Лекция №5
Тождества Маквильямс

Связь м/д. кол-вом векторов заданного веса в C и кол-вом векторов некоторого веса в $C^\perp$.

1. Предв. сведения: Анализ Фурье в булевом кубе

$\mathcal{F}_n = \{ f : \{0,1\}^n \to \mathbb{R} \}$ – мн-во всех ф-ий, принимающих действительные значения, определённые на $\{0,1\}^n$.

$\mathcal{F}_n$ – векторное пр-во размерности 2^n с базисом

$$\{e_\alpha : \alpha \in \{0,1\}^n\} \qquad e_\alpha = \delta_{x\alpha} = \begin{cases} 1, & x=\alpha \\ 0, & \text{иначе} \end{cases}.$$

Опр-ие 1 Внутреннее пр-ие $f, g \in \mathcal{F}_n$: $\langle f, g \rangle = \frac{1}{2^n} \sum\limits_{\substack{x \text{ - обл.} \\ \text{опр-ия}}} f(x) \cdot g(x) = \mathbb{E}_x [f(x) \cdot g(x)]$

Лемма 1 $\forall$ лин. бин. кода $C \subseteq \{0,1\}^n$ и $\alpha \in \{0,1\}^n$

$$\sum_{c \in C} (-1)^{\alpha \cdot c} = \begin{cases} |C|, & \alpha \in C^\perp \\ 0, & \text{иначе} \end{cases}$$

внутр. пр-ие n-мерных векторов mod 2

◁ Док-во на практике ▷

Следствие 2 Для $C = \{0,1\}^n$ $(C^\perp = \{0\})$: $\sum\limits_{c \in C} (-1)^{\alpha \cdot c} = \begin{cases} 2^n, & \alpha = 0 \\ 0, & \text{иначе} \end{cases}.$

Опр-ие 2 $\forall \alpha \in \{0,1\}^n$, определим $\chi_\alpha : \{0,1\}^n \to \mathbb{R}$
$x \mapsto (-1)^{\alpha \cdot x}$ –

характеристическая ф-ия.

Лемма 3 Ф-ии $\{\chi_\alpha\}_\alpha$ образуют ортонормированный базис $\mathcal{F}_n$, т.е.

$$\langle \chi_\alpha, \chi_\beta \rangle = \delta_{\alpha,\beta}.$$

Такой базис называется **базисом Фурье**.

$\triangle$ $$\langle \chi_\alpha, \chi_\beta \rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \chi_\alpha(x)\chi_\beta(x) = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{\alpha\cdot x}\cdot(-1)^{\beta x} = \frac{1}{2^n}\sum(-1)^{\alpha x}(-1)^{-\beta\cdot x} =$$

$$= \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{(\alpha-\beta)x} \overset{\text{Сл-ие } 2}{=} \begin{cases} 2^n\cdot\frac{1}{2^n} = 1, & \alpha-\beta=0 \ (\alpha=\beta) \\ 0, & \text{иначе} \end{cases}$$ $\blacktriangleright$.

Так как $\{\chi_\alpha\}_\alpha$ образует базис $\mathcal{F}_n$, то $\forall f\in\mathcal{F}_n$ $\exists!$ разложение по базису Фурье

$$f = \sum_\alpha \hat{f}(\alpha)\chi_\alpha, \quad \hat{f} = \langle f, \chi_\alpha \rangle$$

Пример $f(x_1,x_2) = OR(x_1,x_2) \in \{0,1\} \subset \mathbb{R}$
$(n=2)$

$$\hat{f}(00) = \langle f, \chi_\alpha \rangle = \frac{1}{4}\sum_{x\in\{0,1\}^2} f(x)\cdot\chi_{00}(x) = \frac{1}{4}\Big[0\cdot(-1)^{\langle 00,00\rangle} +$$

$$+ 1\,(-1)^{\langle 00,01\rangle} + 1\cdot(-1)^{\langle 00,10\rangle} + 1\cdot(-1)^{\langle 00,11\rangle}\Big] =$$

