Weight enumerators, MacWilliams Identity & self-dual codes (Roman §§5.2, 5.4)

An $\mathbb{F}_q$-linear code $\mathcal{C}$ with parameters $[n,k,d]$ has dual code $\mathcal{C}^\perp$ with parameters $[n,n-k,d^\perp]$ in which the min. distances $d = d(\mathcal{C})$, $d^\perp = d(\mathcal{C}^\perp)$ do not determine each other uniquely.

However in her 1962 PhD thesis, MacWilliams showed that a bit more distance info about $\mathcal{C}$ and $\mathcal{C}^\perp$ will determine each other.

DEFINITION: The weight enumerators of $\mathcal{C}$ are

$$A_{\mathcal{C}}(y) := \sum_{v\in\mathcal{C}} y^{wt(v)}$$ (inhomogeneous version)

set $x=1$ $\uparrow$ $\downarrow$ replace y by y/x, then multiply by x^n

$$W_{\mathcal{C}}(x,y) = \sum_{v\in\mathcal{C}} y^{wt(v)} x^{\overbrace{n-wt(v)}^{\#\text{ of zeroes in } v}}$$ (homogeneous version)

EXAMPLES:

① The $\mathbb{F}_p$-linear n-fold repetition code $\mathcal{C}$ is $[n,1,\overset{d}{n}]$

with $\mathcal{C} = \left\{ \underbrace{\begin{bmatrix}0\\0\\\vdots\\0\end{bmatrix}}_{wt=0}, \underbrace{\begin{bmatrix}1\\1\\\vdots\\1\end{bmatrix}, \begin{bmatrix}2\\2\\\vdots\\2\end{bmatrix}, \ldots, \begin{bmatrix}p-1\\p-1\\\vdots\\p-1\end{bmatrix}}_{wt=n} \right\}$

so $A_{\mathcal{C}}(x) = 1 \cdot y^0 + (p-1)\cdot y^n = 1 + (p-1)y^n$

replace y by y/x

$$A_{\mathcal{C}}\left(\frac{x}{y}\right) = 1 + (p-1)\left(\frac{y}{x}\right)^n = 1 + (p-1)y^n x^{-n}$$

multiply by x^n

$$W_{\mathcal{C}}(x,y) = x^n + (p-1)y^n$$

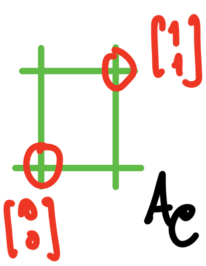
E.g., for $p=2$, $A_{\mathcal{C}}(y) = 1 + y^n$

$W_{\mathcal{C}}(x,y) = x^n + y^n$

---

② For $p=2$, $\mathcal{C}^{\perp}$ is the $[n,n-1,2]$ parity check code:

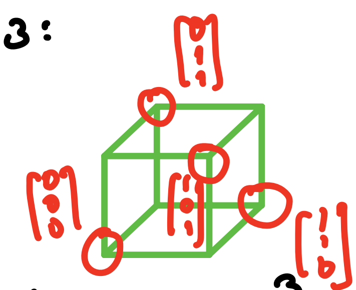
$n=2$:



$A_{\mathcal{C}}(y) = 1 + y^2$

$W_{\mathcal{C}}(x,y) = x^2 + y^2$

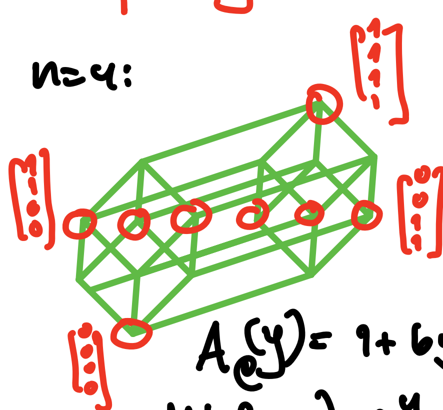
$n=3$:



