Math 406

Assignment 1

Due 2 October 2014

Note: Problems marked with an asterisk (*) are only for graduate students.

[2] 1. Let $C$ be a $q$-ary $(n, M, 3)$-code. Prove that the *Hamming bound* $B_H = q^n/V_q(n, 1)$ is better (i.e., smaller) than the *Singleton bound* $B_S = q^{n-3+1}$ if and only if $n > q + 1$.

[6] 2. The (old) International Standard Book Number (ISBN) system, which was used to uniquely identify books up to 2007, is a code defined over the 11-letter alphabet $F = \{0, 1, \ldots, 9, X\}$, where $X$ represents the number 10. An ISBN codeword has length 10 and is written as $a_1a_2\ldots a_{10}$. (In practice, these numbers are interspersed with several hyphens for readability.) The first nine digits are “information digits” which record data such as country, publisher, title and edition. The tenth digit is a check digit, chosen so that

$$\sum_{j=1}^{10} j \cdot a_j \equiv 0 \pmod{11}.$$  

For example, S. Lang’s Algebra (Springer, 2002) has ISBN 0-387-95385-X.

(a) Find the minimum distance for this code, and use this to show that the nearest neighbour decoder for this code can detect 1 but not 2 errors. Moreover, show that it detects one transposition error ($a_ja_{j+1}$ becomes $a_{j+1}a_j$, for some $j, 1 \leq j \leq 9$).

(b) Verify that this is a linear code and determine its parity check matrix. What are the code parameters (and the code rate) for this code?

(c) In practice, the digit “X” is only allowed in the 10th check digit. Show that the code obtained by imposing this extra restriction is no longer linear. (Give an explicit example which shows the failure of linearity.)

[4] 3. The following is a parity check matrix for a binary $[n, k]$-code $C$:

$$
\begin{pmatrix}
1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1
\end{pmatrix}.
$$

(a) Find $n$ and $k$ and the generator matrix for $C$.

(b) List the codewords in $C$ and determine the minimum distance $d(C)$. 
4. Determine the dimension and minimum distance of the linear code $C$ over $\mathbb{F}_{11}$ (= $\mathbb{Z}/11\mathbb{Z}$, the field of integers modulo 11) with parity check matrix

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & 10^2 \end{pmatrix}.$$ 

5*. A Hadamard matrix of order $n \geq 2$ is an $n \times n$ matrix $H$ whose entries lie in $\{-1, 1\} \subset \mathbb{R}$ such that $HH^t = nI$, where $I$ is the identity matrix.

(a) Show that the Hamming distance of any two rows of $H$ is $n^2/2$.

(b) Suppose that $n = 2^m$, where $m \geq 1$. Let $\mathbb{F}_2^m = \{v_1, \ldots, v_n\}$ be a listing of all vectors in $\mathbb{F}_2^m$, and let $v_i \cdot v_j \in \mathbb{F}_2$ be the dot product of $v_i v_j \in \mathbb{F}_2^m$. Show that the $n \times n$ matrix

$$H = (h_{ij}), \quad \text{where } h_{ij} = (-1)^{v_i \cdot v_j},$$

is a Hadamard matrix of order $n$.

6. MAPLE problem (refer to the MAPLE instruction sheet):

(a) Use a nested sequence command of the form $\text{seq}(\text{seq}(\text{seq}(\text{seq}(...))))$ to construct a list all elements in $\mathbb{F}_2^4$. Use this list to construct a list of all non-zero elements in $\mathbb{F}_2^4$.

(b) Use part (a) and one of Maple’s linear algebra packages to construct a parity check matrix $H$ of the $[15, 11, 3]$ (binary) Hamming code.

(c) Use Maple to interchange suitable columns in your parity check matrix $H$ of part (b) to bring $H$ into the standard form $H_1 = [A|I]$, and hence determine a generating matrix $G$ for a (systematic) Hamming code. Check that $H_1G^t = 0$. 