

تصحیح خطای طرایب

$$0 \xrightarrow{p} 1$$

$$1 \xrightarrow{p} 0$$

$$0 \Rightarrow 000$$

$$1 \Rightarrow 111$$

$$p' = 3p^2(1-p) + p^3$$

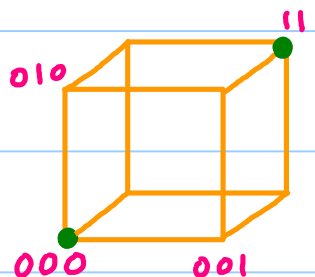
که تکرار سه باره

$$p' = \sum_{k=0}^{2n+1} \binom{2n+1}{k} p^k (1-p)^{2n+1-k}$$

که تکرار $2n+1$ باره

$$p' \approx \binom{2n+1}{n+1} p^{n+1}$$

0 1



$d=3$

$$R = \frac{k}{n}$$

Block Code •

$\mathcal{A} = \text{Alphabet} = \{0, 1\}$.

$\mathcal{A}^n :=$ n character strings from $\mathcal{A}$ $|\mathcal{A}^n| = 2^n$

Block code $C :=$ n character strings

c	w
000	00010
001	01000
010	01101
011	10100
101	00011
110	11000
111	01011

$$R = \frac{k}{n} = \frac{3}{5}$$

} $d = 1$

Not a good Code

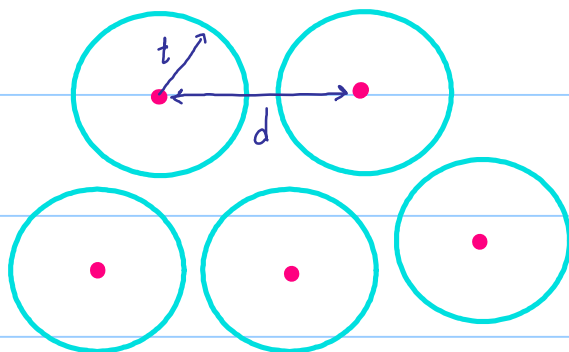
$$R = \frac{\log_2 C}{n}$$

فاصله هامینگ $d_H(x, y)$ بین x و y فاصله هاست

$$d = \min_{x, y \in C} d(x, y)$$

• قضیه: اگر C یک کد باشد، $d = 2t + 1$

در این حالت: t خطا قابل تصحیح هستند.



$$x, y \in \mathcal{A}^n$$

• که در فضای

$$x + y \in \mathcal{A}^n, \quad cx \in \mathcal{A}^n \quad c = 0, 1.$$

$$x + (-x) = 0$$

$$\mathcal{A}^n = \text{فضای برداری}$$

$$\dim(\mathcal{A}^n) = n \quad \text{Basis} = \{(100 \dots 0), \dots, (000 \dots 1)\}$$

• C یک کد خطی است اگر زیرفضای $\mathcal{A}^n$ باشد.

$$\forall x, y \in C \rightarrow x + y \in C.$$

مثال: $C = \{00, 01, 11\}$ یک کد خطی نیست.

مثال: $C = \{00, 11\}$ یک کد خطی است.

A linear Code C has a Basis $\{\vec{v}_1, \vec{v}_2, \dots, \vec{v}_k\}$.

$$\forall x \in C \rightarrow \vec{w} = x_1 \vec{v}_1 + x_2 \vec{v}_2 + \dots + x_k \vec{v}_k \quad x_i = 0, 1.$$

$$\rightarrow \vec{w} = (x_1 \ x_2 \ \dots \ x_k) \begin{pmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_k \end{pmatrix}$$

$$\Rightarrow \vec{w} = x G$$

$$w \in C \quad x \in \mathcal{A}^k \quad G = k \times n \text{ Matrix}$$

Generator Matrix = G ماٹرکس مولد

Consider $C^\perp$ $C^\perp \perp C \rightarrow$

$$\forall x \in C, y \in C^\perp \quad \langle x, y \rangle = 0.$$

$$\dim(C^\perp) = n-k \quad \text{Basis of } C^\perp = \{u_1, u_2, \dots, u_{n-k}\}$$

$$\langle v_i, u_j \rangle = 0 \rightarrow v_i u_j^T = 0 \quad v = (v_1, \dots, v_n) \quad u^T = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix}$$

$$G = \begin{pmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_k \end{pmatrix} \quad H = \begin{pmatrix} \vec{u}_1 \\ \vec{u}_2 \\ \vdots \\ \vec{u}_{n-k} \end{pmatrix} \quad H^T = (u_1^T \ u_2^T \ \dots \ u_{n-k}^T)$$

G generates C .

$$G_{k \times n}, \quad H_{(n-k) \times n}.$$

H generates $C^\perp$ i.e.: $\forall w' \in C^\perp \quad w' = (y_1, \dots, y_{n-k}) H.$

$$GH^T = 0$$

Parity check Matrix

$$\rightarrow H G^T = 0$$

$$\forall w \in C \rightarrow w H^T = x G H^T = 0.$$

$$\forall w' \in C^\perp \rightarrow w' G^T = y H G^T = 0.$$

Errors :

$$w = x G \quad \boxed{\quad} \quad \tilde{w} = w + e$$

$$\tilde{w} H^T = (w + e) H^T = e H^T$$

Error. Syndrome

$$\begin{array}{ccc} e H^T & \xrightarrow{\text{Detection}} & e \\ \tilde{w} & \xrightarrow{\text{Correction}} & \tilde{w} + e = w \end{array}$$