$A_{\mathcal{C}}(y) = 1 + 3y^3$

$W_{\mathcal{C}}(x,y) = x^3 + 3y^3$

$n=4$:



$A_{\mathcal{C}}(y) = 1 + 6y^2 + y^4$

$W_{\mathcal{C}}(x,y) = x^4 + 6x^2y^2 + y^4$

Note that if $\mathbb{1}_n = \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} \in \mathcal{C} \subseteq (\mathbb{F}_2)^n$, then $W_{\mathcal{C}}(x,y) = W_{\mathcal{C}}(y,x)$

since $v \in \mathcal{C} \iff \mathbb{1}_n + v \in \mathcal{C}$ and $wt(\mathbb{1}_n + v) = n - wt(v)$.

EXAMPLES

① We showed that the 1^{st} order Reed-Muller Code

$\mathcal{C} = RM(1,m)$ was an $\mathbb{F}_2$-linear $[2^m, m+1, 2^{m-1}]$ code

in which every codeword $v \in \mathcal{C} - \left\{ \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \right\}$ has $wt(v) = 2^{m-1}$.

Therefore, $A_{\mathcal{C}}(y) = 1 + \underbrace{(2^{m+1} - 2)}_{v \neq \underline{0}, \mathbb{1}} y^{2^{m-1}} + y^{2^m}$

$$W_{\mathcal{C}}(x,y) = x^{2^m} + (2^{m+1} - 2) x^{2^{m-1}} y^{2^{m-1}} + y^{2^m}$$

E.g. $\mathcal{C} = RM(1,3)$ is $[8,4,4]$

with $A_{\mathcal{C}}(x) = 1 + 14y^4 + y^8$

$W_{\mathcal{C}}(x,y) = x^8 + 14x^4y^4 + y^8$

---

② The Golay $[24,12,8]$ binary code contains $\mathbb{1}_{24}$, and has

$A_{\mathcal{C}}(x) = 1 + 759 \cdot y^8 + 2576 y^{12} + 759 y^{16} + y^{24}$

$W_{\mathcal{C}}(x,y) = x^{24} + 759 \cdot x^{16} y^8 + 2576 x^{12} y^{12} + 759 x^8 y^{16} + y^{24}$

THEOREM (MacWilliams Identity 1962)

Any k-dimensional $\mathbb{F}_q$-linear code $\mathcal{C} \subset (\mathbb{F}_q)^n$ has

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{q^k} W_{\mathcal{C}}\left(x+(q-1)y \, , \, x-y\right)$$

In particular, for $\mathbb{F}_2$-linear (binary) codes

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{2^k} W_{\mathcal{C}}\left(x+y \, , \, x-y\right)$$

EXAMPLES

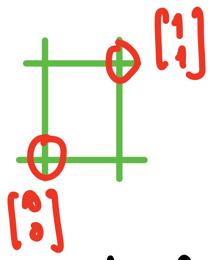
① Since a binary repetition $[n,1,n]$ code

$\mathcal{C} = \{\underline{0}, \underline{1}\}$ has $W_{\mathcal{C}}(x,y) = x^n + y^n$,

its dual $\mathcal{C}^\perp$ the parity check $[n, n-1, 2]$ code has

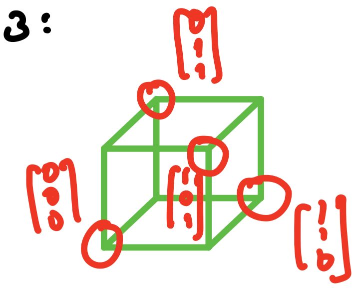
$$\begin{aligned}
W_{\mathcal{C}^\perp}(x,y) &= \frac{1}{2^1}\left((x+y)^n + (x-y)^n\right) \\
&= \frac{1}{2}\left(\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}(-1)^{n-k}\right) \\
&= \frac{1}{2}\sum_{n-k \text{ even}} 2\binom{n}{k}x^k y^{n-k} \\
&= \sum_{n-k \text{ even}} \binom{n}{k}x^k y^{n-k}
\end{aligned}$$

