Info Theory HW 3

24.04.09

> Proof Gilbert-Varshamov Bound Theorem.

We will employ a probabilistic method to prove this theorem.

Consider we generate 2^n m-bit strings $s_1, \cdots, s_{2^n}$ uniformly and independently from $\{0,1\}^m$.

This probability of two particular strings s_1, s_2 with Hamming distance less than δm is

$$P_1 = \frac{1}{2^m} \sum_{i=0}^{\delta m - 1} C_m^i < \frac{1}{2^m} \sum_{i=0}^{\delta m} C_m^i.$$

Note that $\frac{1}{2^m} \sum_{i=0}^{\delta m} C_m^i = \Pr(X \leq \delta m)$, where $X \sim B(m, \frac{1}{2})$.

We use without proof the following inequality (Chernoff Bound):

$$\Pr(X \leq (p-\epsilon)n) \leq e^{-nD_B(p-\epsilon \| p)},$$

where $X \sim B(n,p)$ and $D_B(p \parallel q)$ is defined as $p \ln \frac{p}{q} + (1-p) \ln \frac{1-p}{1-q}$.

Replace n by m, p by $\frac{1}{2}$ and ϵ by $\frac{1}{2} - \delta$, we get

$$P_1 < e^{-m(\ln 2 + \delta \ln(\delta) + (1-\delta)\ln(1-\delta))} = 2^{-m(1-H(\delta))}.$$

So, using the Union Bound, the probability of existing $i \neq j$, such that the Hamming distance of s_i, s_j is less than δm is

$$P_2 \leq C_{2^n}^2 P_1 < \frac{2^n(2^n-1)}{2} 2^{-m(1-H(\delta))} < 2^{2n - m(1-H(\delta))}.$$

If $P_2 < 1$, then we can say for sure that exists such $s_1, \cdots, s_{2^n} \in \{0,1\}^m$ that their pairwise Hamming distances are all larger or equal than δm. To achieve $P_2 < 1$, it is sufficient to let

$$2^{2n - m(1-H(\delta))} \leq 1,$$

or

$$m \geq \frac{2n}{1 - H(\delta)}.$$

Q.E.D.