EE 229B ERROR CONTROL CODING **Spring 2005**

Homework 1 : Due by 10 p.m. on Tuesday February 22

1. *Is there room ?*

   Prove or disprove :

   There is a (12,7) binary linear code with $d_{min} = 5$.

2. (*Extended Hamming code*)

   The first problem relates to a specific (8,4) code. This is an *extension* of the (7,4) Hamming code considered in Example 3.1 on pg. 67 of the text, as you will see after constructing a systematic generator matrix for this code. In general, an extension of a linear code is any code got from it by adding more columns to the generator matrix. This process can be thought of as adding more parity check symbols to the code. The various parts of this problem correspond to individual problems on pp. 95 -96 of the text, as indicated below. The first two parts correspond to problem 3.1 on pg. 95 of the text.

   (a) Consider a binary (8,4) code whose parity-check equations are

   $$\begin{aligned} v_0 &= u_1 + u_2 + u_3 \ , \\ v_1 &= u_0 + u_1 + u_2 \ , \\ v_2 &= u_0 + u_1 + u_3 \ , \\ v_3 &= u_0 + u_2 + u_3 \ . \end{aligned}$$

   where $u_0,\ u_1,\ u_2,\ u_3$ are message digits and $v_0,\ v_1,\ v_2,\ v_3$ are parity-check digits. The codeword is $(v_0, v_1, v_2, v_3, u_0, u_1, u_2, u_3)$. Find systematic generator and parity-check matrices for this code.

   (b) Show that the minimum distance of this code is 4.

   (c) (*This is problem 3.2 on pg. 95 of the text.*)
   Construct (on paper, as a diagram) an encoder for this code.

   (d) (*This is problem 3.3 on pg. 95 of the text.*)
   Construct (on paper, as a diagram) a syndrome circuit for this code.

   (e) (*This is problem 3.9 on pg. 96 of the text.*)
   Determine the weight profile of this code. Compute the probability of undetected error when this code is used over a binary symmetric channel with crossover probability $p = 10^{-2}$ (assuming maximum likelihood decoding and that all codewords are a priori equiprobable).

   (f) (*This is problem 3.11 on pg. 96 of the text.*)
   Construct (on paper, as a diagram) a decoder for this code that is capable of correcting all single-error patterns and simultaneously detecting any combination of double errors. Specifically, if the received vector is at Hamming distance 1 from a codeword, the decoder should return that codeword, while if the received vector is at Hamming distance 2 from a codeword, the decoder should return an indicator that this is the case.

(g) (*This is problem 3.14 on pg. 96 of the text.*)
Show that this code is self-dual.

3. (*Punctured Reed-Muller code*)

The punctured Reed-Muller code $RM^*(r,m)$ is derived from the Reed-Muller code $RM(r,m)$ by deleting the coordinate corresponding to $v_1 = v_2 = \ldots = v_m = 0$ from all the codewords. In general *puncturing* a code is the term used for the process of getting another code by deleting some of the symbols of the original code. This way the number of message symbols remains the same, but the redundancy is reduced.

(a) Verify that $RM^*(r,m)$ is a $(2^m - 1, 1 + \binom{m}{1} + \ldots + \binom{m}{r})$ code with $d_{min} = 2^{m-r} - 1$.

(b) Show that it is possible to reorder the transmitted bits in $RM^*(1,3)$ so that the resulting code is the $(7,4)$ Hamming code considered in Example 3.1 on pg. 67 of the text.

Hint: Argue that, since $RM^*(1,3)$ is a $(7,4,3)$ binary code, it is perfect. What does this say about its dual code ?

(c) Is there any relation between the RM(1,3) code and the (8,4) extended Hamming code considered in the preceding problem ? Explain your answer.

4. (*RM(2,5) code*)

(a) Write down a generator matrix for the RM(1,4) code (which is a (16,5) code with $d_{min} = 8$).

(b) Describe in detail the steps involved in majority logic decoding for this code. Specifically, for each information bit, determine all the check sums whose majority needs to be taken by the majority logic decoder.