Essential Coding Theory
CS 229r - Spring 2017
Due: Wednesday, February 8, 2017

Madhu Sudan

Problem Set 1

Instructions

Collaboration: Collaboration is allowed and encouraged, but you must write everything up by yourselves. You must list all your collaborators.

References: Consulting references is OK. However, 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. Cite all references (in addition to listing all collaborators). Explain why you needed to consult any of the references, if you did consult any.

"Not to be turned in" Problems . If a problem is marked "not to be turned in", you don't have to. But you must include a statement saying you know how to solve the problem. If you are unsure, write up your solution and turn it in. These problems won't count for your grades, but are good review exercises.

Submission: Submit your solutions on Canvas. If you do not have a canvas account, or are not taking this course for credit, but want to submit solutions to the psets anyway, please contact me (madhu) right away and I'll try to find a solution for you.

Algebra Review/Background

Please read up these concepts and make sure you are comfortable with them. The course will be a lot easier afterwards.

1. Review the definition of a field $\mathbb{F}$. Very quickly, a field $\mathbb{F} = (\mathbb{F}, 0, 1, +, *)$ (notice the abuse of notation in the use of $\mathbb{F}$ to denote the set, as well as the set endowed with special operations and elements) is a set with addition and multiplication that are both associative and commutative. 0 and 1 are two special elements of the field that act as the identity for addition and multiplication. In a field, every element has an additive inverse, and every nonzero element has a multiplicative inverse.

2. Verify that the rational numbers $\mathbb{Q}$ as well as $\mathbb{F}_2 = \{0, 1\}$ with addition and multiplication being performed modulo two are fields.

3. When is $\mathbb{F}_p = \{0, \ldots, p-1\}$, with addition and multiplication being integer addition and multiplication modulo p, a field?

4. Review the definition of a vector space V over a field $\mathbb{F}$. Roughly and vector space $V = (V, +, \cdot)$ over a field $\mathbb{F}$ has two operations, an addition of vectors which is commutative and associative and has an identity and additive inverse; and a scalar product $a \cdot v \in V$ for $a \in \mathbb{F}$ and $v \in V$ which distributes over addition.

5. Verify that the codewords of the Hamming code mapping $2^\ell - \ell - 1$ bits to $2^\ell - 1$ bits form a vector space over $\mathbb{F}_2$. (Most of the codes we will work with in this course will be linear codes over some field.)

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 some field $\mathbb{F}$, generating a linear code $C = \{\mathbf{x} \cdot G | \mathbf{x} \in \mathbb{F}^k\}$, show that there exists an $n \times m$ matrix H of rank m, (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) If $\mathbb{F}$ is the field of rational numbers, prove that a column of H can not be identical to a row of G.

   (d) Give an example of G over the field $\mathbb{F}_2$ such that $H = G^T$.

2. (Hamming Code)

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

   (b) Extend the Hamming code to the case of general fields. For a field $\mathbb{F}$ of size q, what are the parameters (i.e., message length) you obtain for codes over $\mathbb{F}$ of length $q^\ell - 1$ and distance at 3? (For the purposes of this question, the cases of $\mathbb{F}_3$ and $\mathbb{F}_5$ will provide sufficient intuition to guess the right answer.) Prove the optimality of your bound.

   (c) (Extra Credit/Open) When q is not a prime power (so no field of size q exists), what are the best parameters you can obtain for a q-ary code of distance 3? What about when $q = 6$?

3. (Capacity Analysis) For $p \in [0, 1]$, determine the capacity of the BEC(p), the Binary Erasure Channel with erasure parameter p, i.e., the channel that transmits a bit b as b with probabilty $1 - p$ and as a "?" with probablility p, and does this independently across each bit. In particular:

   (a) show that there exists an encoding and decoding scheme that can communicate k bit messages at rate artbitrarily close to your capacity with error exponentially small in k.

   (b) Next, prove a converse showing that no encoding and decoding scheme can do better than your capacity.

   (c) For extra credit, show that you can do all this with efficient encoding and decoding algorithms. (It is ok if the "algorithm" is non-uniform. For example, if the encoding is

by multiplying by a matrix, it is sufficient to show that given the matrix, the encoding is efficient (which is obvious). You don't have to worry about how to find the matrix, or any other polynomial sized description of the code.)

4. (Volume of the Hamming Ball) **(Need not be turned in.)** Recall the definitions below of a Hamming distance, sphere, and ball.

   - For $x, y \in \{0,1\}^n$, the Hamming distance between x and y, denoted $\Delta(x,y)$, is given by $\Delta(x,y) = |\{i \in [n] | x_i \neq y_i\}|$.
   - For $x \in \{0,1\}^n$, and integer $0 \leq r \leq n$, let $\text{Sphere}(x,r) = \{y \in \{0,1\}^n | \Delta(x,y) = r\}$. Let $\text{Vol}^=(n,r) = |\text{Sphere}(0^n, r)|$.
   - For $x \in \{0,1\}^n$, and integer $0 \leq r \leq n$, let $\text{Ball}(x,r) = \{y \in \{0,1\}^n | \Delta(x,y) \leq r\}$. Let $\text{Vol}(n,r) = |\text{Ball}(0^n, r)|$.

   (a) Verify that for every $x \in \{0,1\}^n$, $|\text{Sphere}(x,r)| = \text{Vol}(n,r)$.

   (b) Use Stirling's approximation to show that for every fixed p, we have $2^{H(p)n - O(\log n)} \leq \text{Vol}^=(pn, n) \leq 2^{H(p)n + O(\log n)}$. (You can use the following "Stirling's approximation". For every m, $m! = \sqrt{2\pi m}(m/e)^m \lambda_m$ where $1/(12m+1) \leq \lambda_m \leq 1/(12m)$.)

   (c) For $r \leq n/2$ prove that $\text{Vol}(n,r) \leq r \cdot \text{Vol}^=(n,r)$. [For extra credit, give tight bounds on $\text{Vol}^=(n,r)/\text{Vol}(n,r)$ — tight to within constant factors. When this ratio is $1 - o(1)$, determine the $o(1)$ function as a function of r and n.]

   (d) Conclude that for every fixed p, $2^{H(p)n - O(\log n)} \leq \text{Vol}(pn, n) \leq 2^{H(p)n + O(\log n)}$.

5. The Hat Problem: This 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 do get to strategize collectively before seeing any of the hats, but after the hats are assigned, they can not communicate and do not hear the choices made by the other players.) 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 the use 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.)