خطای متفاوت، سندیم متفاوت، نه شسته باشند. ~~برای~~ ~~ن~~ ~~خ~~ ~~ب~~ ~~پ~~

$$e_1 H^T = e_2 H^T \longrightarrow e_1 = e_2$$

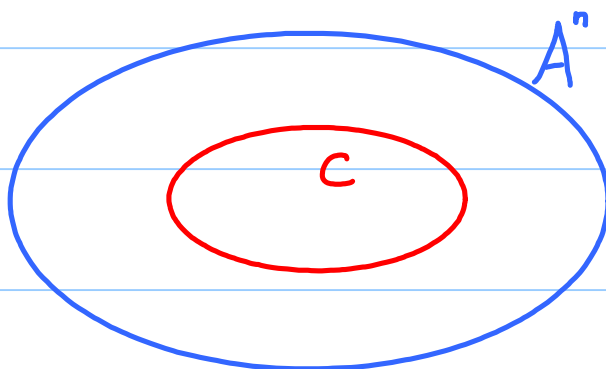
مجموعه تمام $\{e_i\}$ را می‌توان به دو دسته تقسیم کرد، مجموعه خطای قابل تصحیح و مجموعه خطای غیر قابل تصحیح. B به دست می‌دهند.

مثال.

$$C = \{000, 111\} = \text{Span}\{(111)\} \rightarrow v_1 = (111) \quad \dim B = 1 \rightarrow G = (111)$$

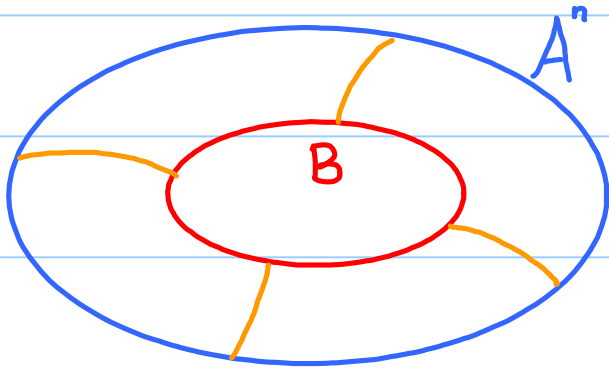
$$C^\perp = \{000, 110, 101, 011\} = \text{Span}\{110, 101\} \rightarrow \dim B^\perp = 2.$$

$$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \rightarrow H^T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow GH^T = 0$$



اگر $e_1 H^T = e_2 H^T$ خطای e_1, e_2 خطای هستند پس یکسان.

نمبری نمی توانیم e_1 و e_2 تصحیح کنیم.



تعریف: $A^n \ni e_1, e_2$

رابطه هم‌ارزی $e_1 \sim e_2$ if $e_1 - e_2 \in C$

$$\Rightarrow e_1 \sim e_2 \text{ if } (e_1 - e_2) H^T = 0.$$

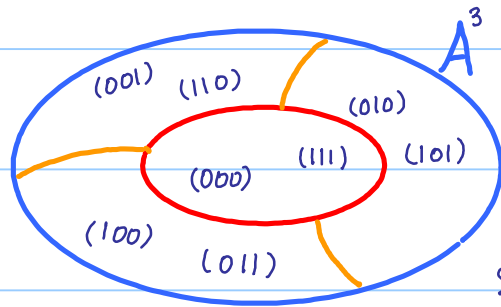
نمبری عنصر درون یک ماس هم‌ارزی لازم نماند تغییر نشود و فقط از هر ماس یک خطا به

تغییر در صحت است.

مثال: $G = (111) \rightarrow \dim C = 1 \rightarrow v_1 = (111) \rightarrow C = \{000, 111\} = \text{span}\{(111)\}$

$C^\perp = \{000, 110, 101, 011\} = \text{span}\{110, 101\} \rightarrow \dim C^\perp = 2.$

$H = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \rightarrow H^T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \rightarrow G H^T = 0$



