Códigos de Reed-Muller

Tobias Briones

April 6, 2021

Universidad Nacional Autónoma de Honduras
Códigos de Reed-Muller, Código Dual

Peso par

Proposición

$\mathscr{RM}(m-1, m)$ consiste en todas las palabras binarias de longitud 2^m de peso par. Por tanto, si $r < m$, $\mathscr{RM}(r, m)$ solo contiene palabras código de peso par.

Prueba:

$\mathscr{RM}(0, 1) = \{00, 11\}$ claramente consiste en todas las palabras binarias de longitud 2. Suponer que esto se cumple para $\mathscr{RM}(m-2, m-1)$. Una palabra código de $\mathscr{RM}(m-1, m)$ tiene la forma $(u, u+v) = (u, u) + (0, v)$ con $u \in \mathscr{RM}(m-1, m-1)$ y $v \in \mathscr{RM}(m-2, m-1)$.

Peso par

Ahora, (u, u) tiene peso par para cualquier u, y $(0, v)$ tiene peso para por la hipótesis de inducción. Entonces:

$$wt((u, u+v)) = wt((u, u)) + wt((0, v)) - 2(u, u) \cdot (0, v)$$

El cual es también par. Entonces $\mathscr{RM}(m-1, m)$ contiene solo vectores pares. ya que $dim(\mathscr{RM}(m-1, m)) = 2^m - 1$, contiene a todos los vectores con peso par. Por último, si $r < m$, entonces $\mathscr{RM}(r, m) \subseteq \mathscr{RM}(m-1, m)$

Peso par

Proposición
Toda palabra código de un código lineal binario auto-ortogonal tiene peso par.

Prueba

Tenemos que $C \subseteq C^{\perp}$ por hipótesis. Para una palabra código $w = (a_1, a_2, ..., a_n)$, $w \cdot w = 0$. Pero $w \cdot w = a_1^2 + a_2^2 + ... + a_n^2$ lo cual es igual al peso de w, $wt(w)$. Entonces $w \cdot w = 0$ en $\mathbb{F}_2$ sii w tiene peso par.

Código Dual

Proposición
$\mathscr{RM}(m-r-1, m)$ y $\mathscr{RM}(r, m)$ son códigos duales.

Prueba:

Para $m = 2$, ambos códigos existen solo si $r = 0$ o 1.

Tenemos que $\mathscr{RM}(0, 2) = \{0000, 1111\}$ y
$\mathscr{RM}(1, 2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$.

Ya que todos los vectores en $\mathscr{RM}(1, 2)$ tiene peso par, entonces todo vector de $\mathscr{RM}(0, 2)$ es ortogonal a todo vector de $\mathscr{RM}(1, 2)$. (1)

Código Dual

Suponer que (1) es cierto para $m-1$. Dadas las matrices generatrices de ambos códigos:

$$G_{r,m} = \begin{pmatrix} G_{r,m-1} & G_{r,m-1} \\ 0 & G_{r-1,m-1} \end{pmatrix}$$

$$G_{m-r-1,m} = \begin{pmatrix} G_{m-r-1,m-1} & G_{m-r-1,m-1} \\ 0 & G_{m-r-2,m-1} \end{pmatrix}$$

Código Dual

Las filas de la forma (a, a) son ortogonales a las de la forma (b, b).

Las filas de la forma (a, a) son ortogonales a las de la forma $(0, d)$ por la hipótesis inductiva. Por la misma razón, las filas de la forma $(0, c)$ son ortogonales a las de forma (b, b).

Ya que $\mathscr{RM}(m-r-2, m-1) \subset \mathscr{RM}(m-r-1, m-1)$, las filas de la forma $(0, c)$ son ortogonales a las de forma $(0, d)$.

Código Dual

Por tanto, $\mathscr{RM}(m-r-1,m) \subset \mathscr{RM}(r,m)^{\perp}$. Ahora:

$$\begin{aligned}
dim(\mathscr{RM}(r,m)^{\perp}) &= 2^m - [1 + \binom{m}{1} + \ldots + \binom{m}{r}] \\
&= \binom{m}{r+1} + \binom{m}{r+2} + \ldots + \binom{m}{m} \\
&= \binom{m}{m-r-1} + \binom{m}{m-r-2} + \ldots + 1 \\
&= dim(\mathscr{RM}(m-r-1,m))
\end{aligned}$$

Por tanto, $\mathscr{RM}(m-r-1,m) = \mathscr{RM}(r,m)^{\perp}$.