Essential Coding Theory Madhu Sudan
6.896
Due: Wednesday, September 11, 2002

Problem Set 1

Instructions

References: In general, try not to run to reference material to answer questions. Try to think about the problem to see if you can solve it without consulting any external sources. If this fails, you may look up any reference material.

Collaboration: Collaboration is allowed, but limit yourselves to groups of size at most four.

Writeup: You must write the solutions in latex, by yourselves. Cite all references and collaborators. Explain why you needed to consult any of the references, if you did consult any.

Problems

1. (Linear Algebra Review): **(Need not be turned in.)**

   (a) Given a $k \times n$ matrix G with 0/1 entries, of rank k over $\mathbb{Z}_2$, generating a linear code $C = \{\mathbf{x} \cdot G | \mathbf{x}\}$, show that there exists an $n \times m$ matrix H, (henceforth referred to as the parity check matrix), such that $C = \{\mathbf{y} | \mathbf{y}H = \mathbf{0}\}$. What is the relationship between m, n and k above?

   (b) Give an efficient algorithm to compute such an H, given G, and vice versa.

   (c) Give an explicit description of the generator matrix of a Hamming code of block length $2^\ell - 1$.

2. (Binary Hamming code & bound):

   (a) What is the rate of the Hamming code of block length $2^\ell - 1$?

   (b) Show that if C is a t-error-correcting code in $\{0,1\}^n$, then $|C| \leq 2^n / \mathrm{Vol}(n,t)$, where $\mathrm{Vol}(n,t) = \sum_{i=0}^{t} \binom{n}{i}$.

   (c) Conclude that the Hamming codes of Part (a) are optimal in their performance.

3. (Extra Credit Question) For general q, give the best construction you can of a q-ary code of minimum distance 3.

4. (Pairwise independent spaces):

   (a) Let H be the $(2^\ell - 1) \times \ell$ parity check matrix of a binary Hamming code. Show that the collection of column vectors $\{H\mathbf{x}^T | \mathbf{x} \in \{0,1\}^\ell\}$ forms a pairwise independent space.

   (b) (Extra Credit Question) Show that any pairwise independent space on n bits must contain at least $n + 1$ points.

5. A Directed Cut (DiCut) in a directed graph $G = (V, E)$ is an ordered partition $(S, \overline{S})$ of V. The size of the DiCut is the number of edges $(u, v) \in E$ with $u \in S$ and $v \in \overline{S}$.

   (a) Show that every graph has a DiCut of size at least $|E|/4$.

   (b) Give a deterministic polynomial time algorithm to find such a DiCut in a given graph.

   (There are two natural solutions to this problem - one that involves pairwise independence and one that doesn't. Guess which one I want.)

6. The Hat Problem:

   (a) Lets say that a directed graph G is a subgraph of the n-dimensional hypercube if its vertex set is $\{0, 1\}^n$ and if $u \rightarrow v$ is an edge in G, then u and v differ in at most one coordinate. Let $K(G)$ be the number of vertices of G with in-degree at least one, and out-degree zero. Show that the probability of winning the hat problem equals the maximum, over directed subgraphs G of the n-dimensional hypercube, of $K(G)/2^n$.

   (b) Using the fact that the out-degree of any vertex is at most n, show that $K(G)/2^n$ is at most $\frac{n}{n+1}$ for any directed subgraph G of the n-dimensional hypercube.

   (c) Show that if $n = 2^\ell - 1$, then there exists a directed subgraph G of the n-dimensional hypercube with $K(G)/2^n = \frac{n}{n+1}$. (This is where the Hamming code comes in.)