Correctable Errors :=

$$\mathcal{E} = \{ (100), (010), (001) \} \text{ or}$$

$$\text{Syndromes} = \{ (111), (110), (011) \}$$

طبیعی کد کے معنوں میں غلطیوں کی اصلاح نہیں کی جا سکتی۔

مثال ● $C = \text{Span} \{ 1100, 0011 \} = \{ 0000, 0011, 1100, 1111 \}$

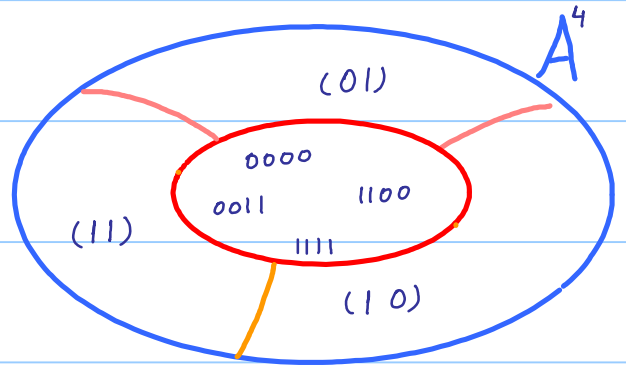
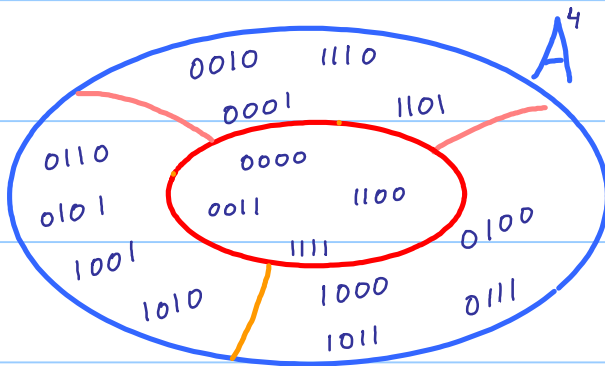
$\dim C = 2 \quad R = \frac{2}{4} = \frac{1}{2}$

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

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \rightarrow H^T = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$$

$B^\perp = B$

$H = G \rightarrow GG^T = 0$



Syndromes (eH^T)

Correctable Errors $E_1 = \{ 1000, 0001, 0110 \}$ or

$$E_2 = \{ 0100, 0010, 0110 \}$$

هم در E_1 ، هم در E_2 خطا برآید یعنی 1000، 0100 و جدا از هم از هم جدا
قابل تمیز نیستند.

این که، در خطا تشخیص برده و بر آن تصحیح می‌لند

$$d = 2 !$$

$$G = \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{bmatrix} \quad G' = \begin{bmatrix} e'_1 \\ e'_2 \\ \vdots \\ e'_k \end{bmatrix} \quad \bullet \text{ } G \text{ و } G' \text{ معادل}$$

$$G' \sim G \quad (\text{generate the same } B) \quad \text{if } e'_i = S_{ij} e_j$$

$$S \text{ (invertible).} \Rightarrow$$

روی G می‌توان اعمال سطری انجام داد:

در سطر i ؛ $\times$ جمع کرد + جابر سطر j شد.

ترتیب بیت‌ها را از چپ به راست تغییر دادیم:

درست‌تر به نظر می‌رسد.

نتیجه: هر ماتریس $G_{k \times n}$ را می‌توان به شکل زیر نوشت:

$$G_{k \times n} = \left[I_k \mid A_{k \times n-k} \right]$$

$$\text{if } G = [I, A] \rightarrow H^T = \begin{bmatrix} A \\ I \end{bmatrix} \rightarrow H = [A^T, I].$$

مثال: Hamming Code

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

$$\dim C = 4, |C| = 16$$

$$R = \frac{4}{7}$$

$$H = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array} \right] = [A^T, I]$$

← چنانچه می‌خواهیم

$$\rightarrow G = [I, A] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$d = 3$$

نصفه که

این که مرتبه خطای رتبه بقیه را تعیین کند. بزرگترین $\frac{1}{3}$ ، بزرگترین آن $\frac{4}{7}$ است که بالا است.

$$H = \left[\begin{array}{cccc|ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array} \right] = [A^T, I]$$

$$\rightarrow G = [I, A] = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array} \right]$$

$$C = \text{Span} \{ 1000110, 0100011, 0010101, 0001111 \} \quad \dim = 4, |C| = 16$$

$$C^\perp = \text{Span} \{ 1011100, 1101010, 0111001 \} \quad \dim C^\perp = 3, |C| = 8$$

• نکته مهم: C و $C^\perp$ لزوماً از یکدیگر جدا نیستند و می‌توانند اشتراک داشته باشند (مگر نه 0).

$$B = \text{Span} \{ 1100, 0011 \} = \{ 0000, 1100, 0011, 1111 \} \quad \bullet \text{ مثال:}$$

$$B^\perp = B.$$

Dual Codes

مثال:

$$C = \text{Span} \{ 011, 110 \} = \{ 000, 011, 110, 101 \}$$

$$C^\perp = \{ 000, 111 \} \rightarrow C^\perp \subset C$$

مثال:

$$C: \begin{cases} \text{generator } G \\ \text{parity check } H \end{cases}$$

$$x \in C \rightarrow x = uG \leftrightarrow xH^T = 0$$

$$C^\perp: \begin{cases} \text{generator } H \\ \text{parity check } G \end{cases}$$

$$y \in C^\perp \rightarrow y = vH \leftrightarrow yG^T = 0$$

$$\text{Now if } HH^T = 0 \Rightarrow C^\perp \subset C$$

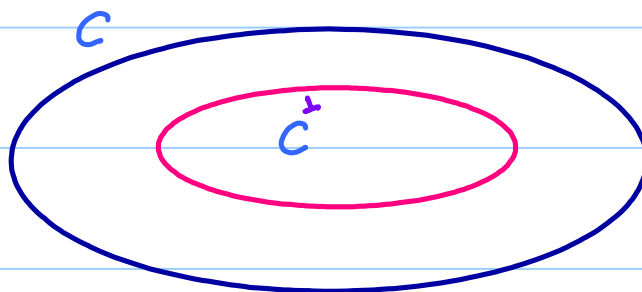
$$\text{if } GG^T = 0 \Rightarrow C \subset C^\perp$$

Hamming Code : دین

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = [A^T, I] \rightarrow G = [I, A]$$

• Easy exercise: $\rightarrow A^T A = I \rightarrow H H^T = 0 \rightarrow C^\perp \subseteq C$

but $A A^T \neq I \rightarrow G G^T \neq 0 \rightarrow C \not\subseteq C^\perp$



The Basic Problem in Coding Theory.

