Algorithms in the Real World (15-853), Fall 08
Assignment #2 Due: 9 October 08

You can look up material on the web and books, but you cannot look up solutions to the given problems. You can work in groups, but must write up the answers individually. Note that there are five problems on two pages. **Due October 9.**

Problem 1: Binary versus q-ary Codes (10pt)

In class we showed a lower bound on the number of code bits required to fix s bit-errors for a binary linear code with with k message bits. In particular by arguing that every codeword requires a ball of radius $(d-1)/2$ around it we derived the formula

$$n \geq k + \log(1 + \sum_{i=1}^{s} \binom{n}{i}) \ .$$

Generalize this to q-ary codes.

Problem 2: Ever Wonder about ISBN? (15pt)

The ISBN is a 10-digit codeword such as 0-471-06259-6. The first digit indicates the language (0 for English), the next group specifies the publisher (471 for Wiley); the next group forms the book number assigned by the publisher. The final "digit" is chosen to make the entire number $x_1 \cdots x_{10}$ satisfy the single check equation: $\sum_{i=1}^{10}(ix_i) = 0 \pmod{11}$.
Note that the first 9 digits lie between 0 and 9, whereas the last "digit" can take any value between 0 and 10, where the value 10 is represented by the letter X.

A. What are the parameters of this code in the $(n, k, d)_q$ notation (i.e., what are n, k, d and q).

B. Calculate the check digit for the message 0-13-200809.

C. It is easy to see that the ISBN code can detect any single digit error. Show that the code can detect the transposition of any two digits (not necessarily consecutive).

D. The sixth digit in the code 0-13-28?796-X was smudged. Find the missing digit.

Problem 3: Reed Solomon (10pt)

Suppose that there is a very inexpensive PCI board that implements an $RS(255, 223)$ Reed Solomon encoder and decoder in hardware. (This is most likely true!) The board encodes or decodes sequences of 223 bytes and can correct up to 16 errors in a sequence. You would like to use Reed-Solomon codes to protect your data against errors as it is transmitted over a wireless communication channel. Unfortunately, your radio experiments show that, at your transmission rate, bursts of errors tend to be longer than 16 bytes. Using the $RS(255, 223)$-encoder/decoder as a building block, design a system that can correct up to 64 consecutive errors in a 1020-byte transmitted message, assuming that there are no other errors in the message. You must preserve the rate of the channel.

Problem 4: Binary cyclic codes (10pt)

How many linear binary cyclic codes of block length 15 are there? In particular, how many distinct generator polynomials are there?

Problem 5: A variant on LDPC codes (15pt)

Consider the following variant on LDPC codes. Like LDPC codes the code is given by a bipartite graph, but now assume that the neighbors for each node on the right must form a proper Hamming code. To be concrete lets assume each vertex on the right has degree 15 and the bits on the neighbors must form a $(15, 11, 3)$ Hamming code. We will assume each vertex on the left has degree $d = 3$ so the number of nodes on the right is $n/5$.

1. What is the rate of this code (i.e. k/n)?
2. Assuming the bipartite graph has expansion (α, β) with $\beta = d/2 = 1.5$ prove that the code has distance at least αn. This is a similar argument to the one given in class for LDPC codes, but for LDPC codes we required that $\beta > d/2$.