

Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 6
Version 28.05.2020

Exercise 1.

Check whether the following given homomorphic codification over the alphabet $B = \{0, 1\}$ are uniquely decodable. If so, then restore the original plain text $c \in A$ of the encoded string $\tilde{c} \in B$. Otherwise, make sure that \tilde{c} cannot be decoded uniquely.

a) $A = \{a, d, k, u\}$, $\tilde{c} = 110011100111010$,

$x \in A$	a	d	k	u
$\gamma(x)$	001	110	11	10

b) $A = \{e, s, u\}$, $\tilde{c} = 10010010$,

$x \in A$	e	s	u
$\gamma(x)$	010	10	100

c) $A = \{n, o, r, t\}$, $\tilde{c} = 1101001110001110100$,

$x \in A$	n	o	r	t
$\gamma(x)$	01	100	11	110

Exercise 2.

Let $n \in \mathbb{N}$. Decide whether the following binary codes are uniquely decodable and give the reason for your decision:

- a) $C = \{0, 101, \dots, 1^n 01^n\}$,
- b) $C = \{0, 01, \dots, 01^n\}$,
- c) $C = \{0, 01, 010, 0101, \dots, 0(10)^n, 0(10)^n 1\}$,
- d) $C = \{01, 0011, \dots, 00^n 1^n 1\}$ and
- e) $C = \{0, 010, \dots, 0(10)^n\}$.

Exercise 3.

Let $n, m \in \mathbb{N}$ be fixed, C_n be the binary repetition code of length n and $\tilde{C}_{n,m} := (C_n)^m$ the m -times Cartesian product of C_n . Find the cardinality, the information transfer rate and the minimum distance of $\tilde{C}_{n,m}$ depending on n and m .

Exercise 4.

- a) Find the maximum cardinality of a binary block code C of length 3 with minimum distance equal 2.
- b) Are there binary block codes with specification $(7,8,5)$ or $(6,10,4)$, respectively? If your answer is positive, construct such a code.