$[n, k, d]$.

①: $\frac{k}{n}$ راجه به آمارها بزرگ باشد.

②: $\frac{d}{n}$ م راجه به آمارها بزرگ باشد.

مقداری از جبر:

$$C_n = \{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\} \quad \text{گروه دوری:}$$

$$\alpha^n = 1$$

$$\alpha^k \alpha^l = \alpha^{k+l} \pmod{\alpha^n}.$$

$$C_4:$$

	1	α	α^2	α^3
1	1	α	α^2	α^3
α	α	α^2	α^3	1
α^2	α^2	α^3	1	α
α^3	α^3	1	α	α^2

همبازی در گروه: (Isomorphism)

$$\phi: G_1 \longrightarrow G_2$$

$$\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$$

$$\text{Example: } \{1, \sigma_x\} \equiv \{0, 1\}_+ = \{1, \alpha\}$$

مرتبه G = تعداد اعضا گروه G = $|G|$

قضیه: در هر آبجی، از هر ترتیب نقطه یک گروه داریم.
up to isomorphism

تعریف: جمع مستقیم در گروه آبجی.

$$G_1 \oplus G_2 = \{ (\alpha, \beta) \mid \alpha \in G_1, \beta \in G_2 \}$$

$$(\alpha, \beta) \cdot (\alpha', \beta') := (\alpha\alpha', \beta\beta') \quad (\alpha, \beta)^{-1} := (\alpha^{-1}, \beta^{-1})$$

$$|G_1 \oplus G_2| = |G_1| |G_2|$$

قضیہ اس کی طرف سے آجی:

$$C_N = C_{p_1^{n_1}} \oplus C_{p_2^{n_2}} \oplus C_{p_3^{n_3}} \oplus \dots \oplus C_{p_k^{n_k}}$$

p_i = prime.

Example 1: $C_6 = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$

$$C_6 = C_3 \oplus C_2$$

$$1 \longrightarrow (1, 1) \qquad \alpha \longrightarrow (g^2, \alpha)$$

$$\alpha^2 \longrightarrow (g, 1) \qquad \alpha^3 \longrightarrow (1, \alpha)$$

$$\alpha^4 \longrightarrow (g^2, 1) \qquad \alpha^5 \longrightarrow (g, \alpha)$$

Exercise: prove that $C_{10} = C_5 \oplus C_2$

Exercise: prove that $C_{12} = C_4 \oplus C_3$

Exercise: prove that
$$\begin{cases} C_8 \neq C_4 \oplus C_2 \\ C_8 \neq C_2 \oplus C_2 \oplus C_2 \end{cases}$$

Fields = $\{F, +, \cdot\}$.

examples: $\{Q, R, C, \mathbb{Z}_p, \mathbb{Z}_{p^n}\}$
prime.

Example: $\mathbb{Z}_3 = \{0, 1, 2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	1	2
1	1	2
2	2	1

Exercise: prove that $\mathbb{Z}_4$ is not a field.

تعریف: مشخصه یک میدان
کوچکترین عدد طبیعی n به طوری که

$$n\alpha = 0 \quad \forall \alpha \in F$$

اگر چنین n ای وجود نداشته باشد $\leftarrow$ مشخصه میدان برابر 0 است.

مثال ۱) $\mathbb{Z}_2 = \{0, 1\}$ دارای مشخصه ۲ است.

$\mathbb{Z}_3 = \{0, 1, 2\}$ دارای مشخصه ۳ است.

$\mathbb{Z}_p = \{0, 1, 2, \dots, p-1\}$ دارای مشخصه p است.

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ دارای مشخصه صفر هستند.

نکته: نام یک اندک هر میدان منتهی (Finite Field) همان نام آن

منحنه غیر همراست.

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0.$$

چند جمله‌ای

$a_i \in \mathbb{R}, x \in \mathbb{R}$ real polynomial.

$a_i \in \mathbb{C}, x \in \mathbb{C}$ complex polynomial

$\mathbb{C}[x]$ = The ring of complex polynomials حلقه چندجمله‌ای مختلط

$\mathbb{R}[x]$ = The ring of real polynomials

$\mathbb{R}[x]$ and $\mathbb{C}[x]$ are Rings.

زیرا چندجمله‌ای لزوماً معکوس ندارند.

$\frac{1}{x+1}$ is not a polynomial.

قضیہ اول کی جبر:

In $C[x]$, every $p_n(x) = a(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$.

ہر چند جبر مختلط حقہ لائنیں ہیں۔

→ $R[x]$ جنبه نیت : مثال : $p_2(x) = x^2 + 1$

$$p_3(x) = x^4 + 1$$

مثال : $F_2[x] =$ مجموعه نیت جنبه بر x ضرایب 0, 1.

Example: $\{x+1, x, x^2+x, x^4+x+1\} \subset F_2[x]$

مثال : $F_3[x] =$ مجموعه نیت جنبه بر x ضرایب 0, 1, 2.

Example: $\{x, 2x+1, 2x^2+x+2, 2x^7+x^6+2x^5+1\} \in F_3[x].$

مثال : $x^3+x+1 \in F_2[x]$ یک جنبه بر x ضرایب 0, 1.

