389.138 Telekommunikation – 2017S
2. Übung

23./24.05.2017

Einen Überblick über die in der Übung verwendete Notation finden Sie in TUWEL.

Beispiel 1 — Quantisierer und Huffman-Code

Gegeben sei die Zufallsvariable X, verteilt nach der PDF

$$f_{\mathsf{X}}(x) = \begin{cases} (2\pi x \mathrm{e}^{x})^{-\frac{1}{2}} & x \geq 0 \\ 0 & \text{sonst} \end{cases}.$$

Die quantisierte Zufallsvariable $\hat{\mathsf{X}} = Q(\mathsf{X})$ wird gebildet gemäß

$$Q(x) = \begin{cases} 0.5 & x < 1 \\ 1.5 & 1 \leq x < 2 \\ 2.5 & 2 \leq x < 3 \\ 3.5 & 3 \leq x < 4 \\ 4.5 & 4 \leq x < 5 \\ 5.5 & x \geq 5 \end{cases}.$$

(a) Geben Sie die Wahrscheinlichkeitsverteilung von $\hat{\mathsf{X}}$ an.

Hinweis: Für $x \geq 0$,

$$\int \frac{1}{\sqrt{x\mathrm{e}^{x}}} dx = \sqrt{2\pi}\, \mathrm{erf}\left(\sqrt{\frac{x}{2}}\right).$$

(b) Entwerfen Sie einen Huffman-Code für $\hat{\mathsf{X}}$. In jedem Schritt werden die wahrscheinlicheren Symbole mit “0” codiert.

(c) Geben Sie die Entropie von $\hat{\mathsf{X}}$ an.

(d) Geben Sie die Effizienz η_{Code} des Huffman-Codes an.

(e) Betrachten Sie die Quantisierung

$$\tilde{\mathsf{X}} = \tilde{Q}(\mathsf{X}) = \lfloor \mathsf{X} \rfloor + 0.5.$$

Welche der Zufallsvariablen $\hat{\mathsf{X}}$ und $\tilde{\mathsf{X}}$ hat die höhere Entropie? Begründen Sie Ihre Antwort.

Hinweis: Sie können folgende Tatsache[1] (ohne Beweis) verwenden: Für jede beliebige Funktion f und Zufallsvariable X gilt $H(\mathsf{X}) \geq H(f(\mathsf{X}))$.

[1] Dies ist eine einfache Folgerung aus der “Data-processing inequality” [1, Theorem 2.8.1].

Beispiel 2 — Faltungscode
Ein Datenstrom mit Symbolen aus GF(2) wird mit Hilfe eines Faltungscodes gesichert. Der Codierer verwendet die Polynome $p_1(x) = 1 + x + x^2$ und $p_1(x) = 1 + x^2$.

(a) Fertigen Sie eine Skizze des Codierers an. Welche Coderate besitzt der Codierer?

(b) Skizzieren Sie das Zustandsdiagramm des Codierers.

(c) Codieren Sie das Datenwort `111`. Nehmen Sie dazu an, dass sich der Codierer am Beginn im Nullzustand befindet. Codieren Sie auch das erweiterte Datenwort `11100`, welches den Codierer nach der Übertragung wieder in den Nullzustand zurückführt.

Aus dem Faltungscode wird nun ein linearer $(10, 3)$-Blockcode $\mathcal{C}$ mit Codewörtern der Länge $N = 10$ und Datenwörtern der Länge $K = 3$ gebildet. Dabei wir das Datenwort immer mit Nullen erweitert um den Codierer in den Nullzustand zurückzuführen.

(d) Geben Sie die Generatormatrix $\mathbf{G}$ und eine Checkmatrix $\mathbf{H}$ dieses linearen Blockcodes an. Begründen Sie warum der so erzeugte Blockcode tatsächlich linear ist. Ist der Code systematisch?

