Algorithms of Information Security

Exercises for *Key generation algorithms* and *Error-correcting codes I*

Key generation algorithms:

1. Let $s = 0, 0, 1, 0, 0, 1, 0, 0, 1, \ldots$ be a sequence. Find:

   a) period and cycle of the sequence

   b) gaps and blocks

   c) $C(0), C(1), C(2)$ and $C(3)$.

   [Results: a) period is 3, cycle is $s^3 = 0, 0, 1$, b) 0,0 is a gap, 1 is a block, etc., c) $C(0) = C(3) = 1, C(1) = C(2) = -\frac{1}{3}$]

2. Let s be a periodic sequence with period $N = 15$ and cycle

   $$s^{15} = 0, 1, 1, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1.$$

   Verify Golomb's randomness postulates.

   [Result: All three postulates are satisfied.]

3. We have a dice and we want to verify whether the dice is regular. We roll the dice 48 times and get the following roll frequencies:

Value	1	2	3	4	5	6
Frequency	10	6	14	2	4	12

   Is the cube regular? Apply Chi-square goodness of fit test and choose the level of significance $\alpha = 0.05$

   [Result: We reject the hypothesis H_0 that the dice is regular.]

4. Let s be a sequence of length $n = 160$, that contains the following subsequence repeated 4 times:

   $$1110001100010001010011101111001001001001.$$

   Apply frequency (monobit) and serial test. The level of significance is $\alpha = 0.05$.

   [Results: The sequence passed both tests.]

Error-correcting codes I:

5. Consider the field F_3 and let the generating matrix of [5,3]-code be as follows:

   $$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

   Convert the matrix G to the standard form and find the parity check matrix H of the code.

   [Results: the matrix in standard form is

   $$G' = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

   and parity check matrix is

   $$H = \begin{pmatrix} 2 & 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

   ]

6. Consider the following binary code $C = \{(0, 0, 0), (1, 0, 1), (0, 1, 1), (1, 1, 0)\}$.

a) Prove that C is a linear code.

b) Find the distance d of the code C.

c) Find the generating matrix G of the code C.

[Results: a) prove that C is a vector space, b) $d = 2$, c)

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

]