IV054 Coding, Cryptography and Cryptographic Protocols

2008 – Exercises I.

1. Consider the ternary code $C = \{0000, 1111, 2222\}$ of length 4.
   (a) Using the nearest neighbour decoding strategy, find all words uniquely decoded as the word 1111.
   (b) Suppose that any symbol is erroneously received with probability p and that all symbols are equally likely. Find probability P of the event that a received word is incorrectly decoded as 1111.
2. For any words $x = x_1 \cdots x_m$ and $y = y_1 \cdots y_n$, let us define the operation $\circ$ as $x \circ y = x_1 \cdots x_m y_1 \cdots y_n$. For any (n, M_1, d_1) code C_1 and (m, M_2, d_2) code C_2, let $C_3 = \{x \circ y \,|\, x \in C_1, y \in C_2\}$ be (x, y, z) code. Determine x, y and z.
3. Consider any perfect binary $(n, M, 7)$ code. There are only two possible values of n. Try to find them.
4. Determine M and d for a q-ary code

$$C = \{x_1 \cdots x_n \mid x_1, \ldots, x_n \in \{0, 1, \ldots, q-1\} \wedge x_1 + \cdots + x_n = kq,\ k \in \mathbb{N}_0\}.$$

5. Consider an ISBN number $0444x50090$. Determine x. Try to find out which book has this ISBN code.
6. Which of the following codes cannot be a Huffman code for any probability distribution.
   (a) $C_1 = \{00, 01, 1\}$
   (b) $C_2 = \{001, 01, 10, 11\}$
7. Let $q > 0$. What is the relation $(\leq, =, \geq)$ between
   (a) $A_q(n, d)$ and $A_q(n/2, d/2)$;
   (b) $A_q(n, d)$ and $A_q(n+2, d+1)$;
   (c) $A_q(n, d)$ and $A_{2q}(n, d)$;
   (d) $A_q(n, d)$ and $A_q(n+2, 2d)$;
   (e) $A_2(n, 2d-1)$ and $A_2(n+1, 2d)$;
   (f) $A_q(n, d)$ and q^{n-d+1}.
8. Show that for $t > 0$ there is no perfect binary $(n, M, 2t+1)$ code, such that $n = 2^k$ for some $k \in \mathbb{N}$.