$x^2+1 \in F_2[x]$ یک جنبه بر x ضرایب 0, 1:

$$x^2+1 = (x+1)(x+1).$$

مثال: $2x^3 + x^2 + 2 \in F_3[x]$ کاهش پذیر است.

$2x^3 + x^2 + 1 \in F_3[x]$ کاهش پذیر است:

$$2x^3 + x^2 + 1 = (x+1)(2x^2 + 2x + 1)$$

↑

No more reducible

تبدیل $F[x]$ از حلقه به میدان.

let $g(x) \in F[x]$ be irreducible.

Define $F = F[x] / \langle g(x) \rangle$

if $p_2(x) = p_1(x) + g(x)k(x)$. then $p_2(x) \equiv p_1(x)$.

مثال:

in $F_2[x]$, $g(x) = x^2 + x + 1$ is irreducible.

$$\text{So } F_2[x]/\langle g(x) \rangle = \{0, 1, x, x^2, 1+x, 1+x^2, x+x^2, 1+x+x^2\}$$

But.

$$\text{So } F_2[x]/\langle g(x) \rangle = \{0, 1, x, \overset{1+x}{x^2}, 1+x, \overset{x}{1+x^2}, \overset{1}{x+x^2}, \overset{0}{1+x+x^2}\}$$

$$\text{So } F_2[x]/\langle g(x) \rangle = \{0, 1, x, 1+x\}$$

.	1	x	1+x
1	1	x	1+x
x	x	1+x	1
1+x	1+x	1	x

: Jin

in $F_3[x]$, $g(x) = x^2 + 1$ is irreducible.

$$F_3[x]/\langle g(x) \rangle = \{ 0, 1, 2, x, 2x, 1+x, 2+x, \\ 1+2x, 2+2x \}$$

$$(1+x)(1+2x) = 1 + 2x^2 = 2(x^2 + 1) + 1 = 1$$

$$(1+x)(1+x) = 1 + 2x + x^2 = 2x$$

$$x(1+x) = x + x^2 = x + (x^2 + 1) + 2 = x + 2$$

$$(2+x)(2+x) = 1 + x + x^2 = x.$$

Exercise: in $F_3[x]$, find an irreducible polynomial
and turn $F_3[x]$ into a field.

قضیه زیری در مورد طاقتهای نهایی میدان درست است.

• $m = p^n$ هر صحیح مثبت:

درین صورت یک میدان با m عضو وجود دارد اگر فقط اگر

$$m = p^n.$$

• یک فقط یک میدان با p^n عضو وجود دارد و آن هم به شکل زیر است.

$$F_p[x]/g(x)$$

where $\deg g(x) = n$.

• اگر $g(x)$ و $h(x)$ هر دو چند جمله‌ای هم‌درجه n باشند، آنگاه:

$$F_p[x]/g(x) \simeq F_p[x]/h(x).$$

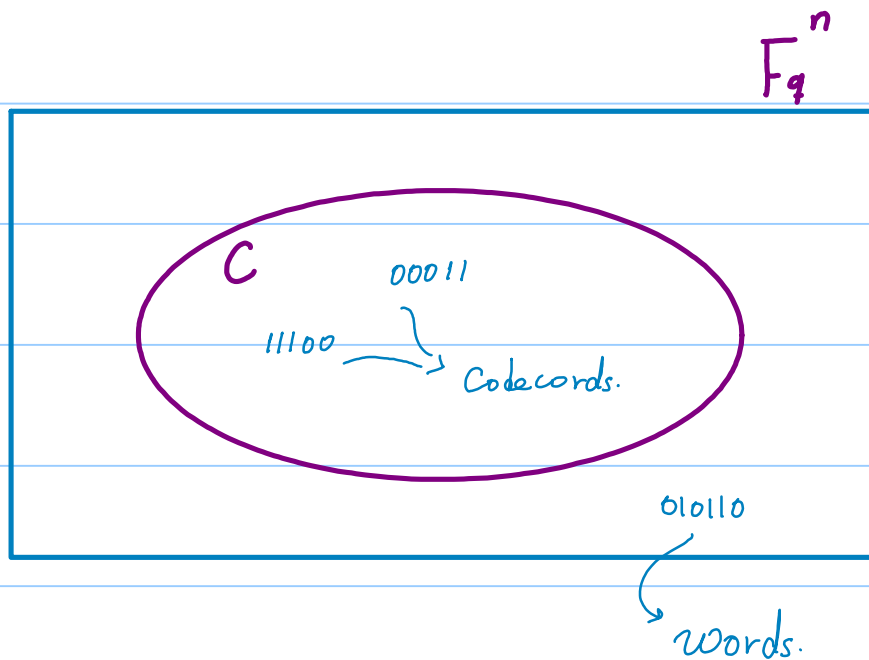
• قضیه: اگر F یک میدان باشد، p^n عنصر، آنگاه:

$F^* := F - \{0\}$ is a Cyclic Group with $p^n - 1$ elements.

Codes. F_q a finite field with q elements.

$$F_q^n = \left\{ (\underbrace{x_1 x_2 x_3 \dots x_n}_{\text{words}}) \mid x_i \in F_q \right\}$$

$$|F_q^n| = q^n$$



Hamming Distance: $d_H: F_q^n \times F_q^n \rightarrow F_q$

$$d_H(x, y) = |\{i \mid x_i \neq y_i\}|$$

Example: For F_3 : $d_H(01210, 11201) = 3$.

