Лекция №5

Тождества МакВильямс

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

0. Предварительные сведения: анализ Фурье в булевом кубе

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

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

$\{ e_\alpha : \alpha \in \{0,1\}^n \}$:

$$e_\alpha = \delta_{x\alpha} = \begin{cases} 1, & x = \alpha \\ 0, & \text{иначе} \end{cases}$$

Опр-ие 1 Внутреннее пр-ие $f, g \in \mathcal{F}_n$:

$$\langle f, g \rangle = \frac{1}{2^n} \sum_{\substack{x\text{ - обл.} \\ \text{опр-ия } f, g}} f(x) \cdot g(x) = \mathbb{E}_x [f(x) \cdot g(x)]$$

Лемма 1 $\forall$ лин. бинарного кода $C \subseteq \{0,1\}^n$

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

$\alpha \cdot c$ — внутр. пр-ие n-мерных векторов mod 2

◁ Док-во на практике ▷.

Следствие 2 Для $C = \{0,1\}^n$ $(C^\perp = \{0\})$:

$$\sum_{c \in C} (-1)^{\alpha c} = \begin{cases} 2^n, & \alpha = 0 \\ 0, & \text{иначе}. \end{cases}$$

Опр-ие 2 $\forall \alpha \in \{0,1\}^n$ определим $\chi_\alpha : \{0,1\}^n \to \mathbb{R}$ — характеристическая функция

$$x \longmapsto (-1)^{\alpha \cdot x}$$

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

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

Это базис называется **базисом Фурье**.

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

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

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

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

Пример $f(x_1,x_2) = OR(x_1,x_2) \in \{0,1\}$

$n=2$

$$\hat{f}(00) = \frac{1}{4} \sum_{s\in\{0,1\}^2} f(s)\,\chi_{00}(s) = \frac{1}{4}\Big(0\cdot(-1)^{\langle 00,00\rangle} + 1\cdot(-1)^{\langle 01,00\rangle} + 1\cdot(-1)^{\langle 10,00\rangle} + 1\cdot(-1)^{\langle 11,00\rangle}\Big)$$

$$= \frac{1}{4}\big(0+1+1+1\big) = \frac{3}{4}$$

$$\hat{f}(01) = \frac{1}{4}\sum f(s)\,\chi_{01}(s) = -\frac{1}{4}$$

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

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

Опр-е 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 $\forall$ лин. кода $C \subseteq \{0,1\}^n$: $\widehat{\mathbb{1}_C} = \dfrac{|C|}{2^n} \mathbb{1}_{C^\perp}$

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

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

Т.е. $\quad \widehat{\mathbb{1}_C}(\alpha) = \dfrac{1}{2^n} |C| \cdot \mathbb{1}_{C^\perp}(\alpha) \quad \forall \alpha \in \{0,1\}^n$. $\blacktriangleright$

1. Тождества МакВильямс

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

Весовым распределением для S будем понимать вектор длины $n+1$:

$$W^S = [W_0^S, W_1^S, \dots, W_n^S]$$

Пример $S = \{0000, 0101, 1010, 1111\}$

$$W^S = [1, 0, 2, 0, 1]$$

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

$$W_\ell^{C^\perp} = \sum_{\substack{\alpha \in \{0,1\}^n \\ wt(\alpha)=\ell}} 1_{C^\perp}(\alpha) = \sum_{\alpha : wt(\alpha)=\ell}' \frac{2^n}{|C|} \cdot \hat{1}_C(\alpha)$$

$$\underset{1 \Leftrightarrow \alpha \in C^\perp}{\parallel}$$

$$= \frac{2^n}{|C|} \sum_{\alpha : wt(\alpha)=\ell} \langle 1_C, \chi_\alpha \rangle =$$

$$= \frac{\cancel{2^n}}{|C|} \sum_{\alpha : wt(\alpha)=\ell} \frac{1}{\cancel{2^n}} \sum_{x \in \{0,1\}^n} 1_C(x) (-1)^{\alpha x}$$

$$= \frac{1}{|C|} \sum_{x \in \{0,1\}^\ell}' 1_C(x) \sum_{\alpha : wt(\alpha)=\ell} (-1)^{\alpha x} \qquad (*)$$

Покажем, что $\sum\limits_{\alpha : wt(\alpha)=\ell} (-1)^{\alpha x}$ зависит только от веса x.

