

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

## احتمال تصحیح خطا

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

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

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

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

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 کمتر می‌نماید،

احتمال خطا را به شرط داشتن یک خروجی، محاسبه می‌کنند (به جای ورودی).

اگر  $d$  دریافت شده باشد، آنگاه:

$$p(\text{err} | d) = 1 - p(f(d) | d)$$

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

بنابراین با متوسط گیری روی تمامی مقادیر خروجی ممکن داریم:

$$p_e = \sum_d p(\text{err} | d) p(d) = 1 - \sum_d p(f(d) | d) p(d)$$

بنابراین برای مینیمم کردن  $p_e$  باید  $\sum p(f(d) | d) p(d)$  را ماکسیم کنیم. ولی چون تمامی

جملات  $p(f(d) | d) p(d)$  مثبت بوده و  $p(d)$  نیز به  $f$  بستگی ندارد، این مقدار ماکسیمم است

اگر و تنها اگر  $p(f(d) | d)$  ماکسیمم باشد. پس تعریف زیر را داریم:

**تعریف.** به ازای یک توزیع ورودی داده شده، قاعده تصمیم زیر که در رابطه زیر صدق می -

$$p(f(d)|d) = \max_c p(c|d) \text{ داشته باشیم}$$

یک مشاهده گر مطلوب (*ideal observer*) نامیده می شود. به عبارت دیگر، یک مشاهده -

گر مطلوب، یک قاعده تصمیم است که احتمال خطای تصمیم یا  $P_e$  را کمترین می کند.

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

**نکته.** مشاهده گر مطلوب دارای معایب و مزایایی است. یکی از مهم ترین معایب آن، این

است که به توزیع ورودی بستگی دارد. یعنی اگر توزیع ورودی تغییر کند، احتمالاً مشاهده -

گر مطلوب نیز تغییر می کند. برای حذف این وابستگی، به جای مینیم کردن  $p_e$ ، می توانیم

$p_e^{\max}$  را مینیم کنیم که در آن:

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

در این حالت  $p_e^{\max}$  تنها به وابستگی 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 کد است. 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، ما کسیم کردن  $p(c|d)$  معادل با ما کسیم کردن  $p(d|c)$  است.

تعریف قاعده تصمیم  $f$  به طوری که  $f(d)$  دارای این خاصیت باشد که به ازای هر خروجی

$$p(d|f(d)) = \max_c p(d|c) \text{ باشیم}$$

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

به عبارت دیگر  $f(d)$  یک رشته ورودی با این خاصیت است که هیچ رشته ورودی دیگری

احتمال دریافت  $d$  را به اندازه آن ما کسیم نمی کند.

**قضیه:** به ازای توزیع ورودی یکنواخت، قاعده مشاهده گر مطلوب همان قاعده تصمیم

بیشترین درستنمایی است.

## قضیه کانال نویز دار.

کانال بدون حافظه با ظرفیت  $\zeta$  را در نظر بگیرید. برای هر مقدار مثبت  $R$  که در آن  $R < \zeta$ ,

یک دنباله  $C_n$  از کدهای  $r$ -تایی و قاعده تصمیم متناظر  $f_n$  با شرایط 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  $n \rightarrow \infty$ ، به صفر می کند؛ یعنی:

$$p_e^{\max}(n) \rightarrow 0$$

**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 ارائه 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 در طول‌های بزرگ وعده می‌دهد که ممکن است از نظر عملی غیر قابل کاربرد باشند. به منظور دست یافتن به قاعده تصمیم مناسب، پژوهشگران به دنبال طراحی و ساخت کدهای جبری و هندسه 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

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

**مثال.** اگر  $x=10112$  و  $y=20110$  آنگاه  $d(m,y)=2$ ، زیرا  $x,y$  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 الفای  $A$  باشند، در این صورت تابع

فاصله همینگ  $d: A^n \times A^n \rightarrow \mathbb{N} \cup \{0\}$  در خواص زیر صدق می کند.

برای هر  $x,y,z$  در  $A^n$  داریم:

$$d(x,y) \geq 0, \quad d(x,y) = 0 \Leftrightarrow x = y \quad \text{۱- (معین مثبت)}$$

$$d(x,y) = d(y,x) \quad \text{۲- (تقارن)}$$

$$d(x,y) \leq d(x,z) + d(z,y) \quad \text{۳- (نامساوی مثلثی)}$$

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

اگر کد کلمه  $c$  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  $P < \frac{1}{4}$ ، این احتمال بیشترین است، اگر  $d(c,d)$  کمترین باشد. بنابراین کد گشایی

MLD (کد گشایی با بیشترین درستنمایی) معادل با انتخاب کد کلمه  $c$  است که به کلمه  $d$  از

همه کلمات دیگر نزدیک تر باشد. به این قاعده، کد گشایی با کمترین فاصله یا قاعده

(MDD minimum distance decoding) می گوئیم.

**مثال.**  $C = \{000, 111\}$  کد تکرار دوتایی به طول ۳ است. با استفاده از قاعده کدگشایی با کمترین فاصله، کدگشا دچار خطا می‌گردد اگر و تنها اگر حداقل دو خطا رخ دهد، بنابراین:

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

### احتمال خطای کدگشایی

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

**نکته.** در اثبات قضیه کدگشایی کانال، از کدگشایی غیر کامل بهره می‌گیریم.

**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 سمبل‌های ممکن دیگر باشد."

**نتیجه.** در کانال BEC با ماتریس کانال  $\begin{bmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{bmatrix}$ ،  $P < \frac{1}{2}$ ، MLD معادل قاعده MDD است.



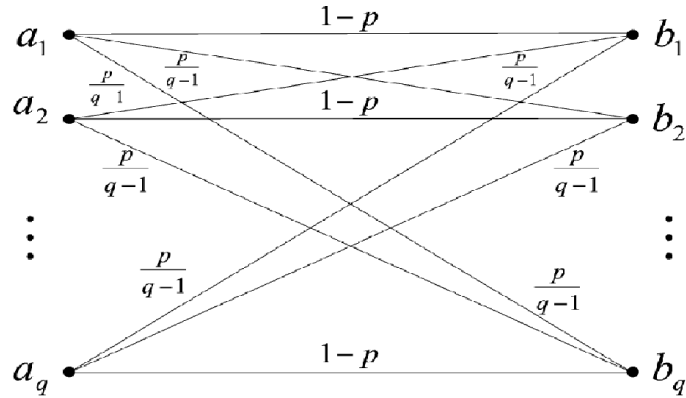
**مثال.** کانال  $q$ -تایی متقارن به صورت زیر است:

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

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 می شود:

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

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 می شود، اگر حداکثر  $t$

خطا (و حداقل یک خطا) روی هر کد کلمه رخ دهد، آنگاه کلمه دریافتی، یک کد کلمه

نباشد. کد  $C$ ، تشخیص دهنده دقیقاً  $t$  خطا نامیده می شود 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 کد کلمه باشد (با این فرض که تمام گره‌ها ( $t$ ies) به عنوان خطا گزارش شوند). کد  $C$ ، تصحیح کننده دقیقاً  $t$  خطاست اگر تصحیح کننده  $t$  خطا بوده، اما تصحیح کننده  $t+1$  خطا نباشد.

**قضیه.** کد  $C$  تصحیح کننده دقیقاً  $t$  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  $d(c, d) \leq t$ . در این صورت  $d$  به  $c$  از همه کدکلمات دیگر نزدیک تر است، زیرا اگر وجود داشته باشد  $c' \in C$  به طوری که  $c' \neq c$  و  $d(c', d) \leq t$ ، آنگاه:

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

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

الف -  $d(C) = 2t+1$ . پس  $c \neq c' \in C$  وجود دارد به طوری که  $d(c, c') = 2t+1$ . حال فرض کنید  $c$  ارسال و  $d$  دریافت شده باشد به طوری که  $d(c, d) = t+1$ ،  $d(c', d) = t$ . در واقع  $d$  به این صورت ساخته می‌شود که در  $t+1$  مکان از  $2t+1$  مکان متفاوت  $c$  و  $c'$ ، با  $c$  برابر بوده و در  $t$  مکان باقیمانده با  $c'$  برابر باشد. بنابراین طبق قاعده کدگشایی MDD،  $d$  به  $c'$  کدگشایی می‌شود که اشتباه است. پس  $C$  تصحیح کننده  $t+1$  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  $d(c', d) = d(c, d) = t + 1$ ، آنگاه یک گره رخ داده و کد گشا اعلام خطا می‌کند.

برعکس، اگر  $C$  تصحیح کننده دقیقاً  $t$  خطا باشد، آنگاه نمی‌توانیم داشته باشیم  $d(c, c') \leq 2t$ . زیرا در غیراین صورت 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  $c'$  کد گشایی می‌گردد، یا اعلام خطا می‌گردد (در حالت گره). بنابراین  $d(C) \geq 2t + 1$ . اما اگر  $d(c) \geq 2t + 3 = 2(t + 1) + 1$  آنگاه طبق قسمت اول، کد  $C$ ، تصحیح کننده  $t + 1$  خطا می‌باشد که با فرض در تناقض است؛ پس

$$d(C) = 2t + 1, 2t + 2$$

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

**مثال.** کد تکرار  $q$ -تایی به طول  $n$  به صورت  $C = \{0 \dots 0, 11 \dots 1, \dots, (q-1) \dots (q-1)\}$  است.

کمترین فاصله این کد  $d(C) = n$  است. بنابراین، این کد، تصحیح کننده دقیقاً  $\lfloor \frac{n-1}{2} \rfloor$  خطا

است. این کد همچنین قادر به تشخیص  $n - 1 = d - 1$  خطا می‌باشد.

### رابطه بین کمترین فاصله و احتمال خطا.

**تعریف.** یک  $(n, M, d)$ -کد، ماکسیمال نامیده می‌شود اگر مشمول در هیچکدی نباشد.

**مثال.** کد  $C = \{000, 111, 333\}$  روی الفبای  $A = \{0, 1, 2, 3\}$  ماکسیمالیست، زیرا  $C$  یک  $(3, 3, 3)$ -کد

است که می‌توان با اضافه کردن کلمه ۲۲۲ مشاهده نمود این کد هنوز یک  $(3, 3, 3)$ -کد

است؛ ولی  $C \cup \{222\}$  ماکسیمال است (چرا؟)

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

برای هر کلمه مانند  $x$ ، یک کد کلمه  $c \in C$  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 کد کلمه دیگری نزدیک تر خواهد بود و لذا در این حالت خطا در کد گشایی 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:

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

بنابراین:

$$P_{\text{decode err}} = 1 - P_{\text{correct}} \leq 1 - \sum_{k=0}^t \binom{n}{k} p^k (1-p)^{n-k}$$

که در آن  $t = \lfloor \frac{d-1}{2} \rfloor$ . حال اگر تعریف کنیم:

$$B_p(n, m) = \sum_{k=0}^m \binom{n}{k} p^k (1-p)^{n-k}$$

آنگاه قضیه زیر را داریم:

**قضیه.** در یک کانال دوتایی متقارن  $BSC(p)$ ، احتمال خطای کدگشایی برای یک کد

$(n, M, d)$  ما کسیمال در رابطه زیر صدق می کند:

$$B_p(n, d-1) \leq p_{\text{decode err}} \leq 1 - B_p(n, \lfloor \frac{d-1}{2} \rfloor)$$

**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 زیر تعریف می شود:

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

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

$$V_q(n, r) = \sum_{k=0}^r \binom{n}{k} (q-1)^k$$

**مثال.** اگر  $A = \{0, 1\}$  آنگاه  $A^3$  را می توان به صورت زیر نمایش داد:

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

\*\*\*

حال فرض کنید  $C_1$  یک کد  $(n, M, d)$  تصحیح کننده  $t$ -خطا باشد. در این صورت:

$$\forall i \neq j \quad S_q(c_i, t) \cap S_q(c_j, t) = \emptyset$$

\*\*\*\*

زیرا در غیر این صورت وجود دارد  $x \in S_q(c_i, t) \cap S_q(c_j, t)$  به طوری که:

$$d(x, c_i) \leq t, d(x, c_j) \leq t \Rightarrow d(c_i, c_j) \leq d(x, c_i) + d(x, c_j) \leq t + t = 2t < d$$

$$(d = 2t+1 \text{ or } 2t+2)$$

**تعریف.** فرض کنید  $C \subseteq A^n$ . شعاع فشردگی  $C$  بزرگترین عدد صحیح  $r$  است که در آن گوی‌های  $S_q(c, r)$  حول کلمات  $C$  مجزا باشند. شعاع پوششی  $C$  کوچکترین عدد صحیح  $s$  است به طوری که گوی‌های  $S_q(c, s)$  فضای  $A^n$  را 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 دقیقاً  $t$  خطاست اگر و تنها اگر  $Pr(c) = t$ .

### کدهای کامل و شبه کامل.

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

**مثال.** کدهای همینگ  $H_2(3)$  یک کد دوتایی  $(7, 4, 3)$  است.

در واقع:

$$H_2(3) = \{c_1c_2\dots c_7 \mid c_i \in \{0,1\}, c_1 + c_4 + c_5 + c_7 \equiv c_2 + c_4 + c_5 + c_7 \equiv c_3 + c_5 + c_6 + c_7 \equiv 0\}$$

$$= \{1101100, 1010100, 0110010, 1110001, 0111100, 1011010, 0011001, 0100101, 1100110, 1000011, 100001110, 1001101, 0010111, 0101011, 11111111, 0000000\}$$

این کد  $t=1$  واضح است که  $|S_2(c,1)|=1+\binom{7}{1}=8$  و  $|A^7|=2^7=128$  اما  $128=8 \times 16$ ، لذا

$$A^n = \bigcup_{C \in C} S_2(c,1)$$

پس این که، 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

$$d = 2t + 1 \text{ خرد باشد و } M.V_q(n,t) = q^n \text{، به عبارت دیگر.}$$

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

## خانواده کدها

۱- کدهای سیستماتیک: یک کد  $q$ -تایی  $(n, q^k)$ ، سیستماتیک نامیده می شود اگر  $k$  مکان

$i_1, \dots, i_k$  با این خاصیت وجود داشته باشند که با تحدید نمودن کد کلمات به این مکانها،

تمامی  $q^k$ ، آرایه  $Q$  تایی به طور  $k$  را داشته باشیم. مکانهای  $\{i_1, \dots, i_k\}$  مجموعه اطلاعات

(*information set*) و سمبل های کد کلمات در این مکانها سمبل های اطلاعات

(*information symbols*) نامیده می شوند.

در این حالت، اگر منبع را بتوان به صورت مجموعه تمامی کلمات  $q$ -تایی به طول  $k$  نمایش

داد، آنگاه یک کد سیستماتیک  $q$ -تایی از اندازه  $q^k$  می تواند به منظور کد گذاری چنین

منبعی، بدون تغییر کلمات به کار رود.

مثال: کد دوتایی  $C = \{000, 011, 100, 101\}$  روی مکان اول و سوم سیستماتیک است بنابراین

اگر منبع  $S = \{0, 1\}$  را به کار ببریم، می توان منبع  $K$  را به صورت زیر کد گذاری نمود:

$00 \rightarrow 000, 01 \rightarrow 100, 11 \rightarrow 101, 10 \rightarrow 101$  چنین کد گذاری، یک کد گذاری سیستماتیک نامیده می -

شود. واضح است که فرآیند کد گشایی در این صورت، بسیار ساده بوده و کافی است تا

کلمات منبع را به طور مستقیم از کد همه دریافتی استخراج کنیم.

مثال: کد دوتایی  $C = \{000, 100, 101, 001\}$  سیستماتیک نیست. (چرا؟)

### میدان های متناهی (finite fields)

برای یان که به کدهای خود، ساختارهای با معنی ببخشیم، فرض می کنیم  $A$  به عنوان الفبای کد

داریا 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 یکرختی یا

دقیقاً یک میدان متناهی از اندازه  $q = p^n$  وجود دارد که آن را با  $GF(q)$  یا  $F_q$  نمایش می دهیم.

علاوه بر این، تمامی میدان های متناهی دارای اندازه  $P^n$  برای مقادری  $p$  اول و صحیح مثبت

$n$  هستند.

مجموعه  $(F_q)^n$  شامل تمام  $n$  تایی های مولفه های متعلق به  $F_q$ ، یک فضای برداری روی

$F_q$  با بعد  $n$  می باشد (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 قبلاً دیدیم) دو کد  $C_1 = \{000, 011\}$ ,  $C_2 = \{000, 101\}$  یکسان است و در عمل هیچ تفاوت با یکدیگر ندارند. دلیل آن، هم ارز بودن  $C_1, C_2$  که به صورت زیر تعریف می‌شود.

تعریف: دو کد  $q$ -تایی  $(n, m)$ ،  $C_1, C_2$  هم ارز (*equivalent*) نامیده می‌شوند. اگر جایگشت  $\sigma$  روی  $n$  مکان مختصات و جایگشت‌های  $\pi_1, \pi_2, \dots, \pi_n$  روی الفبای کد وجود داشته باشد. به

$$طوری که  $c_1 c_2 \dots c_n \in C_1 \Leftrightarrow \pi_1(c_{\sigma(1)}) \pi_2(c_{\sigma(2)}) \dots \pi_n(c_{\sigma(n)}) \in C_2$$$

به عبارت دیگر، دو کد هم ارزش هستند اگر بتوان با جایگشت روی مکان‌های هر کد کلمه (از طریق  $\sigma$ ) و جایگشت روی سمبل‌های هر مکان از هر کد کلمه (از طریق  $\pi_1, \dots, \pi_n$ )، از یکی به دیگری رسید.

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

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

اثبات: کد کلمه  $c_1 c_2 \dots c_n$  را به طور دلخواه از کد  $C$  در نظر بگیرید و جایگشت‌ها را زیر روی مکان‌های آن (به ترتیب)، اعمال کنید.

$$i \text{ مکان } x_i \neq o \Rightarrow \pi_i = \begin{pmatrix} c_i & o & j \\ \downarrow & \downarrow & \downarrow \\ o & c_i & j \end{pmatrix}, j \in A - \{o, c_i\}$$

قضیه: اگر کدهای  $C_1$  و  $C_2$  معادل باشند آنگاه  $d(c_1) = d(c_2)$ ، همچنین احتمال تصحیح خطای کد گشایی  $C_1, C_2$  روی کانال‌های  $q$ -تایی متقارن با یکدیگر برابر است.

## (۲) کدهای خطی (linear codes):

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

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: تمام یکده ای خطی، شامل کد کلمه صفر  $\circ = \circ \dots \circ$  هستند و نیز نرخ و اندازه یک

$$[n, k] \text{ کد } q\text{-تایی به صورت زیر تعریف می‌شود } R = \frac{k}{n}, m = q^k.$$

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 ناصفر  $C$  است.

تعریف: اگر  $x = x_1 \dots x_n$  و  $y = y_1 \dots y_n$  دو کلمه دوتایی باشند، آنگاه اشتراک  $f, x$

(intersection) به صورت زیر تعریف می‌شود:

$$x \cap y = (x_1 y_1, x_2 y_2, \dots, x_n y_n)$$

لم:

$$(1) \quad \text{برای تمامی } x, y \leftarrow V(n, q) \text{ داریم: } d(x, y) = w(x - y)$$

$$(2) \quad \text{برای تمامی } (q=2)x, y \leftarrow V(n, 2) \text{ داریم } d(x, y) = w(x) + w(y) - 2w(x)$$

اثبات: (تمرین)

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

اما در رمورد یک کد خطیف تنها به  $M-1$  محاسبه نیاز داریم (مطابق قضیه زیر)

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

$$d(L) = \min_{C \neq d} d(c, d) = \min_{C \neq d \in L} (c, d) = \min_{\circ \neq C \in L} w(c-d) = \min_{\circ \neq c-d \in L} w(c) = w(L)$$

### کدهای دوری (cyclic codes)

بسیاری از کدهای مهم، به طور قابل ملاحظه‌ای، دارای ساختاری، بیشتر از یک فضای

برداری هستند. کد خطی  $L \subseteq C(n, q)$  به صورت زیر نسبت داد:

$$\phi: C_0 C_1 \dots C_{n-1} \rightarrow C_0 + C_1 x + \dots + C_{n-1} x^{n-1}$$

در واقع،  $\phi$  یک یکرختی 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 یان کار، این است که  $F_q[x]$  دارای ساختار بیشتری از فضای برداری است، در واقع

$F_q[x]$  یک جبر است به عبارت دیگر، ما می‌توانیم تو کد کلمه را در یکدیگر ضرب کنیم

(قبلا در فضای برداری نمی توانستیم) ولی ممکن است ضرب آنها دیگر یک کد کلمه نباشد، برای این منظور ایده خود را ظریف تر می کنیم. فرض کنید  $P(x)$  یک چند جمله‌ای با درجه  $F_q[x]$  باشد، در این صورت.

$$\langle P(x) \rangle = \{f(x)P(x) \mid f(x) \in F_q[x]\}$$

(quotient algebra)، مجموعه تمامی چند جمله‌ای های  $F(x)$  با درجه حداکثر  $n$  است که به صورت زیر تعریف می شود.

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

به عبارت دیگر  $R$ ، مجموعه تمامی چند جمله‌ای ها در  $F_q[x]$  است که در پیمانه  $P(x)$  محاسبه می شوند. (مشابه با حلقه  $Z_m$  که عناصر در پیمانه  $M$  محاسبه می شوند). در این حالت حاصل ضرب هر دو چند جمله‌ای از  $R$  خواهد بود. در این حالت نگاشت  $\phi$  را می توان یک یکرختی از فضای برداری  $L$  به زیر فضای  $\phi(L)$  از  $R$  تصور کرد که در این حالت  $\phi(L)$  یک زیر جبر از  $R$  است ولی: می توان  $\phi(L)$  را به صورت یک ایده آل (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.

$$R_n = \frac{F_q[x]}{\langle x^n - 1 \rangle}$$

حال فرض کنید  $p(x) = x^n - 1$  و  $R_n$  را جبر خارج قسمتی در نظر بگیرید

اگر  $L$  یک ایده آل از  $R_n$  باشد ( $L \Delta R_n$ )، آنگاه ساعت ضرب هر چند جمله‌ای از  $R_n$  بسته است اما این معادل با آن است که ساعت ضرب توسط  $x$  بسته باشد، اما (در  $R_n$  داریم)

$$x(C_0 + C_1x + \dots + C_{n-1}x^{n-1}) = (C_0x + C_1x^2 + \dots + C_{n-1}x^n) \pmod{(x^n - 1)} = C_{n-1} + C_0x + C_1x^2 + \dots + C_{n-2}x^{n-1}$$

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

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

به عبارت دیگر  $C_1 - C_{n-1} \in C_0 \in L \Leftrightarrow C_0C_1 - C_{n-1} \in L$  تعریف زیر را دنبال

دارد.

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

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

به عبارت دیگر،  $L$  دوری است اگر  $L \triangleleft R_n = \frac{F_q[x]}{\langle x^n - 1 \rangle}$

نکته  $R_n$  یک دامنه ایده‌آل 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:

$$C = \langle g(x) \rangle = \{f(x)g(x) \mid F(x) \in R\}$$

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

علاوه بر این  $g(x) \mid x^n - 1$ ، زیرا در غیر این صورت اگر  $r(x)$  باقیمانده ناصفر  $x^n - 1$  بر  $g(x)$

باشد، داریم  $\deg r(x) < \deg g(x)$ ،  $r(m) \in C$  که با فرض  $g(x)$  در تناقض است بنابراین

تمامی ریشه‌های  $g(x)$  ریشه‌های  $x^n - 1$  هستند (یعنی  $x^n = 1$  یا ریشه  $n$ ام واحد) لذا، می-

توانیم یک کد دوری را با تخصیص چند جمله‌ای مولد آن ( $g(x)$ ) یا به طور هم ارز، تعیین ریشه‌های  $n$ ام واحد (ریشه‌های  $x^n - 1$ ) 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  $w, w^2, \dots, w^{n-1}$  را هستند که در آن  $w$  یک ریشه  $n$ ام اولیه واحد است. حال با انتخاب یک چند جمله‌ای  $g(x)$  با کمترین درجه که ریشه آن یک، شامل ریشه‌های متوالی  $1, w, \dots, w^{e-1}$  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  $x^{n-1}$  هستند) چنین کدهایی، کدهای  $BCH$  نامیده می‌شوند که دسته مهمی از کدهای دوری هستند.

## کدهای غیر خطی

این کدها به روش‌های مختلفی ساخته می‌شوند. به طور مثال، برخی از کدهای غیر خطی، از طرح‌های 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 ( $Projective$ ) از مرتبه ۲ یا صفحه فانو ( $Fano plane$ ) می‌دهند که مثالی از یک طرح ترکیباتی است

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

$$V^6 = \{1,2,\dots,7\}$$

ماتریس وقوع این طرح به صورت زیر تعریف می شود

$$Q_{ij} = \begin{cases} 1 & j \in l_i \\ 0 & \dots \end{cases} \quad 1 \leq i, j \leq V$$

$$A = (a_{ij})_{V \times V}$$

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

حال اگر  $r_i$  تا  $v_i$  معرف سطوح های  $A$  و  $S_1$  تا  $S_7$  مکمل های آنها باشند، آنگاه کد

$C = \{r_1, r_2, \dots, r_7, S_1, \dots, S_7\}$  یک  $(7, 16, 3)$  - کد است. (که در آن 0 و 1 بردار 7 تایی صفر و

یک هستند) زیرا:

$$d(r_i, r_j) = 4 = d(x_i, s_j), d(r_i, s_j) = d(r_i, \bar{r}_j) =$$

$$7 - d(r_i, r_j) = 7 - 4 = 3$$

## خانواده کدها

اگر  $C$  یک  $(n, m, d)$  کد باشد، آنگاه نرخ کد به صورت:  $R = R(c) = \frac{\log_q^m}{n}$  تعریف می -

شود. همچنین تعریف می کنیم  $\delta = \delta(C) = \frac{d}{n}$ . برخی کدهای مهم به صورت زیر هستند

1- کد تکرار  $q$  تایی:  $C = \{0, \dots, 1, \dots, 1, \dots, 0, \dots, (q-1), \dots, (q-1)\}$

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

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

$$\delta, \lim_{n \rightarrow \infty} R = 0 \text{ بیشترین است}$$

۲- کدهای همینگ: شاید خانواده کدهای همینگ  $H_q(r)$  مشهورترین کدهای تصحیح

خطا باشند. این کدها 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  $H_q(r)$  (یک کد

$[n, k, d]$  خطی  $q$ -تایی است جایی که  $n = \frac{q^r - 1}{q - 1}$  و  $k = n - r$  و  $d = 3$ . به طور خاص اگر

$q = 2$ ، آنگاه نرخ کدهای همینگ  $R = 1 - \frac{r}{n}$ ،  $\delta = \frac{3}{n}$  بوده. واضح است که  $R \rightarrow 1$  اما

$\delta \rightarrow 0$  ( $n \rightarrow \infty$ ) این کدها تصحیح کننده دقیقاً یک خطا هستند.

