Essential Coding Theory
6.896
Due: Wednesday, October 30, 2002

Madhu Sudan

Problem Set 3

Instructions: See PS1.

1. Asymptotics of codes: Given $\epsilon > 0$ express the rate of the best family of binary codes of relative distance $\frac{1}{2} - \epsilon$, you can (a) construct, and (b) show the existence of. Express the rate in big-Oh notation (i.e., $O(\epsilon^d)$ implies there exist constants c and ϵ_0 such that for all $\epsilon < \epsilon_0$, the rate of the code of relative distance $\frac{1}{2} - \epsilon$ is at least $c\epsilon^d$.) How constructive are your codes in Part (a)?

2. Variants of RS codes: The two parts of this question consider variants of Reed-Solomon codes over $\mathbb{F}_q$, obtained by evaluations of polynomials at n distinct points $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. The message will be speified by a sequence of coefficients $c_0, \ldots, c_{k-1} \in \mathbb{F}_q$ and its encoding will be the evaluation of a polynomial $p(x)$ at $\alpha_1, \ldots, \alpha_n$. What will be different is the definition of $p(x)$ given $c_0, \ldots, c_{k-1}$. Give exact bounds on the distance of the resulting code. (Note, the distance may be a function of the set $\{\alpha_1, \ldots . \alpha_n\}$.)

   (a) $p(x) = \sum_{i=0}^{k-1} c_i x^{i+\ell}$, where ℓ is some non-negative integer.

   (b) $p(x) = \sum_{i=0}^{k-1} c_i x^{2i}$.

3. Hadamard matrices: Recall that an $n \times n$ matrix H all of whose entries are from $\{+1, -1\}$ is a Hadamard matrix if $H \cdot H^T = n \cdot I$ where the matrix product is over the reals and I is the $n \times n$ identity matrix.

   (a) Show that if there is an nxn Hadamard matrix then n is either 1 or 2 or a multiple of 4.

   (b) Given an $n \times n$ Hadamard matrix H_n and an $m \times m$ Hadamard matrix H_m, construct an $(nm) \times (nm)$ Hadamard matrix.

   (c) (Not to be turned in) Let q be a prime power equivalent to 3 modulo 4. Let $H = \{h_{ij}\}$ be the $(q+1) \times (q+1)$ matrix with $h_{ij} = 1$ if $i = 1$ or $j = 1$ or $i = j$, and $h_{ij} = (j-i)^{(q-1)/2}$ otherwise. Verify that H is a Hadamard matrix. (The purpose of this exercise is point out that Hadamard matrices of many size, and not just powers of 2, exist.)

4. Let C be an infinite family of binary codes obtained by concatenation of two infinite families of codes C_1 and C_2. (The ith code of C is obtained by concatenating the ith code of C_1 with the ith code in C_2. The block lengths of the codes in C_1 and C_2 tend to infinity as $i \to \infty$.) Give an upper bound on the rate of C as a function of its minimum distance.

5. Consider the following simple edit distance between strings: $x \in \Sigma^n$ is at distance d from $y \in \Sigma^m$ if y can be obtained from x by first deleting upto d coordinates of x and getting an intermediate string $z \in \Sigma^\ell$ where $\ell \geq n - d$, and then inserting up to d characters into z (at arbitrary locations) to get y. What are the analogs of the Singleton bound, the Hamming (packing) bound on codes, and the Gilbert-Varshamov bounds for this measure of distance?