Problems

Let $B(x, r)$ denote the ball of radius r around x. Let $|B_n(r)|$ denote the volume of the ball of radius r in $\{0,1\}^n$.

1. This problem will give another proof that there exist codes of size $\Omega(\frac{2^n}{|B_n(d-1)|})$ with minimum distance $\geq d$.

   Let $x_1, x_2, \ldots, x_K$ be picked independently and uniformly at random from $\{0,1\}^n$.

   (a) Let A be the expected number of pairs $\{i, j\} \subseteq \{1, \ldots, K\}$ such that $\Delta(x_i, x_j) < d$. Compute A.

   (b) Show that if $K = \frac{2^n}{10|B_n(d-1)|}$ then $A < K/2$.

   (c) Use this to show that there exists a code C with minimum distance d with $|C| \geq \frac{1}{20} \cdot \frac{2^n}{|B_n(d-1)|}$.

2. The goal of this problem is to construct (inefficiently) a large *linear* code with minimum distance $\geq d$. In class we saw a greedy procedure to do this without the linearity constraint.

   Let $C \subseteq \mathbb{F}_2^n$ be a linear code with minimum distance $\geq d$. Show that if $|C| < \frac{2^n}{|B_n(d-1)|}$, then there exists an $x \in \mathbb{F}_2^n$ such that the linear space generated by C and x has minimum distance $\geq d$.

   Use this to prove that there exist linear codes C with $|C| \geq \frac{2^n}{|B_n(d-1)|}$.

3. Suppose k satisfies $2^k < \frac{1}{10} \frac{2^n}{|B_n(d-1)|}$.

   Show that a uniformly random k-dimensional subspace of $\mathbb{F}_2^n$ (or almost equivalently, the span of k uniformly and independently picked vectors), has minimum distance $\geq d$ with high probability.

4. Let H be a $t \times n$ matrix with $\mathbb{F}_2$ entries.

   Let C_H be the linear code:

   $$C_H = \{x \in \mathbb{F}_2^n \mid Hx = 0\}.$$

   Express the property "C_H has minimum distance at least d" in terms of some linear algebra property of the columns of H.

5. We will see an improvement to the existence result for codes (this is most interesting when $d = O(1)$), to get a slightly larger linear code.

   Let $v_1, \ldots, v_r$ be a collection of vectors in $\mathbb{F}_2^t$ such that no $d-1$ of them are linearly dependent. Show that if $B_r(d-2) < 2^t$, then there exists a vector $w \in \mathbb{F}_2^t$ such that no $d-1$ vectors out of

   $$\{v_1, \ldots, v_r, w\}$$

are linearly dependent.

Use this to show that for all d, for infinitely many n, there exists a linear code $C \subseteq \mathbb{F}_2^n$ with minimum distance $\geq d$ such that $|C| \geq \frac{2^n}{|B_n(d-2)|}$.

How does this code look when $d = 3$? This is the Hamming code.

6. Review all your linear algebra, but this time pay attention to which facts hold over finite fields, and which facts don't.

7. Show that there do not exist 4 vectors in $\{0,1\}^n$ with pairwise distance $\geq 2/3n$.

8. **(The Singleton Bound)** Show that if $C \subseteq \Sigma^n$ has minimum distance d, then $|C| \leq \frac{|\Sigma|^n}{|\Sigma|^{d-1}}$.

   In particular, Rate R and relative distance δ satisfy:

$$R + \delta \leq 1 + \frac{1}{n}.$$

9. Prove the Schwartz-Zippel Lemma: if $P(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ is nonzero of degree d, and $S \subseteq \mathbb{F}$, then

$$\Pr_{a \in S^m}[P(a) = 0] \leq \frac{d}{|S|}$$

10. Let C be a Reed-Solomon code of length $n = q$ over $\mathbb{F}_q$, rate 0.9 and relative distance 0.1.

    Let $t = \lfloor 5 \log q \rfloor$. Let $C_{in} \subseteq \{0,1\}^t$ be a code of relative distance 0.1 with $|C| = q$. (Thus the rate of C_{in} is approximately 0.2).

    Use C and C_{in} to somehow produce a code $C^* \subseteq \{0,1\}^{nt}$ with rate ≥ 0.15 and relative distance ≥ 0.005.