Demostración del Teorema de la cota de Hamming

Nicolás Cagliero

26 de junio de 2024

Theorem 1. *Sea $C \subseteq \{0,1\}^2$ un código binario de longitud n. Sea $\delta = \delta(C)$ y $t = \lfloor \frac{\delta-1}{2} \rfloor$. Entonces*

$$|C| \leq \frac{2^n}{1 + n + \binom{n}{2} + ... + \binom{n}{t}}$$

Demostración. Sea

$$A = \bigcup_{v \in C} D_t(v)$$

Como $t = \lfloor \frac{\delta-1}{2} \rfloor$, C corrige t errores $\Rightarrow D_t(v) \cap D_t(w) = \emptyset$ para cualquier palabra de C. Luego, la unión de A es disjunta

$$\Rightarrow |A| = \sum_{v \in C} |D_t(v)|$$

Sean $S_r(v) = \{w \in \{0,1\}^2 : d_H(v,w) = r\}$

$$\Rightarrow |D_t(v)| = \sum_{r=0}^{t} |S_r(v)|$$

Ahora queda ver cuánto vale $|S_r(v)|$. Notar que si $w \in S_r(v)$, entonces w difiere en exactamente r bits de v. Tenemos una biyección entonces entre $S_r(v)$ y el conjunto de subconjuntos de r bits de los n bits posibles. Luego $|S_r(v)| = \binom{n}{r}$.

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

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

Por lo tanto

$$|C| = \frac{|A|}{\sum_{r=0}^{t} \binom{n}{r}}$$

Como $A \subseteq \{0,1\}^2 \Rightarrow |A| \leq 2^n$

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

□