Class 10 Exercises

CS250/EE387, Winter 2022

Warm-Up

What can you say (so far in this class) about the list-decodability of Reed-Solomon codes? That is, what is the best trade-off between R and ρ so that an RS code of rate R is (ρ, L)-list-decodable for, say, polynomial-sized L?

One proof of the Johnson bound

Today we'll prove the (binary) Johnson bound. (You'll see a different proof on your homework). Recall from the lecture videos/notes that

$$J_2(\delta) = \frac{1}{2}(1 - \sqrt{1 - 2\delta}),$$

and that the Johnson bound says:

Theorem 1 (Johnson bound)**.** *Suppose that $\mathcal{C} \subseteq \{0,1\}^n$ is a code of relative distance at least δ. Suppose that $\rho \leq J_2(\delta)$. Then for any $z \in \{0,1\}^n$,*

$$|\mathcal{C} \cap B_2^n(z, \rho)| \leq \textit{something polynomial in } n$$

Towards proving Theorem 1, let $\mathcal{C} \subseteq \{0,1\}^n$ be a code of relative distance at least δ, and choose $\rho < J_2(\delta)$. let $z \in \{0,1\}^n$ be any vector. Suppose that $\mathcal{C} \cap B_2^n(z, \rho) = \{c_1, \ldots, c_M\}$. Our goal is to show that M is not too big.

1. Define a map $\phi : \{0,1\} \to \mathbb{R}^2$ by:

   $$\phi(0) = (0, 1) \qquad \phi(1) = (1, 0).$$

   Extend this to a map $\phi : \{0,1\}^n \to \mathbb{R}^{2n}$ in the natural way. That is,

   $$\phi((x_1, \ldots, x_n)) = \phi(x_1) \circ \phi(x_2) \circ \cdots \circ \phi(x_n),$$

   where $\circ$ denotes concatenation. Define

   $$v := \alpha\phi(z) + \frac{1 - \alpha}{2}\mathbf{1},$$

   where $\alpha \in [0, 1]$ is some parameter that we will define later, and where $\mathbf{1}$ is the all-ones vector of length $2n$.

   What can you say about each of the following quantities? (That is, either simplify them or bound them). Your answers should be in terms of δ, ρ, α.

   (a) $\langle \phi(c_i), \phi(c_j) \rangle$ for $i \neq j$. (Show that this is at most something, using the fact that the amount of agreement between two codewords is at most $(1 - \delta)n$).

(b) $\langle v, \phi(c_i)\rangle$ for any $i = 1, \ldots, M$. (Show that this is at least something, using the fact that the agreement between any of the c_i and z is at least $(1-\rho)n$).

(c) $\langle v, v\rangle$. (Figure out exactly what this is equal to).

2. Choose $\alpha = \sqrt{1-2\delta}$. Show that

$$\langle v - \phi(c_i), v - \phi(c_j)\rangle \leq 0$$

for any $i \neq j$? (Hint, use (i) the previous part, (ii) the assumption that $\rho < J_2(\delta) = \frac{1-\alpha}{2}$ using our choice of α, and (iii) the fact that $(1-\alpha^2)/2 = \delta$ using again our choice of α).

3. It turns out that you can't have too many vectors in $\mathbb{R}^D$ that are all at obtuse angles from each other. More precisely, we have the following fact:

Fact 2. *Let $x_1, x_2, \ldots, x_M \in \mathbb{R}^D$ such that $\langle x_i, x_j\rangle \leq 0$ for all $i \neq j$. Suppose further that there exists a non-zero vector $u \in \mathbb{R}^D$ so that $\langle u, v_i\rangle \geq 0$ for all $i = 1, \ldots, M$. Then $M \leq 2D - 1$.*

Use the fact to prove Theorem 1.

4. **(Bonus).** Use this technique to prove the q-ary Johnson bound.