تئوری اطلاعات و کدینگ : جلسه 21 ، شنبه 22 آذر 99

* برخی تعاریف ریاضی مقدماتی : گروه، میدان، فضای برداری، زیر فضای یک فضای برداری
* تعریف کدهای خطی
* فاصله همینگ و وزن همینگ
* ماتریس مولد و ماتریس چک یک کد خطی
* مثال‌هایی از کدهای خطی

---

* یک گروه یک مجموعه نیمه‌تهی G با یک عملگر باینری $*$ که خواص زیر را ارضا کند:

① $a, b \in G : \quad a * b \in G$

② Associativity یا شرکت‌پذیری : $a, b, c \in G$

$$a * (b * c) = (a * b) * c$$

④ Inverse (عضو معکوس) : $\forall a \in G : \quad \exists a^{-1} \in G$

$$\Rightarrow a * a^{-1} = a^{-1} * a = 1$$

③ Identity (عضو خنثی)

$$: \quad 1 \in G : \quad a * 1 = 1 * a = a$$

* گروه آبلی (Abelian group) : علاوه بر خواص بالا داریم:

$$\forall a, b \in G : \quad a * b = b * a$$

* تعریف میدان (Field):

یک مجموعه F است که حداقل دو عضو 1 و 0 دارد و همراه با دو عملگر "+" و "*" که خواص زیر را دارد:

① اعضای F تحت عمل "+" تشکیل یک گروه آبلی با عضو خنثی 0 می دهد.

② اعضای $F/\{0\}$ تحت عمل "*" تشکیل گروه آبلی با عضو خنثی 1 می دهد.

③ پخشی پذیری ضرب نسبت به جمع:

$\forall a,b,c \in F$ $\quad a*(b+c) = a*b + a*c$

$(a+b)*c = a*c + b*c$

* اعداد $\mathbb{R}$ و $\mathbb{Q}$ و $\mathbb{C}$ تشکیل یک میدان نامتناهی می دهند.

* $\mathbb{Z}$: یک میدان نیست.

* $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$ با عمل جمع و ضرب mod p اگر p اول باشد $\Leftarrow$ یک میدان متناهی با p عضو.

* به صورت خاص می توانیم متناهی : $\mathbb{Z}_2 = \mathbb{F}_2$

$\mathbb{F}_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

* تعریف: فضای برداری (Vector Space)

یک فضای برداری بر روی میدان $\mathbb{F}$ یک مجموعه V که یک عمل با بیشتر جمع دارد و یک ضرب اسکالر بین اعضای میدان و اعضای V تعریف شده است، و خواص زیر را دارد:

① $\forall u,v \in V : \quad u+v = v+u$

② $u,v,w \in V : \quad (u+v)+w = u+(v+w)$

$a,b \in \mathbb{F} \qquad (ab)v = a(bv)$

ضرب میدان $\mathbb{F}$ — ضرب اسکالر — حاصل اسکالر

③ عضو خنثی جمع برداری $\quad \exists\, \underline{0} \in V : \forall v \in V$

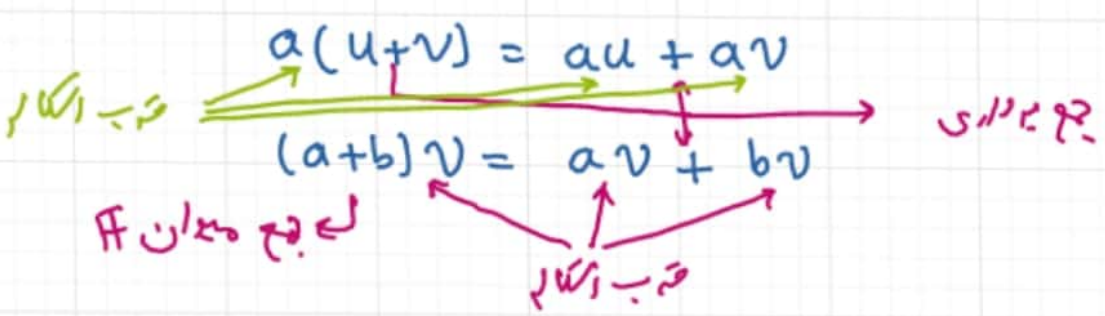
$$\underline{0}+v = v+\underline{0} = v$$

④ عضو معکوس برداری : $\forall v \in V \Rightarrow \exists\, w \in V : \quad v+w = \underline{0}$

⑤ $\forall v \in V : \quad 1v = v$

↳ عضو خنثی عمل ضرب میدان $\mathbb{F}$

⑥ خاصیت شرکتی : $\forall a,b \in \mathbb{F}\ ,\ \forall u,v \in V :$



* مثال: $\mathbb{R}^n$ یک فضای برداری n بعدی است.

* تعریف: زیرفضای یک فضای برداری

می‌گوییم U یک زیرفضای فضای برداری V است اگر که $U \subseteq V$

و U خود به تنهایی یک فضای برداری با همان میدان فضای برداری V را باشد.

