تئوری اطلاعات و کدینگ : جلسه 22 ، 24 آذر 99

---

* ادامه بحث کدهای خطی
* ماتریس مولد و ماتریس چک یک کد خطی
* مثال هایی از کدهای خطی

---

* کد خطی : یک زیر فضای برداری از فضای $\mathbb{F}_q^n$.

لـ یک فضای برداری n بعدی که بر روی میدان متناهی $\mathbb{F}_q$ که q عضو دارد تعریف شده است.

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in \mathbb{F}_q^n \quad , \quad x_i \in \mathbb{F}_q$$

درنتیجه برای هر دو $\underline{c}_1, \underline{c}_2 \in \mathcal{C}$ داریم:

$$\forall a_1, a_2 \in \mathbb{F}_2 : \quad a_1 \underline{c}_1 + a_2 \underline{c}_2 \in \mathcal{C}$$

⇐ کدهای خطی یک ساختار دارند:

$$\forall \underline{c} \in \mathcal{C} \longrightarrow \underline{c} + \mathcal{C} = \mathcal{C}$$

⇐ فضای اطراف هر کدواژه $\underline{c}$ مانند یکدیگر هستند.

همچنین برای کدهای خطی نشان دادیم:

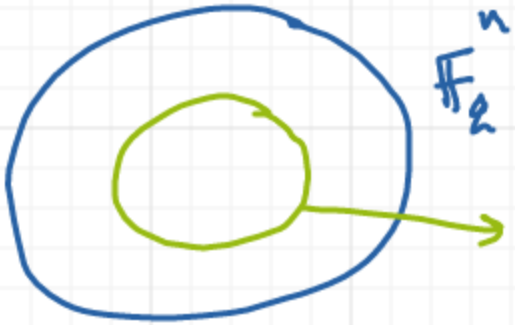
$$d_{min}(\mathcal{C}) = \min_{\substack{\underline{x}, \underline{y} \in \mathcal{C} \\ \underline{x} \neq \underline{y}}} d_H(\underline{x}, \underline{y}) = \min_{\substack{\underline{x} \in \mathcal{C} \\ \underline{x} \neq 0}} W_H(\underline{x})$$

* نحوه نمایش یک خطی C:

$C = [n, k]_q$

n: طول کد

q: بعد فضای C



q^k عدد کد واژه دارد ← تعداد پیام ها قابل کد کردن:

$M = q^k$

$C : \underbrace{\mathbb{F}_q^k}_{\text{از رشته های به طول } k \text{ بر روی میدان } \mathbb{F}_q} \longmapsto \mathbb{F}_q^n$ ← یک نگاشت

* تعریف توسط ماتریس مولد (Generator Matrix):

فرض کنید زیرفضای $\mathcal{C}$ یک k پایه $\underline{g}_1 \dots \underline{g}_k$ داشته باشد. پس:

$$\forall \underline{c} \in \mathcal{C} \Rightarrow \exists\ a_1, \dots, a_k \in \mathbb{F}_2 : \underline{c} = a_1 \underline{g}_1 + \dots + a_k \underline{g}_k$$

یک ماتریس مولد G برای کد $\mathcal{C}$:

$$G = \begin{bmatrix} — & \underline{g}_1 & — \\ & \vdots & \\ — & \underline{g}_k & — \end{bmatrix}_{k \times n} \in \mathbb{F}_2^{k \times n}$$

روش انکدکردن:

$$\underline{a} \in \mathbb{F}_2^k \xrightarrow{G} \underline{a}G$$

* روش تمایلی دوم: ماتریس چک (Parity check matrix):

• ضرب داخلی بین دو بردار $\underline{x}, \underline{y}$ که $\underline{x}, \underline{y} \in \mathbb{F}_2^n$:

و اتفاقا یک ضرب داخلی به معنای دقیق کلمه نیست)

$$\langle \underline{x}, \underline{y} \rangle = \sum_{i=1}^{n} x_i y_i$$

ولی به هر حال اگر $\langle \underline{x}, \underline{y} \rangle = 0$ می‌گوییم که $\underline{x}$ بر $\underline{y}$ عمود است.

