Edgar Santiago Ochoa Quiroga
María Alejandra Rodríguez Ríos

Ejercicio 3
Sea C un código lineal $[n, m, d]$ sobre un cuerpo finito $GF(D)$. El código dual de C es el conjunto

$$C^{\perp} = \{x \in GF(D)^n : \langle x, y \rangle = 0, \forall y \in C\}.$$

Demuestre que $C^{\perp}$ es un código lineal de dimensión $n - m$ y que su matriz generadora corresponde a la matriz de verificación de C.

Demostración. Primero tenemos que probar que el código dual es lineal, para esto basta probar que es un subespacio de $GF(D)^n$.
Primero probemos que es cerrado bajo la suma. Sean $x_1, x_2 \in C^{\perp}$, por definición $\langle x_1, y \rangle = 0$ y $\langle x_2, y \rangle = 0$, para cualquier $y \in C$, luego como el producto interno es lineal en cada componente, tenemos que $\langle x_1 + x_2, y \rangle = \langle x_1, y \rangle + \langle x_2, y \rangle = 0$, así $x_1 + x_2 \in C^{\perp}$. Ahora falta probar que la multiplicación por escalares también es cerrada. Tomemos $\lambda \in GF(D)$, luego si tomamos x_1 igual que en la anterior parte, nuevamente como el producto interno es lineal tenemos que $\langle \lambda x_1, y \rangle = \lambda \langle x_1, y \rangle = 0$. Así como es cerrado para ambas propiedades hemos probado que $C^{\perp}$ es un subespacio y por tanto un código lineal.
Ahora para encontrar la dimensión del código notemos que como C es de dimensión m, existen vectores $g_1, \dots, g_m \in C$, que forman una base para C, tales que

$$G = \begin{bmatrix} g_1 \\ \vdots \\ g_m \end{bmatrix}.$$

Es la matriz generadora de C, recordemos que

$$\ker(G) = \{x \in GF(D)^n : Gx^T = 0\}.$$

La idea sera probar que $C^{\perp} = \ker(G)$. Sea $x \in C^{\perp}$, note que

$$Gx^T = \begin{bmatrix} g_1 \\ \vdots \\ g_m \end{bmatrix} x^T = \begin{bmatrix} \langle x, g_1 \rangle \\ \vdots \\ \langle x, g_m \rangle \end{bmatrix},$$

Note que esto se tiene por la definición del producto de matrices, Pero como cada $g_i \in C$ y $x \in C^{\perp}$ tenemos que $\langle x, g_i \rangle = 0$ para cada $i = 1, \dots, m$. Así $Gx^T = 0$, luego $x \in \ker(G)$. Esto prueba

$C^{\perp} \subseteq \ker(G)$. Para ver la otra contenecia considere $x \in \ker(G)$, por definición

$$0 = Gx^T = \begin{bmatrix} g_1 \\ \vdots \\ g_m \end{bmatrix} x^T = \begin{bmatrix} \langle x, g_1 \rangle \\ \vdots \\ \langle x, g_m \rangle \end{bmatrix}.$$

De esta manera $\langle x, g_i \rangle = 0$ para cada i, pero recordemos que los g_i forman una base para C, luego dado $y \in C$, existen $\alpha_i \in GF(D)$ tales que $y = \sum_{i=1}^{m} \alpha_i g_i$, y por la linealidad del producto interno

$$\begin{aligned} \langle x, y \rangle &= \left\langle x, \sum_{i=1}^{m} \alpha_i g_i \right\rangle \\ &\sum_{i=1}^{m} \alpha_i \langle x, g_i \rangle \\ &= 0, \end{aligned}$$

así como y era arbitrario, tenemos que $\langle x, y \rangle = 0$ para todo $y \in C$, luego $x \in C^{\perp}$, probando así por la doble contenencia la igualdad de los conjuntos.
Con estos hechos por el teorema de rango-nulidad tenemos que

$$\dim(\ker(G)) + \dim(\mathrm{Im}(G)) = n,$$

Pero recordemos que la dimensión de la imagen de una matriz, es la dimensión del subespacio generado por sus filas, como sus filas generan C y este código tiene dimensión m, tenemos que $\dim(\mathrm{Im}(G)) = m$, luego como $\ker(G) = C^{\perp}$, si reemplazamos en la anterior expresión obtenemos

$$\dim(C^{\perp}) + m = n.$$

Así la dimensión de el código dual es $n - m$. Por ultimo nos falta probar que la matriz de verificacion H para C es la matriz generadora de $C^{\perp}$. Sea $G = [\ I_m \mid P\ ]$, donde P es de tamaño $m \times (n - m)$, la matriz sistemática del código C, recordemos que la matriz de paridad esta dada por $H = [\ -P^T \mid I_{n-m}\ ]$, por un hecho visto en clase sabemos que $\dim(\mathrm{Im}(H)) = n - m$, es decir que la dimensión del espacio generado por sus filas es $n - m$, si podemos probar que las filas de H pertenecen a $C^{\perp}$, por la parte anterior, como la dimensión del espacio fila coincide con la de $C^{\perp}$, habremos terminado. Primero notemos que la matriz G es de tamaño $m \times n$, mientras que H es de tamaño $(n - m) \times n$, así que consideremos el siguiente producto matricial

$$GH^T = [\ I_m \mid P\ ] \left[\frac{-P}{I_{n-m}} \right]$$

Note que hacemos esto para que las dimensiones coincidan, el resultado serán matrices de tamaño $m \times (n - m)$, pero ademas podemos notar que la primeras m columnas de G son las entradas de la identidad, mientras que las primeras m filas de H^T son las entradas de $-P$, luego pro el producto de matrices en bloque tenemos que

$$[\ I_m \mid P\ ] \left[\frac{-P}{I_{n-m}} \right] = -I_m P + P I_{n-m} = -P + P = 0.$$

Esto quiere decir que las columnas de H^T son ortogonales a las filas de G, o de manera equivalente, las filas de H son ortogonales a las de G. esto debido a que las entradas del producto matricial son el producto interno usual. Luego como las filas de G son una base para C, por un argumento análogo al hecho en la prueba de $\ker(G) = C^{\perp}$, tenemos que las filas de Hpertenecen a $C^{\perp}$, de esta manera por lo dicho al inicio de la prueba, hemos concluido que la matriz H es la matriz generadora del código dual de C.