کدهای گلی در سال ۱۹۴۸، گلی برخی از کدهای خطی را معرفی نمود،  $G_{12}, G_{11}, G_{24}, G_{23}$

معرفی شدند و کدهای گلی نام دارند. کد  $G_{24}$  یک کد خطی دوتایی  $(24, 4, 8)$  - کد

است که توسط فضاپیمای ویاجر (*Coyager*) به منظور انتقال عکس‌های رنگی از مریخ و

زحل استفاده شده است. کد  $G_{11}$ ، یک کد دوری سه تایی کامل  $(11, 7, 5)$  است و  $G_{12}$



یک کد خطی سه تایی (۶/۷۲۹ و ۱۲) است. مک ویلیامز والسون (Sloot) (۱۹۷۷) به کدهای گلی دوتایی به عنوان مهمترین د (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  $r$  ( $0 \leq r \leq m$ ) این کد رید-مولر  $R(r, m)$  دارای پارامترهای زیر است.

$$n = 2^m, k = 1 + \binom{m}{1} + \dots + \binom{m}{r} \quad d = 2^{m-r}$$

کدهای  $R(1, m)$  مولر مرتبه اول، کدهای

$2^m, 2^{m+1}, 2^{m-1}$  هستند. کد  $R(1/5)$  توسط فضایی ماریسز ۹، به منظور عکس‌های سیاه و سفید از مریخ در سال ۱۹۷۲، بکار گرفته شد. در مورد کدهای رید-مولر، داریم:

$$R = \frac{1 + \binom{m}{1} + \dots + \binom{m}{r}}{2^m}, \delta = \frac{1}{2^r}$$

بنابراین اگر  $r$  ثابت باشد، داریم  $R \rightarrow 0$  زمینی که  $n \rightarrow \infty$  و اگر  $r \rightarrow \infty$  آنگاه  $\delta \rightarrow 0$

زمانی که  $n \rightarrow \infty$

## کدهای BCH و کدهای رید-سولمن

کدهای BCH (Bose- chevlhuri-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  $e-1$  تایی متوالی  $1, w, w^2, \dots, w^{e-1}$  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 مواد

$g(x), C$  باشد آنگاه کد  $C$  دارای پارامترهای زیر است به  $(n, k = n - \deg(g(x)), d \geq e)$

بسیاری از کدهای  $BCH$  دارای  $d=e$  هستند و لذا می‌توانی 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-سولمن

بزرگ (با طول بزرگ) دارای اندازه الفبای بزرگی برای کد هستند که غیر عملی است. اما

آنچنان که خواهیم دید می‌توان این کدها را به کد دو دویی تصویر کرد. همچنین کدهای

رید-سولمن در تصحیح خطای گروهی (*Burst error*) دارای اهمیت. (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. (*quadratic residue codes*) یک عدد صحیح مانند  $X$  یک باقیمانده مربعی در پیمانه  $P$  نامیده می شود.

اگر معادله  $x^2 \equiv a \pmod{P}$  دارای یک جواب باشد. به عبارت دیگر  $a$  ریشه یک عدد در پیمانه  $P$  باشد. در نظریه اعداد، این مطلب اثبات شده است که  $2$  یک ریشه مربعی در پیمانه  $P$  است اگر و تنها اگر در  $P$  به شکل  $4m+1$  باشد. بنابراین کدهای باقیمانده مربعی دارای طول  $p = 4m+1$  (اول هستند) در این حالت، چند جمله ای مولد کد دارای ریشه های زیر است.

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

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

$$g_1(x) = \prod_{r \in QR} (x - w^r), g_2(x) = \prod_{u \in NQR} (x - w^u)$$

که در آن  $QR \subseteq \{1, \dots, p-1\}$  باقیمانده های مربعی در پیمانه  $P$  و  $NQR \subseteq \{1, \dots, p-1\}$  باقیمانده های مربعی در پیمانه  $P$  هستند.

می توان ثابت کرد  $|QR| = |NQR| = \frac{p-1}{2}$ ، بنابراین بعد یک کد باقیمانده مربعی به صورت

$$K = n - \deg(g(x)) = p - \frac{p-1}{2} = \frac{p+1}{2}$$

متأسفانه، تعیین کمترین فاصله یک کد باقیمانده، مربعی مشکل است. اما می توان ثابت کرد

که  $\sqrt{p} \geq$  اما این کران، کران خیلی خوبی نیست. توجه داریم که نرخ یک کد باقیمانده

مربعی حداقل  $R \geq \frac{1}{p}, \frac{1}{q}$  خواص کیفی کدهای باقیمانده مربعی در حالت کلی، یا شناخته است. اما برخی از این کدها با طول کم (مانند کدهای کامل گلی  $G_{11}, G_{23}$ ) 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  $F_q^m$  به همراه یک مجموعه  $L \subseteq F_q^m$  از عناصر ناصفر  $G(x)$  تشکیل شده است کدهای کاپا، خطی هستند، اما در حالت کلی دوری نیستند یکی از زیباترین وجوه کدهای گاپا در این است که کمترین فاصله کد از پایین توسط  $1 + \deg(G(x))$  کراندار است. در واقع اگر  $g = \deg(G(x))$ ، آنگاه پارامترهای کد گاپا در رابطه زیر صدق می‌کند.

$$n = |L|, 1 \leq n - mg, \quad d \geq 1 + g$$

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

### کدهای جاستسن (Justesen Codes)

توجه دارید که در هر یک از حالت‌های قبلی، جایی که نرخ  $R$  و عدد  $n$  مقادیر مشخصی باشند آنگاه زمانی که  $n \rightarrow \infty$ ، داریم  $R \rightarrow 0$  یا  $\delta \rightarrow 0$ . به عبارت دیگر یا نرخ به صفر میل می‌کند یا احتمال خطای کد گشایی زمانی که  $n \rightarrow \infty$  به ۱ میل می‌کند. در ادامه خانواده‌ای از کدهای خطی را مورد مطالعه قرار می‌دهیم که به کدهای جاستس معروف هستند و دارای نرخ ثابت  $R = \frac{1}{p}$  هستند در آن.

$$\delta \rightarrow H^{-1}\left(\frac{1}{p}\right) \approx 0.11$$

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

### کدهای کامل (Perfect codes)

برای مدتی، محققین فکر می‌کردند تنها کدهای کامل غیر بدیهی. کدهای همینگ  $H_q(r)$  و کدهای گلی  $G_{12}$  و  $G_{13}$  هستند. کدهای کامل بدیهی، کدهای تکرار دوتایی با طول فرد، کدهای شامل تنها کد کلمه صفر و کاد شامل همه عناصر  $V(n, q)$  هستند. اما، وسیله  $(Vasil;ev)$  خانواده‌ای از کدهای کامل غیر خطی با پرامترهای مشابه با کد همینگ را یافت.

قضیه مهم زیر (۱۹۷) را درباره کدهای کامل روی الفبای با اندازه توان یک عدد 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  $G_{2^r}$  و  $G_{2^r-1}$  است علاوه بر این:

(۱) اگر  $C$  دارای پارامترهای مشابه با یک یاز کدهای گلی باشد، آنگاه هم ارز با آن کد گلی است.

(۲) اگر  $C$  خطی بوده و دارای پارامترهای مشابه با یک یاز 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 می کنیم.

#### ۱- تصمیم یک کد یا *extending a code*

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

$$\hat{C} = \{c_1 C_2 \dots C_n C_{n+1} \mid C_1, \dots, C_n \in \mathbb{C}, \sum_{k=1}^{n+1} C_k = 0\}$$

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

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

مثال: اگر  $C = \{0, 0, 1, 1, 0, 1, 1, 0\}$  آنگاه  $\hat{C} = \{0, 0, 0, 1, 1, 0, 1, 1, 0\}$  (کد تعمیم یافته  $C$ ) توجه دارید که

$C$  دارای کمترین فاصله است، اما  $\hat{C}$  دارای کمترین فاصله ۲ است.

مثال: کد همینگ  $H_2(r)$  (دوتایی) دارای پارامترهای زیر است:

$$n = 2^r - 1, M = 2^{(2^r - 1 - r)}, d = 3$$

کد همینگ تعمیم یافته  $\hat{H}_2(r)$  که با اضافه نمودن یک بیت توازن کلی به  $H_2(r)$  به دست

می آید، دارای پارامترهای زیر است:

$$\hat{n} = 2^r, \hat{M} = 2^{(2^r - 1 - r)}, \hat{d} = 4$$

بنابراین، با وجود این که تعمیم یافته همینگ دارای قدرت تشخیص خطای بیشتری نسبت به

کد اصلی نیست، اما قدرت تشخیص خطا در آن افزایش می یابد.

۲- پنچر نمودن یک کد یا *puncturing a code*

عکس فرآیند تعمیم یک کد، پنجر نمودن کد است. به این صورت که یک یا دو مکان مختصاتی از کد کلمات حذف کی شوند. اگر  $C$  یک کد  $q$ -تایی  $(n, m, d)$  باشد و  $d \geq 2$  آنگاه کد  $C$  که با پنجر نمودن یک مختص  $C$  به دست آمده دارای پارامترهای زیر است:

$$n^* = n - 1, M^* = M, d^* = d \text{ یا } d - 1$$

مثال: کد گلی  $G_{23}$  با پارامترهای  $(23, 4096/8)$ ، با پنجر نمودن کد  $G_{24}$  با پارامترهای  $(24, 4096/8)$  بدست آمده است. (توجه دارید که پنجر نمودن  $G_{24}$  در هر مکان، یک کد معادل با  $G_{23}$  می دهد).

کد  $G_{24}$  در شرط گوی پوششی (*sphere-packing*) صدق نمی کند. و بنابراین کامل نیست. اما کد  $G_{23}$  کامل است. بنابراین پنجر نمودن یک کد غیر کامل می تواند به یک کد کامل منجر شد

قضیه: یک کد  $(n, m, 2t+1)$  دوتایی وجود دارد اگر و تنها اگر یک کد تعمیم یافته  $C$  که با اضافه نمودن یک توازن کلی به  $C$  به دست آمده است. در این صورت، چون وزن هر کد کلمه در  $C$  زوج است، بنابراین  $d(\hat{C})$  زوج است و لذا  $d(\hat{C}) > d(c) = 2t+1$  پس  $d(\hat{C}) = 2t+1$ . برعکس، فرض کنید  $C$  یک کد دوتایی  $(n+1, M, 2t+2)$  باشد  $d(c, d) = 2t+2$  و  $C$  با پنجر نمودن  $C$  در یک مکان از مکانهای متفاوت  $d, c$  به دست آمده باشد. بنابراین  $C^*$  دارای کمترین فاصله  $2t+1$  است.



پاک کردن یک کد : *Expunging a code*

با حذف تعدادی از کد کلمات یک کد، پاک کردن یک کد رخ می دهد. (برخی از مولفین از کلمه پیراتس *expurgate* استفاده می کنند). 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  $(n, \frac{m}{d}, d')$  به دست می آید که در آن  $d' \geq d$ .

علاوه بر این، چون تمامی کد کلمات باقیمانده دارای وزن زوج هستند، کمترین فاصله کد پاک شده زوج 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 می شود که با اضافه نمودن تعداد کلمه اضافی با عناصر کد به دست می آید. یک روش متداول برای افزایش یک کد دوتایی  $C$ ، اضافه نمودن مکمل هر کد کلمه به آن است. جایی که  $C^c$  (مکمل کد کلمه  $C$ )، با تعویض ۰ و ۱ در  $C$  به دست می آید.

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

لم: اگر  $x, y \in V(n, 2)$  آنگاه  $d(x, y^c) = n - d(x, y)$ .

اثبات:  $c(x, y^c) =$  تعداد مکان‌هایی که  $x$  با  $y^c$  متفاوت است = تعداد مکان‌هایی که  $X$  با  $y$

$$.n - d(x, y) = \text{یکسان است}$$

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.

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

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

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

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

اگر  $L$  کد خطی دوتایی باشد و  $1 = 110001 \in L$  و  $1 = 110001 \in L^c$  اما اگر  $1 \notin L$  آنگاه

$$L \cap L^c = \emptyset \text{ در واقع قضیه زیر را داریم:}$$

قضیه: اگر  $L$  یک کد دوتایی خطی  $(n, m, d)$  باشد که شامل کلمه  $1 = 110001$  نباشد،

آنگاه  $L \cup L^c$  یک کد خطی دوتایی  $(n, 2m, d')$  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 a code*

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 که 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  $X_i = S$  (cross-section) معروف است.

قضیه: اگر  $C$  یک کد خطی دو دویی  $(n, m, d)$  باشد، آنگاه بخش متقاطع  $x_i = 0$  یک کد خطی دو تایی  $(n-1, \frac{1}{p}m, d)$  است.

ساختار جمع مستقیم (Direct sum Construction)

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:

$$n = n_1 + n_2, M = M_1 M_2, d = \min\{d_1, d_2\}$$

ساختار  $(u, u+V)$

این ساختار، نسبت به ساختار جمع مستقیم، بسیار مفید تر است. اگر  $C_1$  یک کد  $(n_1, m_1, d_1)$  و  $C_2$  یک کد  $(n_2, m_2, d_2)$  باشد، که هر دو روی الفبای  $F_q$  تعریف شده‌اند. آنگاه کد  $C_2$  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  $M_1 M_2$  است. حال نشان می‌دهیم

$$U_2 = C_2(C_2 + d_2), u_1 = C_1(C_1 + d_1) \text{ زیرا فرض کنید } d(C_1 \oplus C_2) \geq \min\{2d_1, d_2\}$$

به وضوح طول  $C_1 \oplus C_2$  . 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

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

$$(w(a+b) \geq w(a) - w(b))$$

اما می‌توان 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  $\text{Rep}(2^m)$  کد تکرار دوتایی به طول  $2^m$  باشد که یک کد  $(2^m, 2, 2^m)$

است. در این حالت  $R(1, m) \oplus \text{Rep}(2^m)$  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 می‌تواند مفید باشد.

تعریف: فرض کنید  $C$  یک  $(n, m)$ -کد روی  $F_q$  باشد. گروه خودریختی  $Aot(C)$  از  $C$ ،

مجموعه تمامی تبدیل‌های تک جمله‌ای  $M$  با درجه  $n$  است، به طوری که  $M(C) \subseteq C$ .

زمانی که  $q=2$ ، یک تبدیل تک جمله‌ای، چیزی جز یک جایگشت  $\pi$  روی مکان‌های

مختصات کد نیز یعنی  $\pi C = C_{\pi(1)} C_{\pi(2)} \dots C_{\pi(n)}$

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

تعریف: فرض کنید یک کد دو دویی  $(n, k)$  باشد گروه خودریختی (  $automorphism$

*group*)

$C$  به صورت زیر است:

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

یادآوری می‌کنیم که اگر  $\mu$  یک تبدیل تک جمله‌ای باشد، در این صورت کد

$$C \mu = \{ \pi \in S_n \mid \pi c \in C, \forall c \in C \}$$

است.

قضیه: مجموعه  $Aut(C)$  یک گروه است

در مورد کد دو تایی  $C$ ، گروه  $Aut(C)$  ی زیر گروه از گروه متقارن  $S_n$  است.

مثال: گروه خودریختی کد  $C = \{0000, 1100, 0011, 1111\}$ ، زیر گروهی از  $S_4$  با اندازه 8 به صورت زیر است.

$$Aut(C) = \{id, (12), (34), (12)(34), (13)(24), (14)(23), (1324), (1423)\}$$

مسأله اساسی کد گذاری

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

$Aq(n, d)$ : بزرگترین اندازه  $M$  ممکن به طوری که یک کد  $(n, m, d)$   $q$ -تایی موجود باشد.

اعداد  $Aq(n, d)$  در کد گذاری یک نقش اساسی ایفا می‌ند 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 ملاحظه-

ای به منظور تعیین رفتار مجانبی  $Aq(n, d)$  به عنوان تابعی از  $\delta = \frac{d}{n}$ ، زمانی که  $n \rightarrow \infty$ ،

صورت گرفته است. یک  $(n, m, d)$  کد که در آن  $M = Aq(n, d)$ ، کد بهینه (*Optimal*) نامیده

می‌شود.

قضیه: بار هر  $n \geq 1$  داریم.

$$A_q(n, n) = q \quad (2) \qquad A_q(n, q) = q^n \quad (1)$$

قضیه: برای هر  $n \geq 2$  داریم:

$$A_q(n, d) \leq q A_q(n-1, d)$$

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

این قضیه را به این صورت نیز می توان بیان کرد که اگر  $d$  زوج باشد آنگاه

$$A_2(n, d) = A_2(n-1, d-1)$$

بنابراین، در مورد کدهای دوتایی، کافی است تا  $A_2(n, d)$  را برای تمامی مقادیر فرد  $D$  (یا

برای تمام مقادیر زوج) تعیین کنیم.

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

$$A_q(n, d) \geq \frac{q^n}{\sum_{k=0}^{d-1} \binom{n}{k} (q-1)^k}$$

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:

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

بنابراین، اگر  $K$  بزرگترین عدد صحیح باشد که در شرط فوق صدق می کند. آنگاه

$$A_q(n, d) \geq k$$

کران بالایی روی  $A_q(n, d)$

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

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)

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

توجه دارید که کدی که تساوی در کران نسبه 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  $-q(n, m, d)$  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  $q=2$ ،  $A_2(n, d)$ :

جدول مقابل توسط هیل (Hill) سال ۱۹۸۶ معرفی شد که تعمیمی از کاری است که اسلون

(Sloot) (سال ۱۹۸۲) ارائه نمود.

بسیاری از کران‌های پایینی در این جدول، با استفاده از کدهایی که قبلاً معرفی کردیم،

مانند کدهای همینگ، کد تکرار به همراه کوتاه کردن این کدها به دست آمده‌اند.

$n$	$d=3$	$d=5$	$d=7$
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)  $A_q(n, d) \leq q^{n-d+1}$

اثبات: فرض کنید  $C$  یک  $(n, m, d)$  - کد  $q$ -تایی باشد اگر  $d-1$  مکان آخر را از تمام یکد

کلمات  $C$  حذف کنیم، آنگاه  $M$  کلمه حاصل متمایز هستند (چرا؟)، اما در این حالت طول

تمامی کلمات  $n-d+1$  است، پس  $M \leq q^{n-d+1}$ .

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

مثال:

$$C = \{ \circ \circ \circ, a \circ, bo a, ba \circ, a, ab o, \circ b, \circ \circ, o a b, b \circ, \circ b a, a a a, o b, a \circ, a \circ b, b b b \}$$

یک کد  $(3, 2)$  روی  $F_4 = \{ \circ, a, b \}$  سات بنابراین  $A_4(3, 2) \geq 16$

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

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

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

تعریف: در یک کد خطی  $d = n - k + 1$  یک کد با بیشترین فاصله تفکیک یا  $MDS$  نامیده

می شود. به عبارت دیگر  $D$  دارای بیشترین (*maximum distance separable code*)

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 مکان های 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  $C_2 = \langle C_{21}, C_{22}, \dots, C_{2M_2} \rangle$  و  $C_1 = \langle C_{11}, C_{12}, \dots, C_{1M_1} \rangle$  دو کد به ترتیب

باشند. در این صورت می توان کد کلمات  $C_1, C_2$  به ترتیب  $(n_1, m_1, d_1), (n_2, m_2, d_2)$

(Interleave) نمود و کد جدید  $C_1 \oplus C_2$  را به دست آورد که در آن:

$$C_1 \oplus C_2 = \left\{ \begin{array}{l} \{C_{11}C_{21}, C_{12}C_{22}, \dots, C_{1m_1}C_{2m_1}\} \\ \{C_{11}C_{21}, \dots, C_{1m_2}C_{2m_2}\} \end{array} \right\}$$

اگر  $M_1 > M_2$

می توان نشان داد که  $C_1 \oplus C_2$ ، یک  $(n_1 + n_2, \min\{M_1, M_2\})$  کد است که در آن

اگر  $d \geq d_1 + d_2$  تعریف کنیم:

$$uC = \{uc \mid c \in C\}$$

$$(u \in Z - \{0\})$$

آنگاه قضیه زیر را داریم:

قضیه فرض کنید  $C_2, C_1$  به ترتیب  $(n_1, M_1, d_1)$  و  $(m_2, m_2, d_2)$  که مرتب باشند آنگاه

$uC_1 \oplus \sim C_2$  دارای پارامترهای زیر است:

$$(un_1 + Nm_2, \min\{M_1, M_2\}, d)$$

$$D \geq ud_1 + Nd_2$$

جایی که:

کدهای هادامارد

در اینجا، دسته ای از کدها به نام کدهای هادامارد را تعریف و مورد بررسی قرار می‌دهیم که در کران پلاتکین رابطه تساوی در مورد آنها صدق می‌کند.

تعریف: یک ماتریس هادامارد  $H_n$  از مرتبه  $n$  یک ماتریس  $n \times n$  با درایه‌های  $\pm 1$  است که در شرط  $H_n H_n^T = nI_n$  صدق کند. اگر در سطر اول و ستون اول  $H_n$ ، تمامی عناصر  $\pm 1$  باشد، آنگاه  $H_n$  را نرمال می‌گوئیم.

برای مثال، مابریس هادامارد زیر نرمال است:

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

ثابت شده است که شرط لازم برای وجود یک ماتریس هادامارد  $H_n$  این است که  $n = 1, 2$  یا  $4 \cdot n$ ، اما مشخص نیست که آیا شرط کافی نیز می‌باشد. به سادگی می‌توان ایده وجود ماتریس هادامارد  $H_n$ ، ماتریس هادامارد نرمال شده با اعمال اندازه را نتیجه می‌دهیم. 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 ماتریس هادامارد نرمال باشد، با تعویض تمامی ۱ها با صفر و تمامی -۱ها با ۱ در ماتریس  $H_n$ ، ماتریس  $A_n$  را داریم که ماتریس هادامارد دوتایی نامیده می‌شود. حال با توجه به  $A_n$ ، می‌توانیم کدهای هادامارد زیر را بسازیم.

(۱) سطرهای  $A_n$  (با حذف ستون اول) یک  $(n-1, n, \frac{1}{p}n)$  کد تشکیل می‌دهند که  $Had \setminus_n$  نامیده می‌شود.

(۲) با کوتاه کردن کدها دامارد  $Had \setminus_n$  در مکان اول ( $x_1 = 0$ ) کد هدامارد کوتاه شده  $S Had \setminus_n$  به دست می‌آید که یک  $(n-2, \frac{1}{p}n, \frac{1}{p}n)$  کد است.

(۳) مجموعه  $Had \setminus_n \cup (Had \setminus_n)$  یک کد  $(n-1, 2n, \frac{1}{p}n-1)$  است که با  $Had 2_n$  نمایش داده می‌شود.

(۴) سطرهای  $A_n$  به همراه مکمل‌های این سطرها یک کد  $(n, 2n, \frac{1}{p}n)$  تشکیل می‌دهند که با  $Had 3_n$  نمایش داده می‌شود.

اثبات: (۱) چون سطرهای  $A_n$  متعامند، تعداد مکان‌هایی که در آن هر دو سطر برابرند، با تعداد مکان‌های که در آن، این سطرها متمایزند، برابر است. بنابراین فاصله بین هر دو سطح متمایز  $A_n$  برابر با  $\frac{1}{p}n$  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 ثابت نمودیم.

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

بدیهی است زیرا:

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

$$d(C) \min\left\{\frac{1}{p}n, n - \frac{1}{p}n\right\} = \frac{1}{p}n$$

(۴) مشابه ۳ داریم:

کدهای خطی و دوگان آنها

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

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 مولد برای  $L$  نامیده می‌شود. در این حالت، کد کلمات

موجود در  $L$ ، دقیقاً ترکیبات خطی سطح‌های  $G$  هستند. به عبارت دیگر:

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

این رابطه روش ساده تری برای کد گذاری معرفی می کند. به عبارت دیگر، اگر اعضای یک منبع (Source) را بتوان مجموعه تمامی کلمات  $Q$ -تای یبه طور  $k$  در نظر گرفت، آنگاه می توانیم 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:

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

این کد، می تواند به منظور کد گذاری سمبل های منبع  $V(3, 2)$  به کار رود. به عبارت دیگر اگر  $x = (x_1, x_2, x_3) \in C(3, 2)$  آنگاه کد کلمه 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 رد یک اسکالر ناصفر اضافه نمودن مضرب اسکالری از یک سطر به سطر دیگر)، فضای تولید شده توسط سطرها را تغییر نمی دهد، 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 مکان ها، سیستماتیک است.

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

نکته: یک کد خطی روی  $L$  امکان 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.

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

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 در  $k$  مکان اول کد کلمات ظاهر می‌شود.

قضیه: دو کد خطی  $L_1, L_2$ ، با ماتریس‌های مولد  $G_1, G_2$ ، هم ارز هستند اگر و تنها اگر با اعمال سطری و ضرب یک ستون در یک اسکالر ناصفر، بتوان از  $G_1 \sim G_2$  رسید.

