Exercise List 1

Anup Rao

October 6, 2019

You are not required to turn in exercises. They are here if you want to practice your understanding of the concepts we discussed in class.

1. We start by exploring how to use geometry to give bounds on non-binary codes.

   (a) Show that if $v_1, \ldots, v_q \in \mathbb{R}^n$ are unit vectors with $\langle v_i, v_j \rangle < -\epsilon$ for all distinct i, j and some constant $\epsilon > 0$, then $q \leq 1 + 1/\epsilon$. Hint: consider $\langle \sum_i v_i, \sum_i v_i \rangle$.

   (b) Show that there exist unit vectors $v_1, \ldots, v_q \in \mathbb{R}^q$ with pairwise inner-products at most $-1/(q-1)$. Conclude that the bound from the first step is tight.

   (c) Use the results above to map every codeword of a code $C \subseteq \Sigma^n$ to vectors. Conclude that if $d > (1 - 1/q)n$, then $|C| \leq \frac{qd}{qd-(q-1)n}$.

   (d) Finally, use the idea of taking a random ball in Σ^n to conclude that

   $$R + h_q\Big((1-1/q) \cdot (1 - \sqrt{1 - \frac{q\delta}{q-1}})\Big) \leq 1 + O(\log(n)/n).$$

2. Suppose $C \subseteq F_2^n$ is linear code of dimension k and distance d. Consider the code $C^2 \subseteq \mathbb{F}_2^{n \times n}$ consisting of all $n \times n$ matrices whose rows and columns belong to C. Show that C^2 is a code of dimension k^2 and distance d^2.

3. Prove that the orthogonal complement of the Reed-Solomon code is also a Reed-Solomon code.

4. Show how to use the Fast-Fourier-Transform to encode messages with the Reed-Solomon code in near linear time when the field is of size $q = 2^r + 1$, for some integer r. The key idea is to express a degree $k-1$ polynomial $f(X)$ as $f(X) = g(X^2) + Xh(X^2)$, where g, h have half the degree. Then $f(X)$ can be evaluated on the n points $\gamma, \gamma^2, \ldots, \gamma^n$ by recursively evaluating $g(X), h(X)$ on the points $\gamma^2, \gamma^4, \ldots, \gamma^{2n}$, and combining the results.

5. Show that if you take a code with rate R and relative distance δ, and concatenate it with another code of rate r and relative distance δ' (namely encode the symbols of the first code using the second code), then you get a code with rate Rr and relative distance $\delta\delta'$.

What kind of rate and relative distance can you get if the first code is the Reed-Solomon code, and the second is the binary code promised by the Gilber-Varshamov bound?