بایع با اصناف گفت

تعریف: کد دوگان $C^\perp$ برای کد C :

$$C^\perp = \{ \underline{w} \in \mathbb{F}_2^n \mid \langle \underline{w}, \underline{v} \rangle = 0 \quad \forall \underline{v} \in C \}$$

می‌توان نشان داد که $C^\perp$ (orthogonal complement) خود یک زیرفضای $\mathbb{F}_2^n$ است $\Leftarrow$ خود $C^\perp$ یک کد خطی است.

چند خاصیت :

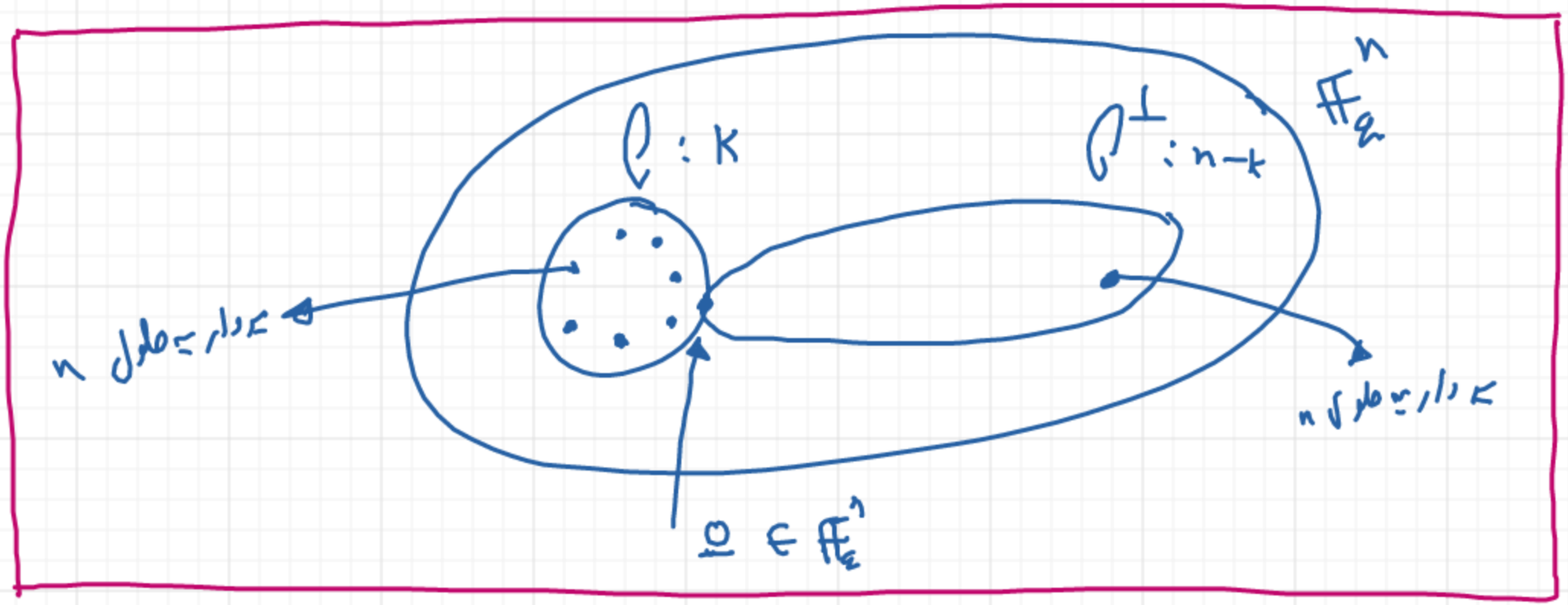
① $C \cap C^\perp = \{\underline{0}\}$

② $\dim(C^\perp) = n - k$

پس اگر $\underline{h}_1, \dots, \underline{h}_{n-k}$ پایه‌های فضای $C^\perp$ باشند، ماتریس چک کد C را به صورت زیر تعریف می‌کنیم :

$$H = \begin{bmatrix} \text{---} & \underline{h}_1 & \text{---} \\ & \vdots & \\ \text{---} & \underline{h}_{n-k} & \text{---} \end{bmatrix}_{(n-k)\times n} \in \mathbb{F}_2^{(n-k)\times n}$$

$\forall \underline{x} \in \mathcal{C} \iff H\underline{x} = \underline{0} \to \in \mathbb{F}_q^{n-k} \iff$