دوگان یک کد خطی



فضای برداری  $V(n, q)$  دارای یک ضرب داخلی طبیعی است، به خصوص، اگر

در  $V(n, q)$  باشند، آنگاه ضرب داخلی  $y, x$  با می توان به صورت  $y = y_1 \dots y_n$ ,  $x = x_1 \dots x_n$

زیر تعریف کرد:

$$x, y = x_1 y_1 + \dots + x_n y_n$$

or  $\langle x, y \rangle$

مفهوم زیر، یک نقش کلیدی در کدهای خطی دارد.

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

کد دوگان  $L$  نامیده می شود.

قضیه (۱) اگر  $G$  ماتریس مولد  $L$  باشد آنگاه:

$$L^\perp = \{x \in V(n, q) \mid xG^t = 0\}$$

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

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

اثبات: (۱) این مطلب، از این واقعیت نتیجه می شود 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 می شود که بیان می کند  $L^\perp$  فضای جواب یک دستگاه با  $k$  معادل

$n$  متغیر است که دارای رتبه  $k$  می باشد. (۳)  $L \subseteq L^{\perp\perp}$  و  $\dim L = \dim L^{\perp\perp}$ ، پس حکم

واضح است.

توجه: خواص فضای دو گان یک کد روی یک میدان متناهی، می توان از خواص فضای دو گان یک فضای برداری روی اعداد حقیقی کاملاً متمایز باشد. به طور مثال، اگر  $W$  یک زیر فضا 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، همواره در مورد کدهای خطی درست نیست. در واقع، همان طور که مثال بعد نشان می دهد، حتی می توانیم داشته باشیم  $L^\perp = L$ .

مثال: برای کد دوتایی  $[4, 2]$ ،  $L = \{0000, 1100, 0011, 1111\}$  داریم  $L \subseteq L^\perp$  و از آنجایی که  $L^\perp$  نیز یک  $[4, 2]$ -کد دوتایی است، داریم  $L = L^\perp$ .

تعریف: کد خطی  $L$ ، به طوری که  $L = L^\perp$ ، خود دو گان (*self-dual*) نامیده می شود.

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

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

فرض کنید  $L$  یک کد خطی با ماتریس مولد  $G = (I_k | A)$  (به شکل استاندارد) باشد.

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

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

بنابراین، سطرهای  $H$  بر سطرهای  $G$  عمود هستند و از آنجایی که

$$rank(H) = n - k = \dim(L^\perp)$$

است.

ماتریس  $H$  همچنین ماتریس بررسی توازن کد  $L$  نامیده می شود. دلیل این نامگذاری این

$$x \in L \Leftrightarrow xH^t = 0 \quad \text{است که :}$$

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

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

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 می شوند.

ماتریس بررسی به شکل  $(B | I_m)$ ، فرم استاندارد نامیده می شود.

مثال: در مثال قبل، ماتریس زیر یک ماتریس مولد استاندارد برای کد  $H_2(3)$  معرفی شد.

$$G = (I_4 | A) \quad , \quad A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

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

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad \text{معادلات بررسی توازن} \begin{cases} x_2 + x_3 + x_4 + x_5 = 0 \\ x_1 + x_3 + x_4 + x_6 = 0 \\ x_1 + x_2 + x_4 + x_7 = 0 \end{cases}$$

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

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

روش کارایی برای تعیین کمترین فاصله که از روی ماتریس مولد (به طور مستقیم) وجود ندارد. اما می توان از روی ماتریس بررسی توازن  $H$  از کد  $L$ ، این کار را انجام داد. به خصوص، فرض کنید ستون های  $C_1, \dots, C_n$  وجود دارند که دقیقاً  $W$  تا از آنها ناصفر بوده و داریم:

$$C_1 k_1 + \dots + C_n k_n = 0$$

این معادل با  $CH^t = 0$  است، جایی که  $C = C_1 \dots C_n$  و لذا  $C \in L$  - علاوه بر این چون  $C$  یک

$$-d(W) = W(L) \leq W \quad \text{کد کلمه با وزن } W \text{ است، داریم:}$$

از طرف دیگر، اگر  $C$  یک کد کلمه با وزن  $W$  باشد، آنگاه داریم  $CH^t = 0$  و لذا  $W$  ستون

$H$  وابسته خطی هستند. این مطلب، قضیه بسیار مفید زیر را ثابت می کند.

قضیه: فرض کنید  $L$  یک  $[n, k, d]$  - کد با ماتریس بررسی توازن  $H$  باشد. در این صورت  $d$

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)

کد گشایی سیندروم

با استفاده از ماتریس بررسی توازن یک کد خطی، می توان یک الگوریتم کد گشایی کارا

برای آن طراحی می نمود.

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

$V(n, q)$  در پیمانه  $L$  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 برداری و ضرب اسکالر زیر را می‌توان دیده فضای خارج قسمتی روی  $F_q$

، خود یک فضای برداری است.

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

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:

$$xH^t = yH^t \Leftrightarrow (x - y)H^t = 0 \Leftrightarrow x - y \in L \Leftrightarrow x + L = y + L$$

کد گشایی سیندروم

حال فرض کنید کد کلمه  $a$  ارسال و کلمه  $x$  دریافت شده باشد. قاعده کمترین فاصله ایجاد می کنیم که  $x$  را به کد کلمه  $c$  که در آن  $e = x - c$  دارای کمترین وزن باشد. کد گشایی کنیم.

اما چون  $C \in L$  پس  $e$  در هم دسته  $x + L$  است. بنابراین، قاعده کمترین فاصله ایجاب می کند که  $x$  را به کد کلمه  $x'' + e$  کد گشایی 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  $L = \{0, C_1, \dots, C_m\}$ ، در این صورت جدول زیر یک آرایه استاندارد برای  $L$  است:

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

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  $e_1$  ها با عناصر  $C$ ، سطرهای  $L$  را می‌سازی. 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،  $x = e_i + C_j$  (برای برخی  $0 \leq j \leq m, 1 \leq i \leq s$ )، آنگاه  $X$  را به  $c_j$  (سرستون  $x$ ) کد گشایی می‌کنیم. در این حالت  $e_i$  دارای سیدنروم یکسان با  $X$  بوده و در ابتدای سطری خواهد بود که  $X$  قرار دارد.

مثال: فرض کنید  $L$  کد [۴و۲] 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.

$$\begin{aligned}
\circ + C &= \{000, 010, 110, 100\} \\
1000 + C &= \{100, 110, 010, 000\} \\
0010 + C &= \{001, 011, 111, 101\} \\
1010 + C &= \{101, 111, 011, 001\}
\end{aligned}$$

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

$$\begin{array}{cccc} \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ 1 & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & 1 & \cdot \end{array}$$

با اضافه نمودن سطر دوم  $G$  به سطر اول، ماتریس مولد در شکل استاندارد را داریم:

$$G^t = \begin{pmatrix} 1 & \cdot & \cdot & 1 \\ \cdot & 1 & \cdot & \cdot \end{pmatrix} \rightarrow H = \begin{bmatrix} \cdot & \cdot & 1 & \cdot \\ 1 & \cdot & \cdot & 1 \end{bmatrix}$$

ماتریس بررسی توازن

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

مقدار سیندروم  $s_i = s(e_i) e_i \leftarrow$  سر دسته

$$\begin{array}{cc} \cdot & \cdot \\ 1 & \cdot \\ \cdot & 1 \\ 1 & 1 \end{array}$$

حال برای کد گشایی کلمه دریافتی  $x = 1110$ ، کافی است سیندروم آن را حساب کنیم.

$$s(x) = 1110 \times H^t = 11 = S(1010)$$

پس کد گشایی به صورت  $C = x - e = 1110 - 1010 = 0100$  خواهد بود.

توجه: در کد گشایی سیندروم، خطا به درستی تصحیح می گردد 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  $e$  یک یا ز سردسته ها باشد، آنگاه کد گشایی سیندروم، آن را به  $(c + e) - e = c$  کد گشایی می کنید که درست است در غیر این صورت، اگر  $E$  از سردسته ها نباشد و سردسته  $x$ ،  $e_i \neq e$ ، آنگاه کد گشایی سیندروم،  $x$  را به  $(c + e) - e_j (\neq c)$  کد گشایی می کند که در نتیجه کد گشایی اشتباه کرده است.

نکته: اگر  $L$  دارای کمترین فاصله  $d$  باشد، آنگاه تمامی کلمات موجود در  $V(n, q)$  با وزن حداکثر  $t = \lfloor \frac{d-1}{2} \rfloor$  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  $2t$  است که تناقض است  $(d-1)$

نکته: کد  $L$  کامل است اگر و تنها اگر تمامی سردسته ها، کلمات با وزن حداکثر  $t = \lfloor \frac{d-1}{2} \rfloor$  باشند.

### احتمال کد گشایی صحیح

فرض کنید  $L$  یک کد خطی باشد و  $\infty_i$  تعداد سردسته های با وزن  $i, 0 \leq i \leq n$ ، در جدول استاندارد باشند. در این صورت زماين احتمال کد گشایی صحیح برابر با احتمال ان است که خطاها، یکی از این سردسته ها باشند، بنابراین.

$$\text{احتمال کد گشایی صحیح} = \sum_{i=0}^n \infty_i P^i (1-p)^{n-i}$$

## احتمال تشخیص خطا

فرض کنید کد کلمه  $C$  ارسال شده و کلمه  $d$  دریافت شده باشد، کد گشا، در صورتی

متوجه وجود خطا نمی شود که  $d$  یک کد کلمه متمایز با  $C$  باشد، بنابراین:

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

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

که در آن  $A_k$  تعداد کد کلمات با وزن  $k$ ،  $1 \leq k \leq n$  می باشد.

کد گشایی با منطق اکثریت (*Majority Logic decoding*)

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

فرض کنید

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

همچنین  $G$  همچنین  $H_7(3)$  باشد.

ماتریس بررسی توازن کد دوگان همینگ  $H_7(3)$  نیز هست که آن را به  $C$  نمایش می دهیم.

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

باقی می ماند.

$$G_7 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \xrightarrow{r_1 + r_2 + r_3 \rightarrow r_2}$$

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix} \xrightarrow[\substack{r_1+r_i \rightarrow r_i \\ 2 \leq i \leq 4}]{G}$$

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

$$x_1 + x_2 + x_3 = 0$$

$$x_1 + x_4 + x_5 = 0$$

$$x_1 + x_6 + x_7 = 0$$

در این معادلات توجه دارید که ضریب  $x_1$  در تمامی معادلات برابر با  $\perp$  و ضریب سایر

متغیرها، تنها در یکی از معادلات برابر با  $\perp$  است 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  $x_i$  رد هر یک از معادلات این دستگاه دارای ضریب  $\perp$  و هر متغیر

دیگر، تنها در یکی از معادلات دارای م ضرب ۱ باشد. به طور نمونه، معادلات بالا  $i$ نسبت

به  $x_i$  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 (\*) باشند، نتیجه می‌گیریم که حداقل ۲ خطا رخ داده است.

به این قاعده، کد گشایی با منطق اکثریت (*Majority logic decoding*) می‌گویند.

به عنوان تمرین، می‌توان نشان داد که با انتخاب حریصانه اعمال سطری، می‌توان کد گشایی

با منطق اکثریت را روی تما ۷ مکان  $C$  مشاهده کرد.

در حالت کلی، فرض کنید در یک کد خطی  $[n, k]$ ،  $r$  معادله بررسی توازن داریم. فرض کنید این معادلات نسبت به متغیر  $x_i$  متعامد باشند. در این حالت فرض کنید  $t \leq \frac{r}{4}$  خطا در انتقال رخ داده باشد.

اگر یکی از این خطاها در مکان  $I$  رخ داده باشد، «گام حداکثر  $t-I$  معادله برقرار هستند و لذا حداقل  $1 + \frac{r}{4} - (t-1) \geq \frac{r}{4} + 1$  معادله، برقرار نیستند. از طرف دیگر، اگر در  $I$  امین مکان، خطا رخ نداده باشد، آنگاه حداکثر  $t \leq \frac{r}{4}$  معادله، برقرار نیستند. بنابراین  $I$  امین مکان از کلمه دریافتی دچار خطا شده است و تنها اگر  $0$  اکثر معادلات برقرار نباشند.

#### کدهای خود دوگان

یک کد خطی مانند  $L$ ، خود متعامد (*self-orthogonal*) نامیده می شود 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  $L$  خود متعامد است اگر و تنها اگر سطرهای  $G$  بریکدیگر عمود بوده و دارای وزن بخش پذیر بر  $Q$  باشند.

قضیه: ارگ سطرهای متمایز ماتریس مولد یک کد خطی دو تایی مانند  $L$  بوده و دارای وزن بخش پذیر بر  $4$  باشند، آنگاه  $L$  خود متعامد بوده و وزن تمام یکد کلمات  $L$  بر  $4$  بخش پذیر است.

اثبات: خود متعامد بودن  $L$  از قضیه مبل نتیجه می شود. از طرف دیگر داریم.

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

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

مثال: کد دوتایی  $[7, 3]$ - $L$  با ماتریس مولد زیر را در نظر بگیرید:

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

این کد، خود متعامد بوده و وزن تمامی کد کلمات بر 4 بخش پذیر است. بنابراین  $L$  دارای

7 کد کلمه با وزن بخش پذیری بر 4 هستند می باشد. و لذا وزن آنها، دقیقاً 4 است. (چرا؟)

علاوه بر این  $L^\perp$  یک  $[7, 4]$ -کد که شامل  $L$  است. از طرف دیگر  $1 \in L^\perp$  (چرا؟)

بنابراین ماتریس  $\begin{pmatrix} 1 \\ G \end{pmatrix}$  یک ماتریس مولد برای  $L^\perp$  است.

تعریف: کد  $L$  خود متعامد (*self-dual*) نامیده می شود اگر  $L = K^\perp$ . در این حالت  $L$  می-

بایست یک  $[n, \frac{n}{2}]$ -کد باشد. (اگر  $n$  زوج باشد). در واقع یک  $[n, k]$ -کد خطی  $L$  خود

دوگانه است اگر و تنها اگر خود متعامد باشد و  $K = \frac{n}{2}$ .

مثال: اگر یک بیت توازن کلی به کد موجود در مثال قبل اضافه کنیم آنگاه کد  $L$  با ماتریس

مولد زیر به دست می آید:

$$G^\perp = \begin{pmatrix} 1 \\ G \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \Rightarrow G' = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$L$  یک کد خود دوگان است، زیرا خود متعامد بوده و [۸و۴]-کد است.

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

نکته: اگر کد  $L$  خود دگان 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  $G = (I_r | A)$  یک ماتریس مولد برای  $L$  باشد.  $H = (-A^t | I_n)$  نیز یک ماتریس مولد است.

قضیه: یک کد خود دوگان  $\left[ n, \frac{n}{4} \right]$  موجود است اگر و تنها اگر یکی از شرایط زیر برقرار باشد.

(۱)  $n$  و  $q \equiv 1 \pmod{4}$  و  $n$  زوج باشد  $q \equiv 3 \pmod{4}$  و  $n$  بخش پذیر باشد.

نتیجه همواره به ازای تمامی اعداد صحیح زوج  $n$ ، یک کد دوتایی خوددگان  $\left[ n, \frac{n}{4} \right]$  موجود است. و یک کد خود دوگان سه تایی  $\left[ n, \frac{n}{4} \right]$  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 با زوج می‌باشند. در این حالت، اگر وزن تمامی کد کلمات بر ۴ بخش پذیر باشد، یک کد و با زوج (*doubly even*) نامیده می‌شود.

قضیه: یک کد و بار زوج  $\left[ n, \frac{n}{2} \right]$  وجود دارد اگر و تنها اگر  $n$  بر ۸ بخش پذیر باشد.

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

در انتقاب لرخی اوقات، خطاها به صورت گروهی یا خوشه‌ای رخ می‌دهند. برای مثال، داخل‌های الکتریکی، برخی اوقات بیشتر 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  $C(n, q)$  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 کد شامل رشته‌ها در  $V(n, q)$  با صفرهای موجود در  $n - b$  مکان آخر را در نظر بگیرید. (توجه داشته باشید که  $b$  مکان اول می‌تواند شامل هر مقدار، از جمله صفر، باشند).

در این حالت، اگر دو رشته از  $S$  در یک هم دسته  $L$  قرار گیرند. آنگاه تفاضل آنها یک خطای گروهی به طور  $b$  خواهد بود که غیر ممکن است. بنابراین تعداد هم دسته‌های  $L$ ، که

برابر با  $q^{n-k}$  است می‌بایست از اندازه  $S$  که  $q^b$  است، بزرگتر باشد. یعنی

$$. n - k \geq b \Leftrightarrow q^{n-k} \geq q^b$$

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  $[n, n-b]$  - د 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  $k \leq n - b$ .

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.

$$\begin{array}{cccc} 1 & 0 & \dots & 0 \\ \underbrace{\hspace{2cm}} & & & \\ \text{بسمیل} & & & \end{array} \quad \begin{array}{cccc} 1 & 0 & \dots & 0 \\ \underbrace{\hspace{2cm}} & & & \\ \text{بسمیل} & & & \end{array} \quad \begin{array}{cccc} 1 & 0 & \dots & 0 \\ \underbrace{\hspace{2cm}} & & & \\ \text{بسمیل} & & & \end{array} \quad \begin{array}{cccc} 1 & 0 & \dots & 0 \\ \underbrace{\hspace{2cm}} & & & \\ \text{سمیل} \leq b & & & \end{array}$$

. کتبی سطرهای  $H$ ، با شیف سطر اول به اندازه یک واحد به سمت راست از سطر قبلی به

دست آمده باشد (به عبارت دیگر با اضافه 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  $k \leq n - 2b$ .  
 اثبات: اگر  $2 \leq l \leq 2b$ ، آنگاه هر خطای گروهی با طول  $l$  را می‌توان به صورت تفاضل  $e_1 - e_2$  از دو خطای گروهی  $e_1, e_2$  با طول  $b$  نوشت. از آنجایی که  $L$  نمی‌تواند یک کد کلمه باشد. چون یک خطای گروهی با طول  $l$  را نمی‌تواند یک کد کلمه باشد، می‌توان با جایگذاری  $b$  با  $2b$  در لم قبل به دست آوریم  $ok \leq n - 2b$  زیرا رد این حالت می‌توان نشان داد خطاهای گروهی با اندازه  $2b$  (در  $2b$  مکان اول) که تعداد آنها  $a^{2b}$  است، نمی‌توانند در هم دسته یکسانی باشند، زیرا تفاضل آنها کد کلمه خواهد بود. که تناقض است، پس  $q^{2b} \leq q^{n-k}$  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 نمی‌گیرند. 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:

$$A_i : \underbrace{\times \dots \times}_b \circ \dots \circ_{n-b} \quad k \leq n - b + 1 - \log_q((q-1)(n-b)+1)$$

اثبات: تمرین

$$A_i : \underbrace{\circ \dots \circ}_b \times \dots \times_{n-b+1}, \quad 1 \leq i \leq n - b + 1, \quad A_i = \{b \text{ مکان } i \text{ ام خطای گروهی اند}\}$$

زیرا امکان اول در هر  $A_i$  (بجز  $A_i$  آخر یک عضو، صفر

$$A_{n-b+1} : \underbrace{\circ \dots \circ}_{n-b+1} \times \dots \times_b \quad \text{از } F_q \text{ است و بقیه دلخواهند (}$$

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

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

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

*MDS*

مسأله اصلی کدگذاری در مورد کدهای خطی می تواند 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 دیده ایم، این مسأله در حالت کلی کاملاً سخت

است.

از طرف دیگر، مامی توانیم  $n$  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 سادهتری است و به برخی از قضایای جالب منجر می شود از کران سینگلتون، داریم:

$$A_q(n, d) \leq q^{n-d+1} . \text{ با توجه به این کران،}$$

در مورد کدهای خطی داری:

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

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 می شود.

کدهای  $MDS$  بدیهی به آسان می توان دید که کدهای  $q$ -تایی  $MDS$  با پارامترهای  $[n, m, 1]$ ،  $[n, 1, n]$  و  $[n, n/2]$  وجود دارند. این کدها به کدهای  $MDS$  بدیهی معروف هستند. بنابراین هر  $[n, k]$ -کد  $MDS$  غیر بدیهی در رابطه  $2 \leq k \leq n-2$  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  $MDJ$  است که 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  $J$  باشد. بنابراین  $H$  ماتریس مولد کد  $L^\perp$  است. چون هر  $(n-k) \times (n-k)$  زیر ماتریس  $H$ ، وارون پذیر است. تمام یترکیبات خطی سطرهاى  $H$ ، دارای حداکثر  $n-k-1$  درایه صفر هستند. بنابراین، تمام یترکیبات خطی غیر بدیهی سطرهاى  $H$  دارای وزن حداقل  $n-(n-k-1) = k+1$  درایه صفر هستند. بنابراین، تمام یترکیبات خطی غیر بدیهی سطرهاى  $H$  دارای وزن حداقل  $n-(n-k-1) = k+1$  می باشند. به عبارت دیگر، کمترین فاصله  $L^\perp$  برابر با  $k+1 = n-(n-k)+1$  است، که بیان می کند  $L^\perp$  یک کد  $MDS$  است.

نکته با استفاده از قضایای فوق، می توان کدهای  $MDS$  را بر حسب ماتریس مولد آنها، مشخص نمود که  $K$  یک  $[n, k]$ -کد  $MDS$  است اگر و تنها اگر  $L^\perp$  یک  $[n, n-k]$ -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  $G$  در این صورت  $L$ ،  $MDS$  است اگر و تنها اگر هر  $k$  و ستون  $G$  مستقل خطی باشند.

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

در اینجا، مشخصه زیبایی دیگری از کدهای  $MDS$  را بیان می کنیم.

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

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

با تعویض سطرها و ستون های  $G$ ، می توانیم فرض کنیم  $B_u$  در گوشه چپ بالایی  $A$  واقع است. حال ماتریس  $M$ ، متشکل از  $k-u$  ستون آخر  $k-u$  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 می شود.

اثبات عکس قضیه به عنوان تمرین واگذار می شود.

تعریف: محمل ( $support$ ) بردار  $x \in V(n, q)$ ، مجموعه تمامی مکان های 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 به ازای هر  $d$  مفروض از آن، یک کد کلمه (با کمترین وزن) وجود داشته باشد به طوری که محمل این کد کلمه دقیقاً در این مکان ها باشد.

اثبات: فرض کنید  $L$  یک  $[n, k]$ -کد  $MDS$  باشد.  $d = n - k + 1$  ماکن از آن، مثلاً  $i_1, \dots, i_d$  را انتخاب کنید. مکان  $i_1$  به همراه  $k-1$  مکان انتخاب نشده  $j_1, \dots, j_{k-1}$  را در نظر بگیرید. چون  $k$  مکان  $i_1, j_1, \dots, j_{k-1}$ ، سمبل های اطلاعات هستند، بنابراین کد کلمه  $C$  وجود دارد که دارای سمبل ۱ در مکان  $i_1$  و سمبل صفر در سایر مکان های  $j_1, \dots, j_{k-1}$  است. بنابراین، محمل  $C$ ، همان  $i_1, \dots, i_d$  می باشد (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 که  $I_{n-d+1}$  یک ماتریس همانی و  $i_{d-1}$  یک  $(d-1) \times (d-1)$  ماتریس با درایه های تماماً ۱ است.

این سطرها، مستقل خطی هستند و دارای وزن  $D$  می باشند. چون یک کد کلمه  $C_i \in L$  وجود دارد که دارای محمل یکسان با سطر  $I$  ام  $M$  است، نتیجه می گیریم  $k \geq n - d + 1$ ، که این مطلب  $MDS$  بدون  $L$  را نشان می دهد.

مطالب فوق را می توان 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  $MDS$  است.

(۵) اگر  $G = (I | A)$ ، یک شکل استاندارد از ماتریس مولد  $L$  باشد، آنگاه هر زیر ماتریس

مربعی  $A$ ، نامنفرد است.

(۶) به ازای هر  $d$  مکان مفروض، یک کد کلمه (با کمترین وزن) وجود دارد که محمول آ»

دقیقاً این مکان هاست.

کدهای  $MDS$  ساخته شده از ماتریس واندروموند (*Vandermonde*)

ساخت خانواده‌ای از کدهای  $MDS$ ، سخت نیست برای این منظور، فرض کنید  $\alpha_1, \dots, \alpha_u$

عناصر ناصفر از یک میدان باشند. ماتریس واندروموند بر پایه این عناصر به صورت زیر است.

$$V(x_1, \dots, x_u) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_u \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_u^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{u-1} & \alpha_2^{u-1} & \dots & \alpha_u^{u-1} \end{pmatrix}$$

لم: دترمینان ماتریس واندروموند به صورت زیر است:

$$\det(C(\alpha_1, \dots, \alpha_u)) = \prod_{1 \leq i < j \leq u} (\alpha_j - \alpha_i)$$

به خصوص اگر  $\alpha_i$  ها متمایز باشند، آناه  $V(\alpha_1, \dots, \alpha_u)$  نامنفرد است.

اثبات: فرض کنید  $p(x) = \det(V(\alpha_1, \dots, \alpha_{u-1}, x))$  در این صورت  $P(x)$  یک چند جمله‌ای با درجه  $u-1$  بر حسب  $X$  است. چون هر یک از  $x_1, \dots, x_{u-1}$  ها، یک ریشه از  $p(x)$  هستند،

$$\text{بنابراین } p(x) = \beta \prod_{i=1}^{u-1} (x - \alpha_i) \text{، جایی که } \beta \text{ (نسبت به } X \text{) ثابت است.}$$

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

$$\det[V(x_1, \dots, x_u)] = \det[V(\alpha_1, \dots, \alpha_{u-1})] \prod_{i=1}^{u-1} (\alpha_u - \alpha_i)$$

حال، فرض کنید  $f_q = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\}$  و ماتریس  $(q-k+1) \times (q+1)$  زیر، حاصل از یک ماتریس واندرموند با اضافه نمودن دو ستون اضافی زیر را در نظر بگیرید.

