Lecture 6: Bounds on Code Parameters

In this lecture, we shall take a look at how the parameters n, M, d of a code are related to one another.

Crucially, via such inter-relationships, we shall arrive at estimates of an answer to the fundamental question we are chasing after:

How does the size of a code (rate) relate to its error-correcting capability (distance)?

Remark: Note that we are back to the setting of adversarial errors (i.e., the setting where there is a bound on the total # of errors) as opposed to the setting of stochastic/random errors.

Adversarial errors $\longleftrightarrow$ Random errors

"Hamming model" "Shannon model"

Recall the following definition:

Def 1 (Block code): An (n, M, d) block code is a subset $\mathcal{C} \subseteq \mathcal{X}^n$ with $|\mathcal{C}| = M$ and minimum distance $d_{min}(\mathcal{C}) = d$.

Recall that rate $R \triangleq \frac{\log M}{n}$; further, we define

the relative distance of $\mathcal{C}$ to be $\delta \triangleq d/n$.

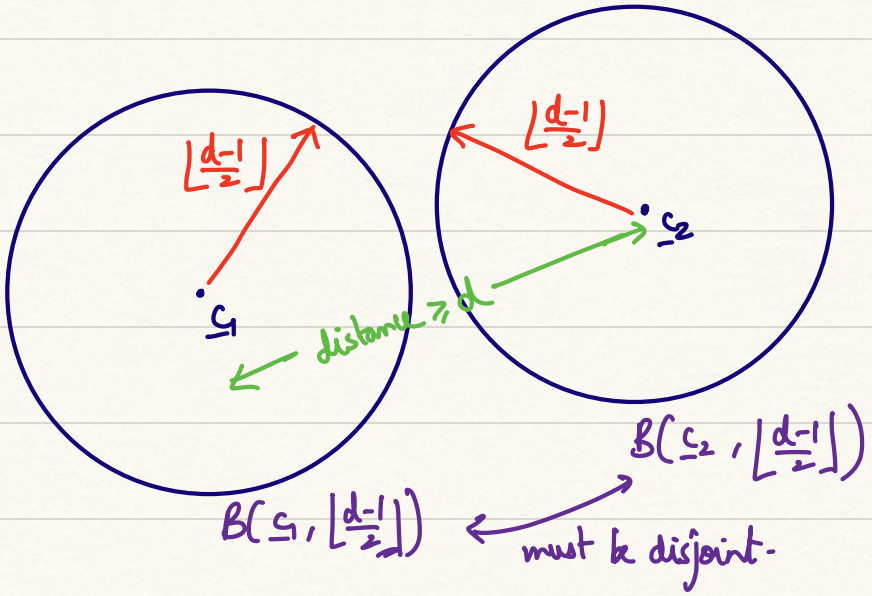
① Sphere-Packing Bound (Upper bound on M)

Thm 1: For any (n, M, d) block code over the alphabet $\mathbb{F}_q$, we have

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \leq \frac{q^n}{M}, \text{ i.e.,}$$

$$M \leq q^n \Big/ \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i .$$

Proof: For a code to have distance d, we must have that for $\underline{c}_1, \underline{c}_2 \in \mathcal{C}$,



Hence, $q^n \geq |\mathcal{C}| \cdot \mathrm{Vol}\left(B\left(\underline{c}_1, \lfloor \frac{d-1}{2} \rfloor\right)\right)$ [for any $\underline{c}_1 \in \mathcal{C}$]

$$= M \cdot \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \qquad \blacksquare$$

↳ extended version from binary to q-ary.

Codes that meet the sphere-packing bound with equality are called "perfect codes".

The sphere-packing bound, when specialized to linear codes, is called the "Hamming bound".

Remark: Consider the "trivial codes" $\mathcal{C}_1 = \mathbb{F}_q^n$ and $\mathcal{C}_2 = \{\underline{0}, \underline{1}\}$ (over $\{0,1\}$). For $\mathcal{C}_1$, we have that $d_{min}(\mathcal{C}_1) = 1$ and $|\mathcal{C}_1| = q^n$, leading to equality in the sphere-packing bound.

For $\mathcal{C}_2$, with n odd, we have that $d_{min}(\mathcal{C}_2) = n$ and $|\mathcal{C}_2| = 2$. Now, note that for this code,

$$\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} \cdot (q-1)^i = \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i} \quad [\text{since } q=2]$$

$$= 2^{n-1}. \quad [\text{Why?}]$$

Hence, $M \cdot \sum_{i=0}^{\frac{d-1}{2}} \binom{n}{i} (q-1)^i = 2^n$, achieving equality again in the sphere-packing bound.

Recall the definition of an $[n, K, d]$ linear code.

Corollary: For an $[n, K, d]_q$ linear code $\mathcal{C}$, we must have that

$$K \leq \log_q \left(q^n \Big/ \sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} (q-1)^i \right).$$

HW: Verify that the $[7,4,3]_2$ Hamming code meets the above bound with equality.

FACT: In fact, there are only 4 families of linear codes that are perfect; for all others, the sphere-packing bound is not tight!

These codes are: (i) $\mathbb{F}_q^n$, (ii) the repetition code, (iii) a Hamming code, and (iv) the binary/ternary Golay code.

② Singleton Bound (Upper bound on M)

Thm 3: For any (n, M, d) block code over $\mathbb{F}_q$, we have

$$d \leq n - \lceil \log_q M \rceil + 1.$$

Proof: Set $\ell = \lceil \log_q M \rceil - 1$, such that $q^\ell < M$.

Since there are $M > q^\ell$ codewords, some two codewords $c_1, c_2 \in \mathcal{C}$ must agree on the first ℓ positions. Hence,

$$d_{\min}(\mathcal{C}) \leq n - \ell = n - \lceil \log_q M \rceil + 1. \quad \square$$

Corollary 4: For an $[n,k,d]_q$ code $\mathcal{C}$, we have

$$d \leq n - k + 1.$$

A linear code that meets the Singleton bound is called a maximum distance separable (MDS) code.

HW: Verify that the single parity-check code over $\mathbb{F}_2$ is an MDS code.

③ Gilbert-Varshamov (GV) bound (lower bound on M)

Thm 5: There exists an (n, M, d) code such that

$$M \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i}.$$

Aside: Via arguments similar to those done previously, we have

$$q^{n(h_q(d/n)-o(1))} \leq \mathrm{Vol}_q(B(0, d-1)) \leq q^{n h_q(d/n)}, \text{ where}$$

$$h_q(p) \triangleq -p \log_q p - (1-p) \log_q (1-p) + p \log_q (q-1).$$

Asymptotics ($n \to \infty$):

① Sphere-packing bound: $R \leq 1 - h_q(\delta/2)$.

② Singleton bound: $R \leq 1 - \delta$.

③ GV bound: $R \geq 1 - h_q(\delta)$.