Def: Hamming weight w_H :

$$w_H(x) = |\{x_i \mid x_i \neq 0\}|$$

Thm: d_H is a metric: i.e.

$$1) \quad d_H(x, y) \geq 0, \quad d_H(x, y) = 0 \leftrightarrow x = y$$

$$2) \quad d_H(x, y) = d_H(y, x)$$

$$3) \quad d_H(x, z) \leq d_H(x, y) + d_H(y, z)$$

proof of 3).

$$D(x, z) = \{i \mid x_i \neq z_i\}$$

$$D(x, y) = \{i \mid x_i \neq y_i\}$$

$$D(y, z) = \{i \mid y_i \neq z_i\}$$

$$D'(x,y) \cap D'(y,z) = D'(x,z)$$

$\Downarrow$

$$D(x,z) = D(x,y) \cup D(y,z)$$

$\Downarrow$

$$|D(x,z)| \leq |D(x,y)| + |D(y,z)|$$

$\Downarrow$

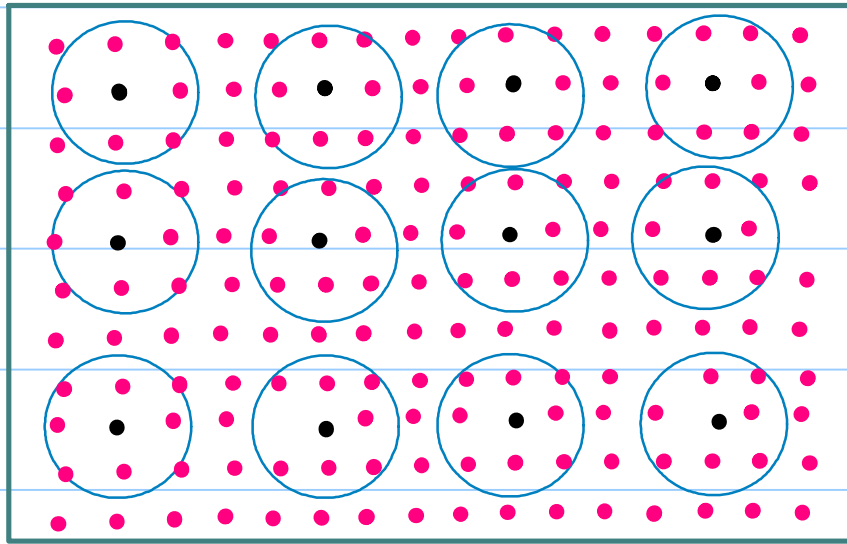
$$d_H(x,z) \leq d_H(x,y) + d_H(y,z)$$

$n := \text{length of code words.}$: پارانز، پارانز

$$k := \log_2 |C|$$

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

Objectives: $\begin{cases} \text{Increase } \frac{d}{n} \\ \text{Increase } \frac{k}{n} \end{cases}$ As much as possible



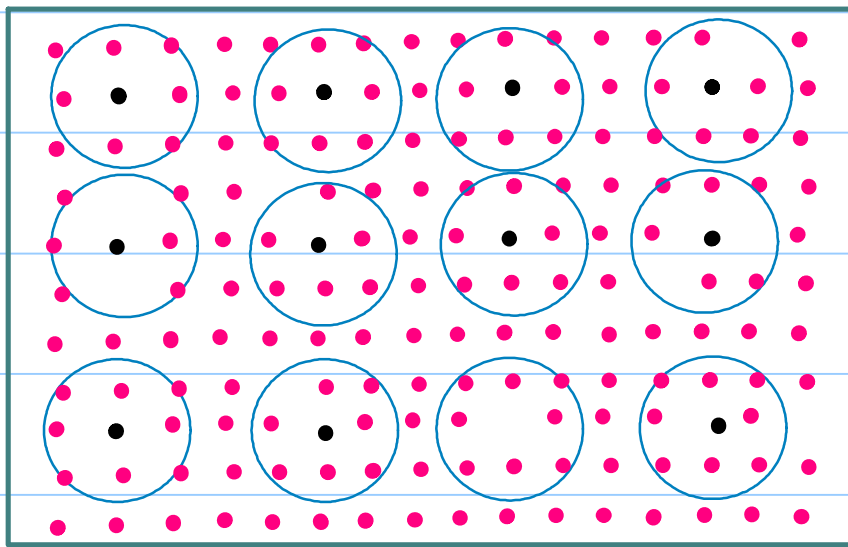
افزایش $k \leftarrow$ افزایش تعداد کدها؟

افزایش $d \leftarrow$ افزایش فاصله کدها؟

Bounds on Codes.