E.g. $n=2$:



$$W_{\mathcal{C}}(x,y) = x^2 + y^2$$

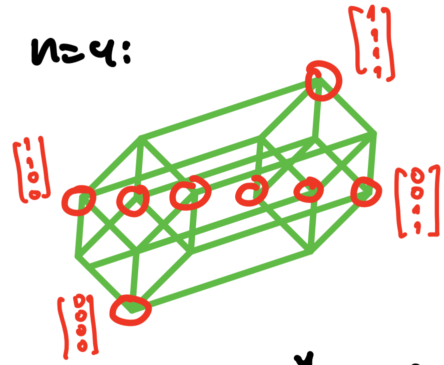
$n=3$:



$$W_{\mathcal{C}}(x,y) = x^3 + 3xy^2$$

$\binom{3}{1}$

$n=4$:



$$W_{\mathcal{C}}(x,y) = x^4 + 6x^2y^2 + y^4$$

$\binom{4}{2}$

---

② It turns out that these three codes with $k = n/2$

- $[2,1,2]$ binary parity check

$$W_{\mathcal{C}}(x,y) = x^2 + y^2$$

- $[8,4,4]$ 1st order Reed-Muller $RM(1,3)$

$$W_{\mathcal{C}}(x,y) = x^8 + 14x^4y^4 + y^8$$

- $[24,12,8]$ binary Golay code

$$W_{\mathcal{C}}(x,y) = x^{24} + 759 \cdot x^{16}y^8 + 2576\, x^{12}y^{12} + 759\, x^8 y^{16} + y^{24}$$

are the first few (binary) examples of

self-dual codes $\mathcal{C}^\perp = \mathcal{C}$,

so that $W_{\mathcal{C}}(x,y) = W_{\mathcal{C}^\perp}(x,y) = \frac{1}{2^{n/2}} W_{\mathcal{C}}(x+y,\, x-y)$

EXAMPLE $[8,4,4]$ 1st order Reed-Muller $RM(1,3)$ has

$$W_C(x,y) = x^8 + 14x^4y^4 + y^8$$

so
$$\frac{1}{2^{4/2}} W_C(x+y,\, x-y) = \frac{1}{2^4}\Big[(x+y)^8 + 14(x-y)^4(x+y)^4 + (x-y)^8\Big]$$

$$= \frac{1}{16}\Big[(x+y)^8 + (x-y)^8 \quad + 14(x^2-y^2)^4\Big]$$

$$= \frac{1}{16}\Big[\sum_{8-k \text{ even}} 2\binom{8}{k} x^k y^{8-k} + 14\left(x^8 - 4x^6y^2 + 6x^4y^4 - 4x^2y^6 + y^8\right)\Big]$$

$$= \frac{1}{16}\Big[2x^8 \cancel{+2\underbrace{\binom{8}{2}}_{28}} x^6y^2 + 2\underbrace{\binom{8}{4}}_{70} x^4y^4 \cancel{+2\underbrace{\binom{8}{6}}_{28}} x^2y^6 + 2y^8$$
$$+ 14x^8 \cancel{-56}\, x^6y^2 + 84x^4y^4 - \cancel{56}\, x^2y^6 + 14y^8\Big]$$

$$= \frac{1}{16}\Big[16x^8 + 224x^4y^4 + 16y^8\Big]$$

$$= x^8 + 14x^4y^4 + y^8 \;=\; W_C(x,y)$$

Let's prove at least the binary special case of MacWilliams's Identity; the ideas in the $\mathbb{F}_q$-linear case are similar.

proof: Want to show a k-dimensional $\mathbb{F}_2$-linear code $\mathcal{C} \subseteq (\mathbb{F}_2)^n$ has $W_{\mathcal{C}^\perp}(x,y) = \frac{1}{2^k} W_{\mathcal{C}}(x+y, x-y)$.

