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

Madhu Sudan

Problem Set 3

Instructions: As usual

Problems

1. (Duality)
   (a) Prove that the dual of a Reed-Muller code with parameters m (number of variables), q (Field size), and r (degree of polynomials) is a Reed-Muller code. What is the degree parameter of the dual?
   (b) A linear code is said to an MDS (Maximum distance seperable) code if it is an $[n, k, n-k+1]_q$ code. Prove that the dual of an MDS code is an MDS code.

2. **(Need not be turned in.)** (Abstract decoding: Filling in details). Fill in the details of the abstract decoding algorithm using error-locating pairs. Specifically:
   (a) Specify the conditions under which codes $\mathcal{E}$ and $\mathcal{W}$ form a t-error-locating pair for code $\mathcal{C}$.
   (b) Describe the decoding algorithm.
   (c) Prove that it corrects every pattern of up to t errors.
   (d) How many errors + erasures can you correct?

3. (AG codes and decoding). Say that a collection of vectors $v_0, \ldots, v_{n-1} \in \mathbb{F}_q^n$ form an algebraic space of genus g if for every i, $C_i = \text{span}\{v_0, \ldots, v_{i-1}\}$ is a code of distance $\geq n - i + 1$ and dimension $\geq i - g$, and for every i, j it is the case that $v_i * v_i \in C_{i+j}$. The codes C_i are referred to as the algebraic geometry (AG) codes over this space.

   Show that for every i, the AG code C_i is decodable in polynomial time from $(n-i)/2 - O(g)$ errors.

4. (Concatenation and Capacity.) In this problem we will show that achieving the capacity with arbitrarily small error probability leads to achieving capacity with exponentially small error probability without losing much in algorithmic efficiency.

   Fix $p \in (0, 1/2)$ and *suppose* the following is true: For every $\epsilon > 0$ there is a code C_ϵ of block length $\text{poly}(1/\epsilon)$ of rate $1 - H(p) - \epsilon$ such that encoding and decoding with this code take time $\text{poly}(1/\epsilon)$ and this code can recover from the BSC(p) channel (the one that flips bits

independently with probability p) with failure probability at most ϵ. (So probability that the decoding of a corrupted encoding of a random message does not equal the message is at most ϵ).

Then prove that for every $\epsilon > 0$ there is a $\delta > 0$ such that for every n there is a code $C_{n,\epsilon}$ of block length n, rate $1 - H(p) - \epsilon$ that can be encoded and decoded in time $\mathrm{poly}(n/\epsilon)$ such that this code recovers from $\mathrm{BSC}(p)$ with failure probability at most $2^{-\delta n}$.