(e) Geben Sie alle Codewörter von $\mathcal{C}$ an. Berechnen Sie das minimale Codegewicht $w_{\min}$ und die minimale Hamming-Distanz $d_{\min}$.

(f) Wieviele beliebig angeordnete Fehler können vom Empfänger erkannt werden? Wieviele können korrigiert werden?

(g) Decodieren Sie das Empfangswort `1111110111` mit Hilfe des Viterbi-Algorithmus. Nehmen Sie dazu an, dass das codierte Datenwort mit zwei Nullen erweitert wurde, um den Codierer wieder in den Nullzustand zu versetzen. Wie viele Fehler wurden korrigiert?

(h) Wie viele Einträge hätte die Syndromtabelle für $\mathcal{C}$? Würde das Ergebnis der Syndromdecodierung von `1111110111` mit dem Ergebnis aus Punkt (g) übereinstimmen? Kann es passieren, dass Viterbi- und Syndrom-Decodierung unterschiedliche Ergebnisse liefern, wenn weniger (oder gleich viele) Fehler auftreten als korrigiert werden können?

Beispiel 3 — Linearer Code
Es sei $\mathcal{C} \subseteq \mathrm{GF}(2)^6$ der kleinstmögliche lineare Blockcode, für den gilt

$$(0, 0, 1, 0, 1, 1)^T \in \mathcal{C}\ , \qquad (0, 1, 0, 1, 0, 1)^T \in \mathcal{C} \qquad \text{und} \qquad (1, 1, 1, 0, 0, 0)^T \in \mathcal{C}\ .$$

(a) Geben Sie alle Codewörter von $\mathcal{C}$ an.

(b) Berechnen Sie n, k und die Coderate R.

(c) Geben Sie $d_{\min}$ und $w_{\min}$ an. Wie viele Fehler können erkannt bzw. korrigiert werden?

(d) Geben Sie eine Generatormatrix $\mathbf{G}$ und eine Checkmatrix $\mathbf{H}$ für den Code $\mathcal{C}$ in Standardform an.

(e) Ein Code $\mathcal{C}$ heißt *selbst-orthogonal* wenn für jedes Codewort $\mathbf{c} \in \mathcal{C}$ gilt: $\mathbf{c}^{\mathrm{T}}\mathbf{c} = 0$. Ist der Code $\mathcal{C}$ selbst-orthogonal?

(f) Geben Sie eine Generatormatrix $\mathbf{G}'$ für $\mathcal{C}$ an, sodass der Code nicht mehr systematisch ist.

Beispiel 4 — Blockcode

Der Blockcode $\mathcal{C} \subseteq \mathrm{GF}(2)^N$ bestehe aus allen binären Sequenzen der Länge N mit Hamming-Gewicht w. Nehmen Sie an, dass $N, w \in \mathbb{N}$ und $N \geq w$.

(a) Ist $\mathcal{C}$ ein linearer Blockcode? Begründen Sie Ihre Antwort.

(b) Welche Rate hat der Code? Geben Sie die minimale Hamming-Distanz sowie das minimale Hamming-Gewicht von $\mathcal{C}$ an.

(c) Geben Sie den kleinsten linearen Blockcode $\mathcal{C}_1$ an, welcher $\mathcal{C}$ enthält.

Hinweis: Betrachten Sie die Fälle $N = w$, $w \in 2\mathbb{N}$ und $w \notin 2\mathbb{N}$ getrennt.

Beispiel 5 — Morsecode

In Tabelle 1 finden sie die genäherten relativen Auftrittswahrscheinlichkeiten der acht häufigsten Buchstaben im Deutschen. Wir verwenden die Zufallsvariable X mit dem Alphabet $\mathcal{X} = \{\mathrm{E, N, I, S, R, A, T, D}\}$ und verteilt gemäß den Werten in Tabelle 1 als idealisiertes Modell für die deutsche Sprache. Die Zufallsvariable Y sei gleichverteilt auf $\mathcal{X}$.

