Teorema de la cota de Hamming

Enunciar el **teorema de la cota de Hamming** y probarlo

El teorema de *Hamming* nos dice que, sea C un código de longitud n, $\delta = \delta(C)$ y $t = \lfloor \frac{\delta-1}{2} \rfloor$, entonces

$$\#C \leq \frac{2^n}{\sum_{i=0}^{t} \binom{n}{i}}$$

Para demostrarlo, vamos a recordar la definición de distancias, los discos y sus propiedades:

- Dado un código C, la distancia de Hamming entre dos palabras v y w es la cantidad de bits de diferencia entre v y w. Denotamos a esta como $d(v, w)$.
- Dada una palabra $v \in \{0,1\}^n$ y $r \in N_0$, definimos el *disco de radio r alrededor de v* como $D_r(v) = \{w \in \{0,1\}^n : d(v,w) \leq r\}$
- Un código C detecta r errores si $D_r(v) \cap C = \{v\} \forall v \in C$
- Un código C corrige r errores si $D_r(v) \cap D_r(w) \neq \emptyset \forall v, w \in C : v \neq w$
- Sea C un código y $\delta = \delta(C)$, entonces
  - C detecta $\delta - 1$ errores pero no detecta δ
  - Si $t = \lfloor \frac{\delta-1}{2} \rfloor$, entonces C corrige t errores pero no corrige $t+1$ errores

Dicho esto, consideremos $A = \cup_{v \in C} D_t(v)$.
Como $t = \lfloor \frac{\delta(C)-1}{2} \rfloor$, entonces C corrige t errores. Luego, esto significa que $D_t(v) \cap D_t(w) = \emptyset \forall v, w \in C$.
Por ello, entonces, A es una unión disjunta, por lo que $\#A = \sum_{v \in C} \#D_t(v)$.

Ahora, para ver los D_t, consideremos los conjuntos $S_r(v) = \{w \in \{0,1\}^n : d(v,w) = r\}$.
Luego, por definición de disco, tenemos que $D_t(v) = \cup_{r=0}^{t} S_r(v)$, la cual es, claramente, una unión disjunta (porque las distancias son distintas por r). Luego, $\#D_t(v) = \sum_{r=0}^{t} \#S_r(v)$.

Ahora, si vemos S_r, notemos que si $w \in S_r(v)$ entonces significa que difiere de v en exactamente r posiciones.
Dado esto, quiero ver cuántas w posibles hay. Para ello, notemos que si difiere en r posiciones, entonces hay $\binom{n}{r}$ conjuntos de posiciones distintos para considerar.
Ahora, como solo tenemos los elementos $0, 1$, entonces que sea distinto significa que se le asigna el otro posible valor.
Luego, para $S_r(v)$ hay $\binom{n}{r} \times 1^r = \binom{n}{r}$ posibles elementos.

Dicho esto, si reemplazamos todo tenemos que:

$$\#S_r(v) = \binom{n}{r}$$

$$\#D_t(v) = \sum_{r=0}^{t} S_r(v) = \sum_{r=0}^{t} \binom{n}{r}$$

$$\#A = \sum_{v \in C} \#D_t(v) = \sum_{v \in C} (\sum_{r=0}^{t} \binom{n}{r})$$

Luego, como la última suma considerada para $\#A$ no depende de v, tenemos que

$$\#A = \#C \times \sum_{r=0}^{t} \binom{n}{r}$$

Ahora, como A es un subconjunto de $\{0, 1\}^n$, entonces $\#A \leq 2^n$.
Dicho esto, tenemos que:

$$\#C = \frac{\#A}{\sum_{r=0}^{t} \binom{n}{r}} \leq \frac{2^n}{\sum_{r=0}^{t} \binom{n}{r}}$$

con lo que queda demostrado.