جایی که  $0 \leq k \leq q$  (به ازای  $k=q$ ، ماتریس  $H_1$  ماتریس سطری شامل تمامی درایه‌ها است). این مطلب به خواننده واگذار می‌شود که هر  $q-k+1$  ستون  $H_1$  یک ماتریس نامنفرد تشکیل می‌دهد بنابراین، قضیه زیر را داریم:

قضیه برای  $1 \leq k \leq q$ ، ماتریس  $H$ ، ماتریس بررسی توازن یک  $[q+1, k]$ -کد  $MDS_q$ -تایی است.

تذکر: توجه کنید که در حالت کلی، نمی‌توانیم ستون‌های اضافی به ماتریس  $H_1$  را اضافه کنیم و یک ماتریس بررسی توازن برای یک کد  $MDS$  بسازی برای نمونه، ماتریس زیر را در نظر بگیرید.



$$H_{\gamma} = \begin{pmatrix} 1 & \dots & 1 & 1 & 0 & \dots \\ \alpha_1 & \dots & \alpha_{q-1} & 0 & 1 & \dots \\ \alpha_1^2 & \dots & \alpha_{q-1}^2 & 0 & 0 & \dots \\ \vdots & \dots & \vdots & \vdots & \vdots & \vdots \end{pmatrix}$$

حال بیایی، دو ستون  $H_{\gamma}H$  از میان  $q-1$  ستون اول را به همراه  $q+1$  امین ستون در نظر

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

به ازای هر انتخاب ناصفر  $\alpha_i$  و  $\alpha_j$ ، میدان  $F_q$  باید در رابطه  $x^2 \neq y^2 \Rightarrow x \neq y$  صدق کند. به

عنوان تمرین می توان نشان داد که این رابطه برقرار است اگر و تنها اگر مشخصه  $F_q$ ،  $2$

باشد، یعنی اگر و تنها اگر  $Q$  توازنی از  $2$  باشد.

بنابراین، تنها در حالتی که  $H_{\gamma, q} = 2^m$  ماتریس بررسی توازن یک  $[q+2, q-1]$ -کد

$MDS_q$ -تایی است. با در نظر گرفتن کدهای دوگان و مطالب فوق نتیجه زیر را داریم.

نتیجه به ازای  $1 \leq K \leq q$  کدهای  $MDS [q+1, k]$  وجود دارند. به ازای  $q = 2^m$

، کدهای  $MDS$  و  $[q-1, 2q-1]$  و  $[q+2, 3q-1]$  وجود دارند.

برخی کدهای خطی

در این فصل، نگاهی به سه دسته از معروف ترین خانواده از کدهای خطی می پردازیم،

کدهای همینگ

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

این کدها، به طور مستقل توسط گلی در سال ۱۹۴۹ و همیگ سال ۱۹۵۰ کشف شدند این کدها خطی و کامل بوده و به روش بسیار جالبی کد گشایی می‌وشند. علاوه بر این، تمامی کدهای همینگ دوتایی هم ارز با کدهای دوری بوده و برخی (نه همه) کدهای همینگ غیر دودویی ارزیبا کدهای دوری هستند.

قبلاً مشاهده کردیم که کمترین فاصله یک  $[n, k]$ -کد خطی با ماتریس بررسی توازن  $H$  و کوچکترین عدد صحیح  $d$  است که برس آن  $d$  ستون وابسته خطی از  $H$  وجود دارند. بنابراین، ماتریس بررسی توازن یک  $[n, k, 3]$ -کد دارای این خاصیت است هیچ دو ستون آن وابسته خطی نیستند، یعنی هیچ ستونی مضرب اسکالر ستون دیگر نیست، اما بریخ از سه ستون‌ها وابسته خطی‌اند به ازای یک الفبای کد مفروض  $F_q$ ، می‌توانیم یک ماتریس 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

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

را انتخاب کنید. برداشتن ستون‌های ناصفر و سپس دور انداختن تمامی مضارب اسکالر ستون‌های انتخاب شده تا زمانی که دیگر انتخابی نداشته باشیم را ادامه می‌دهیم. از آنجایی

که

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

نتیجه: یک ماتریس بررسی توازن با  $\frac{q^r - 1}{q - 1}$  ستون خواهد بود، به طوری که در آن هیچ دو ستونی نیستند، اما برخی از سه ستون ها وابسته اند. ماتریس حاصل، یک ماتریس همینگ از مرتبه  $r$  خواهد بود که ماتریس بررسی توازن یک  $[n, k, 3]$ -کد  $q$ -تایی خطی با پارامترهای زیر است.

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

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

همچنین توجه دارید که انتخاب ستون ها، یکتان نیست. و بنابراین ماتریس های همینگ متفاوتی دارند و در نتیجه کدهای همینگ متفاوتی با پارامترهای یکسان وجود دارند. اما، هر کد همینگ می تواند اندازه دیگری (با پارامترهای یکسان) با استفاده از جایگشت ستون ها 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. در واقع، تحت هم ارزش (با ضرب اسکالر). کدهای همینگ با استفاده از پارامترا و این که خطی هستند، یکتا می باشد.

حالت دوتایی کدهای همینگ، بیسار معروف است. جایی که  $H_2(r)$  یک  $[n, k, 3]$ -کد دو دویی خطی، با پارامترهای زیر است.

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

در این حالت، ستون‌های ماتریس همینگ از مرتبه  $r$ ، نمایش‌های دودویی  $2^r - 1$  عددس صحیح متوالی است. به سادگی می‌توان دید کدهای همینگ کامل هستند.

کد گشایی کد 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 می‌کنیم. بنابراین به طور مثال، ماتریس بررسی توازن کد همینگ  $H_1(r)$  به صورت زیر است:

$$H_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

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

مثال: ماتریس  $H_1 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$  را در نظر بگیرید، اگر خطا به صورت

$e_3 = 0010000$  باشد، آنگاه مقدار سیندروم به صورت زیر است.

$$e_{\gamma} H_{\gamma}^t = (\dots 1 \dots) \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} = (011) = (011)_{\gamma} = (3)_{\gamma}.$$

یعنی مکان خطا، مکان سوم بوده و

$$e = e_{\gamma} = \dots 1 \dots$$

توجه در حالت غیر دودویی، به طور مشابه می‌توانیم ستون‌های ماتریس بررسی توازن کد را به ترتیب صعودی (نمایش سه‌تایی اعداد از کوچک به بزرگ) انتخاب کنیم. اما اور درایه‌ها ما اور درایه ناصفر در این نمایش‌های سه‌تایی، برابر با  $\underline{1}$  باشد.

مثال ماتریس بررسی توازن  $x_{\gamma}(3)$  به صورت زیر است:

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

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

مثال اگر ماتریس  $H_2$  در مثال قبل را به کار ببریم، آنگاه سیندروم کلمه دریافتی

$$y = 1101112211201 \text{ به صورت زیر است}$$

$$yH_2^t = [2 \ 0 \ 1] = 2[1 \ 0 \ 2] = 2 \times (\text{ستون } H_2) \text{ (۷امین ستون)}$$

بنابراین، با کم نمودن ۲ از ۷امین مان  $y$  کد کلمه زیر بدست می آید:

$$C = 1101110211201$$

میدان های متناهی و کدهای دوری

میدان های متناهی، دارای یک نقش اساسی در نظریه کدگذاری است و بنابراین به دست

آوردن یک فهم عمیق از ساختار این میدان ها مهم است. همچنین، فهم ساختار چند جمله-

ای هایی که ضاریب آنها متعلق به یک میدان متناهی است، دارای اهمیت است. به طور مثال.

این که چند جمله ای مینیمال یک عوض را روی میدان متناهی بیابیم که نیاز است تا چند

جمله ای  $x^0 - 1$  را روی یک میزان متناهی تجزیه کنیم.

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

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 می دهیم.

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

$$|k|=|F|^d.$$

اثبات: فرض کنید  $\{x_1, \dots, x_d\}$  یک پایه برای  $k$  روی  $F$  باشد. در این صورت هر عضو  $k$

دارای نمایش یکتای به صورت  $a_1 \alpha_1 + \dots + a_d \alpha_d$  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

$(a_1, \dots, a_d)$  ترکیب خطی  $a_1 \alpha_1 + \dots + a_d \alpha_d$  نیز متفاوت خواهند بود، بنابراین  $|k|=|F|^d$ .

قضیه: اگر  $F$  یک میدان متناهی باشد، آنگاه  $F$  دارای یک مشخصه اول می باشد. علاوه بر این

اگر  $Char(F) = P$ ، آنگاه  $F$  دارای  $P^n$  عضو می باشد (برای یک مقدار صحیح مثبت  $n$ ).

اثبات: در یک میدان با مشخصه صفر است. بنابراین، مشخصه  $F$ ، کوچکترین عدد صحیح

مثبت  $n$  است که رد آن  $nl = 0$  حال فرض کنید  $char(F) = n$ . اگر  $n = pq$  جایی که

$P, q < n$  آنگاه  $Pq = 0$  بنابراین  $(p)(q)$  که ایجاب می کند  $p=0$  یا  $q=0$ . در هر حالت، با

این که  $n$  کوچکترین عدد صحیح مثبت است که در آن  $n=0$  در تناقض است. پس  $n$  باید

اول باشد. پس  $Char(F) = P$  یک عدد اول است، در این حال، می توان 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. 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

ضربه می‌دهند. اگر  $|F| = q$ ، آنگاه  $|F^*| = q - 1$  و چون مرتبه هر عضو در یک گروه، مرتبه

آن گروه را عادی کند، بنابراین داریم:  $\alpha \in F^* \Rightarrow \alpha^{q-1} = 1$  یا به طور هم ارز  $x \in F \Rightarrow x^q = x$

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 ریشه‌های

$f_q(x)$  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 جمله ای، یکرخت هستند، نتیجه می گیریم که میدان های متناهی با اندازه یکسان، یکرخت 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 ریشه های  $f_q(x)$  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 زیر میدانی از  $k$  است که در نتیجه  $R = k$  علاوه بر

$$Df_q(x) = qx^{q-1} - 1 = -1 \quad \text{این، چون (در } Z_p \text{)}$$

پس  $DF_q(x)$  با  $F_q(x)$  دارای هیچ ریشه مشترکی نیست. بنابراین  $F_q(x)$  دارای هیچ ریشه تکراری نمی باشد. ولذا  $R$  دقیقاً یک میدان با اندازه  $q$  است. با توجه به مطالب باین 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 یکرختی) از اندازه  $q$  وجود دارد 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 معمولاً 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 میدان‌های یک میدان متناهی

هدف ما، در اینجا، \*\*\*\* 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

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 زیر میدان یکتا از اندازه  $P^d$  می‌باشد.

برای مشاهده این مطلب، فرض  $k$  دارای یک زیر میدان یکتا از اندازه  $P^n$  باشد و  $d|n$  اما

$f_p(x)$  روی میدان  $k$  را می‌توان به عوامل خطی تجزیه کرد. بنابراین  $f_p(x)$  نیز حاصل

ضربی از برخی از این عوامل خطی است. به بیان دیگر  $K$  شامل یک میدان شکافنده از  $F_{p^d}(x)$  است، یعنی  $k$  شامل یک زیر میدان با اندازه  $P^d$  است.

به وضوح، چنین زیر میدانی با اندازه  $P^d$  یکتاست، زیرا در غیر این صورت  $F_{p^d}(x)$  دارای بیشتر از  $P^d$  ریشه است که تناقض است (زیرا  $\deg F_{p^d}(x) = P^d$ ) با توجه به مطالب فوق، قضیه زیر را اثبات کرده ایم.

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

#### ساختار ضربی یک میدان متناهی

مجموعه  $F^*$ ، شامل تمامی عناصر ناصفر میدان  $F$ ، تحت ضرب تشکیل یک هدف ما، اثبات این مطلب، با نشان دادن این گزاره است که اگر  $|F^*| = q-1$  آنگاه  $F^*$  دقیقاً دارای  $\phi(d)$  عضو از مرتبه  $d$  است (برای هر  $d|q-1$ ) جایی که در آن  $\phi$ ، تابع اویلر است. به خصوص،  $F^*$  باید حداقل یک عضو از مرتبه  $q-1$  را شامل باشد و در نتیجه  $F^*$  دوری خواهد بود.

بیاید درباره گروه‌های دوری مطلبی را یاد آوری کنیم. اگر  $G$  یک گروه دوری از مرتبه  $n$

باشد آنگاه  $G$  شامل دقیقاً  $\phi(d)$  عضو از مرتبه  $d$  است (که  $n$  را عاد می‌کند). بنابراین:

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

حال فرض کنید  $|F^*| = q-1$  و  $\infty$  یک عضو  $F^*$  از مرتبه  $d$  باشد. در این صورت  $d|q-1$ .

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

$$\langle \infty \rangle = \{1, \infty, \infty^2, \dots, \infty^{d-1}\}$$

مرتبه هر عضو  $\langle \infty \rangle$  بر  $d$  بخش پذیر است، بنابراین هر عضو  $\langle \infty \rangle$ ، یک ریشه از  $x^d - 1$

است اما چند جمله‌ای  $x^d - 1$  در  $F$  دارای حداکثر  $d$  ریشه مجزا است (این در جایی است

که ما از این واقعیت بهره می‌گیریم که  $f$  یک میدان است)، بنابراین  $\langle \infty \rangle$ ، مجموعه تمامی

ریشه‌های  $x^d - 1$  است به خصوص تمامی عناصر  $F$  از مرتبه  $d$  می‌بایست در  $\langle \infty \rangle$  باشند.

اما گروه دوری  $\langle \infty \rangle$  دارای دقیقاً  $\phi(d)$  عضو از مرتبه  $d$  است و لذا دقیقاً  $\phi(d)$  عضو از  $F$

دارای مرتبه  $d$  هستند. بنابراین، اگر  $F$  دارای یک عضو از مرتبه  $d$ ،  $d|q-1$ ، 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  $\psi(d) = 0$  اما داریم:

$$q-1 = \sum_{d|q-1} \psi(d) \leq \sum_{d|n} \phi(d) = q-1$$

لذا  $\psi(d) = \phi(d)$  (برای تمامی  $d | q-1$ )، پس قضیه زیر را اثبات کرده ایم.

قضیه اگر  $F$  یک میدان متناهی با  $q$  عضو باشد، آنگاه  $F$  دارای دقیقا  $\phi(d)$  عضو از مرتبه  $d$  می باشد، که در آن  $d | q-1$ .

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

تعریف: هر عضو  $F_q$  که گروه دوری  $F_q^*$  را تولید کند، یک عضو اولیه ( $F_q$  Primitive) نامیده می شود.

توصیف عناصر یک میدان متناهی

در حالت کلی، چندین روش وجود دارد که در آن می توان عناصر یک میدان متناهی را

توصیف کرد. یک روش، استفاده از حلقه تجزیه به صورت  $\frac{F_q[x]}{\langle p(x) \rangle}$  است، جایی که

$P(x)$  یک چند جمله ای تحویل ناپذیر می باشد. روش دیگر، استفاده از این واقعیت می باشد

که  $F_q^*$  دوری می باشد و بنابراین عناصر آن تمامی توان هیا یک عضو اولیه هستند. آنچنان

که خواهیم دید، اولین نمایش مناسب بازمانی است که بخواهی عملیات جمع بین عناصر

$F_q^*$  را انجام دهیم و نمایش دوم، مناسب عملیات ضرب است. اما، خوشبختانه می توانیم

این دو روش را با یکدیگر ترکیب کنیم.

می‌دانیم اگر  $P(x)$  یک چند جمله‌ای تحویل ناپذیر روی  $F_q$  باشد، آنگاه حلقه تجزیه

$$K = \frac{F_q[x]}{\langle p(x) \rangle}$$

یک میدان است در واقع، اگر  $\deg(p(x)) = d$ ، آنگاه  $k$  دارای درجه‌ی  $d$

روی  $F_q$  می‌باشد، بنابراین  $k = F_q d$  این نمایش، روشی برای توصیف عناصر یک میدان نشان می‌دهد.

$$F_q d = \frac{F_q[x]}{\langle p(x) \rangle} = \{r(x) + \langle p(x) \rangle \mid \deg(r(x)) < d\}$$

چون:

پس  $F_q d$  را می‌توان با تمام چند جمله‌ای‌های با درجه حداکثر  $d-1$  به همراه عمل جمع و ضرب پیمانه‌ای (در پیمانه  $p(x)$ ) یکسان در نظر گرفت.

اگر  $\infty$  یک ریشه از  $P(x)$  در یک میدان شکافنده باشد، آنگاه می‌توانیم میدان  $F_q d$  را مجموعه تمام چند جمله‌ای‌ها بر حسب  $\infty$  با درجه حداکثر  $d-1$  در نظر بگیریم که جمع و ضرب در پیمانه  $p(x)$  صورت می‌گیرد. این مطلب، بیان غیر رسمی آن است که بگوییم

$$\frac{F_q[x]}{\langle p(x) \rangle} \text{ با } F_q(x) \text{ یکرخت است.}$$

مثال چند جمله‌ای  $p(x) = x^4 + x^3 + x^2 + x + 1$  روی  $F_7$  تحویل ناپذیر است.

زیرا در غیر اینصورت  $p(x)$  شامل عامل خطی نیست. برای این که نشان دهیم

$$p(1) \neq 0, p(0) \neq 0$$

، بنابراین  $p(x)$  شامل عامل خطی نیست. برای این که نشان دهیم  $p(x)$

شامل هیچ عامل درجه دومی نیست، تمامی عوامل درجه روی  $F_7$  به صورت زیر هستند.

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

اما به آسانی می توان دید  $p(x)$  شامل حاصل ضرب هیچ دوتا از این عوامل نیست. حال

$$q=2 \text{ و } d=4, \text{ پس}$$

$$\frac{F_4[x]}{\langle x^4 + x^3 + x^2 + x + 1 \rangle}$$

بنابراین، با این که  $\infty$  ریشه‌ای از  $p(x)$  باش، می توانیم عناصر  $F_4$  را به صورت چند جمله -

ای های با درجه ۳ یا کمتر، بر حسب  $\infty$  بنویسیم.

۱، ۰: متادیر ثابت

خطی:  $\infty, \infty + 1$

درجه ۲:  $\infty^2, \infty^2 + 1, \infty^2 + \infty, \infty^2 + \infty + 1$

درجه ۳:  $\infty^3, \infty^3 + 1, \infty^3 + \infty, \infty^3 + \infty^2, \infty^3 + \infty + 1, \infty^3 + \infty^2 + 1,$   
 $\infty^3 + \infty^2 + \infty, \infty^3 + \infty^2 + \infty + 1$

هر چند جمله‌ای  $F(\infty) \in F_4[\infty]$  را می توان در پیمانه  $p(x)$  کاهش داد؛ برای این کار کافی

است قرار دهیم  $p(x) = 0$  پس در این مثال:

$$\infty^4 = \infty^3 + \infty^2 + \infty + 1$$

در این حالت، محاسبات تا حدودی با توجه به این واقعیت که  $\infty$  دارای مرتبه نسبتاً کوچکی

خواهد بود، ساده ترین به نظر می رسد.

$$\infty^5 = \infty \cdot \infty^4 = \infty (\infty^3 + \infty^2 + \infty + 1) = \infty^4 + \infty^3 + \infty^2 + \infty + 1$$

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

با استفاده از این نمایش، جمع کاملاً ساده به نظر می آید. کافی است چند جمله‌ای های با

درجه حداکثر ۳ را به یکدیگر جمع کنید، برای مثال؛ در  $F_4$  داریم  $2=0$ ؛ پس

$$(\alpha^3 + \alpha + 1) + (\alpha^3 + \alpha^2 + 1) = \alpha^2 + \alpha$$

اما، ضرب کردن ساده نیست، زیرا باید حاصل ضرب را در پیمانه  $p(\alpha)$  کاهش دهیم. به

عنوان نمونه، در این مثال:

$$(\alpha^3 + \alpha + 1)(\alpha^3 + \alpha^2 + 1) = \alpha^6 + \alpha^5 + \alpha^3 + \alpha^4 + \alpha^3 + \alpha + \alpha^3 + \alpha^2 + 1 =$$

$$\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + 1 = \alpha H + \alpha^4 + \alpha^3 + 1 = \alpha^4 + \alpha^3 + \alpha$$

در مورد میدان‌های بزرگتر، حاصل ضرب چند جمله‌ای غیر عملی است، به خصوص در

نمایش تناوبی بعداً در نظر می گیریم.

اگر  $\beta$  یک عضو اولیه از  $F_q$  باشد، آنگاه:  $F_q = \{1, \beta, \dots, \beta^{q-2}\}$

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

اما در این نمایش جمع کردن اصلاً واضح نیست. از طرف دیگر، اگر چند جمله‌ای مینمال

$P(x)$  برای  $\beta$  را داشته باشیم، آنگاه می توانیم عناصر  $F_{16}$  را به صورت چند جمله‌ای هایی بر

حسب  $\beta$  در نظر گرفته و از آنها به منظور جمع بهره گیریم. بیایید مثال زیرا در نظر بگیرید.

مثال: چند جمله‌ای  $q(x) = x^4 + x + 1$  تحویل ناپذیر است (روی  $F_4$ ) فرض کنید  $\beta$  یک ریشه

از این، چند جمله‌ای باشد. بنابراین. مانند مثال قبل، می توانیم عناصر  $F_{16}$  را به صورت

مجموعه چند جمله‌ای های با درجه حداکثر ۳ برحسب  $\beta$  در نظر بگیریم، که در آن

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



از طرف دیگر:

$$\begin{aligned} \beta^{15} &= (\beta^5)^3 = (\beta \cdot \beta^4)^3 = (\beta(\beta+1))^3 = \beta^3(\beta+1)^3 = \\ &\beta^3(\beta^3 + \beta^2 + \beta + 1) = \beta^6 + \beta^5 + \beta^4 + \beta^3(\beta^3 + \beta^2) + (\beta^2 + \beta) + \\ &(\beta + 1) + \beta^3 = 1 \end{aligned}$$

این رابطه نشان می‌دهد که مرتبه  $\beta$  باید ۱۵ را عا د کند. ولی  $\beta^5 \neq 1, \beta^3 \neq 1$  پس

$ord(\beta) = 15$  و لذا  $\beta$  اولیه است. چون  $\beta$  یک عضو اولیه  $F_{16}$  است، پس عناصر ناصفر  $F_{16}$

را می‌توان به صورت توان‌های  $\beta, \beta^2, \dots, \beta^{14}, \beta^{15}$  در نظر گرفت. حال می‌توانیم بین این دو

نمایش (ضرب و جمع) یک ارتباط برقرار کنیم، برای این کار می‌توان هر عضو  $\beta^k$  را به

صورت یک چند جمله بر حسب  $\beta$  با درجه حداکثر ۳ نمایش داد. با استفاده از این واقعیت

$$\text{که } \beta^4 = \beta + 1 \text{ داریم:}$$

$$\begin{aligned} \beta^4 = \beta + 1 &\Rightarrow \beta^5 = \beta \cdot \beta^4 = \beta(\beta + 1) = \beta^2 + \beta, \beta^6 = \beta \cdot \beta^5 = \beta^3 + \beta^2 \\ \beta^7 = \beta \cdot \beta^6 &= \beta^4 + \beta^3 = \beta^3 + \beta + 1 \end{aligned}$$

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

در این جدول به جای  $\beta^k$ ، تنها  $k$  را نوشته‌ایم و به جای چند جمله‌ای

$$a_3\beta^3 + a_2\beta^2 + a_1\beta + a_0 \text{ (به منظور سادگی)، رشته } a_3a_2a_1a_0 \text{ را نوشته‌ایم.}$$

محاسبات، در این جدول، کاملاً سراسر است.

به عنوان مثال، داریم:

$k; \beta^k$	$a_3a_2a_1a_0; a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3$	$(\beta^8 + \beta^4 + 1)(\beta^3 + \beta) = \beta^{11} + \beta^9 + \beta^7 +$
۰	۰۰۰۱	$\beta^5 + \beta^3 + \beta = 1110 + 1010 + 1011 +$

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  $\beta$  یک عضو اولیه از میدان  $F_q^n$  باشد. چندجمله‌ای مینیمال  $\beta$  روی

$F_q$  یک چند جمله‌ای اولیه (*Primitive polynomial*) برای  $F_q^n$  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  $F_q^n$  یک چند جمله‌ای

تکین تحویل ناپذیر روی  $F_q$  است که تمامی ریشه‌های آن، عناصر اولیه  $F_q^n$  می‌باشند. همچنین، خواهیم دید که تمامی چند جمله‌ای‌های اولیه برای  $F_q^n$  روی  $F_q$  دارای درجه هستند.

در حالت کلی، یافتن چند جمله‌ای‌های اولیه کار آسانی نیست. روش‌های متفاوتی وجود دارند که در حالت‌های خاصی، تا حدی موفق بوده‌اند، اما در اینجا به آنها نمی‌پردازیم. خوشبختانه، جدول‌های گسترده‌ای از چند جمله‌ای‌های اولیه و میدان‌ها، داده شده‌اند. برای این کار، می‌توان کار لیدل (*Lidl*) و نیدریتز (*Niederreiter*) (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  $\phi$  زیر است.

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

می‌توان نشان داد که ماتریس همراه یک چند جمله‌ای، در آن چند جمله‌ای صدق می‌کند، یعنی  $(C) = 0$

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 جمله‌ای‌ها بر حسب  $C$  با درجه کمتر از  $d$ ، نمایش داد، جایی که جمع و ضرب در پیمانه  $P(C)$  هستند. اما چند جمله‌ای‌های بر حسب  $C$ ، فقط ماتریس هستند؛ بنابراین می‌توانیم نمایشی از عناصر  $F_q$  را به صورت ماتریس‌های روی  $F_q$  رد نظر بگیریم.