$$= \frac{1}{4}[0+1+1+1] = \frac{3}{4}$$

$$\hat{f}(01) = \hat{f}(10) = \hat{f}(11) = -\frac{1}{4}$$

$$\Rightarrow OR(x_1,x_2) = \frac{3}{4}\chi_{00} - \frac{1}{4}\chi_{01} - \frac{1}{4}\chi_{10} - \frac{1}{4}\chi_{11}$$

$$\Big(\underset{1}{\underset{\shortparallel}{OR(10)}} = \frac{3}{4}(-1)^{\langle 00,10\rangle} - \frac{1}{4}\cdot(-1)^{\langle 01,10\rangle} - \frac{1}{4}(-1)^{\langle 10,10\rangle} - \frac{1}{4}(-1)^{\langle 11,10\rangle} = \frac{3}{4} - \cancel{\frac{1}{4}} + \cancel{\frac{1}{4}} + \frac{1}{4} = 1.\Big)$$

Опр-ие 4 **Характеристическая ф-ия** мн-ва $S\subseteq\{0,1\}^n$:

$$\mathbb{1}_S : \{0,1\}^n \to \mathbb{R}$$

$$\mathbb{1}_S(x) = \begin{cases} 1, & x\in S \\ 0, & \text{иначе} \end{cases}$$

Лемма 5 $\forall$ линейного бинарного $C \in \{0,1\}^n$: $\widehat{1\!\!1_C} = \frac{|C|}{2^n} 1\!\!1_{C^\perp}$

$\triangleleft$ $\forall \alpha \in \{0,1\}^n$ $\widehat{1\!\!1_C} = \langle 1\!\!1_C, \chi_\alpha \rangle = \frac{1}{2^n} \sum\limits_{x \in \{0,1\}^n} 1\!\!1_C(x) \cdot \chi_\alpha(x) =$

$$= \frac{1}{2^n} \sum_{x \in C} 1 \cdot \chi_\alpha(x) = \frac{1}{2^n} \sum_{x \in C} (-1)^{\alpha \cdot x} = \begin{cases} \frac{1}{2^n} \cdot |C|, & \alpha \in C^\perp \\ 0, & \text{иначе} \end{cases}.$$

т.е. $\widehat{1\!\!1_C}(\alpha) = \frac{|C|}{2^n} 1\!\!1_{C^\perp}(\alpha)$ $\forall \alpha \in \{0,1\}^n$ $\blacktriangleright$

2. Тождества МакВильямс

Опр-ие 6 $\forall S \subseteq \{0,1\}^n$, определим $W_i^S = |\{x \in S : wt(x) = i\}|$

Весовым распределением для S назовём вектор длины $n+1$

$$W^S = [W_0^S, W_1^S, .., W_n^S]$$

Пример $S = \{0000, 0101, 1010, 1111\}$: $W^S = [1, 0, 2, 0, 1]$

Рассмотрим C - лин. код, $C^\perp$ - его дуальный, $i \in \{0, .., n\}$

$$W_i^{C^\perp} = \sum_{\substack{\alpha \in \{0,1\}^n \\ wt(\alpha) = i}} 1\!\!1_{C^\perp}(\alpha) \overset{\text{Лемма 5}}{=} \sum_{\substack{\alpha \in \{0,1\}^n \\ wt(\alpha) = i}} \frac{2^n}{|C|} \cdot \widehat{1\!\!1_C}(\alpha) = \frac{2^n}{|C|} \sum_{\alpha : wt(\alpha) = i} \langle 1\!\!1_C(\alpha) \cdot \chi_\alpha \rangle$$

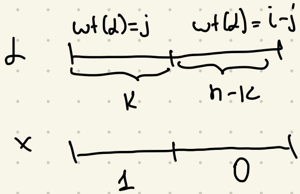
$$= \frac{\cancel{2^n}}{|C|} \sum_{\alpha : wt(\alpha) = i} \frac{1}{\cancel{2^n}} \sum_{x \in \{0,1\}^n} 1\!\!1_C(x) \cdot (-1)^{\alpha \cdot x} = \frac{1}{|C|} \sum_{x \in \{0,1\}^n} \underbrace{1\!\!1_C(x) \cdot \sum_{\alpha : wt(\alpha) = i} (-1)^{\alpha \cdot x} \ldots}_{(*)}$$

Лемма 6 $\forall x \in \{0,1\}^n$, $wt(x) = k$ $\sum\limits_{\alpha : wt(\alpha) = i} (-1)^{\alpha \cdot x} = \sum\limits_{j=0}^{i} (-1)^j \binom{k}{j} \binom{n-k}{i-j}$.