• $A_q(n, d)$ = ماکزیم اندازۀ کد بهر n, d معنی

• Gilbert - Varshamov Bound



تعداد کدها = سایز کد = M

کدها به شعاع $d-1$ و قطر بزرگتر در هر کدها رسم شدند

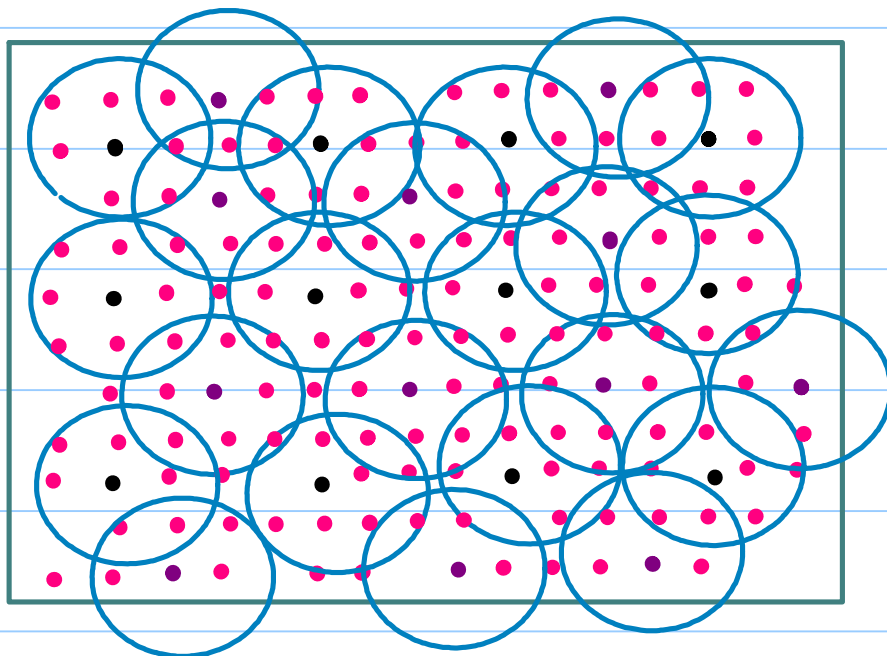


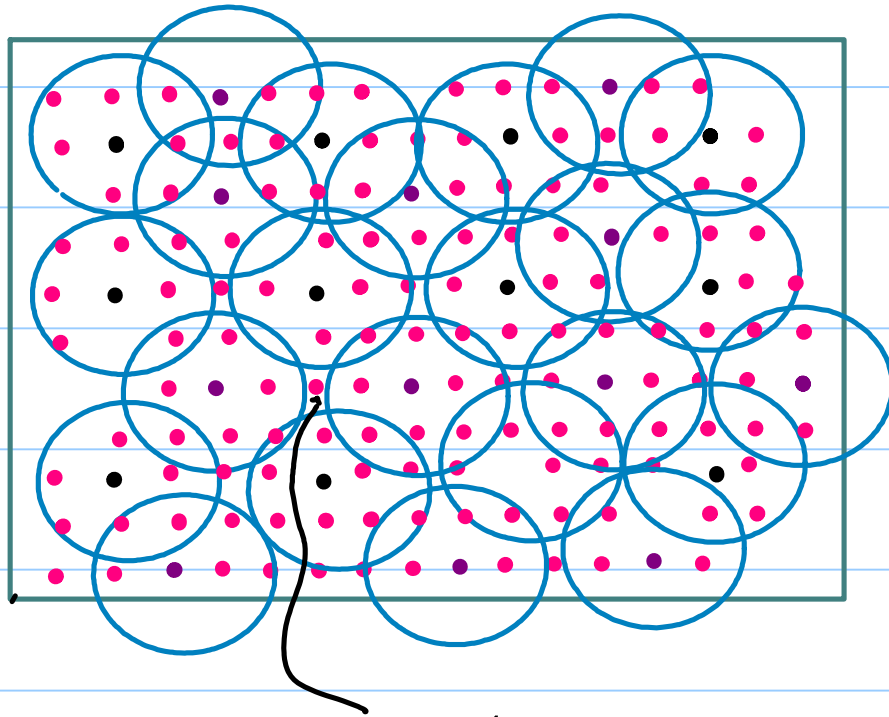
اگر n تا از حروف را تغییر دهیم یک کلمه درست می‌شود یا نه؟
 تعداد را می‌توانیم کلمه دیگری بنویسیم یا نه؟
 تعداد این کلمات:

$$\binom{n}{i} (q-1)^i$$

تعداد فعلی که در n تکرار d است یک کلمه تکرار گرفته از n است:

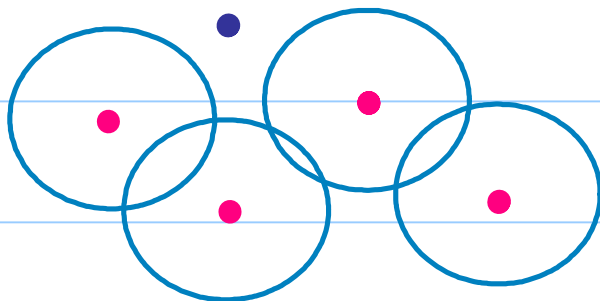
$$\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i$$





این نقطه را می توان به C اضافه کرد و یک k دیگر ساخت.

هرگاه دو حرکت که یک گره به شعاع d را رسم کند، اجتماع تمام این گره ها
 یک گره در $\mathbb{F}_7^n$ باشد. زیرا اگر چنین نباشد، یعنی این k یک
 گره جدید است که از حرکت k دیگر حاصل می شود. d بیشتر است.



