Advanced Proof Systems - Homework 2

Yosef Goren

December 8, 2022

1 Random Linear Codes (Gilbert-Varshamov Bound)

Let

- $\epsilon > 0$
- $n := \Omega(\frac{ck}{\epsilon^2})$
- $A \leftarrow^{\$} \{0,1\}^{n \times k}$
- $C(x) := Ax$

Use $hw(\cdot)$ to denote the Hamming weight of a vector.
Let m be a vector of length k with $hw(m) = \Omega(\frac{ck}{\epsilon^2})$.
Let $X_i = (Am)_i, X = \frac{1}{n}\sum_{i=1}^{n} X_i$.
Since $(Am)_i = A_{:,i}m$, and each colomn of A is a random vector, X_i is a random variable.

Thus using chernoff we can see (*):

$$Pr\left[X < \frac{1}{2} - \epsilon\right] \leq Pr\left[|X - \frac{1}{2}| < \epsilon\right] \leq 2^{-\frac{1}{2}\epsilon^2 n} \leq 2^{-ck}$$

Since C is linear, we know it's absolute distance is given by:

$$d = min\{hw(C(m)) \mid m \neq 0\}$$

Thus:

$$\Pr\left[\frac{d}{n} < \frac{1}{2} - \epsilon\right] = \Pr\left[\frac{min\{hw(C(m)) \mid m \neq 0\}}{n} < \frac{1}{2} - \epsilon\right]$$

$$= \Pr\left[\exists m \neq 0 : \frac{hw(C(m))}{n} < \frac{1}{2} - \epsilon\right] = \Pr\left[\bigcup_{m \neq 0}\left(\frac{hw(C(m))}{n} < \frac{1}{2} - \epsilon\right)\right]$$

$$\leq_{UB} \sum_{m \neq 0} \Pr\left[\frac{hw(C(m))}{n} < \frac{1}{2} - \epsilon\right] = \sum_{m \neq 0} \Pr\left[\frac{|\{i \mid (Am)_i \neq 0\}|}{n} < \frac{1}{2} - \epsilon\right]$$

$$= \sum_{m \neq 0} \Pr\left[\frac{\sum_{i=1}^{n}(Am)_i}{n} < \frac{1}{2} - \epsilon\right] = \sum_{m \neq 0} \Pr\left[\frac{\sum_{i=1}^{n} X_i}{n} < \frac{1}{2} - \epsilon\right]$$

$$= \sum_{m \neq 0} \Pr\left[X < \frac{1}{2} - \epsilon\right] \leq_{(*)} \sum_{m \neq 0} 2^{-ck} = (2^k - 1) \cdot 2^{-ck} < 2^k \cdot 2^{-ck} = 2^{k(1-c)} \leq_{(**)} 0.01$$

(**) Since we want to bound the probability of the relative distance with 0.01, we require that this bound will be smaller than $2^{-7} = \frac{1}{128} < 0.01$:

$$2^{k(1-c)} < 2^{-7} \Leftrightarrow k(1-c) < -7 \Leftrightarrow 1 - c < -\frac{7}{k} \Leftrightarrow c - 1 < \frac{7}{k} \Leftrightarrow c < \frac{7}{k} + 1$$

Thus if c, k satisfiy these conditions, we have the required bound on the relative distance.