$\triangleleft$ Значение $\sum\limits_{\alpha : wt(\alpha) = i} (-1)^{\alpha \cdot x}$ в силу симметрии внутр. пр-ия зависит только от $wt(x)$, а не от позиций 1-ц в нём. $\Rightarrow$ поэтому можем полагать,

$$x = 1^k 0^{n-k}$$

$\forall\ \alpha: wt(\alpha)=i$: имеет j единиц на первых k координатах $\Rightarrow$ $i-j$ единиц на оставшихся $n-k$ координатах



В таком случае, $(-1)^{\alpha\cdot x}=(-1)^j$

Кол-во всевозможных α с таким весовым распределением есть

$$\binom{k}{j}\binom{n-k}{i-j}.$$

Лемма следует из того, что j принимает значения от 0 до i ∎

<u>Замечание</u> $\binom{a}{b}=0$ для $a<b$.

<u>Опр-ие 7</u> Величина $K_i(k)=\sum\limits_{j=0}^{i}\binom{k}{j}\binom{n-k}{i-j}$ – многочлен Кравчука в k

$$K_i(x)=\sum_{j=0}^{i}\binom{x}{j}\binom{n-x}{i-j}$$ – i-ым многочлен Кравчука

$\deg K_i(x)=i$, $K_0(x)=1$, $K_1(x)=n-2x$

Продолжим вычислять $(*)$:

$$W_i^{C^\perp}=\frac{1}{|C|}\sum_{x\in\{0,1\}^n}1\!\!1_C(x)\cdot\sum_{\alpha:wt(\alpha)=i}(-1)^{\alpha\cdot x}\overset{\text{лемма 6}}{=}\frac{1}{|C|}\sum_{x\in C}1\cdot K_i(wt(x))$$

$$=\frac{1}{|C|}\sum_{k=0}^{n}\sum_{\substack{x\in C\\ wt(x)=k}}K_i(k).$$

В итоге,

$$\boxed{W_i^{C^\perp}=\frac{1}{|C|}\cdot\sum_{k=0}^{n}W_k^{C}\cdot K_i(k)}\quad\forall i=\overline{0,n}.$$

↑ тождество Мак Вильямс

Генерирующая ф-ция вектора W^C – многочлен из $\mathbb{Z}[x]$

$$W^C(x) := \sum_{i=0}^{n} W_i^C \cdot x^i$$ – весовой энумератор

$$W^C(x,y) = y^n \cdot W^C\left(\frac{x}{y}\right) = \sum_{i=0}^{n} W_i^C \, x^i \cdot y^{n-i}$$ – гомогенная версия весового энумератора

Тождество МакВильямс для весового энумератора

$$W^{C^\perp}(x,y) = \frac{1}{|C|} W^C(y-x,\, y+x)$$

Пример

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$ – проверочная матрица C_{HAM} (или порождающая $\underbrace{C^\perp_{HAM}}_{\text{simplex code}}$)

$$C^\perp_{HAM} = \{\, 0000000,\ 0001111,\ 1010101,\ 1011010,\ 0110011,\ 0111100,\ 1100110,\ 1101001 \,\}$$

$|C^\perp_{HAM}| = 8$ $\qquad (|C|_{HAM} = 2^4 = 16)$

$$W^{C^\perp_{HAM}} = \underbrace{1}_{W_0^{C^\perp_{HAM}}} \cdot x^0 \cdot y^7 + 7 \cdot x^4 \cdot y^3$$

Тогда для C_{HAM} $\quad W^{C_{HAM}}(x,y) = \frac{1}{8} W^{C^\perp_{HAM}}(y-x,\, y+x) =$

$$= \frac{1}{8}\left((y+x)^7 + 7 \cdot (y-x)^4 \cdot (y+x)^3 \right) = x^7 + 7x^4y^3 + 7x^3y^4 + y^7$$

Вывод: $[7,4,3]$ код Хэмминга содержит 1 вектор веса 0
1 —"— 7
7 векторов веса 3 и 4.