Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Gottfried Herold

Hausübungen zur Vorlesung

Diskrete Mathematik II

SS 2011

Blatt 7 / 28. Juni 2011 / Abgabe **bis spätestens Dienstag 12. Juli, 09:00 Uhr**

AUFGABE 1:

Sei X, Y beliebige Zufallsvariablen, die Werte aus (endlichen) Mengen A, B annehmen können. Zum Beispiel könnte X das erste von einer Quelle Q ausgegebene Symbol sein.
Wir definieren die Entropie einer Zufallsvariable genauso wie für Quellen als
$H(X) = -\sum_{a \in A} \mathbb{P}[X = a] \cdot \log_2 \mathbb{P}[x = a]$, wobei $0 \cdot \log_2 0 = 0$.
Zeigen Sie:

(a) Für eine beliebige Funktion $f : A \to C$ ist $H(f(X)) \leq H(X)$, d.h. die Entropie der Zufallsvariablen $f(X)$ mit Werten in C ist höchstens die von X. [4P]

(b) Wenn X, Y unabhängig sind, gilt $H((X, Y)) = H(X) + H(Y)$. Dabei ist $H((X, Y))$ die Entropie der Zufallsvariablen (X, Y), die Werte in $A \times B = \{(a, b) \mid a \in A, b \in B\}$ annehmen kann. [3P]

(c) Es gilt stets (d.h. für potentiell nicht unabhängige X, Y) $H((X, Y)) \leq H(X) + H(Y)$ [3P]

Hinweise:
Zu (a): Berechnen Sie $H(X)$, indem Sie zunächst über diejenigen $a \in A$ summieren, die dasselbe Bild unter f haben.
Zu (c): Lösen Sie zunächst Teil (b). Benutzen Sie dann für (c) das Lemma über Wechsel Ws-Verteilung aus der Vorlesung.

Bitte wenden!

AUFGABE 2:

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

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

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

(a) Ergänzen Sie den Code $C_1 = \{00000, 11100, 00111, 11011\}$ um ein Paritätsbit auf gerade Parität. Welche Parameter haben C_1 und $\widetilde{C}_1$. [2.5P]

(b) Sei C nun ein beliebiger Code und $\widetilde{C}$ der wie oben beschrieben erzeugte. Zeigen Sie, dass die Anzahl der korrigierbaren Fehler von C und $\widetilde{C}$ die gleiche ist. [3P]

(c) Zeigen Sie: Falls C ein beliebiger *linearer* Code ist, so ist auch $\widetilde{C}$ ein linearer Code. [2P]

(d) Sei P eine Parity-Check Matrix für einen linearen Code C. Geben Sie eine einfache Konstruktion an, eine Parity-Check Matrix $\widetilde{P}$ für $\widetilde{C}$ mittels P zu konstruieren und begründen Sie, warum Ihre Konstruktion funktioniert. [3P]

AUFGABE 3:

Betrachten Sie einen binären symmetrischen Kanal, in dem einzelne Bits mit Wsk. $p = 0,2$ kippen.
Wir betrachten den binären Blockcode $C = \{C_1, C_2, C_3\}$ mit $C_1 = 00, C_2 = 10, C_3 = 01$ mit *nicht-gleichverteilten* Sendewahrscheinlichkeiten
$\mathbb{P}[C_1 \text{ gesendet}] = 0.5.$
$\mathbb{P}[C_2 \text{ gesendet}] = 0.4.$
$\mathbb{P}[C_3 \text{ gesendet}] = 0.1.$

(a) Geben Sie einen Maximum-Likelihood Dekodierer an. [2P]

(b) Konstruieren Sie den Dekodierer, der die Wahrscheinlichkeit des korrekten Dekodierens maximiert. [5P]

AUFGABE 4:

Betrachten Sie den linearen Code C mit Generatormatrix

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

(a) Konstruieren Sie eine Standard-Array-Tabelle für diesen linearen Code. [3P]

(b) Konstruieren Sie eine Parity-Check Matrix für C und eine zugehörige Syndom-Tabelle für C. [4P]

(c) Was sind die Parameter von Distanz von C? Was sind die Parameter von $C^{\perp}$? [2P]

AUFGABE 5:

Geben Sie je einen Code mit folgenden Paramtern an (wenn Ihr Code Linear ist, dürfen Sie entscheiden, ob Sie den Code als Menge oder per Generatormatrix angeben) oder begründen Sie, warum kein solcher existiert:

(a) $(5, 2, 5)$ [1.5P]

(b) $(5, 3, 5)$ [1.5P]

(c) $[12, 3, 7]$[2P]

(d) $[4, 3, 2]$ [2P]

(e) $[7, 5, 4]$ [2P]