IV054 Coding, Cryptography and Cryptographic Protocols

2009 – Exercises I.

1. a) Construct a Huffman code for letters A, B, C, D and E with frequencies of use given in the following table.

letter	frequency
A	40%
B	30%
C	20%
D	5%
E	5%

   b) Find the average word length.

2. a) Consider the ISBN number 0486x00973. Determine x. Which book has this ISBN code?

   b) Consider the code $C = \{x \in \mathbb{Z}_{10}^9 \mid \sum_{i=1}^{9} ix_i = 0 \pmod{10}\}$. Show that this version of the ISBN code is not able to detect transposition errors.

3. Find the minimal distance of the code $C = \{10001, 11010, 01101, 00110\}$. Decode the strings 11110, 01101, 10111, 00111 using the nearest neighbour decoding strategy.

4. Consider a binary symmetric channel.

   a) Show that the nearest neigbour decoding strategy and the maximal likelihood decoding strategy are the same.

   b) Why there is an assumption that probability of error $p < \frac{1}{2}$?

5. A (v, b, k, r, λ) block design D is a partition of v elements $e_1, e_2, \ldots, e_v$ into b sets (blocks) $s_1, s_2, \ldots, s_b$, each of cardinality k, such that each of the objects appears exactly in r blocks and each pair of them appears exactly in λ blocks. An incidence matrix of a (v, b, k, r, λ) block design is a $v \times b$ binary matrix M such that for any $(i, j) \in \{1, 2, \ldots, v\} \times \{1, 2, \ldots, b\}$ $m_{i,j} = 1$ if $v_i \in s_j$ and $m_{i,j} = 0$ otherwise.

   Let D be a (v, b, k, r, λ) block design. Consider a code C whose codewords are rows of the incidence matrix of D:

   a) Show that each codeword of C has the same weight.

   b) Find the minimal distance of C.

   c) How many errors is C able to correct and detect?

6. Show that the following codes are perfect:

   a) codes $C = \mathbb{F}_q^n$;

   b) codes consisting of exactly one codeword;

   c) binary repetition codes of odd length;

   d) binary codes of odd length consisting of a vector c and the vector c' with 0s and 1s interchanged.