مثلا $\mathbb{R}^2$ یک زیرفضای $\mathbb{R}^3$ است.

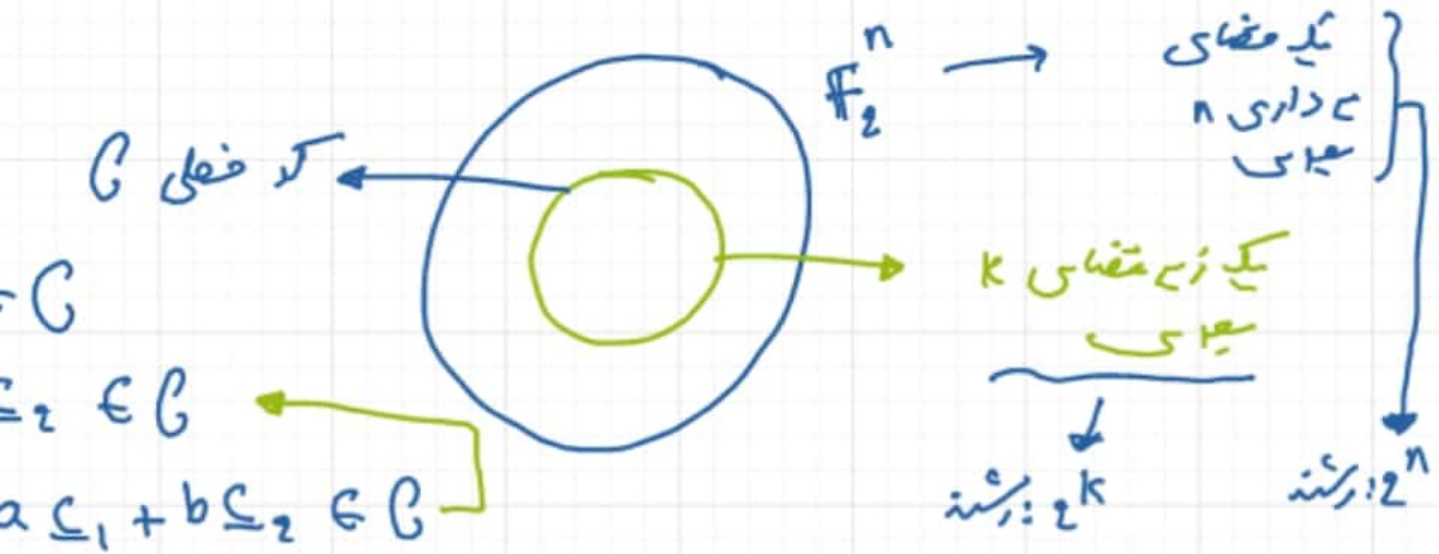
---

* تعریف کدهای خطی (linear codes)

کدهای خطی را بر روی میدان‌های متناهی تعریف می‌کنیم.

یک کد خطی $C \subseteq \mathbb{F}^n$ یک زیرفضای برداری از فضای برداری $\mathbb{F}^n$ است.

در ادامه $\mathbb{F} = \mathbb{F}_2$ و بنابراین کدواژه‌های ما دنباله‌هایی از 0 و 1 هستند.



$c_1, c_2 \in C$

$\Rightarrow c_1 + c_2 \in C$

$a, b \in \mathbb{F}_2 : \; a c_1 + b c_2 \in C$

عملا کد خطی C یک زیرفضای باینری به طول k برای گیرنده و یک زیرفضای باینری به طول n تولید می‌کند $\Leftarrow$ تعداد پیام‌های این کد $M = 2^k$

---

* فاصله همینگ بین دو کلمه $\underline{x}, \underline{y} \in \sum$ تعریف می‌شود:

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

* وزن همینگ یک کلمه $\underline{x} \in \sum$

$$w_H(\underline{x}) = d_H(\underline{x}, \underline{0})$$

---

* کمترین فاصله یک کد $\mathcal{C}$:

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

* برای کدهای خطی می‌توانیم بنویسیم:

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

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

$$= \min_{\substack{\underline{x},\underline{y}\in\mathcal{C} \\ \underline{x}\neq\underline{y}}} w_H(\underline{x}-\underline{y})$$

$$= \min_{\substack{\underline{x}\in\mathcal{C} \\ x\neq\underline{0}}} w_H(\underline{x})$$

* درکدهای خطی : اگر فضای حول کدواژه $\underline{c}$ دلخواه را در شکل بگیریم، این فضا مانند فضا اطراف کدواژه $\underline{0}$ است.

مثلا فضای حول این کدواژه هم مانند بقیه کدواژه ها است.

فرض کنید $\underline{c}_1, \dots, \underline{c}_l$ فاصله همینگ d از کدواژه $\underline{c}$ داشته باشند.

$\Leftarrow$ $\underline{c}_1 - \underline{c}, \dots, \underline{c}_l - \underline{c}$ فاصله همینگ d از کدواژه صفر دارند.