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

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

به صورت زیر هستند:

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

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

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

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

و عناصر  $F_q$  به صورت زیر هستند:

$$\begin{aligned}
 \circ &= \begin{bmatrix} \circ & \circ \\ \circ & \circ \end{bmatrix}, A^1 = \begin{pmatrix} \circ & 1 \\ 1 & \circ \end{pmatrix}, A^2 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}, A^3 = \begin{pmatrix} 2 & 2 \\ 2 & \circ \end{pmatrix}, \\
 A^4 &= \begin{pmatrix} 2 & \circ \\ \circ & 2 \end{pmatrix}, A^5 = \begin{pmatrix} \circ & 2 \\ 2 & \circ \end{pmatrix}, A^6 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, A^7 = \begin{pmatrix} 1 & 1 \\ 1 & \circ \end{pmatrix}, \\
 A^8 &= \begin{pmatrix} 1 & \circ \\ \circ & 1 \end{pmatrix}
 \end{aligned}$$

در هر حالت، جمع و ضرب با استفاده قواعد جبر ماتریس ها به دست می آید. مزیت این

نمایش ها این است که محاسبات به صورت خود کار صورت می گیرد، برای نمونه،

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

از طرف دیگر، اگر  $\deg(p(x))$  بزرگ باشد، آنگاه ماتریس ها بزرگ خواهند شد و لذا

محاسبات پیچیده می گردد.

### چند جمله ای های تحویل ناپذیر میدان های متناهی

در این بخش، درباره خواص اصلی چند جمله ای های تحویل ناپذیر روی میدان های متناهی

بحث می کنیم. فرض کنیم میدان شکافنده یک چند جمله ای  $f(x)$  را با  $split(f(x))$  یا

$split(f)$  نمایش دهیم. لم زیر بسیار مفید است.

**لم:** فرض کنید  $f(x)$  یک چند جمله ای تحویل ناپذیر روی  $F_q$  باشد و  $\infty$  یک ریشه از  $f(x)$

در میدان تعمیم یافته باشد. بنابراین، اگر  $f(x) \in F_q[x]$  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 ناصفیری از چند جمله‌ای مینیمال  $\infty$  روی  $f(x)$  است، نتیجه می‌شود. بحث اصل خود را با طرح اساسی ترین سوال در این باره، یعنی وجود چنین میداین آغاز می‌کنیم.

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

اثبات: فرض کنید  $\beta$  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  $\beta$  روی  $F_q$  می‌بایست دارای درجه  $d$  باشد.

### میدان شکافنده یک چند جمله‌ای تحویل ناپذیر

در یک میدان نامتناهی مانند  $F$ ، اگر  $\infty$  یک ریشه چند جمله‌ای تحویل ناپذیر  $f(x) \leftarrow F[x]$  باشد، آنگاه میدان  $F(x)$ ، حاصل از الحاق  $\infty$  به  $F$ ، در حالت کلی میدان شکافنده  $F(x)$  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. برای مشاهده دلیلی این مطلب، فرض کنید  $F(x)$  با درجه  $d$  روی  $F_q$  تحویل ناپذیر باشد. فرض کنید  $\infty$  ریشه‌ای از  $F(x)$  در  $split(f)$

باشد. میدان‌های زیر را در نظر بگیرید:  $F_q < F_q(\infty) < \text{split}(f)$  چون  $[F_q d(x) = F_q] = d$

پس  $|F_q(x)| = q^d$  و لذا  $F_q(\infty)$  مجموعه تمامی ریشه‌های چند جمله‌ای  $f_q d(x) = x^q - x$

است. به خصوص،  $\infty$  ریشه‌ای از  $f_q d(x)$  نیز هستند و بنابراین، این ریشه‌ها متعلق، به  $F_q(\infty)$

می‌باشند. لذا:  $F_q(\infty) = \text{split}(f)$ ، این مطلب، به اثبات قضیه زیر منجر می‌شود.

**قضیه:** فرض کنید  $f(x) \leftarrow f_q[x]$  یک چند جمله‌ای تحویل ناپذیر با درجه  $D$  باشد و  $\infty$

ریشه دلخواهی از  $F(\infty)$  باشد. در این صورت، میدان شکافنده  $F(\infty)$  به صورت زیر است:

$$\text{split}(f) = F_q(\infty) = F_q d$$

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

**نتیجه:** فرض کنید  $f(x) \in F_q[x]$  چند جمله‌ای تحویل ناپذیر با درجه  $d$  باشد در این

صورت.

صورت  $f(x) \leftarrow F_q[x]$  اگر و تنها اگر  $d|n$

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

$$\text{split}(f) < \text{split}(x^{q^n} - x) \Leftrightarrow d | n \quad \text{از قبل،}$$

حال، اگر  $f(x) | x^{q^n} - x$  آنگاه هر ریشه  $f(x)$ ، ریشه‌ای از  $x^{q^n} - x$  است. در نتیجه،

$\text{split}(f) < \text{split}(x^{q^n} - x)$  و لذا  $d|n$ . برعکس، اگر  $d|n$  آنگاه  $\text{split}(f) < \text{split}(x^{q^n} - x)$  و

لذا هر ریشه  $\infty$  از  $f(x)$ ، در  $\text{split}(x^{q^n} - x)$  قرار می‌گیرد. اما،  $\text{split}(x^{q^n} - x)$  مجموعه

تمامی ریشه‌های  $(x^{q^n} - x)$  است و لذا  $\infty$  می‌بایست ریشه‌های 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  $f_{qd}$  هستند که در آن:  $d = \deg(f(x))$ .

فرض کنید  $f(x) = a_0 + a_1x + \dots + a_dx^d$  که در آن  $a_i \in F_q$ . اگر یک ریشه از  $f(x)$  باشد،

آنگاه:

$$f(x) = a_0 + a_1 \infty + \dots + a_d \infty^d = 0$$

حال از این مزیت که با یک میدان با مشخصه  $p$  کار می‌کنیم، به صورت زیر بهره می‌گیریم.

چون  $a_i \in F_q$ ، می‌دانی  $a_i^q = a_i$  و نیز.

$$f(x^q) = a_0 + a_1 \infty^q + \dots + a_d \infty^{qd} = a_0^q + a_1^q \infty^q + \dots + a_d^q \infty^{qd} =$$

$$a_0^q + (a_1 \infty)^q + \dots + (a_d \infty^d)^q = (a_0 + a_1 \infty + \dots + a_d \infty^d)^q =$$

$$(f(x))^q = 0$$

بنابراین اگر  $\infty$  ریشه‌ای از  $f(x)$  باشد،  $\infty^q$  نیز ریشه‌ای از  $f(x)$  خواهد بود. به همین

ترتیب، می‌بینیم که  $\infty, \infty^q, \infty^{q^2}, \dots, \infty^{q^{d-1}}$  نیز ریشه‌هایی از  $f(x)$  هستند. حال اگر نشان

دهیم این ریشه‌ها متمایز هستند، آنگاه اینها، تمامی ریشه‌های  $f(x)$  خواهند بود. اگر

$\infty^{q^i} = \infty^{q^j}$  آنگاه دوطرف را به توان  $q^{d-j}$  می‌رسانیم، پس داریم:

$$(i < j)$$



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

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

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

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

همچنین، توجه داریم که  $D$  کوچکترین عدد صحیح مثبتی است که در آن  $\infty a^d = \infty$

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 درجه  $d$  باشد. اگر  $\infty$

یک ریشه از  $f(x)$  در  $split(f) = F_q^d$  باشد، آنگاه، تمامی ریشه‌های  $f(x)$  به صورت زیر

می‌باشند.

$$\infty, \infty q, \infty q^2, \dots, \infty q^{d-1}$$

علاوه بر این،  $d$  کوچکترین عدد صحیح مثبتی است که در آن  $\infty q^d = \infty$ .

**نتیجه:** فرض کنید  $f(x) \in F_q[x]$  تحویل ناپذیر باشد. در این صورت، تمامی ریشه‌های

$f(x)$  در  $split(f)$  دارای مرتبه یکسانی می‌باشند.

**اثبات:** این مطلب با توجه به این که  $(split(f))$  دارای مرتبه  $a^q - 1$  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  $o(f)$  نمای شداده می‌شود.

توجه به 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 (*conjugate*) نامیده می‌شوند اگر آنها ریشه‌های چند جمله‌ای تحویل ناپذیر تکین یکسانی روی  $F_q$  باشند؛ یعنی دارای چند جمله‌ای آنها ریشه‌های چند جمله‌ای تحویل ناپذیر تکین یکسانی روی  $F_q$  باشند؛ یعنی دارای چند چند جمله‌ای مینیمال یکسانی روی  $F_q$  باشند.

**نتیجه:** مدوج های  $\alpha \in F_q^n$  روی  $F_q$  به صورت زیر هستند.

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

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 چند جمله‌ای مینیمال هر عضو  $\alpha \in F_q$  را یافت.

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

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

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

مثال: قبلا دیدیم چند جمله‌ای  $P(x) = x^4 + x + 1$  برای  $F_{16}$  روی  $F_4$ ، اولیه می‌باشد. بنابراین،

هر ریشه  $\beta$  از  $p(x)$ ،  $F_{16}$  را تولید می‌کند. حال بیابید، چند جمله‌ای مینیمال عناصر  $F_{16}$  را

بیابیم.

با محاسبه مزدوج‌ها، شروع می‌کنیم: (توجه داریم که  $\beta^{15} = 1$ )

$$\beta, \beta^2, \beta^4, \beta^8 \quad (\beta^{16} = \beta)$$

$$\beta^3, \beta^6, \beta^{12}, \beta^{24} = \beta^9 \quad (\beta^{48} = \beta^3)$$

$$\beta^5, \beta^{10}$$

$$\beta^7, \beta^{14}, \beta^{28}, \beta^{56}, \beta^{112} \quad (\beta^{112} = \beta^7)$$

حال فرض کنید  $m_k(x)$  چند جمله‌ای مینیمال  $\beta^k$  باشد، در اینصورت به طور نمونه

$$m_{15}(x) = m_{10}(x) = (x - \beta^5)(x - \beta^{10}) = x^2 - (\beta^5 + \beta^{10})x + \beta^{15}$$

$$\beta^5 + \beta^{10} = 0.110 + 0.111 = \dots = \beta^0 = 1 \quad \text{اما طبق جدول قبل داریم:}$$

$$m_{15}(x) = m_{10}(x) = x^2 + x + 1 \quad \text{و چون } \beta^{15} = 1 \text{ داریم}$$

سایر چند جمله‌ای هی مینیمال نیز به طور مشابه، محاسبه می‌شوند. لیست کامل به صورت

زیر است.

$$m_0(x) = x + 1$$

$$m_1(x) = m_2(x) = m_4(x) = m_8(x) = x^4 + x + 1$$

$$m_3(x) = m_6(x) = m_{12}(x) = m_{24}(x) = x^4 + x^3 + x^2 + x + 1$$

$$m_5(x) = m_{10}(x) = x^2 + x + 1$$

$$m_7(x) = m_{14}(x) = m_{28}(x) = m_{56}(x) = x^4 + x^3 + 1$$

## 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

$\sigma: F_q^n$  است که در آن:

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) \quad (1) \quad \sigma(\alpha \beta) = \sigma(\alpha)\sigma(\beta) \quad (2)$$

$$(3) \quad \text{اگر } a \in F_q \text{ آنگاه } \sigma(a) = a$$

شرط آخر، بیان می‌کند که  $\sigma$  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  $\beta$  یک عضو اولیه از  $F_q^n$  باشد. در این صورت  $\beta^c$  دارای مرتبه  $q^n - 1$

است و لذا چند جمله‌ای مینیمال آن  $m(x)$ ، دارای ریشه‌های زیر است.

$$\beta, \beta^q, \beta^{q^2}, \dots, \beta^{q^{n-1}}$$

حال، فرض کنید  $f(x)$  یک چند جمله‌ای روی  $F_q$  باشد. چون یک خودریختی تا از  $F_q^n$

روی  $F_q$ ، ضرایب  $f(x)$  را ثابت نگه می‌دارد، می‌بینیم که  $f(\alpha) = 0$ ، اگر و تنها اگر

$f(\tau(\alpha)) = 0$ . به بیان دیگر،  $\tau$  ریشه‌های  $f(x)$  را که در  $F_q^n$  هستند، جایگشت می‌دهد. به

خصوص  $\tau$  می‌بایست  $\beta$  (ریشه  $m(x)$ ) را به ریشه دیگری تصویر کند، یعنی  $\tau(\beta) = \beta^{q^i}$

(برای مقدرای  $i$ ). اما چون  $\beta$  یک عضو اولیه از  $F_q^n$  است،  $F_q^n$  کاملاً توسط مقادیر آن

روی  $\beta$  تعیین می‌شود و چون:

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

نتیجه می‌گیریم که  $\tau = \sigma_q^i$ . بنابراین، تمامی خودریختی‌های  $F_q^n$  روی  $F_q$  به شکل  $\sigma_q^i$  هستند (برای مقداری  $i$ )

### ریشه‌های واحد (The roots of unity)

در این بخش با این سوال که چگونه می‌توانیم چند جمله‌ای  $x^n - 1$  را روی یک میدان متناهی مانند  $F_q$  تجزیه کنیم، پاسخ می‌دهیم. این سوال، ما را به بحث کدهای دوری راهنمای می‌کند. اگر  $q, n$  نسبت به هم اول نباشند، آنگاه می‌توانیم بنویسیم  $n = mp^k$  که در آن  $(m, q) = 1$  و  $P$  مشخصه  $F_q$  است. در این حالت؛

$$x^n - 1 = x^{mp^k} - 1 = (x^m - 1)^{p^k}$$

بنابراین، از اینجا به بعد فرض خواهیم کرد  $q, n$  نسبت به هم اول هستند.

**توجه:** فرض کنید  $F_q S$ ، میدان شکافنده  $x^n - 1$  روی  $F_q$  باشد. در این صورت چند جمله‌ای

$x^n - 1$  دارای ریشه تکراری در هیچ یک از توسیع‌های  $F_q$  نیست، زیرا

$$D(x^n - 1) = nx^{n-1}$$

دارای هیچ ریشه مشترکی با  $x^n - 1$  نیست. بنابراین  $x^n - 1$  دارای  $n$  ریشه متمایز در میدان شکافنده  $F_q S$  است. (توجه دارید که این مستلزم آن است که  $(n, q) = 1$ ).

تعریف: ریشه‌های  $x^n - 1$  در میدان شکافنده  $F_q S$ ، ریشه‌های  $n$ ام واحد در  $F_q$  نامیده می‌شوند. مجموعه ریشه‌های  $n$ ام واحد با  $E^{(n)}$  نمایش داده می‌شوند.

نکته: توجه دارید که ریشه‌های  $n$ ام واحد، حتی زمانی که  $a, n$  نسبت به هم اول نباشند

تعریف شده هستند. اما در این حالت، تعداد ریشه‌های متمایز، کمتر از  $n$  خواهد بود.

زمانی که  $(n, q) = 1$ ، مجموعه  $E^{(n)}$  دارای ساختار خاص و جالبی خواهد بود.

قضیه: مجموعه  $E^{(n)}$  شامل ریشه‌های  $n$ ام 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 این صورت:

$$(\alpha \beta^{-1})^n = \alpha^n (\beta^n)^{-1} = 1 \Rightarrow \alpha \beta^{-1} \in E^{(n)}$$

بنابراین  $E^{(n)}$  یک زیر گروه دوری از  $F_q^s$  است و لذا دوری است.

تعریف: یک ریشه  $n$ ام واحد از مرتبه  $n$  با  $\alpha$ ، ریشه اولیه  $n$ ام واحد روی  $F_q$  نامیده می‌شود از

اینجا به بعد قرار داد می‌کنیم  $W$  یک ریشه اولیه واحد است.

از آنجایی که  $E^{(n)}$  دوری است، نتیجه زیر را داریم.

نتیجه: دقیقاً  $\phi(n)$  ریشه  $n$ ام اولیه واحد روی  $F_q$  وجود دارند. به خصوص، چون  $\phi(n) > 0$ ،

یک ریشه اولیه  $n$ ام 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  $F_q^s$  یک

میدان شکافنده است) بر حسب  $n$  بیابیم. در این حالت، اگر  $w$  ریشه  $n$ ام اولیه واحد باشد،

آنگاه  $w$  از مرتبه  $n$  بوده و چون  $w \neq 0$  داریم:

$$w \in F_{q^r} \Leftrightarrow w^{q^r} = w \Leftrightarrow w^{q^r - 1} = 1 \Leftrightarrow n | r - 1$$

چون  $s$  کوچکترین عدد  $R$  است که در آن  $w \in F_{q^r}$ ، نتیجه زیر را اثبات کرده ایم.

نتیجه: اگر  $F_{q^s}$  میدان شکافنده  $x^n - 1$  روی  $F_q$  باشد، آنگاه  $s$  کوچکترین عدد صحیح مثبت

است که در آن  $n | q^s - 1$ ، یعنی  $S$  کوچکترین عدد صحیح مثبت است. که در  $q^s \equiv 1 \pmod{n}$  به بیان

دیگر،  $s$  مرتبه  $q$  در پیمانه  $n$  است که با  $on(q)$  نمایش داده می شود.

عناصر اولیه میددان و ریشه های اولیه واحد

تفاوت بین یک عضو اولیه میدان شکافنده  $F_{q^s}$  از  $x^n - 1$  و یک ریشه اولیه  $n$ م واحد بسیار

حائز اهمیت است. با استفاده از تعریف،  $\beta$  یک عوض اولیه میدان  $F_{q^s}$  است.

اگر  $\beta$  گروه دوری  $F_{q^s}$  را تولید کند. از طرف دیگر، با استفاده از تعریف،  $w$  یک ریشه

$n$ م اولیه واحد است، اگر آن زیر گروه دوری  $E^{(n)}$  را تولید کند. بنابراین

$$\beta \in F_{q^s} \text{ عضو اولیه } F_{q^s} \Leftrightarrow F_{q^s}^* = \{1, \beta, \beta^2, \dots\}$$

$$w \in E^{(n)} \text{ یک ریشه } n \text{م اولیه واحد است.} \Leftrightarrow E^{(n)*} = \{1, w, w^2, \dots\}$$

اما، توجه دارید که یک ریشه اولیه  $n$ م واحد  $w$ ،  $F_{q^s}$  را روی  $F_q$  (به عنوان یک عضو

میدان که ضرب و جمع را اجازه می دهد). تولید می کند. یعنی  $F_q(w) = F_{q^s}$ .

این مطلب، از این واقعیت نتیجه می شود:

$$F_q(w) = F_q(E^{(n)}) = F_{q^s}$$

اگر  $\beta$  یک عضو اولیه  $F_{q^s}$  باشد، آنگاه  $\beta$  دارای مرتبه  $q^s - 1$  است. چون  $n | q^s - 1$  پس

$$q^n - 1 = nr \quad (\text{برای یک } r \in \mathbb{Z}), \text{ بنابراین}$$

$$O(\beta^k) = \frac{q^s - 1}{(k, q^s - 1)} = \frac{nr}{(k, nr)}$$

بنابراین،  $\beta^k$  یک ریشه  $n$ ام اولیه واحد است اگر و تنها اگر:

$$\frac{nr}{(k, nr)} = n$$

یا به طور هم ارز  $(k, nr) = r$ ، اما این، رابطه برقرار است اگر و تنها اگر  $K = ra$ ، جایی که

$(u, n) = 1$  چون  $\phi(n)$  ریشه  $n$ ام اولیه دقیقا وجود دارند، بنابراین قضیه زیر را اثبات کرده ایم.

قضیه فرض کنید  $\beta$  یک عضو اولیه میدان شکافنده  $F_{q^s}$  از  $x^n - 1$  باشد در این صورت

$\phi(n)$  ریشه اولیه  $n$ ام واحد روی  $F_q$ ، دقیقا به صورت زیر هستند.

$$\{\beta^k \mid k = \frac{q^s - 1}{n} u, u < n, (u, n) = 1\}$$

به خصوص،  $\beta^{\frac{q^s - 1}{n}}$  یک ریشه  $n$ ام اولیه واحد است.

اثبات: قضیه زیر به عنوان تمرین واگذاری می شود.

قضیه فرض کنید  $F_q$  یک میدان متناهی باشد. همچنین فرض کنید  $\Omega$  مجموعه ریشه های

$n$ ام اولیه روی  $F_q$  باشد و  $F$  مجموعه عناصر اولیه میدان شکافنده  $F_{q^s}$  از  $x^n - 1$  باشد. در

این صورت، یا  $\Omega \cap F = \emptyset$  یا در غیر این صورت  $\Omega = F$ ؛ همچنین حالت دوم در زمانی رخ

می دهد که  $n = q^s - 1$ .



## روشی برای تجزیه $x^{n-1}$

برای  $(n, q) = 1$ ، می‌توانیم چند جمله‌ای  $x^n - 1$  را روی  $F_q$ ، با استفاده از این واقعیت که  $x^n - 1$  دارای  $n$  ریشه، متمایز است که، تجیه کنیم. بنابراین  $x^n - 1$  حاصل ضرب چند جمله‌ای‌های مینیمال متمایز این ریشه‌هاست. این چند جمله‌ای‌های مینیمال می‌توانند با استفاده از روش‌های موجود در بخش قبل، محاسبه شوند. اشکال اصلی این روش این است که ما باید در میدان شکافته:  $F_{q^s}$ : (که میدان بزرگتر است) کار کنیم. فرض کنیم  $\beta$  یک عوض اولیه  $F_{q^s}$  باشد که در آن  $S = o_n(q)$ . با استفاده از مطالب قبل، می‌توانیم یک ریشه  $n$ ام اولیه واحد  $w$  را به صورت زیر بدست آوریم.

$$w = \beta \frac{q^s - 1}{n}$$

بنابراین، ریشه‌های  $x^n - 1$  به صورت زیر هستند.

$$1, w, w^2, \dots, w^{n-1}$$

حال، تنها چیزی که نیاز داریم محاسبه چند جمله‌ای‌های مینیمال این ریشه‌ها و سپس ضرب نمودن این چند جمله‌ای‌های متمایز است. برای  $i = 0, \dots, n-1$ ، مزدوج‌های  $w^i$  به صورت زیر می‌باشند.

$$w^i, w^{qi}, w^{iq^2}$$

جایی که  $d$  کوچکترین عدد صحیح مثبت است که در آن  $w^{iq^d} = w^i$ . اما

$$w^{iq^d} = w^i \Leftrightarrow w^{iq^{d-1}} = 1 \Leftrightarrow n \mid iq^{d-1} \Leftrightarrow iq^d \equiv i$$

بنابراین، می‌توانیم شرط  $ia^d \equiv i$  را برای تعیین نامی مزدوج‌ها به کار ببریم.

لذا، چند جمله‌ای مینیمال ریشه‌های  $x^n - 1$  به صورت زیر است.

تعریف: مجموعه  $C_i = \{i, iq, \dots, iq^{d-1}\}$ ، جایی که  $d$  کوچکترین عدد صحیح مثبت باشد که

ردان  $i, iq^d \equiv i$ ،  $i$  امین هم‌دسته دوری (*i-Th cyclotomic coset*) برای  $q$  در پیمانه  $n$  نامیده

می‌شود. این مجموعه‌ها می‌توانند بدون مراجعه خاص به یک دسته  $n$  ام اولیه واحد تعریف

شوند.

حال در اینجا، مثالی برای روشن شدن بحث می‌آوریم.

مثال: چند جمله‌ای  $h_{15}(x) = x^{15} - 1$  روی  $F_7$  را در نظر بگیرید.

در اینجا  $q=2, n=15$ . چون  $s = \circ_{15}(2) = 4$ ، میدان شکافنده  $h_n(x)$  به صورت  $F_{q^s} = F_{16}$

است. از طرف دیگر چند جمله‌ای  $x^4 + x + 1$  یک چند جمله‌ای اولیه روی  $F_7$  می‌باشد،

بنابراین اگر  $\beta$  ریشه این چند جمله‌ای باشد،  $\beta$  یک عضو اولیه از میزان  $F_{16}$  می‌باشد. با

استفاده از  $\beta$ ، می‌توانیم  $w$  را به عنوان ۱۵ امین ریشه اولیه واحد بیابیم:

$$w = \beta \frac{q^s - 1}{n}$$

در این حالت،  $\beta$  هم یک عضو اولی و هم یک ریشه اول خواهد بود. بنابراین،  $x^{15} - 1$  به

صورت زیر هستند:

$$1, \beta, \beta^2, \dots, \beta^{14}$$

چند جمله‌ای مینیمال این ریشه‌ها، قبلاً محاسبه شده اند (یک مثال). بنابراین:

$$x^{15} - 1 = (x+1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x^3 + 1)$$

مثال: برخی اوقات، اطلاع از هم دسته‌های دوری می‌تواند تجزیه خاصی از  $x^n - 1$  را به ما نشان دهد (یعنی همان تجزیه و چند جمله‌ای‌های تحویل ناپذیر). برای نمونه، چند جمله‌ای  $x^9 - 1$  روی  $F_7$  را در نظر بگیرید. چون  $q=2$  و  $n=9$ ، هم دسته‌های دوری به صورت زیر می‌باشند.

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 7, 5\}, C_3 = \{3, 6\}$$

بنابراین  $x^9 - 1$  را می‌توان به عوامل خطی تحویل ناپذیر، یک عامل درجه دو تحویل ناپذیر و یک عامل تحویل ناپذیر از درجه ۶ تجزیه کرده اما، به آسانی می‌توان دید که روی  $F_7$  داری:

$$x^9 - 1 = (x^3)^3 - 1 = (x^3 - 1)(x^6 + x^3 + 1) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

و بنابراین، تجزیه خواسته شده، حاصل می‌گردد.

### مرتبه چند جمله‌ای تحویل ناپذیر

یادآوری می‌کنیم که مرتبه  $o(f)$  از یک چند جمله‌ای تحویل ناپذیر  $f(x)$  با مرتبه هر یک از ریشه‌های آن در میدان شکافنده  $F_q$  از  $F(x)$  برابر است.

قضیه: فرض کنید  $f(x)$  یک چند جمله‌ای تحویل ناپذیر روی  $F_q$  باشد.

$$(1) \text{ اگر } \deg(f(x)) = d \text{ آنگاه } q^d - 1 \mid o(f)$$

$$(2) f(x) \mid x^n - 1 \Leftrightarrow o(f(x)) \mid n$$

(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  $x^{q^d} - 1$  نیز هست و لذا مرتبه

آن ریشه،  $q^d - 1$  را عاد می کند. 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

$x^{n=1} = x^{ko(f)} - 1 | x^{o(f)} - 1$  و مابقی اثبات، با توجه به قسمت (۲) بدیهی است.

