Essential Coding Theory (MIT 6.440) Lecturer: Madhu Sudan
Problem Set 1 Due: Wednesday, February 27, 2013

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 try to limit yourselves to groups of size at most four.

Writeup: You must write the solutions by yourselves. Cite all references and collaborators. Explain why you needed to consult any of the references, if you did consult any. Submit the solutions electronically as a pdf file. Deadline is 11pm on due date.

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) Prove that for every positive integer ℓ, there is a "Hamming" code mapping $2^\ell - \ell - 1$ bit messages to $2^\ell - 1$-bit codewords that can correct any single bit error, and that this is optimal. Specifically:
   (b) Describe the "generator matrix" G and "parity check" matrix H for this code. (The description need not be fully explicit — it suffices to describe it to the extent that one can perform encoding and decoding in polynomial time.)
   (c) Prove that the matrices above lead to a code correcting single bit errors.
   (d) Prove that no single bit error-correcting code of length $2^\ell - 1$ can have more codewords than the code you've designed.
3. (Extra Credit Question) For general Σ, give the best construction you can of a code over alphabet Σ of minimum distance 3. (What can you do when $|\Sigma|$ is a power of a prime number? What can you do in other cases?)

4. (Pairwise independent spaces): A set $S \subseteq \{0,1\}^n$ is a *pairwise independent* space, if, for every pair $i \neq j \in \{1,\ldots,x\}$, it is the case that if you pick a random element of S and project it onto the ith coordinate and $j$the coordinate you get a *pair* of independent bits drawn uniformly from $\{0,1\}$.

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

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

5. The Hat Problem: **Oops!** *The earlier version of the pset was missing the description of the hat problem. Added now. Sorry!*

   The Hat Problem involves n people in a room, each of whom is given a black/white hat chosen uniformly at random (and independent of the choices of all other people). Each person can see the hat color of all other people, but not their own. Each person is asked if (s)he wishes to guess their own hat color. They can either guess, or abstain. Each person makes their choice without knowledge of what the other people are doing. They either win collectively, or lose collectively. They win if all the people who don't abstain guess their hat color correctly *and* at least one person does not abstain. They lose if all people abstain, or if some person guesses their color incorrectly. Your goal below is to come up with a strategy that will allow the n people to win, with pretty high probability. The problem involves some careful modelling, and some knowledge of Hamming codes!

   (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 $u \to v$ 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.)