قضیه: فرض کنید H ماتریس چک کد خطی $\mathcal{C}$ باشد. آنگاه:

هر مجموعه متشکل از $d-1$ ستون H را در نظر بگیریم، مستقل خطی باشد $\iff d_{min}(\mathcal{C}) \geq d$

* مثال هایی از کد های خطی :

. کد های تکرار شونده (Repetition Codes) :

$$[n, 1, n]_2 \leftarrow \mathcal{C} = \{ \underbrace{0 \cdots 0}_{\in \mathbb{F}_2^n} , \underbrace{1 \cdots 1}_{\in \mathbb{F}_2^n} \}$$

($d_{min}(\mathcal{C})$: فاصله مینیمم)

نرخ کد ← نرخ بدی دارد : $R = \frac{\log_2 |\mathcal{C}|}{n} = \frac{1}{n} \xrightarrow{n \to \infty} 0$

$$G = [1 \cdots 1]_{1 \times n}$$

encoding : aG

$\hookrightarrow \in \{0, 1\}$

$$H = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & 0 \cdots & 0 \\ \vdots & & \ddots & & \\ 1 & 0 & 0 \cdots & & 0\ 1 \end{bmatrix}_{(n-1) \times n}$$

مثال دوم: کد همینگ $[7,4,3]_2$

$$d_1\ d_2\ d_3\ d_4 \longmapsto d_1\ d_2\ d_3\ d_4\ P_1\ P_2\ P_3$$

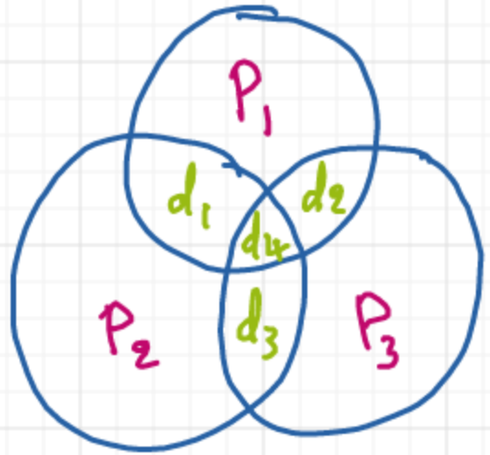
Xor : f_2 جمع پیمانه‌ای

$$P_1 = d_1 + d_2 + d_4$$

$$P_2 = d_1 + d_3 + d_4$$

$$P_3 = d_2\ d_3 + d_4$$

$\Leftarrow$



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

یک ماتریس مولد برای کد همینگ:

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}_{4\times 7}$$

$d_1\ d_2\ d_3\ d_4\ P_1\ P_2\ P_3$

یک ماتریس چک برای کد هیمنگ:

$$H=\left[\begin{array}{ccccc|ccc} 1 & 1 & 0 & 1 & & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & & 0 & 0 & 1 \end{array}\right]_{3\times 7}$$

اگر ستون های H را در نظر بگیریم: هر دو ستون مستقل خطی هستند ← $d_{min} \geq 3$

از طرف دیگر: ستون های اول و دوم و سوم وابسته خطی هستند. ← $\boxed{d_{min}=3}$

قبلا دیدیم که اگر یک کدی $d_{min} \geq 2t+1$ داشته باشد ← همیشه می‌تواند تا t خطا را اصلاح کند.

برای کد هیمنگ $d_{min}=3$ ⇐ $t=1$ خطا را اصلاح کند.

* یا قرص اینکه یک خطا اتفاق افتاده : بررسی سارومیرای دیکودکردن کد همینگ :

$\underline{x} \longrightarrow \underline{y} = \underline{x} + \underline{e}_i$

$\underline{x}$ ← رشته اولیه ← $\in \mathbb{F}_2^7$

$\underline{y}$ ← رشته دریافتی

$\underline{e}_i$ ← بردار خطا : همه‌جا صفر، در محل ام 1

$H\underline{y} = \underbrace{H\underline{x}}_{=\underline{0}} + H\underline{e}_i = H\underline{e}_i = [\,]$ می‌دانیم:

ستون ام H

$[0\ 0\ 0\ 1\ 0\ \cdots] \in \mathbb{F}_2^7$

↑ محل ام