

$$\Rightarrow \tilde{f}(y) = \prod_{(0), (1)} (1-z)^{|\{i | y_i \neq 0\}|} (1+z)^{|\{i | y_i = 0\}|} = (1-z)^{w(y)} (1+z)^{n-w(y)}$$

Dimostrazione dell'identità di MacWilliams. Fissiamo $z \in \mathbb{C}$ e consideriamo la funzione $f(x) = z^{w(x)}$. La sua trasformata di Hadamard é:

$$\begin{aligned} \tilde{f}(y) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle y, x \rangle} z^{w(x)} \\ &= \sum_{x_1 \in \mathbb{F}_2} \cdots \sum_{x_n \in \mathbb{F}_2} (-1)^{\sum_{i=1}^n x_i y_i} z^{\sum_{i=1}^n w(x_i)} \quad (\text{si definisce } w(x) = 1 \iff x = 1) \\ &= \sum_{x_1 \in \mathbb{F}_2} \cdots \sum_{x_n \in \mathbb{F}_2} \prod_{i=1}^n (-1)^{x_i y_i} z^{w(x_i)} \\ &= \prod_{i=1}^n \left(\sum_{x \in \mathbb{F}_2} (-1)^{x y_i} z^{w(x)} \right) \quad (0) \end{aligned}$$

Il termine $\sum_{x \in \mathbb{F}_2} (-1)^{x y_i} z^{w(x)} \stackrel{\mathbb{F}_2 = \{0, 1\}}{=} 1 + (-1)^{y_i} z$ é uguale a $1 + z$ se $y_i = 0$, o ad $1 - z$ se $y_i = 1$. Segue che $\Rightarrow$

$$\tilde{f}(y) = (1+z)^{n-w(y)} (1-z)^{w(y)} \quad (2)$$

Quindi

$$\begin{aligned} A_{C^\perp} &\stackrel{\text{eq. 5.1.1, pg 11}}{=} \sum_{x \in C^\perp} z^{w(x)} = \sum_{x \in C^\perp} f(x) \\ &= \frac{1}{\#C} \sum_{y \in C} \tilde{f}(y) \quad \text{per il lemma 5.1} \\ &\stackrel{(2)}{=} 2^{-k} \sum_{y \in C} (1+z)^{n-w(y)} (1-z)^{w(y)} \\ &= 2^{-k} (1+z)^n \sum_{y \in C} \left(\frac{1-z}{1+z} \right)^{w(y)} \\ &\stackrel{\uparrow}{=} 2^{-k} (1+z)^n A_C \left(\frac{1-z}{1+z} \right) \end{aligned}$$

da cui la tesi. $\square$

eq. 5.1.1 pg 11

Applicazione.

Usiamo la formula di MacWilliams per calcolare la distribuzione di pesi di un codice di Hamming binario, di tipo $[2^r - 1, 2^r - 1 - r, 3]$. Per fare ciò prima dobbiamo conoscere la distribuzione dei pesi del suo duale.