(۴) این قسمت، با توجه به قسمت (۳) نتیجه می شود.

نکته می توانیم درجه  $d$  یک چند جمله‌ای تحویل ناپذیر از مرتبه  $E$  را به صورت زیر بیابیم.

اگر  $\infty$  ریشه‌ای از  $f(x)$  رد  $F_q d$  باشد، آنگاه طبق قضیه‌ای از قبل داریم:

$$F_q \infty = F_q(\infty)$$

اما  $\infty$ ،  $e$  امین ریشه اولیه واحد است و لذا:

$$F_q(\infty) = F_q(E^{(n)}) = split(x^e - 1) = F_q s$$

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 می‌کند. (به طور یکتا)؛ اما عکس آن همواره برقرار نیست. به طور مثال چند جمله‌ای  $f(x) = x^4 + x + 1$  و  $p(x) = x^4 + x^3 + x^2 + x + 1$ ، هر دو دارای درجه ۴ هستند. اما  $o(f(x)) = 15$ ،  $o(p(x)) = 5$ . 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 جمله‌ای 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  $(n, d) = 1$ .

**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  $q^d - 1$  را به عوامل اول آن تجزیه می‌کنیم.

$$q^d - 1 = \prod_i p_i^{r_i}$$

حال، چون  $o(f) | q^d - 1$  داریم:

$$p_i^{r_i} | o(f) \Leftrightarrow o(f) \nmid \frac{q^d - 1}{p_i} \Leftrightarrow f(x) \nmid \frac{(q^d - 1)}{p_i} - 1 \Leftrightarrow x \frac{q^d - 1}{p_i} \nmid f(x) \neq 1$$

بنابراین، با محاسبه باقی مانده‌های  $x \frac{q^d - 1}{p_i}$  (در پیمانه  $f(x)$ )، می‌توانی بیشترین توان هر  $p_i$

که  $o(f)$  را عادی می‌کند. بیابیم.

مثال: چند جمله‌ای تحویل ناپذیر  $f(x) = x^6 + x + 1$  روی  $F_7$  را در نظر بگیرید. چون  $q = 7$ ،

داریم  $q^6 - 1 = 6^6 - 1 = 3^2 \times 7$ . حال می‌بینیم که  $3^2$ ، مرتبه  $f$  یا  $o(f)$  را عادی می‌کند یا خیر.

$$3^2 | o(f) \Leftrightarrow x^2 \nmid 1 \pmod{x^6 + x + 1} \quad \text{چون } \frac{6^6}{3} = 21 \text{، داریم:}$$

اما به سادگی می‌توان دید:  $x^2 + x \neq 1$  و  $x^2 \nmid \underline{\underline{x^6 + x + 1}}$  و لذا  $3^2 | o(f)$  حال

عدد اول 7 را بررسی می‌کنیم. داریم:  $V | o(f) \Leftrightarrow x^7 \nmid (x^6 + x + 1)$

اما  $x^7 \pmod{x^6 + x + 1} = x$ ، لذا  $V | o(f)$ . بنابراین  $o(f) = 6^3$ . لذا  $f$  یک چند جمله‌ای اولیه روی

$F_7$  است.

مثال

چند جمله‌ای تحویل ناپذیر  $g(x) = x^6 + x^4 + x^2 + x + 1$  را در نظر بگیرید. در این حالت داریم:

$$3^2 lo(g) \Leftrightarrow x^{21} \not\equiv 1 \pmod{(x^6 + x^4 + x^2 + x + 1)}$$

اما  $x^{21} \pmod{(x^6 + x^4 + x^2 + x + 1)} = 1$  و لذا  $3^2 lo(f)$  بنابراین باید مقسوم علیه ۳ را بررسی کنیم.

$$3^2 lo(g) \Leftrightarrow x^9 \not\equiv 1 \pmod{(x^6 + x^4 + x^2 + x + 1)}$$

اما  $x^9 \pmod{(x^6 + x^4 + x^2 + x + 1)} = x^5 + x^3 + x^2 + x \neq 1$  لذا  $3 lo(g)$ . سرانجام، باید عامل را بررسی کنیم.

$$7 lo(g) \Leftrightarrow x^9 \not\equiv 1 \pmod{(x^6 + x^4 + x^2 + x + 1)}$$

چون  $x^9 \pmod{(x^6 + x^4 + x^2 + x + 1)} = x^4 + x^2 + 1 \neq 1$  لذا  $7 lo(g)$ . پس  $lo(g) = 21$

### کدهای دوری یا (Cyclic codes)

کدهای دوری، به دلایل بسیاری مهم هستند. جدا از این که این کدها دارای ساختار ریاضی بسیار غنی هستند این کدها از دیدگاه عملی نیز حائز اهمیت هستند؛ زیرا کد گذاری و کد گشایی این کدها با استفاده از مدارهای سوئیچ کننده خطی به روش کاملاً کارایی صورت می‌گیرد.

در سراسر بحث خود درباره کدهای دوری، فرض بر این است که  $q, n$  نسبت به هم اول هستند. به خصوص، اگر  $q=2$  آنگاه  $n$  باید فرد باشد. حال بیایید تعریف کدهای دوری را مرور

کنیم اگر  $L$  یک کد خطی  $q$ -تایی باشد، آنگاه به هر کد کلمه  $C = C_0 C_1$  در  $L$ ، یک چند جمله‌ای از  $F_q[x]$  به صورت زیر را نسبت می‌دهیم.

$$\phi: c_0 c_1 \dots c_{n-1} \rightarrow c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$$

نگاشت  $\phi$  یک یکریختی فضای برداری از  $L$  به زیر فضای  $F_q[x]$  است. به طور معمول، از این نگاشت صرف نظر کرده و کد کلمات در  $L$  را به صورت چند جمله‌ای در نظر می‌گیریم و \*\*\*

تعریف: یک کد خطی  $L \subseteq V(n, q)$  خطی است، اگر:

$$c_0 c_1 \dots c_{n-1} \in L \Rightarrow c_{n-1} c_0 c_1 \dots c_{n-2} \in L$$

در این حالت، اگر کد کلمات را به صورت چند جمله‌ای در نظر بگیریم، کد  $L$  خطی است

$$\text{اگر ایده‌الی از حلقه } R_n = \frac{F_q[x]}{\langle x^n - 1 \rangle} \text{ باشد.}$$

یادآوری می‌کنیم که  $R_n$  مجموعه تمامی چند جمله‌ای‌های روی  $F_q$  با درجه کمتر از  $n$

است جمع و ضرب در  $R_n$ ، مانند جمع و ضرب چند جمله‌ای‌ها در  $F_q[x]$  است، با این

تفاوت که به جای  $x^n$ ، قرار می‌دهیم  $\perp$ ، (یعنی  $x^n = 1$ )، چون تمامی چند جمله‌ای‌ها در

پیمانه  $x^n = 1$  هستند، این نماد را به کار می‌گیریم که  $f(x) \equiv q(x)$  معرف هم‌نهستی در

پیمانه  $x^n = 1$  باشد.

توجه داریم که مطابقت با تعریف، کد خطی  $C$  دوری است اگر تحت شیفت دوری زیر بسته

باشد.



$$c_0 c_1 \dots c_{n-1} \rightarrow c_{n-1} c_0 c_1 \dots v_{n-2}$$

در این حالت، می توان دید که  $C$  تحت جایگشت های دوری نیز پایاست.

$$c_0 c_1 \dots c_{n-1} \rightarrow c_{n-1} c_0 c_1 \dots v_{n-2}$$

اگر  $p(x) \in R_n$ ، آنگاه ایده هال تولید شده توسط  $p(x)$  که با  $\langle p(x) \rangle$  نمایش داده می شود،

کوچکترین ایده ال در  $R_n$  شامل  $p(x)$  است، به عنوان تمرین، می توان دید:

$$\langle p(x) \rangle = \{f(x)p(x) \mid f(x) \in R_n\}$$

جایی که تمامی چند جمله ای هادر پیمان  $x^n - 1$  حساب شده اند.

چند جمله ای 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 ایده ال های اصلی است.

(۱) یک چند جمله ای تکین یکتا با کمترین درجه در  $C$  وجود دارد. این چند جمله ای، کد  $C$

را تولید می کند. یعنی  $C = \langle g(x) \rangle$ ؛  $g(x)$  چند جمله ای مولد نامیده می شود. (توجه داریم

که چند جمله ای مولد یکتانیت، یعنی تنها چند جمله ای نیست که کد  $C$  را تولید می کند.)

$$g(x) \mid x^n - 1 \quad (۲)$$

(۳) اگر  $\deg(g(x)) = r$  آنگاه  $C$  دارای بعد  $n-r$  است. در واقع

$$C = \langle g(x) \rangle = \{r(x)g(x) \mid \deg r(x) < n-r\}$$

(۴) اگر  $g(x) = g_0 + g_1 x + \dots + g_r x^r$  آنگاه  $g_0 \neq 0$ ،  $C$  دارای ماتریس مولد زیر است.

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \dots & g_r & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & g_2 & \dots & g_r & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & g_0 & g_1 & g_2 & \dots & 0 & \dots & g_2 \end{pmatrix}$$

جایی که هر سطر  $G$ ، شیفت دوری سطر قبلی است.

اثبات: (۱) فرض کنید  $C$  شامل دو چند جمله‌ای تکین متمایز  $g_1(x), g_2(x)$  با کمترین درجه  $r$

باشد. آنگاه  $g_1(x) - g_2(x)$  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  $\langle g(x) \rangle \subseteq C$ . از طرف دیگر، فرض کنید

$$p(x) \in C \text{ و قرار دهید، } p(x) = q(x)g(x) + r(x) \text{ جایی که } \deg r(x) < r.$$

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  $p(x) = q(x)g(x) \in \langle g(x) \rangle$ . بنابراین  $C \subseteq \langle g(x) \rangle$  و؛ در نتیجه

$$C = \langle g(x) \rangle.$$

(۳) ایده‌آل تولید شده توسط  $g(x)$  به صورت زیر است.

$$\langle g(x) \rangle = \{f(x)p(x) \mid f(x) \in R_n\}$$

که در پیمانۀ  $x^n - 1$  محاسبه شده است، باید نشان دهیم که کافی است  $f(x)$  را به چند

جمله‌ای‌های 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:

$$f(x)g(x) = q(x)h(x)g(x) + r(x)g(x) = q(x)(x^n - 1) + r(x)g(x)$$

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  $C, \{g(x), xg(x), \dots, x^{n-r-1}g(x)\}$  را تولید می‌کند و

چون این مجموعه، مستقل خطی نیز می‌باشد، یک پایه برای  $C$  است. بنابراین

$$\dim(C) = n - r$$

(۴) اگر  $g_0 = 0$ ، نگاه  $g(x) = xg_1(x)$  جایی که  $\deg(g_1(x)) < r$ . اما در این صورت داریم:

$$g_1(x) = \log_1(x) \equiv x^n \cdot g_1(x) = x^{n-1}g_1(x)$$

جمله‌ای در  $C$  دارای درجه کمتر  $r$  است، در تناقض می‌باشد. بنابراین  $g_0 \neq 0$ . سرانجام،  $G$

یک ماتریس مولد  $C$  است، زیرا  $\{g(x), xg(x), \dots, x^{n-r-1}g(x)\}$  یک پایه برای  $C$  است.

توجه یک کد دوری می‌تواند توسط چند جمله‌ای بجز چند جمله‌ای مولد، تولید شود.

مثال کد دوری  $C = \langle 1+x \rangle$  در  $R_3 = \frac{F_2[x]}{\langle x^3 - 1 \rangle}$  را در نظر بگیرید. با توجه به قضیه قبل

می‌دانیم:  $\dim(C) = 3 - 1 = 2$  و  $C$  شامل کد کلمات زیر است:

$$0, 1+x, x(1+x) = x+x^2, (1+x)(1+x) = 1+x^2$$

$$C = \{0, 1+x, 1+x^2, x+x^2\} = \{00, 11, 10, 01\} \quad \text{بنابراین:}$$

خواننده می‌تواند نشان دهد که:

$$\langle 1+x^2 \rangle = \{f(x)(1+x^2) \mid f(x) \in R_3\} = C$$

و لذا  $C$  توسط چند جمله‌ای  $1+x^2$  نیز تولید شده است.

نکته: در مثال قبل، دیدیم  $C = \langle 1+x \rangle = \langle 1+x^2 \rangle$ . می‌توانیم نماد  $C = \langle\langle p(x) \rangle\rangle$  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  $C = \langle p(x) \rangle$  کد دوری تولید شده توسط  $p(x)$  باشد. اگر  $p(x) \mid x^n - 1$  را

عاد نکنند، 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  $C = \langle p(x) \rangle$  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

$g(x) \in \langle p(x) \rangle$ ، داریم  $g(x) \equiv a(x)p(x)$ ، برای یک  $a(x) \in R_n$ .

حال با ضرب طرفین در  $f(x)$  داریم:

$$g(x)f(x) = a(x)p(x)f(x) \equiv a(x)(x^n - 1) \equiv 0$$

اما  $\deg(g(x)f(x)) < \deg(p(x)f(x)) = n$  و لذا  $g(x)f(x) = 0$  که غیر ممکن است بنابراین

$$p(x) = g(x)$$

نکته: قضیه فوق مبین این مطلب است که نگاشت  $\phi: g(x) \rightarrow \langle\langle g(x) \rangle\rangle$  که هر چند جمله‌ای تکین  $g(x)$ ، که در آن  $x^n - 1 \mid g(x)$ ، را به کد دوری  $\langle\langle g(x) \rangle\rangle$  می‌برد. یک تناظر یک به یک بین مجموعه  $x^n - 1$  و مجموعه  $I_n$  شامل تمامی کدهای دوری در  $R_n$  است. این مطلب نشان می‌دهد که چرا می‌توانیم  $x^n - 1$  را روی یک میدان متناهی تجزیه کنیم.

مثال: از قبل دیدیم که چند جمله‌ای  $x^n - 1$  روی  $F_7$  را می‌تواند به عوامل تحویل ناپذیر به صورت زیر تجزیه کرد:

$$x^9 - 1 = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$$

بنابراین  $2^3 = 8$  کد دوری در  $R_7$  وجود دارد. برای نمونه، کد دوری  $C_1 = \langle\langle x^6 + x^3 + 1 \rangle\rangle$  دارای بعد  $3 = 9 - 6$  و ماتریس مولد زیر است.

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

مثال:  $x^{23} - 1$  روی  $F_7$  را می‌توان به عوامل تحویل ناپذیر به صورت زیر تجزیه کرد:

$$x^{23} - 1 = (x + 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$

نیز، می‌توان نشان داد که کد دوری دوتایی  $C_1 = \langle\langle x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1 \rangle\rangle$

دارای پارامترهای مشابه با کد گلی  $G_{23}$  است. جزئیات آن تقریباً واضح است. بنابراین با توجه به قضیه یکتایی برای کدهای گلی  $G_{23}$  هم ارز با کد دوری  $C_1$  است.

به روش مشابه، روی  $F_3$  داریم:

$$x^{11}-1=(x-1)(x^5+x^4-x^3+x^2-1)(x^5-x^3+x^2-x-1)$$

و کد دو تایی سه تایی  $C_7 = \langle\langle x^5+x^4+x^3+x^2-1 \rangle\rangle$  دارای پارامترهای مشابه با کد گلی  $G_{11}$  است. بنابراین  $G_{11}$  هم ارز با کد دوری  $C_7$  است.

نکته: نگاشت  $\phi: g(x) \rightarrow \langle\langle g(x) \rangle\rangle$  با توجه به ترتیب جزئی روی  $P_n$  و  $I_n$  دارای خواص مشابهی است توجه کنید اگر  $C_7, C_1$  در  $R_n$  دوری باشند، آنگاه مجموع:

$$C_1 + C_7 = \{c_1 + c_7 \mid c_1 \in C_1, C_7 \in C_7\}$$

کوچکترین کد دوری شامل  $C_7, C_1$  در  $R_n$  است. کسانی با اصطلاح شبکه (*lattice*) آشنا باشند، متوجه می شوند که  $\phi$  یک پاد یکرخیختی (*anti-isomorphism*) از شبکه  $(Q_n, 1)$  به شبکه  $(I_n, 1)$  است. اثبات قیه زیر را به عنوان یک تمرین به خواننده واگذاری می کنیم.

قضیه: فرض کنید  $C_1 = \langle\langle g_1(x) \rangle\rangle, C_7 = \langle\langle g_7(x) \rangle\rangle$  کدهای دوری در  $R_n$  باشند. در این صورت.

$$(1) \quad C_1 \subset C_7 \text{ اگر } g_7(x) \mid g_1(x).$$

$$(2) \quad C_1 \cap C_7 = \langle\langle lcm(g_1(x), g_7(x)) \rangle\rangle \text{ (کوچکترین مضرب مشترک } a, b \text{ است)}$$

$$(3) \quad C_1 + C_7 = \langle\langle gcd(g_1(x), g_7(x)) \rangle\rangle$$

چند جمله ای توازن یک کد دوری

از آنجایی که چند جمله‌ای مولد  $g(x)$  از یک کد دوری  $[n, n-r]$  در  $R_n$ ،  $x^n - 1$  را عادی می‌کند، داریم.

$$x^n - 1 = g(x)h(x)$$

جایی که  $h(x)$  یک چند جمله‌ای از درجه  $n-r$  است. چند جمله‌ای توازن (*check*)  $C$  (polynomial) 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:

$$C = \{p(x) \in R_n \mid P(x)h(x) \equiv 0\}$$

(۲) اگر  $h(x) = h_0 + h_1x + \dots + h_{n-r}x^{n-r}$ ، آنگاه یک ماتریس بررسی توازن کد  $C$  به صورت زیر است.

$$H = \begin{pmatrix} h_{n-r} & 0 & h_0 & 0 & 0 & 0 \\ 0 & h_{n-r} & \dots & h_0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ 0 & \dots & 0 & h_{n-r} & \dots & h_0 \end{pmatrix}_{r \times n}$$

(۳) کد دوگان یا  $C^\perp$ ، کد دوری با بعد  $r$  و ماتریس مولد زیر است:

$$h^\perp(x) = h_0^{-1}x^{n-r}h(x^{-1}) = h_0^{-1}(h_0x^{n-r} + h_1x^{n-r-1} + \dots + h_{n-r})$$

جایی که چند جمله‌ای 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

برای  $p(x) = t(x)g(x)$  بنویسیم

$$p(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) \equiv 0$$

از طرف دیگر، اگر  $p(x) \in R_n$ ،  $p(x)h(x) \equiv 0$ ، 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  $c(x) \in C$ ، آنگاه  $c(x)h(x) \equiv 0$  حال  $\deg(C(x)h(x)) < 2n - r$  و با توجه به این مطلب

نتیجه می‌گیری که ضرایب  $x^{n-1}, \dots, x^{n-r+1}, x^{n-r}$  در حاصل ضرب  $C(x)h(x)$  باید صفر

باشد، یعنی.

$$\begin{cases} C_0 h_{n-r} + C_1 h_{n-r-1} + \dots + c_{n-r} h_0 = 0 \\ C_1 h_{n-r} + C_2 h_{n-r-1} + \dots + c_{n-r+1} h_0 = 0 \\ \dots \\ C_{r-1} h_{n-r} + C_r h_{n-r-1} + \dots + c_{n-r} h_0 = 0 \end{cases}$$

اما این معادلات، هم ارز با این است که  $(C_0 C_1 \dots C_{n-1}) H^t = 0$  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 عادی می‌کند، آنگاه  $h^\perp(x)$  چند جمله‌ای مودر کد دوری

$\langle h^\perp(x) \rangle = C^\perp$  خواهد بود که دارای ماتریس مولد  $H$  است؛ بنابراین  $\langle h^\perp(x) \rangle = C^\perp$  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:  $h^\perp(x) | x^n - 1$

مثال کد  $C_1 = \langle x^6 + x^3 + 1 \rangle$  دارای چند جمله‌ای توازن زیر است:

$$h(x) = (x-1)(x^2 + x + 1) = x^3 - 1 \quad (n=9)$$

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 چند جمله‌ای مولد آن به

دست آوریم، معرفی می‌کند.

قضیه 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:

$$x-1 | g(x) \text{ اگر و تنها اگر } c \in \langle g(x) \rangle \subset E_n \quad (1) \quad E_n = \langle x-1 \rangle$$

اثبات برای اثبات قسمت (1) که می‌بینیم که در کد دوری  $\langle x-1 \rangle$

$$h(x) = \frac{x-1}{x-1} = x^{n-1} + x^{n-2} + \dots + 1 = h^\perp(x) \quad \text{داریم:}$$

$$\langle\langle x-1 \rangle\rangle^\perp = \langle\langle x^{n-1} + x^{n-2} + \dots + 1 \rangle\rangle = \{0,1\} \quad \text{و لذا:}$$

$$\langle\langle x-1 \rangle\rangle^{\perp\perp} = \langle\langle x-1 \rangle\rangle^{\perp\perp} = \{0,1\}^\perp = E_n \quad \text{بنابراین:}$$

قسمت (۲) از قسمت (۱) نتیجه می شود و این که اگر  $\langle\langle g_1(x) \rangle\rangle \subseteq \langle\langle g_2(x) \rangle\rangle$  آنگاه

$$g_2(x) | g_1(x)$$

مثال: کد  $C_1 = \langle\langle x^6 + x^3 + 1 \rangle\rangle$ ،  $(n=q)$ ، دارای کد کلات با وزن فرد است. زیرا

$x-1 \nmid x^6 + x^3 + 1$ . اما کد  $C_2 = \langle\langle (x-1)(x^6 + x^3 + 1) \rangle\rangle$ ، زیر کدی از  $C_1$  است ه تنها دارای

کد کلمات با وزن زوج است.

### صفرهای یک کد دوری (The zeros of a cyclic code)

اگر بتوانیم ریشه های چند جمله ای  $x^n - 1$  (یعین ریشه های  $n$ ام واحد) را بیابیم، آنگاه قادر

خواهیم بود تا کدهای دوری در  $R_n$  را مشخص کنیم (با استفاده از معرفی چند جمله ای 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  $\infty$  یک ریشه از  $m_i(x)$  (در میدان گسترش یافته ای از  $F_q$ ) باشد آنگاه  $m_i(x)$  چند

جمله ای کمین  $(m.\text{himal})$ ،  $\infty$  روی  $F_q$  است. بنابراین برای هر چند جمله ای  $f(x) \in F_q[x]$

، داریم  $f(x) = 0$  ارگ و تنها اگر  $f(x) = a(x)m_i(x)$ ، برای یک چند جمله‌ای  $a(x)$  . به

خصوصاً، اگر  $f(x) \in R_n$  آنگاه  $f(x) = 0$  اگر و تنها اگر  $f(x) \in \langle\langle m_i(x) \rangle\rangle$ .

قضیه فرض کنید  $g(x) = q_1(x) \dots q_t(x)$ ، حاصلضرب عوامل تحویل ناپذیر  $x^n - 1$  باشد و

فرض کنید  $\{\alpha_1, \dots, \alpha_u\}$  ریشه‌های  $g(x)$  در میدان شکافنده  $x^n - 1$  روی  $F_q$  باشد.

در این صورت:  $\langle\langle g(x) \rangle\rangle = \{f(x) \in R_n \mid f(x_1)f(x_2) \dots = F(x_u) = 0\}$

علاوه بر این، می‌توانیم تنها یک ریشه از هر عامل تحویل ناپذیر  $g(x)$  را در نظر بگیریم.

یعنی، اگر  $\beta_i$  یک ریشه از  $q_i(x)$  (برای  $1 \leq i \leq t$ ) باشد. آنگاه:

$$\langle\langle g(x) \rangle\rangle = \{v(x) \in R_n \mid f(\beta_1) = \dots = f(\beta_t) = 0\}$$

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  $\{\alpha_1, \dots, \alpha_u\}$  یک مجموعه از ریشه‌های  $x^n - 1$  باشند، آنگاه

چند جمله‌ای .

مولد کد:

$$C = \{f(x) \in R_n \mid f(\alpha_1) = \dots = f(\alpha_u) = 0\}$$

کوچکترین مضرب مشترک چند جمله‌ای‌های مینیمال ریشه‌های  $\alpha_1, \dots, \alpha_u$  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  $\{\alpha_1, \dots, \alpha_u\}$  مجموعه‌ای از ریشه-

های  $x^n - 1$  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  $\sum_1 f_j \alpha_i^j = 0$ . 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  $\alpha_i^j$  را به صورت یک بردار ستونی  $[\alpha_i^j]$  با طول  $d$  روی  $F_q$  در نظر بگیریم. علاوه بر این چون  $f_j \in F_q$  داریم:

$$[f_j \alpha_i^j] = f_j [x_i^j]$$

بنابراین:

$$\sum_i f_j [x_i^j] = [\sum_i f_j \alpha_i^j] = 0$$

و قرار دهیم  $f = (f_0, \dots, f_{n-1}) =$  آنگاه:

$$f(x_i) = (\forall 1 \leq i \leq u) \Leftrightarrow f H^t = 0$$

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 را در نظر می‌گیریم. قضیه: کد همینگ  $H_2(r)$  هم ارز با یک کد دوری است.

اثبات: یادآوری می‌کنیم که کد همینگ دوتایی  $H_2(r)$  دارای پارامترهای  $[2^r - 1, 2^r - 1 - r]$  است و ستون‌های ماتریس بررسی توازن آن، تمامی  $2^r - 1$  بردار دوتایی ناصفر است.

