Códigos de Hamming: Versión Alternativa con Combinaciones

Julián Tricanico

18/08/2020

Supongamos que estamos en las condiciones de la clase 2, y tenemos cuatro bits b_3, b_2, b_1 y b_0, y tres bits de redundancia p_0, p_1 y p_2, ahora con el truco de estar en orden ascendente.

Lo que haremos es definir a p_i para cada $i \in \mathbb{Z}_3$ como $p_i = \bigoplus_{j \in \mathbb{Z}_4 \setminus \{i\}} b_j$.

Definimos nuevamente a s_i como $s_i = p_i \oplus \bigoplus_{j \in \mathbb{Z}_4 \setminus \{i\}} b_j$, con lo cual,
si falla b_3, $s_0 = 1$, $s_1 = 1$ y $s_2 = 1$;
si falla b_2, $s_0 = 1$, $s_1 = 1$ y $s_2 = 0$;
si falla b_1, $s_0 = 1$, $s_1 = 0$ y $s_2 = 1$;
si falla b_0, $s_0 = 0$, $s_1 = 1$ y $s_2 = 1$;
si falla p_0, $s_0 = 1$, $s_1 = 0$ y $s_2 = 0$;
si falla p_1, $s_0 = 0$, $s_1 = 1$ y $s_2 = 0$;
si falla p_2, $s_0 = 0$, $s_1 = 0$ y $s_2 = 1$;
cumpliéndose así lo deseado.

Se puede ver que colocando a los p_i's en las potencias de 2 como mencionado en clase, el algorítmo nos muestra qué bit falló. Pero ordenado como está arriba, se ve que es la forma canónica de elegir combinaciones, así que podríamos considerar este órden en vez del usual, y nos diría también la posición del bit que falló.

Con esta sintáxis, generalizar es sencillo.
Si $n \in \mathbb{N}$ y r es tal que $2^r > n + r$, sólo debemos considerar para $i \in \mathbb{Z}_r$, $p_i := \bigoplus_{j \in \mathbb{Z}_n \setminus \{i\}} b_j$.

Más interesantemente, sean $p_{i,j} := \bigoplus_{k \in \mathbb{Z}_n \setminus \{i,j\}} b_k$, con $0 \leq i \leq j < r$, y volvamos a $n = 4$ para facilitar.

Es decir que tenemos b_3, b_2, b_1, b_0, $p_{0,0}$, $p_{0,1}$, $p_{0,2}$, $p_{1,1}$, $p_{1,2}$ y $p_{2,2}$. Explayemos cómo se vería una tabla de esto:

b_3	b_2	b_1	b_0	$p_{0,0}$	$p_{0,1}$	$p_{0,2}$	$p_{1,1}$	$p_{1,2}$	$p_{2,2}$
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1	1	1
0	0	1	0	1	0	1	0	0	1
0	0	1	1	1	0	1	1	1	0
0	1	0	0	1	1	0	1	0	0
0	1	0	1	1	1	0	0	1	1
0	1	1	0	0	1	1	1	0	1
0	1	1	1	0	1	1	0	1	0
1	0	0	0	1	1	1	1	1	1
1	0	0	1	1	1	1	0	0	0
1	0	1	0	1	1	0	0	1	0
1	0	1	1	0	1	0	0	0	1
1	1	0	0	0	0	1	0	1	1
1	1	0	1	0	0	1	1	0	0
1	1	1	0	1	0	0	0	1	0
1	1	1	1	1	0	0	1	0	1

Se puede ver que tiene distancia 4.

Uno se ve motivado a conjeturar entonces que esto se generaliza para cualquier n, y lo que es más, para $p_I := \bigoplus_{k \in \mathbb{Z}_n \setminus I} b_k$, con $0 \leq i_1 \leq \cdots \leq i_m < r$, con $I = \{i_1, i_2\} = \{i, j\}$ en el ejemplo de arriba; y que tendría una distancia de $m + 2$.

Queda como ejercicio para el lector.