Algorithms in the Real World
Assignment #1 Due Date: 26 September 02

Problem 1: (30pt)
Let $H = \left[A^T I_{n-k}\right]$ be the parity check matrix for a binary linear block code, as described in class. Prove that the minimum Hamming distance between any two codewords is d, where $d \geq 2$, if and only if the columns of H are $(d-1)$-wise independent. (The columns of H are $(d-1)$-wise independent if and only if no column can be expressed as a sum of $d-2$ or fewer columns. For $d = 2$, this implies that no column is all zeroes. For $d = 3$, this implies that no two columns are identical.)

Problem 2: (10pt)
The NASA Mariner deep-space probes launched between 1969 and 1977 were equipped with a (32,6,16) Reed-Muller code for the transmission of pictures from the Moon and from Mars. As mentioned in class, Reed-Muller codes are the dual of extended Hamming codes. In particular the (32,6,16) Reed-Muller code is the dual of the (32,26,4) extended Hamming code. These codes have the feature that they can detect up to $n/2$ errors and are hence well suited for very noisy channels. Give three codewords for the (32,6,16) Reed-Muller code. These must be in systematic form—i.e. from a generator matrix in standard form.

Problem 3: (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: (10pt) How many binary cyclic codes of block length 15 are there? In particular, how many distinct generator polynomials are there?

Problem 5: (10pt) Consider a $(3, 1, 3)_4$ RS code. The symbols are from the field GF(2^2) over polynomials modulo $x^2 + x + 1$ ($00 = 0, 01 = 1, 10 = x, 11 = x + 1$). Consider $\alpha = 10$ with $g = (x - \alpha)(x - \alpha^2)$. List the valid codewords (e.g. is 00 01 10 a codeword?). As in the notes and class, the leftmost symbol is the most significant.