پس این که عدد زیر توان باشد C افشانده و به n بزرگتر رفت. بنابراین

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

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

- Singleton Bound

$$d \leq n - k + 1$$

or

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

proof:

نگاشت زیر را در نظر بگیرید:

$$\phi : C \longrightarrow \mathbb{F}_q^{n-d+1}$$

$$\phi(\underbrace{\bullet \bullet \bullet \bullet \bullet \bullet \bullet}_{n-d+1} | \underbrace{\bullet \bullet}_{d-1}) = \bullet \bullet \bullet \bullet \bullet \bullet \bullet$$

این نگاشت یک یک به یک است. زیرا هر دو بردار، بردشان از d بزرگتر است، با یک کسب فقط $d-1$ حرف نمی توان در آنها مثل همگی.

چون نگاشت یک به یک است ←

$$|C| \leq q^{n-d+1}$$

$$k \leq n-d+1. \quad \square$$

بنابراین، بزرگترین در حد می:

$$\frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i} \leq A_q(n, d) \leq q^{n-d+1}$$

- Hamming Bound

if a Code can correct t errors, then

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

where $t = \left\lfloor \frac{d-1}{2} \right\rfloor$

proof: if the code corrects t errors $\rightarrow$

$$d > 2t + 1$$

all the spheres of radius t are disjoint. $\rightarrow$

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

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

$$\frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i} \leq A_q(n, d) \leq q^{n-d+1}$$

قضیه: اگر در ماتریس H ، هر $d-1$ ستون مستقل خطی باشند، آنگاه رتبه آن $d-1$ است.

اثبات: لزوم این حرف استفاده کنیم. فرض کنیم رتبه آن d کمتر از $d-1$ است. (استدلال برعکس در این مورد کاربرد دارد). در این صورت چون d خطی است پس حتماً یک d که مثل b وجود دارد که در آن $d-1$ است. یعنی در

$$b = b_1 b_2 b_3 \dots b_n$$

$d-1$ از b_i غیر صفر هستند مثل

$$b_{i_1}, b_{i_2}, \dots, b_{i_{d-1}}$$

لذا آنچه که $\forall b, b^t H b = 0$,

$$H = (h^{(1)}, h^{(2)}, \dots, h^{(n)})$$

$$\Rightarrow (b_1, b_2, \dots, b_n) \begin{pmatrix} h^{(1)} \\ h^{(2)} \\ \vdots \\ h^{(n)} \end{pmatrix} = b_{i_1} h^{(i_1)} + b_{i_2} h^{(i_2)} + \dots + b_{i_{d-1}} h^{(i_{d-1})} = 0$$

غیر صفر

بنابرین کتون $h^{(i)} \dots h^{(i_{\max})}$ مستقل نمی‌باشند و قف لازمائی بران خلف
 ثابت می‌گردد.

Hamming Codes over F_q^n .

که در Hamming که می‌باشند که یک خطا را تصحیح می‌کنند. بنابرین
 $d = 3$.

پس در ماتریس H هر دو ستونی مرتب است لازم مستقل باشند
 یعنی ضرب هم نباشند.

$$m := n - k \quad \leftarrow \begin{cases} n = H \\ k = \text{تعداد} \end{cases}$$

$$H_{m \times n}.$$

H دارای n ستون و m سطر است که هیچ دو سطر یکی با هم مشابه نیستند.

تعدادی برابر q^m است :

$$n = \frac{q^m - 1}{q - 1}$$

اثبات : تمام بردار m مولفه در F_q^m تعدادی برابر است :

$$q^m - 1$$

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} \dots$$

برای هر بردار $(q-1)$ بردار دیگر وجود دارد که با آن متعام است. بنابراین

تعداد کل بردار پس از حذف بردار $\vec{0}$ هم متعام است :

$$n = \frac{q^m - 1}{q - 1}$$

$$\Rightarrow k = n - m = \frac{q^m - 1}{q - 1} - m$$

$$R = 1 - \frac{m}{n} = 1 - \frac{m(q-1)}{q^m - 1}$$

$$n = 2^m - 1$$

$$q=2 : \text{JLs}$$

$$k = 2^m - 1 - m \quad R = \frac{k}{n}$$

$$m=3 \rightarrow n=7, k=4 \Rightarrow R = \frac{4}{7}$$

$$m=4 \rightarrow n=15, k=11 \Rightarrow R = \frac{11}{15}$$

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

$$GH^T = 0$$

$$w \in G \rightarrow w = x_1 x_2 x_3 x_4 x_5 \dots x_{15}$$

$$\rightarrow \begin{cases} x_1 + x_3 + x_5 + x_7 + x_9 + x_{11} + x_{13} + x_{15} = 0 \\ x_2 + x_3 + x_6 + x_7 + x_{10} + x_{11} + x_{14} + x_{15} = 0 \\ x_4 + x_5 + x_6 + x_7 + x_{12} + x_{13} + x_{14} + x_{15} = 0 \\ x_8 + x_9 + x_{10} + x_{11} + x_{12} + x_{13} + x_{14} + x_{15} = 0 \end{cases}$$

الطريقة: ← H

$$H = [I_{4 \times 4} \mid A_{4 \times 11}]$$

$$H^T = \left[\begin{array}{c} I_{4 \times 4} \\ A_{11 \times 4}^T \end{array} \right]$$

$$G = [A_{11 \times 4}^T \mid I_{11 \times 11}]$$

$$GH^T = A^T + A^T = 0.$$

$$H = \left[\begin{array}{cccc|cccccccccccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{array} \right]$$

$$m=6 \rightarrow n=63, k=57 \Rightarrow R = \frac{57}{63}$$

■ ننتهي ■