حال فرض کنید  $n = 2^r - 1$  و  $W$  یک ریشه  $n$ ام اولیه واحد روی  $F_r$  باشد. چون  $o_n(2) = r$ ، سپس میدان شکافنده  $x^n - 1$  برابر با  $F_{2^r}$  است و چون  $W$  دارای مرتبه  $n = 2^r - 1$  است، پس  $W$  یک عضو اولیه میدان  $F_{2^r}$  می باشد. در نتیجه، توان های  $W$ ، تمامی عناصر ناصفر میدان  $F_{2^r}$  و در نتیجه ستون های ماتریس  $H$  را تشکیل می دهند. پس:

$$H = [[w^0], [w^1], \dots, [w^{n-1}]]$$

شامل تمامی بردارهای دو تایی ناصفر به طول  $r$  است. این مطلب، نشان می دهد که کد همینگ  $H_2(r)$  با این ماتریس بررسی توازن یک کد دوری است که تنها صفرهای آن، یک ریشه اولیه واحد  $W$  است (ریشه  $x^{2^r} - 1$  است) و تمامی صفرهای دیگر آن، ریشه های چند جمله ای مینیمال  $W$  هستند.

مثال: کد همینگ  $H_2(r)$  را در نظر بگیرید. در این حالت،  $n = 2^4 - 1 = 15$  و میدان شکافنده  $x^n - 1$  برابر با  $F_{16}$  است. اگر  $\beta$  یک عضو اولیه از  $F_{16}$  باشد، آنگاه  $\beta$  همچنین ۱۵ امین ریشه اولیه واحد نیز هست. مزدوج های  $\beta$  به صورت زیر می باشند.

$$\beta, \beta^2, \beta^4, \beta^8$$

چون  $\beta^{16} = \beta$ . بنابراین، چند جمله ای مینیمال  $\beta$  به صورت زیر است.

$$(x - \beta)(x - \beta^2)(x - \beta^4)(x - \beta^8)$$

که با در نظر گرفتن چند جمله ای اولیه  $x^4 + x + 1$  (یعنی  $f_4(x) = \frac{F_4[x]}{\langle x^4 + x + 1 \rangle}$ ) برای  $F_{16}$ ،

$H_2(4)$  کد دوری تولید شده توسط  $f(x) = x^4 + x + 1$  در  $(R_{16})$  خواهد بود.

برای حالت غیر دودویی نیز می توان 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 همینگ  $-q$ -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 که می توانند از تجزیه  $x^n - 1$  به عوامل تحویل ناپذیر روی  $F_q$  به دست آیند، مشاهده کردیم. اما، تجزیه  $x^n + 1$  کار ساده ای نیست. یک روش برای انجام این کار، این است که در ابتدا یک ریشه  $n$ ام واحد را به دست آوریم که برای این کار، باید با میدان شکافنده  $F_{q^s}$  از  $x^n - 1$  کار کنیم. در اینجا، روش دیگری برای توصیف کدهای دوری به دست می آوریم که به جای چند جمله ای مولد (*generator polynomial*) با نوع دیگری از چند جمله ای های تولید کننده (*generationg polynomial*) کار می کنیم.

تعریف یک چند جمله ای  $e(x) \in R_n$ ، خود توان (*idempotent*) در  $R_n$  نامیده می شود اگر

$$e^2(x) \equiv e(x).$$

مثال چند جمله ای  $x^3 + x^5 + x^6$  در  $R_n$  باشد (با چند جمله ای مولد  $g(x)$  و چند جمله ای توازن  $h(x)$ ).

در میان صورت  $g(x)$  و  $h(x)$  نسبت به هم اول بوده و لذا چند جمله‌ای های  $b(x), a(x)$  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  $C = \langle e(x) \rangle$ .

اثبات: اگر  $e_1, e_2$  هر دو در  $C$  یکه باشند آنگاه  $e_1(x)e_2(x) \equiv e_1(x) \equiv e_2(x)$ ، بنابراین

$e_1(x) = e_2(x)$  پس اگر یک یک وجود داشته باشد آنگاه یکتاست چون  $g(x)h(x) = x^n - 1$

دارای هیچ ریشه تکراری در هر میدان گسترش یافته نیست،  $g(x), h(x)$  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 عضویکه در  $C$  می‌باشند و لذا  $e(x)$ ،  $C$  را تولید می‌کند

زیرا هر چند جمله در  $C$  یک م ضرب  $e(x)$  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 می کند می بایست برابر با  $e(x)$  چون  $f(x)$ ،  $C$  را تولید می کند، لذا  $q(x) \in R_n$  وجود دارد که در آن  $e(x) \equiv q(x)f(x)$  بنا بر این.

که در نتیجه  $f(x) = e(x)$  و اثبات کامل می شود.

تذکر به چند جمله ای  $e(x)$  در قضیه بالا، خود توان تولید کننده ( *generating* )  $C$  (*idempotent*) گفته می شود، و می نویسیم  $C = [e(x)]$ . همچنین در قضیه فوق، با استفاده از الگوریتم اقلیدسی، می توانیم  $e(x)$  را از  $g(x)$  به دست آوریم. قضیه بعد، نحوه این کار را تشریح می کند:

قضیه: چند جمله ای مولد که  $[e(x)]$  به صورت زیر است:

$$g(x) = \gcd(e(x), x^n - 1)$$

اثبات: می دانیم  $x^n - 1 = g(x)h(x)$  و نیز  $e(x) = a(x)g(x)$ . لذا داریم:

$$\gcd(e(x), x^n - 1) = \gcd(a(x)g(x), h(x)g(x)) = g(x)$$

زیرا  $a(x)$  و  $h(x)$ ، نسبت به هم اول هستند

قضیه فرض کنید  $C_1 = [[e_1(x)]]$ ،  $C_2 = [[e_2(x)]]$ ، کدهای دوری در  $R_n$  باشند.

در این صورت: (۱) اگر و تنها اگر  $C_1 \subset C_2$  اگر  $e_1(x)e_2(x) \equiv e_1(x)$

$$C_1 \cap C_2 = [[e_1(x)e_2(x)]] \quad (۲)$$



$$C_1 + C_2 = [[e_1(x) + e_2(x) - e_1(x)e_2(x)]] \quad (3)$$

که در آن تمامی چند جمله‌ای‌ها در پیمانه  $x^n - 1$  بدست آمده‌اند.

تذکره: قضیه زیر یک رابطه جالب بین چند جمله‌ای مولد و خودتوان تولیدکننده یک کد دوری مطرح می‌کند.

قضیه: فرض کنید  $C$  یک کد دوری در  $R_n$  با چند جمله‌ای مولد  $g(x)$  و خودتوان تولیدکننده  $g(x)$  باشد. در این صورت  $e(x), g(x)$  دقیقاً دارای ریشه‌های یکسانی در میدان شکافته  $x^n - 1$ ، در میان ریشه‌های  $n$ ام واحد، هستند.

علاوه بر این اگر  $f(x)$  در  $R_n$  خودتوان باشد و در میان ریشه‌های  $n$ ام واحد، دارای ریشه-

های یکسانی با  $g(x)$  باشد، آنگاه  $f(x)$  خودتوان تولیدکننده  $\langle\langle g(x) \rangle\rangle$  خواهد بود.

اثبات: فرض کنید  $w$  یک ریشه  $n$ ام اولیه واحد باشد. چون  $e(x) \equiv a(x)g(x)$ ، در نتیجه

$g(w^i) = 0$  ایجاب می‌کند  $e(w^i) = 0$  و تنها اگر  $h(w^i) \neq 0$ ، بنابراین  $e(w^i) = 0$  ایجاب می‌کند

کند  $h(w^i) \neq 0$  که در نتیجه  $g(w^i) = 0$ . 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  $n$ ام 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:

$$\gcd(f(x), x^n - 1) = \gcd(f(x), h(x)g(x)) = g(x)$$

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 چند جمله‌ای توازن  $h(x)$  باشد. ر این

صورت کد دوری  $\langle\langle h(x) \rangle\rangle$  دارای خود توان تولید کننده  $1-e(x)$  است و

$C^\perp = \langle\langle h^\perp(x) \rangle\rangle$  دارای خود توان تولید کننده  $(1-e(x^{n-1})) \bmod (x^n - 1)$  می‌باشد.

اثبات: چون  $h(x)(1-e(x)) \equiv h(x)(1-a(x)g(x)) \equiv h(x)$

می‌بینیم که  $1-e(x)$  در  $\langle\langle h(x) \rangle\rangle$  یکه است به طور مشابه چون:

$$h^\perp(x) = h_0^{-1} x^k h(x-1) \equiv h^\perp(x) - h_0^{-1} x^k h x^{n-1} e(x^{n-1}) \equiv$$

$$h^\perp(x) - h_0^{-1} x^k h(x^{n-1}) a(a^{n-1}) g(z^{n-1}) \equiv h^\perp(x)$$

بنابراین  $(1-e(x^{n-1})) \bmod (x^n - 1)$  در  $C^\perp = \langle\langle h^\perp(x) \rangle\rangle$  یکه است.

## یافتن خود توان های تولید کننده

حال به دنبال جواب این سوال هستیم که بدون داشتن تجزیه  $x^n - 1$ ، چگونه می‌توانیم خود

توان‌ها را بیابیم. در اینجا، توجه خود را روی حالت  $q=2$  معطوف می‌کنیم.

در  $F_7[x]$ ، داریم  $f(x^2) = f^2(x)$  و لذا یک چند جمله‌ای  $e(x) = e_0 + e_1x + \dots + e_{n-1}x^{n-1}$  در  $R_n$  خود توان است اگر و تنها اگر  $e(x^2) \equiv e(x)$ . اما این رابطه در  $R_n$  برقرار است اگر و تنها اگر زمانی که  $e_i \neq 0$  داشته باشیم  $e_{2i \pmod n} \neq 0$ ، در نتیجه  $e(x)$  می‌بایست مجموعه چندجمله‌ای‌هایی به صورت زیر باشد:

$$x^i + x^{2i} + \dots + x^{2^{d-1}i}$$

جایی که توان‌ها، تشکیل یک هم دسته‌ی دوری می‌دهند. لذا قضیه زیر را اثبات کرده‌ایم.

قضیه: فرض کنید  $q = 2$ ، خود توانهای موجود در  $R_n$  دقیقاً مجموع چند جمله‌ای‌های به صورت  $x^i + x^{2i} + \dots + x^{2^{d-1}i}$  هستند، جایی که  $C_i = \{i, 2i, \dots, 2^{d-1}i\}$  یک هم دسته‌ی دوری برای  $2$  پیمانه  $n$  می‌باشد.

مثال: فرض کنید  $n = q$ . هم دسته‌های دوری برای  $2$  پیمانه  $q$  به صورت زیر می‌باشند،

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 7, 5\}, C_3 = \{3, 6\}$$

و لذا  $2^3 = 8$  خود توان به صورت زیر وجود دارند.

$$\begin{aligned} e_0(x) &= x^0 = 1 & e_1(x) &= 0 \\ e_2(x) &= x^2 + x^4 & e_3(x) &= x + x^2 + x^4 + x^5 + x^7 + x^8 \\ e_4(x) &= e_2(x) + e_3(x) & e_5(x) &= e_2(x) + e_3(x) \\ e_8(x) &= e_4(x) + e_3(x) & e_7(x) &= e_3(x) + e_4(x) \end{aligned}$$

چند جمله‌ای های مولد متناظر نیز با استفاده از قضایای قبل، قابل حصول هستند. برای نمونه،

$$q_3(x) = (\gcd(e_3(x), x^3 - 1) = x + 1) \text{ داریم:}$$

## BCH کدهای

کران BCH: ابتدا بر مطالب قبل یک مرز مختصر می‌کنیم. از قبیل می‌دانیم که یک کد

دوری توسط صفرهای آن تعریف می‌شود. به خصوص، اگر  $\alpha_1, \dots, \alpha_u$  ریشه‌های

$$C = \{p(x) \in R_n \mid p(\alpha_1) = \dots = p(\alpha_u) = 0\}$$
 نام واحد در  $F_q$  باشد، آنگاه

یک کد دوری است که چند جمله‌ای مولد  $g(x)$ ، حاصل ضرب چند جمله‌ای های مینیمال

$\alpha_1, \dots, \alpha_u$  روی  $F_q$  است. این رویکرد، این مطلب را پیشنهاد می‌ند که ما می‌توانیم برخی

کدهای جالب را با تخصیص مجموعه ریشه‌های  $n$  نام واحد به عنوان صفرهای  $g(x)$  بیابیم.

یادآوری می‌کنیم که اگر  $x^n - 1 = \prod_i m_i(x)$ ، تجزیه  $x^n - 1$  به عوامل تحویل ناپذیر روی

$F_q$  باشد، آنگاه ریشه‌های چند جمله‌ای  $m_i(x)$  مزدوج هستند، یعنی این ریشه‌ها به صورت

$\{w^i, w^{iq}, \dots, w^{iq^{d-1}}\}$  هستند، جایی که  $d$  کوچک ترین عدد صحیح مثبت است به طوری که

$$i \cdot d \equiv 1 \pmod{n} \text{ نیز، یادآوری می‌کنیم که مجموعه.}$$

$$m_i(x) = \{i, a_i, \dots, a^{d-1}i\}$$

$I$  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  $n$ ام 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.

$$w^b, w^{b+1}, \dots, w^{b+\delta-2} \quad (b \geq 0)$$

در این صورت،  $C$  دارای کمترین فاصله حداقل  $\delta$  خواهد بود.

نکته این قضیه، این مطلب را به ما می‌گوید که ما می‌توانیم یک کد با کمترین، فاصله حداقل  $\delta$  را با تخصیص چند جمله‌ای 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:  $w^b, w^{b+r}, \dots, w^{b+(\delta-2)r}$  در میان 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  $\delta$  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 دسته‌ها بسیار مهم هستند. برای نمونه، این کدها دارای قدرت تصحیح خطای خوبی هستند، جایی که طول آنها زیاد بزرگ 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  $n$ ام واحد روی  $F_q$  باشد و  $q(x)$  چند جمله‌ای تکین روی  $F_q$  با کمترین درجه باشد به طوری که  $\delta - 1$  مقادیر زیر:

$$w^b, w^{b+1}, \dots, w^{b+s-2}$$

در میان صفرهای  $g(x)$  باشند، جایی که  $\delta \geq 1, b \geq 0$  بنابراین:

$$g(x) = \text{lcm}\{m_b(x), m_{b+1}(x), \dots, m_{b+s-2}(x)\}$$

که دوری  $-q$  تایی  $B_q(n, \delta, w, b)$  با طول  $n$  و چند جمله‌ای مولد  $g(x)$ ، یک کد BCH با فاصله مطرح (designed dist)  $\delta$  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.

آنگاه  $B_a(n, \delta, w, b)$  یک کد  $BCH$  اولیه نامیده می‌شود.

نکته: کدهای  $BCH$  بامعنی باریک، تعمیمی از کدهای همینگ هستند. به خصوص، قبلاً مشاهده کردیم. تعریف شوند که در آن  $g(x)$  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 باری فاصله مطرح آن (یعنی  $\delta$ ) است. علاوه بر این، 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

$$\dim(B_q(n, \delta, w, b)) = n - \deg(g(x)) \geq n - s(s-1) \quad \text{و} \quad \deg(m_{b+i}(x)) \leq s$$

بنابراین:

قضیه کد  $BCH$ ،  $q$ -تایی  $B_a(n, \delta, w, b)$  با طول  $n$  و فاصله مطرح  $\delta$  دارای پارامترهای

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:

$$B_q(n, \delta, w, b) = \{p(x) \in R_n \mid p(w^b) = p(w^{b+1}) = \dots = p(w^{b+s-2}) = 0\}$$

و لذا اگر  $[w^i]$  معرف بردار ستونی  $w^i \in F_a^s$  در میدان شکافنده  $F_q^s$  از  $x^n - 1$  باشد،

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 می دهند و همین که سطرهای وابسته

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) باشد، آنگاه  $u \in C_k$

اگر و تنها اگر  $u \in c_k \pmod{n}$ . بنابراین  $M_i(x) = m_{\gamma_i}(x)$ . این مطلب، ایجاب می کند که

چند جمله ای های:

$$g_1(x) = lcm\{m_1(x)m_{\gamma}(x), \dots, m_{\gamma E}(x)\}$$

$$g_2(x) = lcm\{m_1(x)m_{\gamma}(x), \dots, m_{\gamma E-1}(x)\}$$

$$g_3(x) = lcm\{m_1(x)m_{\gamma}(x), \dots, m_{\gamma E-1}(x)\}$$

یکی باشند. توجه دارید که مجموعه چند جمله ای های آخر  $m_i(x)$  تنها دارای اندیس های

فرد هستند).

چون  $g_2(x) = g_1(x)$ ، داریم:  $B_{\gamma}(n, 24+1, w) = B_{\gamma}(n, 24, w)$



بنابراین می‌توانیم توجه خود را معطوف کدهای  $BCH$  با معنی باریک با طول  $n$  و فاصله مطرح  $\delta = 24 + 1$  کنیم در این حالت بعد حداقل  $n - 4o_n(2)$  است، جایی که  $o_n(2)$  مرتبه ۲ در پیمانه  $n$  است به بیان دیگر:

$$\dim(b_r(n, 24+1, w)) \geq n - 4o_n(2)$$

مثال: فرض کنید  $q = 2$ ،  $q = 2$ ،  $n = 2^5 - 1 = 31$ ، برای تعیین کدهای  $BCH$  با معنای باریک (اولیه)  $B_r(31, \delta, w)$  با فاصله‌های مطرح متفاوت ابتدا هم دسته‌های دوری را محاسبه می‌کنیم.

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 16\}, C_3 = \{3, 6, 12, 24, 17\}, C_5 = \{5, 10, 20, 9, 18\}$$

$$C_7 = \{7, 14, 28, 25, 19\}, C_{11} = \{11, 22, 13, 26, 21\}, C_{15} = \{15, 30, 29, 27, 23\}$$

چند جمله‌ای مولد کد  $BCH$  با معنای باریک  $B_r(31, 9, w)$  با فاصله مطرح  $\delta = 9$ ، برای نمونه به صورت زیر است:

$$g(x) = \text{lcm}\{m_1(x), \dots, m_\lambda(x)\} = m_1(x)m_5(x)m_7(x)$$

بنابراین، بعد  $B_r(31, 9, w)$  برابر با  $31 - 20 = 11$  است.

توجه دارید که این کران پایین، با کران  $BCH$  مطابقت دارد.

نیز توجه دارید که چون  $9 \in C_5$ ، داریم  $x_9(x) = m_5$  و لذا:

$$B_r(31, 11, w) = B_r(31, 9, w)$$

بنابراین، در این حالت، کران پائین  $BCH$  برابر با  $6 = 31 - 25$  است که به طور اکید از بعد واقعی کمتر است. جدول زیر، شامل لیست کاملی از تمام کدهای  $BCH$  دوتایی به معنای باریک با طول ۳۱ است. در این جدول، نماد زیر قرار داد کرده ایم.

$$m_{i_1, i_2, \dots, i_k}(x) = m_{i_1}(x) \dots m_{i_k}(x)$$

فاصله مطرح	چند جمله‌ای	بعد	فاصله
۱	۱	۳۱	۱
۳	$m_1(x)$	۲۶	۳
۵	$m_{1,3}(x)$	۲۱	۵
۷	$m_{1,3,5}(x)$	۱۶	۷
۹ یا ۱۱	$m_{1,3,5,7}(x)$	۱۱	۱۱
۱۳ یا ۱۵	$m_{1,3,5,7,9}(x)$	۶	۱۵
۱۹, ۱۷, ..., ۳۱	$x^{31} - 1$	۱	۳۱

نکته: مثال قبل، نشان می‌دهد که یک کد  $BCH$  با فاصله مطرح فرد  $\delta$  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  $\delta$  که در آن  $B$  یک کد  $BCH$  با حاصله مطرح  $\delta$  باشد، یک فاصله بوز (Bose) از کت نامیده می‌شود.

**مثال:** فرض کنید  $q = 2, n = 23$ . چون  $s = o_{23}(2) = 11$ ، لذا میدان شکافنده  $23 - 1$ ، برابر با  $F_{211}$  است. هم دسته‌های دوری ۲ در پیمانه ۲۳ به صورت زیر هستند.

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\},$$

$$C_5 = \{5, 10, 20, 17, 11, 22, 21, 19, 15, 7, 14\}$$

لذا کد BCH با معنای باریک  $B_r(23, 5, w)$  با فاصله مطرح  $\delta = 5$  دارای ماتریس مولد:

$$g(x) = lcm\{m_1(x), m_2(x), m_3(x)\} = m_1(x)$$

است به خصوص،  $B_r(23, 5, w)$  یک کد  $[23, 12]$  - دودویی است. به آسانی می‌توان دید که  $B_r(23, 5, w)$  هم ارز با کد گلی  $G_{23}$  با کمترین فاصله 7 است بنابراین، در این حالت، کمترین فاصله واقعی کد بزرگتر از فاصله مطرح آن است.

### کد رید-سولومن (Reed-Soloman)

در اینجا، دسته خاصی از کدهای BCH، معروف به کدهای رید-سولومن را معرفی می‌کنیم.

این، کدها، در عمل به ندرت مورد استفاده قرار می‌گیرند. در واقع، به کارگیری این کدها، در ترکیب با کدهای غیر بلوکی، روش استاندارد در NASA، از زمان پرواز فضاپیمای ویاگر در سال 1977، بوده است. نی 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  $a \geq 3$ . یک کد رید-سولومن (RS)  $R = R(n, \delta, w, b)$  یک کد BCH و  $q$ -تایی،  $B_q(q-1, \delta, w, b)$  با طول  $n = q-1$  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 چند جمله‌ای  $x^{q-1} - 1$ ، دقیقاً، عناصر ناصفر  $F_q$  هستند.

$$\text{لذا داریم: } x^n - 1 = x^{q-1} - 1 = \prod_{\alpha \in F_q} (x - \alpha)$$

بنابراین، اگر  $w$  یک  $(q-1)$ امین ریشه اولیه واحد روی  $F_q$  باشد (یعنی یک عضو اوریه  $F_q$ ) در این صورت،  $m_i(x) = x - w^i$ . نتیجه، یک کد رید-سولومن با فاصله مطرح  $\delta$  دارای ماتریس مولد است.

$$g(x) = (x - w^b)(x - w^{b+1}) \dots (x - w^{b+s-1}) \quad (b \geq 0)$$

**مثال:** فرض کنید  $q = 8$  و لذا  $n = 7$ . یک ریشه  $w$  از چند جمله‌ای اولیه  $x^3 + x + 1$  روی

$F_8$ ، یک عوض اولیه  $F_8$  را به ما می‌دهد. برای به دست آوردن یککد RS با بعد 5، می-

خواهیم  $\deg(g(x)) = 7 - 5 = 2$  در این حالت، داریم:

$$g(x) = (x - w)(x - w^2) = x^2 - (w + w^2)x + w^3 = x^2 + w^6x + w^3$$

### خواص کدهای رید-سولومن

#### ۱- کدهای رید سولومن، MDS هستند.

ماتریس مولد یک کد رید-سولومن با فاصله مطرح  $\delta - 1$   $\deg(g(x)) = \delta - 1$  است.

$$\text{لذا: } k = \dim(R(n, \delta, w, b)) = n - \deg(g(x)) = n - \delta + 1$$

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 بر این، کمترین فاصله یک کد رید-سولومن برابر با کمترین فاصله آن است.

لذا، کدهای  $RS$  دارای بیشترین فاصله ممکن در میان تمامی کدهای  $q$ -تایی با طول  $n$ ،  $n=q$  و بعد  $k = n - \delta + 1$  هستند.

## ۲- دوگانگی یک کد رید سولومن:

در حالت کلی دوگان یک کد  $BCH$  ممکن است یک کد  $BCH$  دیگر نشود. برای نمونه، فرض کنید  $n=25, q=2$ . هم دسته های دوری  $q$  در پیمانه  $n$  به صورت زیر هستند.

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 16, 7, 14, 3, 6, 12, 24, 23, 21, 17, 9, 11, 18, 13, 22, 19, 15\}$$

$$C_5 = \{5, 10, 20, 15\}$$

فرض کنید  $B = B_r(25, 1, w)$ ، کد  $BCH$  با یک صفر تعریف شده  $w$  باشد، کد دوگان  $B^\perp$  دارای صفرهایی یکسان با عناصر متقابل (reciprcals) عناصر ناصفر  $B$  است و لذا  $B^\perp$  دارای صفرهای زیر است.

$$\{w^0, w^{-5}, w^{-10}, w^{-20}, w^{-15}\} = \{w^0, w^{20}, w^{15}, w^5, w^{10}\}$$

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  $C$  یک  $(n, m, d)$  - کد  $q$ -تایی باشد،

آنگاه کد گسترش یافته  $\hat{C}$  با اضافه کردن یک بیت توازن کلی  $C_n$  به هر کد کلمه،

$$\sum_{k=0}^n C_k = 0 \quad \text{حاصل می‌شود.} \quad C = C_0 \dots C_{n-1}$$

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

$$\hat{n} = n + 1, \hat{M} = m, \hat{d} = d + 1$$

از طرف دیگر، در مودر کدهای رید-سولومن، کمترین فاصله کد گسترش یافته از کمترین فاصله کد اصلی.

قضیه فرض کنید  $C$  یک کد رید سولومن  $[n, k, d]$  با چند جمله‌ای مولد زیر باشد.

$$g(x) = (x-w)(x-w^2) \dots (x-w^{d-1})$$

در این صورت، کد گسترش یافته  $\hat{C}$ ، یک  $[n+1, k, d+1]$  - کد است.

اثبات: فرض کنید  $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$  یک کد کلمه در  $C$  با وزن  $d$  باشد. با

گسترش  $c(x)$  داریم  $\hat{C}(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1} + c_nx^n$  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 که

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،  $g(1) \neq 0$ ، آنگاه چند

جمله‌ای  $g_1(x) = (x-1)g(x)$  را عادی می‌کند. بنابراین،  $C(x)$  در کد دوری تولید شده

توسط  $g_1(x) = (x-1)(x-w)(x-w^2)\dots(x-w^{d-1})$  که شامل  $d$  صفر متوالی،  $w^0, \dots, w^{d-1}$  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  $\{\alpha_1, \dots, \alpha_m\}$  یک پایه مرتب برای  $f_2^m$  روی  $F_2$  باشد. برای هر عضو  $F_2^m$  مانند  $a$ ، داریم:  $a = a_1 \alpha_1 + \dots + a_m \alpha_m$  و لذا می‌توان به  $a$  رشته  $a_1 \dots a_m$  را نسبت داد. این تخصیص را می‌توان به صورت:

$$a \rightarrow C_{i_1} \dots C_{i_m}$$

آنگاه، می‌توان به هر  $C \in C$ ، رشته  $(C_{11} \dots C_{1m})(C_{21} \dots C_{2m}) \dots (C_{m1} \dots C_{mm})$  با طول  $mn$  را نسبت داد. (پرانتزها، تنها به منظور سادگی در خواندن گذاشته شده اند) کد  $C \rightarrow$  شامل چنین رشته‌هایی، یک کد دوتایی با طول  $mn$  خواهد بود.

