

IV054 Coding, Cryptography and Cryptographic Protocols
2018 - Exercises I.

1. Give an example of
 - (a) a binary $(3, 3, 2)$ code;
 - (b) a ternary $(4, 9, 3)$ code.
2. Let C_1 and C_2 be two block codes of length n . Show that the following holds
 - (a) $h(C_1 \cap C_2) \geq \max\{h(C_1), h(C_2)\}$.
 - (b) $h(C_3) = h(C_1) + h(C_2)$, where

$$C_3 = \{x_1y_1x_2y_2 \dots x_ny_n \mid x_1 \dots x_n \in C_1, y_1 \dots y_n \in C_2\}.$$

3. Any two equivalent q -ary codes have the same (n, M, d) parameters. Are any two q -ary codes with the same (n, M, d) parameters equivalent? Prove your answer.
4. Consider a worker in a supermarket finds out a product with corrupted EAN-13 barcode 858x035361404. Help him to find the missing digit x .
5. Show that the Hamming distance satisfies the triangle inequality, *i.e.*

$$h(x, z) \leq h(x, y) + h(y, z),$$

for any words x, y, z .

6. You are going to pay a conference fee for a coding theory conference. Organizers decided to test your knowledge by sending you an incomplete bank account number CZ85 2018 0000 0012 3423 x091 written in the International Bank Account Number (IBAN) format. Determine the missing number.
7. Let $y = (1, 4, 3, 5, 6, 7, 2)$ be the weight vector. Consider a code with codewords such that $\sum_{i=1}^7 y_i x_i \equiv 0 \pmod{8}$.
 - (a) Can this code detect or correct any single error?
 - (b) Can this code detect or correct any transposition error?

Justify your answer.

8. Consider a source is producing symbols with the following probabilities:

A		0.1
B		0.4
C		0.1
D		0.2
E		0.2

- (a) Construct a binary Huffman code with minimum variance of codeword length.
- (b) Calculate the average bit length of the code constructed in (a).