IV054 Coding, Cryptography and Cryptographic Protocols
2019 - Exercises I.

1. *(2 points)* Your friend wants to recommend you an interesting book. To save time, she sends the ISBN code instead of the complete book title. Unfortunately, you have received the following incomplete 13-digit ISBN code:

   978-80-74?2-498-7

   Find the missing digit and reveal the title of the book.

2. *(8 points)* Consider the following code constructions and calculate the corresponding (n, M, d) parameters.

   (a) **m-fold repetition:** Each ℓ bit message is copied m times to create a codeword. Formally,

   $$C_{\ell,m} = \{w^m \mid w \in \{0,1\}^\ell\}.$$

   (b) **Checksum of neighboring pairs of bits:** Each ℓ bit message is appended with XORs (denoted $\oplus$) of all *neighboring* pairs of bits. Note that the last bit is XORed with the first one. Formally,

   $$C_\ell = \{w_1 \dots w_\ell b_1 \dots b_\ell \mid (w_1 \dots w_\ell) \in \{0,1\}^\ell, b_i = w_i \oplus w_{(i+1) \mod \ell}\}.$$

   (c) **Checksum of each pair of bits:** Each ℓ bit message is appended with XORs (denoted $\oplus$) of *all* pairs of bits. Formally,

   $$C_\ell = \{w_1 \dots w_\ell b_{1,2} \dots b_{i,j} \dots b_{\ell-1,\ell} \mid (w_1 \dots w_\ell) \in \{0,1\}^\ell, b_{i,j} = w_i \oplus w_j, i < j\}.$$

3. *(4 points)* Consider the following binary codes:

   (a) $C_1 = \{001, 110\}$;

   (b) $C_2 = \{0000, 1110, 0101\}$.

   i. For each possible received word find the codeword which will be determined by maximal likelihood principle as the one that was sent (only for cases when such codeword can be uniquely determined).

   ii. For each codeword calculate the probability that the codeword will be decoded correctly given that the probability of bit error is $p = 0.05$.

4. *(4 points)* Decide which of the following pairs are equivalent codes. Explain your answer:

   (a) $C_1 = \{0000, 1100, 1010, 1110, 0011\}$,
   $C_2 = \{1111, 0011, 0101, 0001, 1100\}$

   (b) $C_1 = \{0000, 1110, 1100, 1010, 0011\}$,
   $C_2 = \{1111, 1110, 0111, 1101, 0110\}$

   (c) $C_1 = \{x_1x_2x_3x_4x_5 \mid x_i \in \{0,1\}, \sum_{i=1}^5 x_i \equiv 0 \pmod 2\}$,
   $C_2 = \{x_1x_2x_3x_4x_5 \mid x_i \in \{0,1\}, \sum_{i=1}^5 x_i \equiv 0 \pmod 3\}$

More on next page >>>

5. *(6 points)* Consider a source X producing symbols A, B, C, D, E, and F with the following probabilities:

symbol	probability
A	0.30
B	0.15
C	0.15
D	0.20
E	0.10
F	0.10

   (a) Calculate the entropy of the source X.

   (b) Design the Huffman code and calculate its average codeword length and compare its efficiency for:

      i. bits and a binary code and

      ii. trits and ternary code.

   (Note that for a non-binary code, to ensure we have enough symbols to combine in each step of the code construction, we may need to add dummy symbols with probability 0.)

6. *(6 points)*

   (a) Determine $A_2(8, 5)$ and find a binary $(8, M, 5)$-code such that $M = A_2(8, 5)$.

   (b) Let $A_q(n, d, w)$ is the largest M such that there is a q-ary (n, M, d)-code whose codewords have weight w.
   Determine $A_q(n, d, w)$ if $d > 2w$. Prove your answer.