علاوه بر این،  $C \rightarrow$  یک فضای برداری روی  $F_2$  با اندازه  $|C| = (2^m)^k = 2^{mk}$  است. بنابراین،  $C \rightarrow$  روی  $F_2$  دارای بعد  $mk$  است. سرانجام اگر  $a \neq b$  و

$$a \rightarrow a_1 \dots a_m, \quad b \rightarrow b_1 \dots b_m$$

آنگاه، برای حداقل یک  $i$ ، داریم  $a_i \neq b_i$  و لذا کمترین، فاصله  $C \rightarrow$ ، 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  $\{\infty_1, \dots, \infty_m\}$  یک پایه مرتب برای  $F_{2^m}$  روی  $F_2$  باشد. که  $C \rightarrow$ ، تولید شده به وسیله جایگذاری هر سمبل  $a = \sum a_i \infty_i$  در هر کد کلمه از  $C$  با رشته  $m$ -تایی متناظر با آن  $a_i, \dots, a_m$ ، یک  $[n \rightarrow, k \rightarrow, d \rightarrow]$ -کد دوتایی است، جایی که:

$$n \rightarrow = mn, k \rightarrow = mk, d \rightarrow \geq d$$

علاوه بر این علاوه بر جایگذاری هر جایگذاری هر سمبل کد کلمه در  $C$  با رشته  $m$  تایی متناظر با آن، می توانیم یک سمبل بررسی توازن به هر کد کلمه از این رشته  $m$  تایی به صورت زیر اضافه کنیم:

$$C \rightarrow (C_{11}, \dots, C_{1m} s_1) (c_{21}, \dots, c_{2m} x_2) \dots (c_{n1}, \dots, c_{nm} x_n)$$

جایی که  $C_{i1} + \dots + C_{im} + x_i = 0$  (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  $d \uparrow \geq 2d$ ، می بینیم که حداقل  $d$  تا از ریشه های  $m$  تایی اصلی

در هر کد کلمه از  $C \rightarrow$  باید ناصفر باشند. اما اگر یکی از این رشته ها دارای وزن ۱ باشد.

آنگاه اضافه نمودن یک بیست توازن، وزن «را به ۲ افزایش می دهند. 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  $2d$  است. توه 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  $m$  های به اندازه کافی بزرگ، نسبت به نرخ اصلی  $C$ ، زیاد کوچک نیست. از طرف دیگر کمترین فاصله کد جدید، حداقل دوبار از کمترین فاصله  $C$  بیشتر است. بنابراین، با به کارگیری یک روش نسبتاً ساده، می توانیم 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  $C^\uparrow$  لزوماً دوری نیستند. همچنین کمترین فاصله کد  $C^\rightarrow$  می تواند به انتخاب پایه های  $F_m$  روی  $F_2$  وابسته باشد.

مثال فرض کنید  $k=2, n=3, q=4$ ، چند جمله ای  $x^2+x+1$ ، یک چند جمله ای اولیه برای  $F_4$  روی  $F_2$  است. بنابراین، اگر  $w$  یک ریشه از این چند جمله ای باشد، آنگاه داریم

$$F_4 = \{0, 1, w, w^2\}$$

یک کد  $[3, 2, 2]$  - رید سولومن 4 تایی  $C$  دارای چند جمله ای مولد با درجه 1 است.

بیاید، فرض کنیم  $g(x) = x - w$ . در این صورت، کد  $C$  به صورت زی راست.

$$C = \{p(x)(x-w) \mid \deg(p(x)) \leq 1\}$$

برای نمونه، کی کد کلمه در  $C$  به صورت  $x^2 - w^2 = (x+w)(x-w)$  است که به صورت رشته  $w^2 0 1$  می توان آن را نشان داد. می توان دید که تمامی 16 کد کلمه موجود در  $C$  به صورت رشته های زیر هستند.

$$\begin{aligned} & 000, w10, w^2w0, 1w^20 \\ & 0w1, 0w^2w, 01w^2, ww^21 \\ & w^201, 111, www, w^21w \\ & 10w, www^2, w^2w^2w^2, 1ww^2 \end{aligned}$$

که در آن  $\{1, n\}$  یک پایه مرتب برای  $F_4$  روی  $F_2$  است. تحت این پایه، داریم و لذا کد

$[6, 4]$  دوتایی  $C \rightarrow$  به صورت زیر می باشد.

000000, 011000, 110100, 101100  
 000110, 001101, 001011, 011100  
 110010, 101010, 010101, 111101  
 100001, 010111, 111111, 100111

به طریق مشابه، می توان کد  $C^\wedge$  را مشخص کرد.

### تصحیح خطای گروهی (Burst error Correction)

کد دوتایی گسترش یافته  $C \rightarrow$  می تواند خواص تصحیح خطای گروهی بسیار خوبی داشته باشد اگر کد اصلی  $C$ ، تصحیح کننده  $t$  خطا باشد، آنگاه کد گسترش یافته  $C \rightarrow$  می تواند خطاهای گروهی با طول حداکثر  $b = (t-1)m + 1$  را تصحیح کند. زیرا هر خطای گروهی با طول  $b$  بیت یا کمتر می تواند حداکثر روی  $t$  رشته به طول  $m$ ، تأثیر بگذارد.

\*\*\*

مثال: فرض کنید می خواهیم یک کد دوتایی، بر پایه یک کد رید سولومن، بیابیم که بتواند خطاهای گروهی با طول  $b=13$  یا کمتر را تصحیح کند. در این صورت می خواهیم:

$$(T+1)m+1=13 \Rightarrow (t-1)m=12$$

حال اگر فرض کنیم  $d=2t+1$  (کمترین فاصله فرد باشد)، آنگاه رابطه فوق معادل با رابطه زیر است:  $(d-3)m=24$ .

حال، چون  $d \leq n = 2^m - 1$ ، می توانیم  $m=4$  و  $d=9$  را اختیار کنیم.

در این حالت، کد رید-سولومن  $C$  دارای پارامترهای  $[15, 7, 9]$  خواهد بود (روی  $F_6$ ).

کد دوتایی گسترش یافته  $C \rightarrow$  نیز دارای پارامترهای  $[n, k, d]$  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  $n = q - 1$ . فرض کنید.

$$a(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{یک رشته پیام است، قرار می‌دهیم:}$$

و پیام  $a(x)$  را به چند جمله‌ای  $C(x) = \sum_{j=0}^{n-1} a(w^j) x^j$  کد می‌کنیم. البته باید نشاندهیم

$C(x)$  یک کد کلمه در  $C$  است، یا به عبارت دیگر باید نشان دهیم:  $C(w) = \dots C(w^{d-1})$

برای این منظور، فرض می‌کنیم  $a(x) = \sum_{i=0}^{n-1} a_i x^i$ ، که در آن به ضرایب اضافی  $a_i$  ( $i \geq k$ )

برابر با صفر در  $n$  گرفته شده‌اند، در نتیجه داریم:

$$a_j = \frac{1}{n} \sum_{i=0}^{n-1} a(w^i) w^{-ij} = \frac{1}{n} C(w^{-1}) = \frac{1}{n} C(w^{n-i})$$

و لذا  $C(w^{n-i}) = n a_j$  به خصوص برای  $j \leq d-1 = n-k$ ، داریم:

$$C(w^j) = n a_{n-j} = 0 \quad (a_{n-j} = 0 \text{ و لذا } n-j \geq k)$$

که نشان می‌دهیم  $C(x)$  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 کد گشایی سولومن

بر پایه منطق اکثریت می‌آوریم. متأسفانه، این روش، زمانی که  $[n, k, d]$ -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  $a = a_0 a_1 \dots a_{k-1}$  و کد کلمه  $C$  را به صورت:

$$C = C_0 C_1 \dots C_{n-1} = a(1) a(w) \dots a(w^{n-1})$$

در نظر گرفت، حال فرض کنید  $u = u_0 u_1 \dots u_{n-1}$  کلمه دریافتی و  $e = e_0 \dots e_{n-1}$  بردار خطا

باشد. در این صورت،  $u_i = e_i + c_i = e_i + a(w^i)$ ، و داریم.

$$u_0 = e_0 + a_0 + a_1 + \dots + a_{k-1}$$

$$u_1 = e_1 + a_0 + w a_1 + \dots + w^{k-1} a_{k-1}$$

$$u_2 = e_2 + a_0 + w^2 a_1 + \dots + w^{2(k-1)} a_{k-1}$$

$$e_{n-1} = e_{n-1} + a_0 + w^{n-1} a_1 + \dots + w^{(k-1)(n-1)} a_{k-1}$$

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  $a_0, \dots, a_{k-1}$  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. بیاید معادلاتی را که در آن  $e_i \neq 0$  به معادلات

بدو معادلاتی را که  $e_i = 0$ ، به معادلات خوب تعبیر کنیم. بنابراین،  $t$  معادله بدو  $n-t$

معادله وب داریم. اگر ماتریس  $k$  معادله ها از  $\binom{n}{k}$  زیر دستگاه از معادلات فوق را شامل

تمامی معادلات خوب را حل کنیم، آنگاه می‌توانیم  $a_i$  های 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 می تواند حداکثر در  $t+k-1$  معادله صدق کند. یعنی حداکثر در

$$\binom{t+k-1}{k} \text{ زیر دستگاه از دستگاه فوق، بنابراین، اگر } \binom{n-1}{k} > \binom{t+k-1}{k} \text{ آنگاه جواب}$$

حداکثر (magrity solution) در میان  $\binom{n}{k}$  جواب مقادیر صحیح  $a_i$  ها را مشخص

خواهد کرد. اما این رابطه برقرار است اگر و تنها اگر  $t+k-1 > 1-t$ ، یعنی، اگر و تنها اگر

$$d = n - k + 1 > 2t$$

**مطالب فوق را می توان در قضیه زیر خلاصه کرد.**

قضیه: فرض کنید  $C$  یک کد رید-سولومن  $[n, k, d]$  باشد. روش کد گشایی با منطق

اکثریت می تواند حداکثر  $t < \frac{1}{4}d$  خطا را در انتقال با هینه، داشتن حل  $\binom{n}{k}$  دستگاه از

معادلات با اندازه  $k \times k$ ، تصحیح کند.

### کدهای باقیمانده مربعی (Quadratic Residue codes)

فرض کنید  $w$  یک ریشهام واحد روی  $F_q$  باشد و قرار دهید.

$$x^n - 1 = \prod_i m_i(x)$$

جایی که چند جمله‌ای های مینیمال  $m_i(x)$  به صورت زیر داده شده‌اند.

$$m_i(x) = \prod_{j \in C_i} (x - w^j), C_i = \{i, iq, \dots, iq^{d-1}\}$$

و  $C_i$ ،  $i$  امین همه دسته دوری در پیمان  $q$  باشد.

قبلاً مشاهده کردیم که یک کد دوری می تواند توسط صفرهای آن،  $Z$ ، کاملاً مشخص

شود، جایی ه:

$$Z = \{w^i : i \in Z\}$$

و  $Z$  یک اجتماع از هم دسته‌های دوری در پیمانه  $q$  است. در مودر کدهای BCH، ما زیر مجموعه‌ای از صفرها را اختیار کردیم که در آن توان‌ها اعداد صحیح متوالی به صورت زیر بودند:

$$S = \{w^j = b, b+1, \dots, b+\delta-2\}$$

و سپس، مجموعه صفرها را با در نظر گرفتن اجتماع تمامی هم دسته‌های دوری که اعداد  $b, b+1, \dots, b+\delta-2$  را شامل شوند، به دست آوردیم. در مورد کدهای ریدسولومن، هم دسته‌های دوری تک عضو هستند و لذا  $S$  تمامی ریشه‌های آن کد خواهد بود. نکته‌ای 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:

$$x^2 \equiv a \pmod{p}$$

اگر چنین  $X$  وجود نداشته باشد، آنگاه  $a$  را یک غیر باقیمانده مربعی در پیمانه  $P$  می‌نامیم. به عبارت دیگر،  $a$  یک باقیمانده مربعی است (در پیمانه  $P$ ) اگر پیمانه  $P$ ، دارای رشد باشد. مجموعه باقیمانده‌های مربعی در پیمانه  $P$  را که متعلق به مجموعه  $Z_p^* = \{1, 2, \dots, p-1\}$  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.

$$QR = \{1^2, 2^2, \dots, (\frac{P-1}{2})^2\}$$

جایی که اعداد در پیمانۀ P محاسبه شده‌اند، همچنین  $QR = \{1^2, 2^2, 3^2, 4^2, 5^2\} = \{1, 4, 9, 16, 25\}$

تعریف: فرض کنید P یک عدد اول باشد و  $(a, p) = 1$ . نماد لژاندر  $\left(\frac{a}{p}\right)$  به صورت زیر

تعریف شده است:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \in QR \\ -1 & a \in NQE \end{cases} \quad \text{اگر}$$

قضیه: (خواص نماد لژاندر) اگر q, p اعداد اول متمایزی باشند و  $(a, p) = (b, p) = 1$

آنگاه:

$$1) \left(\frac{1}{p}\right) = \left(\frac{a^2}{p}\right) = 1$$

$$2) a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

$$3) \text{ (محک اویلر)} \left(\frac{a}{p}\right)^p \equiv a \pmod{p}$$

$$4) \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

$$5) \left(\frac{-1}{p}\right)^p \equiv \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$$

$$6) \left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{8}$$

$$7) \left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{12}$$

نتیجه: حاصل ضرب دومانده مربعی (همان باقیمانده مربعی) در پیمانۀ p، یک مانده مربعی

دیگر در پیمانۀ p خواهد بود. حاصل ضرب دو نا مانده مربعی (همان باقیمانده مربعی)، در

پیمانۀ P، غیر یک مانده مربعی در پیمانۀ P است. حاصل ضرب یک مانده مربعی و یک

نامانده مربعی در پیمانۀ P، یک نامانده مربعی در پیمانۀ خواهد بود.

نتیجه: اگر  $S \in QR$ ، آنگاه  $QR = \{sR \pmod{p} \mid r \in QR\}$

مثال: چون  $x^2 \equiv -a^2 \pmod{p}$  می بینیم  $\left(\frac{-a^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a^2}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$  دارای یک جواب

است اگر و تنها اگر  $x^2 \equiv -a^2 \pmod{p}$  دارای یک جواب استو تنها اگر  $p \equiv 1 \pmod{4}$ .

مثال: هم نهشتی  $x^2 \equiv 15 \pmod{19}$  را در نظر بگیرید. داریم:

$$\left(\frac{15}{19}\right) = \left(\frac{-4}{19}\right) = \left(\frac{-1}{19}\right)\left(\frac{4}{19}\right) = \left(\frac{-1}{19}\right) = -1$$

زیرا  $19 \equiv 3 \pmod{4}$ . بنابراین، این همنهشتی دارای جوابی نیست.

### کدهای باقیمانده مربعی

در اینجا، تنها روی حالت دوتایی تأکید می کنیم. اما، به آسانی می توان تعریف را برای

حالت غیر دودویی نیز تعمیم داد. می دانیم  $|QR| = NQR = \frac{p-1}{2}$  و لذا  $NQR, QR$  یک

افزار  $\{1, 2, \dots, p-1\}$  به بلوک های با اندازه یکسان هستند. حال، فرض کنید  $w$  یک ریشه

اولیه  $P$  واحد روی  $F_q$  باشد.

بنابراین، ریشه های  $P$  واحد به صورت مجموعه  $\{1, w, w^2, \dots, w^{p-1}\}$  هستند.

در اینجا می توان دید  $Z = \{w^i \mid i \in QR\}$  یک مجموعه کامل از ریشه های یک کد دوری  $q$ -

تایی هستند (برای یک عدد اول  $q$ ). برای مشاهده این مطلب، کافی است نشان دهیم  $QR$

اجتماعی از هم دسته های دوری در پیمانه  $q$  است. یعنی باید داشته باشیم.

$$i \in QR \Rightarrow C_i = \{i, iq, \dots, iq^{d-1}\} \subseteq QR$$

اما طبق فضای 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:

$$x^p - 1 = (x-1)q(x)n(x)$$

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 پیمانۀ  $p$  باشد.

کدهای دوری  $q$ -تایی

$$Q(p) = \langle\langle q(x) \rangle\rangle, \overline{Q(p)} = \langle\langle (x-1)q(x) \rangle\rangle$$

$$N(p) = \langle\langle n(x) \rangle\rangle, \overline{N(p)} = \langle\langle (x-1)n(x) \rangle\rangle$$

با طول  $p$ ، در  $R_p = \frac{F_q[x]}{\langle x^p - 1 \rangle}$ ، کدهای باقیمانده مربعی نامیده می‌شود.

چون ما تنها با کدهای باقیمانده مربعی دودویی کار خواهیم کرد، نیاز داریم تا  $q=2$  یک مانده مربعی در پیمانۀ  $P$  باشد و لذا از این جا به بعد، فرض می‌کنیم  $P$  یک عدد اول به شکل  $4m \pm 1$  باشد. واضح است که:

$$\overline{Q(p)} \subseteq Q(p), \quad \overline{N(p)} \subseteq N(p)$$

در واقع،  $\overline{Q(p)}$  زیر مجموعه‌ای از  $Q(p)$  شامل تمامی کد کلمات 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:

$$\dim(Q(p)) = p - \deg(q(x)) = p - |QR| = \frac{p+1}{2}$$

$$\dim(N(p)) = p - \deg(n(x)) = p - |NQR| = \frac{p+1}{2}$$

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  $\prod_{\gamma} (i) = V_i \pmod{p}$  را در نظر بگیرید.

توجه دارید که  $\Pi_v$  می‌تواند با جایگذاری  $x^v$  به جای  $v$  و سپس کاهش در پیمانه  $x^p - 1$

$$\Pi_v(f(x)g(x)) = \Pi_v(f(x))\Pi_v(g(x)) \quad \text{به دست آید؛ جایی که علاوه بر آن:}$$

برای مشاهده این مطلب که  $\Pi_v$ ،  $Q(p)$  را به  $N(p)$  تصویر می‌کند، قرار می‌دهیم

$$p(x) = \Pi_v(q(x)) \equiv q(x^v) \equiv \prod_{r \in QR} (x^v - w^r) \pmod{(x^p - 1)} \quad \text{در این صورت}$$

و لذا یک چند جمله‌ای  $a(x)$  وجود دارد که در آن:

$$p(x) = \prod_{r \in QR} (x^v - w^r) + a(x)(x^p - 1)$$

از آنجایی که حاصل ضرب دو نامانده مربعی، یک مانده مربعی است، نتیجه می‌گیریم که

برای هر  $uv$  در  $QR$  است. لذا:

$$P(w^u) = \prod_{r \in QR} (w^{uv} - w^r) + a(w^u)(w^{up} - 1) = 0$$

در نتیجه،  $p(x), x - w^u$  را عاد می‌کند. (برای تمامی  $u \in NQR$ ) و لذا  $n(x) | p(x)$ . بنابراین

$n(x)$  نیز  $p(x)$  را در پیمانه  $x^p - 1$  عاد می‌کند؛ که در نتیجه:

$$\Pi_v(Q(p)) = \langle q(x^v) \pmod{(x^p - 1)} \rangle \subseteq \langle n(x) \rangle = N(p)$$

اما، چون  $\Pi_v$  یک به یک بوده و  $Q(p), N(p)$  دارای اندازه یکسان هستند، داریم

$\Pi_v(q(p)) = N(p)$  و لذا  $Q(p), N(p)$  هم ارز هستند. مطالب فوق‌ار می‌توان در قضیه زیر

خلاصه کرد.

قضیه: برای کدهای باقیمانده مربعی به طول  $p$ ، داریم.

$$\dim(Q(p)) = \dim(N(p)) = \frac{p+1}{2}$$

$$\dim(q(p)) = \dim(N(p)) = \frac{p-1}{2}$$

علاوه بر این، کدهای  $Q(p)$ ،  $N(p)$  هم ارز هستند. همچنین کدهای  $\overline{Q(p)}$ ،  $\overline{N(p)}$  هم ارز می‌باشند.

مثال بعد، نشان می‌دهد که کدهای  $Q(p)$ ،  $N(p)$  می‌توانند با جایگزینی یک ریشه  $p$ -ام اولیه واحد  $w$  با ریشه دیگر به دست آینده

مثال: فرض کنید  $p = 7$ . در این صورت:  $QR = \{1, 4, 2\}$ ،  $NQR = \{3, 5, 6\}$

بنابراین، اگر  $w$  یک ریشه هفتم اولیه، واحد روی  $F_7$  باشد، آنگاه.

$$Q(x) = (x - w)(x - w^2)(x - w^4) = x^3x + 1$$

$$n(x) = (x - w^3)(x - w^5)(x - w^6) = x^3 + x^2 + 1$$

بنابراین،  $Q(7) = \langle\langle x^3 + x + 1 \rangle\rangle$ ، کد همینگ  $[7, 4, 3]$  ( $H_7(3)$ ) است. توجه داشته باشید

که  $H_7(3)$  می‌تواند به صورت یک کد دوری با صفر  $w$  مشخص شود.

به طور مشابه، کد  $N(7) = \langle\langle x^3 + x^2 + 1 \rangle\rangle$ ، کد دوری با صفر  $w^3$  است (که  $w^3$  نیز یک

ریشه ۷ام اولیه واحد است) و لذا کد همینگ  $H_7(3)$  نیز دوری است.

### و کدهای گلی به عنوان کدهای باقیمانده مربعی

قبلا مشاهده کردیم که چگونه می‌توان  $x^n - 1$  را تجزیه کرد. (به عوامل تحویل ناپذیر

روی  $F_q[x]$ ). با به کارگیری این روشن.

$$x^{23} - 1 = (x + 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$

تجزیه  $x^{23} - 1$  به عوامل تحویل ناپذیری روی  $F_7$  است. حال چون ۲ یک مانده مربعی در

$$x^{23} - 1 = (x - 1)q(x)n(x) \quad \text{لذا:}$$

بنابراین، کد گلی  $G_{73}$  هم ارز با کد باقیمانده مربعی  $Q(23)$  خواهد بود.

به روش مشابه، روی  $F_7$  داریم:

$$x^{11} - 1 = (x-1)(x^5 + x^4 - x^3 + x^2 - 1)(x^5 - x^3 + x^2 + x - 1)$$

جایی که عوامل فوق، تحویل ناپذیر بوده و چون ۳ یک مانده مربعی در پیمانه ۱۱ است، نتیجه می‌گیریم که  $G_{11}$  هم ارز با یک کد باقیمانده مربع سه تایی  $Q(11)$  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)، متترین فاصله  $d$  از کدهای دوتایی  $N(p), Q(p)$  در رابطه

$$d^2 \geq p \text{ صدق می‌کند. علاوه بر این اگر } p = 4m - 1 \text{ آنگاه:}$$

$$d^2 - d + 1 \geq p$$

می‌توان دید که اگر  $u \in NQR$  آنگاه  $C(x) = c(x^u) \bmod (x^p - 1)$  یک کلمه با وزن مینیمم

$d$  در  $N(P)$  است. بنابراین، چند جمله‌ای

$$P(x) = [c(x)\overline{c(x)}] \bmod (x^p - 1) = [c(x)c(x^u)] \bmod (x^p - 1)$$

\*\*\*\*\*

$$q(x)n(x) = \frac{x^p - 1}{x - 1} = 1 + x + x^2 + \dots + x^{p-1}$$

در واقع، از این که  $Q(p)$  دارای کمترین وزن فرد است؛ نتیجه می‌شود:

$p(x) \neq 0$  به طور خلاصه  $p(x)$  ناصفر است، بر  $q(x)n(x)$  بخش پذیر است و دارای

درجه حداکثر  $P-1$  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  $c(x), c(x^u)$  دارای  $d$  جمله ناصفر

هستند و لذا این حاصل ضرب نمی‌تواند دارای بیشتر از  $d^2$  جمله ناصفر باشد. لذا

$$d^2 \geq p$$

اگر  $p = 1m - 1$ ، آنگاه  $C(x)C(x-1)$  دارای حداکثر  $d^2$  جمله ناصفر است که  $d$  جمله آن

به صورت  $a_i x^i x^{-i} = a_i$  است که ثابت می‌باشد. بنابراین همه این جملات به یک جمله

تبدیل شده و  $C(x)c(x^{-1})$  دارای وزن حداکثر  $d^2 - d + 1$  خواهد بود که در نتیجه:

$$d^2 - d + 1 \geq p$$

مثال: کدهای باقیمانده مربعی دوتایی با طول  $p = 7$  دارای کمترین فاصله  $d$  هستند که

در رابطه  $d^2 - d + 1 \geq 7$  صدق می‌کند. لذا  $d \geq 3$  آنچنان که قبلاً مشاهده کردیم، کد

باقیمانده مربعی  $[7, 4]$  دارای کمترین فاصله  $d = 3$  است.

توجه جدول زیر، برخی پارامترهای مربوط به کدهای مانده دوتایی را به همراه کران‌های

پائینی کمترین فاصله (از قضیه قبل) لیست کرده است.

p	k	d	کران پایین روی d
7	4	3	3
17	9	5	4
23	12	7	6
31	16	7	6
41	21	9	6
47	24	11	8
71	36	11	9
73	37	13	9
79	40	15	10

۸۹	۴۵	۱۷	۹
۹۷	۴۹	۱۵	۹
۱۰۳	۵۲	۱۹	۱۱
۱۲۷	۶۷	۱۹	۱۲
۱۵۱	۷۶	۱۹	۱۳