Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Stefan Hoffmann

Hausübungen zur Vorlesung

Diskrete Mathematik 2
Einführung in die theoretische Informatik

Sommersemester 2014

Blatt 6 / 8./9. Juli 2014

Abgabe: 8. Juli 2014, 09:15 Uhr (vor der Vorlesung), Kasten NA 02

AUFGABE 1 (5 Punkte)**:**

Konstruieren Sie jeweils einen Präfixcode $C = \{C_1, \dots, C_n\}$ oder zeigen Sie, dass kein solcher Code existiert.

(a) $n = 4$, $|C_1| = 2$, $|C_2| = 2$, $|C_3| = 2$, $|C_4| = 2$

(b) $n = 5$, $|C_1| = 2$, $|C_2| = 2$, $|C_3| = 2$, $|C_4| = 3$, $|C_5| = 3$

(c) $n = 6$, $|C_1| = 2$, $|C_2| = 2$, $|C_3| = 2$, $|C_4| = 3$, $|C_5| = 3$, $|C_6| = 3$

(d) $n = 7$, $|C_1| = 1$, $|C_2| = 3$, $|C_3| = 3$, $|C_4| = 4$, $|C_5| = 4$, $|C_6| = 4$, $|C_7| = 4$

(e) $n = 8$, $|C_1| = 2$, $|C_2| = 2$, $|C_3| = 3$, $|C_4| = 3$, $|C_5| = 3$, $|C_6| = 4$, $|C_7| = 5$, $|C_8| = 5$

AUFGABE 2 (5 Punkte)**:**

Betrachten Sie einen binären, symmetrischen Kanal, in dem einzelne Bits mit Wahrscheinlichkeit $p = 1/10$ kippen. Wir betrachten den binären Blockcode $C = \{00, 01, 10\}$ mit *nicht-gleichverteilten* Sendewahrscheinlichkeiten

$$\mathrm{Ws}[00 \text{ gesendet}] = 11/20, \qquad \mathrm{Ws}[01 \text{ gesendet}] = 7/20, \qquad \mathrm{Ws}[10 \text{ gesendet}] = 1/10.$$

(a) Geben Sie einen *Maximum-Likelihood-Dekodierer* an.

(b) Konstruieren Sie einen Dekodierer, der die Wahrscheinlichkeit des korrekten Dekodierens maximiert.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Betrachten Sie den linearen Code C, gegeben durch die Generatormatrix

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

(a) Zeigen Sie: $C^\perp = C$.

(b) Geben Sie die Parameter von C an.

(c) Konstruieren Sie ein Standardarray sowie eine Syndromtabelle für C.

(d) Dekodieren Sie die Nachrichten $0001, 1000, 1100, 1111$ mit Hilfe Ihres Standardarrays.

(e) Dekodieren Sie die Nachrichten $0001, 1000, 1100, 1111$ mit Hilfe Ihrer Syndromtabelle.

AUFGABE 4 (5 Punkte)**:**

Sei C ein (n, M, d)-Code. Es kann ein neuer Code $\tilde{C}$ erzeugt werden, indem ein Paritätsbit zu jedem Codeword hinzugefügt wird, so dass das neue Codewort gerade Parität hat.

$$C \ni c \to \tilde{c} = \begin{cases} c0, & \text{wenn } \mathsf{wt}(c) \text{ gerade} \\ c1, & \text{wenn } \mathsf{wt}(c) \text{ ungerade} \end{cases}$$

Hierbei bezeichnet $\mathsf{wt}(c)$ das Hamming-Gewicht von c. Der resultierende Code $\tilde{C}$ hat dann Länge $n+1$ und Größe M.

(a) Betrachten Sie den Code $C_1 = \{00000, 00111, 11011, 11100\}$ und konstruieren Sie $\tilde{C}_1$. Welche Parameter haben C_1 und $\tilde{C}_1$?

(b) Sei C nun ein beliebiger Code und $\tilde{C}$ der wie oben beschrieben erzeugte. Zeigen Sie, dass die Anzahl der korrigierbaren Fehler von C und $\tilde{C}$ die gleiche ist.

(c) Zeigen Sie: Falls C ein beliebiger linearer Code ist, so ist auch $\tilde{C}$ ein linearer Code.

(d) Sei P eine Parity-Check-Matrix für einen linearen Code C. Geben Sie eine einfache Konstruktion an, eine Parity-Check-Matrix $\tilde{P}$ für $\tilde{C}$ mittels P zu konstruieren und begründen Sie, warum Ihre Konstruktion funktioniert.