Institut für Mathematische Optimierung
TU Braunschweig

Prof. Dr. Sándor Fekete
Nils Schweer

SS 2006

Coding Theory / Discrete Mathematics II
Assignment 1 (April 27, 2006)

(This assignment is due on May 04, 2006, 1.00 p.m., by dropping it into the wooden box **in front of** F 310)

Exercise 1 (Hamming Code):

We assume that the (original) data we want to send is given by a sequence of zeros and ones. We call a 0 or 1 a *digit* and a vector of a certain number of digits a *word*. The *length* of a word is the number of digits in the word. An *(n,k) code* turns data with words of length k into words of length n.
Now let us consider a particular (7,4) code, the *(7,4) Hamming code*: let (b_1, b_2, b_3, b_4) be an original word. Then the code word $(c_1, c_2, \ldots, c_7)$ is built as follows: $c_1 = b_1, c_2 = b_2, c_3 = b_3, c_4 = b_4, c_5 = b_2 + b_3 + b_4, c_6 = b_1 + b_3 + b_4, c_7 = b_1 + b_2 + b_4$, with addition being defined modulo 2, i.e., $0 + 0 = 0$, $1 + 0 = 1$, $0 + 1 = 1$, $1 + 1 = 0$. For example, the word $(0, 0, 1, 1)$ gets mapped to the code word $(0, 0, 1, 1, 0, 0, 1)$. Let C be the resulting code, i.e., the set of code words that can occur, and consider the Hamming distance $x, y \in C$, i.e., *d(x,y) = Number of different bits in x and y*. Recall that the *Hamming distance of a code C* is defined as $min\{d(x, y) : x, y \in C, x \neq y\}$.

a) Give an explicit description of the code by listing all words of length 4 and the corresponding code words.

b) Show that the (7,4) Hamming code has Hamming distance 3.

(30 Points)

Exercise 2 (Correcting errors):

A code word $c = (c_1, c_2, \ldots, c_n) \in C$ is transmitted over a noisy channel. Because of transmission errors, some bits are changed and c is turned into the word $\tilde{c} = (\tilde{c}_1, \tilde{c}_2, \ldots, \tilde{c}_n)$. In order to correct these errors, $\tilde{c}$ is mapped to the code word $\hat{c}$ closest to it. If $\hat{c} = c$, then the errors are *corrected*.
Now let C be an arbitrary (n,k) code with Hamming distance $2m + 1$ for some $m \in \mathbb{N}$. Prove that one can correct up to m errors.
(Hint: You can use the fact that $d(a, c) \leq d(a, b) + dist(b, c)$ for $a, b, c \in \{0, 1\}^n$.)

(30 Points)