We compute ...

$$W_{\mathcal{C}}(x+y, x-y) = \sum_{v \in \mathcal{C}} (x+y)^{\overbrace{n-wt(v)}^{\#0\text{'s in } v}} \cdot (x-y)^{\overbrace{wt(v)}^{\#1\text{'s in } v}}$$

since
$x+y = x+(-1)^0 y$
$x-y = x+(-1)^1 y$

$$= \sum_{\substack{v=[v_1,v_2,\dots,v_n] \\ \in \mathcal{C}}} \underbrace{(x+(-1)^{v_1}y)(x+(-1)^{v_2}y)\cdots(x+(-1)^{v_n}y)}$$

picking one term from this product is a choice $u = [u_1,\dots,u_n] \in (\mathbb{F}_2)^n$ where

$$u_i = \begin{cases} 0 & \text{if } x \text{ is chosen from } i^{\text{th}} \text{ parenthesis} \\ 1 & \text{if } y \text{ is picked from } i^{\text{th}} \text{ parenthesis} \end{cases}$$

$$= \sum_{\substack{v=[v_1,v_2,\dots,v_n] \\ \in \mathcal{C}}} \sum_{\substack{u=[u_1,u_2,\dots,u_n] \\ \in (\mathbb{F}_2)^n}} x^{n-wt(u)} y^{wt(u)} (-1)^{\overbrace{u_1v_1+u_2v_2+\dots+u_nv_n}^{u \cdot v}}$$

$$= \sum_{u \in (\mathbb{F}_2)^n} x^{n-wt(u)} y^{wt(u)} \sum_{v \in \mathcal{C}} (-1)^{u \cdot v}$$

$$= \sum_{u \in \mathcal{C}^\perp} x^{wt(u)} y^{n-wt(u)} \sum_{v \in \mathcal{C}} \underbrace{(-1)^{u \cdot v}}_{\substack{=+1 \\ \text{since} \\ u \in \mathcal{C}^\perp \\ v \in \mathcal{C}}} + \sum_{u \in (\mathbb{F}_2)^n - \mathcal{C}^\perp} x^{wt(u)} y^{n-wt(u)} \underbrace{\sum_{v \in \mathcal{C}} (-1)^{u \cdot v}}_{\substack{=0 \text{ since} \\ \text{any } v_0 \in \mathcal{C} \text{ with} \\ u \cdot v_0 = 1 \text{ gives} \\ \text{a bijection } \mathcal{C} \to \mathcal{C} \\ v \mapsto v + v_0 \\ \text{with } (-1)^{u \cdot (v+v_0)} = -(-1)^{u \cdot v}}}$$

$$= W_{\mathcal{C}^\perp}(x,y) \cdot |\mathcal{C}| \quad + \quad 0$$

$$= 2^k \cdot W_{\mathcal{C}^\perp}(x,y).$$

Hence $\quad W_{\mathcal{C}^\perp}(x,y) = \frac{1}{2^k} W_{\mathcal{C}}(x+y, x-y) \quad \blacksquare$

REMARK:

MacWilliams's advisor Gleason was later (1970) able to use the fact that self-dual $[n, n/2, d]$ binary codes $\mathcal{C}$ containing $\mathbb{1}_n$ have weight enumerators with so much symmetry

- $W_{\mathcal{C}}(x,y) = W_{\mathcal{C}}(y,x)$ from $\mathbb{1}_n \in \mathcal{C}$
- $W_{\mathcal{C}}(x,y) = \frac{1}{2^{n/2}}(x+y, x-y)$ from MacWilliams Identity

along with some further algebra (invariant theory of finite groups) to place severe constraints on how $W_{\mathcal{C}}(x,y)$ can look.