

Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Homework Sheet 4
Version 04.06.2020

Homework 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) $A = \{e, i, t, x\}$, $\tilde{c} = 1001001100$,

$x \in A$	e	i	t	x
$\gamma(x)$	10	001	100	01

b) $A = \{a, e, g, l, r\}$, $\tilde{c} = 01101011101010110100$,

$x \in A$	d	i	m	n	o
$\gamma(x)$	100	10	011	1101	0101

Homework 2.

Decide whether the code $C = \{\heartsuit\diamondsuit\clubsuit, \clubsuit\spadesuit, \heartsuit\diamondsuit, \spadesuit\heartsuit, \heartsuit\diamondsuit\heartsuit, \spadesuit\diamondsuit\diamondsuit, \spadesuit\clubsuit, \spadesuit\diamondsuit\}$ is uniquely decodable over the alphabet $B = \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ and give the reason for your decision.

Homework 3.

Consider the following block code $C \subseteq \mathbb{Z}_5^4$:

$$C := \{(c_1, \dots, c_4) \in \mathbb{Z}_5^4 \mid 2c_1 + 3c_2 + c_3 = 0, 4c_1 + 3c_2 + c_4 = 0\}.$$

- (a) Find the information transfer rate of C .
- (b) Show that C is MDS code but it's not perfect.

Homework 4.

- a) Find the maximum cardinality of a binary block code C of length 4 with minimum distance equal 3.
- b) Are there binary block codes with specification $(5,4,3)$? If your answer is positive, construct such a code.
- c) Find the *control character* of the ISBN13 code 978342311821□ of the 15th. edition of the novel "Die Blechtrommel" in the publisher Deutschen Taschenbuchverlag.