IV054 Coding, Cryptography and Cryptographic Protocols
2013 - Exercises I.

1. Determine d and M for a q-ary code

$$C = \{x_1 \dots x_n \mid \Sigma_{i=1}^{n} x_i = 0 \pmod q\}.$$

2. Consider an ISBN number 063201x364. Determine x and find out which book has this ISBN code.

3. Consider a source that generates symbols 0 and 1 with frequencies 0.9 and 0.1, respectively. These symbols are consequently transferred by a

   a) binary symmetric channel,

   b) Z-channel (binary asymmetric channel)

   with $p = 0.15$.

   What is the probability that the symbol 1 was sent provided that the symbol 0 was received? (Recall that in Z-channel, $1 \to 0$ occurs with probability p whereas $0 \to 1$ never occurs.)

4. Let $C = \{111111, 110000, 001100, 000011\}$. Suppose that the codewords are transmitted using a binary symmetric channel with error probability p. Determine the probability that the receiver does not notice that a codeword has been corrupted during a transfer.

5. Let $q > 0$. What is the relation ($\leq$, $=$, $\geq$) between

   a) $A_2(n, 2d-1)$ and $A_q(n+1, 2d)$,

   b) $A_q(n, d)$ and q^{n-d+1},

   c) $A_q(n, d)$ and $A_q(n+2, 2d)$,

   d) $A_q(n+1, d)$ and $A_q(n, d)$.

6. For each of the following pairs of binary codes, prove their equivalence or prove that they are not equivalent:

   a)
$$A = \left\{\begin{matrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{matrix}\right\} \qquad B = \left\{\begin{matrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{matrix}\right\},$$

   b)
$$C_0 = \{0\} \qquad C_{i+1} = \left\{ \begin{array}{c|c} C_i & \begin{matrix} 1 \\ 0 \\ 1 \\ 0 \\ \vdots \end{matrix} \\ \hline 1 \;\; 0 \;\; 1 \;\; 0 \;\; \dots & (1+(-1)^i)/2 \end{array} \right\}$$

$$D_0 = \{1\} \qquad D_{i+1} = \left\{ \begin{array}{c|c} D_i & \begin{matrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{matrix} \\ \hline 0 \;\; 1 \;\; 1 \;\; \dots \;\; 1 & 1 \end{array} \right\}.$$

More on next page >>>

7. Assume a source **X** sends messages `A`, `B`, `C`, `D` with the following probabilities:

symbol	probability
`A`	0.8
`B`	0.1
`C`	0.05
`D`	0.05

a) Calculate the entropy of the source **X**.

b) Create a Huffman code (binary) for the source **X**. Determine the average number of bits used per symbol.

c) Assume the source sends sequences of thousands of messages in blocks of length `16`. Assume that the probability of each symbol occuring is independent of the symbol that have previously occured.

Find a way to modify the creation of Huffman code so that the average number of bits used per source symbol decreases to a value no greater than 110% of source entropy. Design a code using this modification and determine the average number of bits per symbol achieved.