d.h. $\chi(a+b) = \chi(a)\cdot\chi(b)$ für alle $a, b \in A$ gilt.

Dann ist

$$\sum_{x\in A} \chi(x) = \begin{cases} 0, & \text{falls } \chi \neq 1 \\ |A|, & \text{falls } \chi = 1. \end{cases}$$

<u>Bew.:</u> Der Fall $\chi = 1$ ist klar. Sei $\chi \neq 1$. Wähle $a \in A$ mit $\chi(a) \neq 1$. Dann gilt

$$\sum_{x\in A} \chi(x) = \sum_{x\in A} \chi(x+a) = \sum_{x\in A} \chi(x)\,\chi(a)$$

$$= \underbrace{\chi(a)}_{\neq 1} \sum_{x\in A} \chi(x) \implies \sum_{x\in A} \chi(x) = 0. \quad \boxtimes$$

Zurück zum Bew. der MacWilliams Identität:

Wähle $\chi : \mathbb{F}_q \to \mathbb{C}^\times$, $\chi \neq 1$.

Definiere für $u \in C$

$$g_u(X,Y) = \sum_{v\in\mathbb{F}_q^n} \chi\Big(\sum_{i=1}^n u_i v_i\Big) X^{n-w(v)} Y^{w(v)}.$$

Betrachte Summe

$$\sum_{u\in C} g_u(X,Y) = \sum_{v\in\mathbb{F}_q^n} \sum_{u\in C} \chi\Big(\sum_{i=1}^n u_i v_i\Big) X^{n-w(v)} Y^{w(v)}$$

Falls $v \notin C^\perp$, dann ist die Abbildung $u \mapsto \chi\left(\sum_{i=1}^{n} u_i v_i\right)$ ein nicht-trivialer Charakter ($\neq 1$) der Gruppe $(C,+)$.

Also (Lemma): $\displaystyle\sum_{u \in C} \chi\left(\sum_{i=1}^{n} u_i v_i\right) = 0.$

Falls $v \in C$, dann ist $\chi\left(\sum_{i=1}^{n} u_i v_i\right) = 1$ für alle $u \in C$,

d.h. $\displaystyle\sum_{u \in C} \chi\left(\sum_{i=1}^{n} u_i v_i\right) = |C|.$

Somit:

$$\sum_{u \in C} g_u(X,Y) = |C| \, W_{C^\perp}(X,Y).$$

Andererseits ist

$$g_u(X,Y) = \sum_{v_1,\dots,v_n \in \mathbb{F}_q} \prod_{i=1}^{n} \chi(u_i \cdot v_i)\, X^{1-w(v_i)}\, Y^{w(v_i)}$$

$$= \prod_{i=1}^{n} \underbrace{\sum_{t \in \mathbb{F}_q} \chi(u_i \cdot t)\, X^{1-w(t)}\, Y^{w(t)}}_{\overset{t=0}{\underbrace{\chi(0)}_{=1} X} \; + \; \overset{t \neq 0}{\left(\sum_{t \in \mathbb{F}_q \setminus \{0\}} \chi(u_i \cdot t)\right) Y}}$$

Es ist (Lemma)

$$\sum_{t \in \mathbb{F}_q \setminus \{0\}} \chi(\mu_i \cdot t) = \begin{cases} q-1, & \text{falls } \mu_i = 0 \\ -1, & \text{falls } \mu_i \neq 0 \end{cases}$$

Also

$$g_\mu(X, Y) = \left(X + (q-1)Y\right)^{n - w(\mu)} (X-Y)^{w(\mu)} .$$

Somit

$$\sum_{\mu \in C} g_\mu(X,Y) = W_C\left(X + (q-1)Y,\ X-Y \right).$$

$\boxtimes$

Bsp.: Sei $n \in \mathbb{N}$

$C \subseteq \mathbb{F}_2^n$ ein $[n, 1]$-Code mit Erzeugermatrix $G = [1 \ldots 1]$.

Dann ist $C^\perp = \{x \in \mathbb{F}_2^n : w(x) \text{ gerade}\}$.

$$W_C(X,Y) = 1 \cdot X^n Y^0 + 1 \cdot X^0 Y^n$$
$$= X^n + Y^n.$$

$$W_{C^\perp}(X,Y) = \frac{1}{2} W_C(X+Y, X-Y)$$
$$= \frac{1}{2}\left((X+Y)^n + (X-Y)^n\right)$$
$$= \frac{1}{2}\left(\sum_{i=0}^{n} \binom{n}{i} X^{n-i} Y^i + \sum_{i=0}^{n} \binom{n}{i} X^{n-i} (-1)^i Y^i\right)$$
$$= \sum_{\substack{i=0 \\ i \text{ gerade}}}^{n} \binom{n}{i} X^{n-i} Y^i.$$

D.h. $C^\perp$ enthält $\binom{n}{i}$ Codewörter vom Gewicht i, falls i gerade ist, und $C^\perp$ enthält keine Codewörter mit ungeradem Gewicht.