Лемма 7 $\quad \forall x \in \{0,1\}^n,\ wt(x) = i : \quad \sum\limits_{\alpha : wt(\alpha)=\ell} (-1)^{\alpha x} = \sum\limits_{j=0}^{\ell}{}' (-1)^j \binom{i}{j}\binom{n-i}{\ell-j}$

$\triangle$ Значение $\sum\limits_{\alpha : wt(\alpha)=\ell} (-1)^{\alpha x}$ в силу симметрии зависит только от $wt(x)$, а не от позиций 1-ц в нём. $\Rightarrow$ можем полагать

$$x = 1^i 0^{n-i}.$$

$\forall \alpha$ $wt(\alpha) = \ell$ имеет j единиц на первых i поз-ях $\Rightarrow$ $\ell - j$ единиц на оставшихся $n-i$ позициях

$$\alpha: \underbrace{\overbrace{\qquad\qquad}^{wt(\alpha)=j}}_{i}\ \underbrace{\overbrace{\qquad\qquad}^{wt(\alpha)=\ell-j}}_{n-i}\ {}_n$$

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

Кол-во всевозможных α с таким весовым распр-ем

$\binom{i}{j}\binom{n-i}{\ell-j}$. Лемма следует из того, что j принимает все значения от 0 до ℓ. $\blacktriangle$

Замечание $\binom{a}{b}=0, \ a<b$

Величина $K_\ell(i)=\sum_{j=0}^{\ell}(-1)^j\binom{i}{j}\binom{n-i}{n-j}$ — многочлен Кравчука в i

$$K_\ell(x)=\sum_{j=0}^{\ell}(-1)^j\binom{x}{j}\binom{n-x}{n-j}$$ — ℓ-ый м-н Кравчука

$\deg K_\ell(x)=\ell$

$K_0(x)=1, \quad K_1(x)=n-2x$

Продолжим вычислять (*)

$$W_\ell^{C^\perp}=\frac{1}{|C|}\sum_{x\in\{0,1\}^n}\mathbb{1}_C(x)\sum_{\alpha:\,wt(\alpha)=\ell}(-1)^{\alpha x}=$$

$$=\frac{1}{|C|}\sum_{x\in C}1\cdot K_\ell(wt(x))=$$

$$=\frac{1}{|C|}\sum_{i=0}^{n}\sum_{\substack{x\in C\\ wt(x)=i}}K_\ell(i)$$

В итоге, $\boxed{W_\ell^{C^\perp}=\frac{1}{|C|}\sum_{i=0}^{n}W_i^C\cdot K_\ell(i)}$ $\forall \ell=\overline{0,n}$

Тождество Мак Вильямс

$$W^C=\{|\{x\in C: wt(x)=i\}|\}_{i=\overline{0,n}}$$

Генерирующая ф-ия списка W^C - многочлен из $\mathbb{Z}[x]$

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

Часто удобно работать с гомогенной версией весового энумератора

$$W^C(x,y) = y^n \cdot W^C\left(\frac{x}{y}\right) = \sum_{i=0}^{n} w_i^C x^i y^{n-i}$$

Тождество Мак Вильямс для весового энумератора имеет вид:

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

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 C_{HAM} или порождающая $C_{HAM}^\perp$ (simplex code)

$n=7$

$$C_{HAM}^\perp = \{ \begin{matrix} 0000000 & 0001111 \\ 1010101 & 1011010 \\ 0110011 & 0111100 \\ 1100110 & 1101001 \end{matrix} \}$$

$|C^\perp| = 8$, $(|C| = 2^4 = 16)$

$$W^{C_{HAM}^\perp}(x,y) = 1 \cdot x^0 \cdot y^{7-0} + 7 \cdot x^4 \cdot y^3$$ $\leftarrow y^7 + 7x^4y^3$

Тогда для C_{HAM} выполняется $W^{C_{HAM}}(x,y) = \frac{1}{8} \cdot W^{C_{HAM}^\perp}(y-x,\, x+y)$

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

[7, 4, 3] - код Хэмминга содержит
1 вектор веса 7
1 вектор веса 0
7 векторов веса 3, 4