Buchstabe	E	N	I	S	R	A	T	D
Häufigkeit	26%	14.5%	11.5%	11%	10.5%	10%	9%	7.5%
Morsezeichen	`.`	`-.`	`..`	`...`	`.-.`	`.-`	`-`	`-..`

Tabelle 1: Buchstabenhäufigkeit und Morsealphabet (Beispiel 5)

(a) Berechnen Sie die Entropie $H(\mathsf{X})$ in bit.

(b) Entwerfen Sie einen Huffman Code für X. Begründen Sie warum der Huffman Code fortlaufend dekodierbar ist. Codiervorschrift: Pfad mit höherer Wahrscheinlichkeit mit `0`, Pfad mit niedriger Wahrscheinlichkeit mit `1` codieren.

(c) Geben Sie die mittlere Codewortlänge l_x und die Effizienz η_x des Huffman Codes für X an.

(d) Der selbe Huffman Code wird nun verwendet um Y zu codieren. Berechnen Sie entsprechende mittlere Codeworlänge l_y und die Effizienz η_y. Vergleichen Sie das Ergebnis mit Punkt (c).

(e) Dekodieren Sie das Empfangswort $w = (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1)$. Was würde passieren wenn das erste Bit fehlerhaft übertragen wird?

In Tabelle 1 finden Sie auch die Morsezeichen nach dem internationalen Morse Alphabet. Nachdem der Morse Code nicht eindeutig dekodierbar ist wird bei der Übertragung am Ende jedes Symbols eine Pause (Symbol `p`) übertragen um den Code dekodierbar zu machen.

(f) Berechnen Sie die mittlere Codewort-Länge des Morse-Codes für X, wobei `.`, `-` und `p` jeweils als ein Zeichen zählen.

(g) Berechnen Sie die Effizient des Morse Codes für X. *Hinweis: Beachten Sie, dass das Morse Alphabet aus 3 Zeichen (`.`, `-`, `p`) besteht. Zur Berechnung der Effizienz muss daher die Entropie in* trit *verwendet werden. Diese wird mit dem Logarithmus zur Basis 3,* $\log_3$ *berechnet.*

Beispiel 6 — 3 Codes

Gegeben sei der Code $\mathcal{C}_1$ durch folgende Codiervorschrift: Ein Datenwort $\mathbf{d}_1 \in \mathrm{GF}(2)^{k_1}$ der Länge $k_1 = 3$ wird durch den Coder g_1 auf einen Codevektor $\mathbf{c}_1 \in \mathrm{GF}(2)^4$ abgebildet, gemäß

$$\mathbf{d}_1 = \begin{pmatrix} d^{(1)} \\ d^{(2)} \\ d^{(3)} \end{pmatrix} \mapsto \quad \mathbf{c}_1 = g_1(\mathbf{d}_1) = \begin{pmatrix} d^{(1)} \\ d^{(1)} + d^{(2)} \\ d^{(3)} \\ d^{(1)} \wedge d^{(3)} \end{pmatrix}$$

Ein weiterer Code $\mathcal{C}_2$, gegeben durch die Codiervorschrift g_2, bildet ein Datenwort $\mathbf{d}_2 \in \mathrm{GF}(2)^{k_2}$ der Länge $k_2 = 4$ auf ein Codewort $\mathbf{c}_2 \in \mathrm{GF}(2)^5$ ab, wobei

$$\mathbf{d}_2 = \begin{pmatrix} d^{(1)} \\ d^{(2)} \\ d^{(3)} \\ d^{(4)} \end{pmatrix} \mapsto \quad \mathbf{c}_2 = g_2(\mathbf{d}_2) = \begin{pmatrix} d^{(1)} \\ d^{(1)} + d^{(2)} \\ d^{(3)} \\ d^{(3)} \vee d^{(4)} \\ (d^{(4)} + d^{(1)}) \wedge d^{(3)} \end{pmatrix}$$

gilt. Durch Hintereinanderausführung der beiden Codiervorschriften für $\mathcal{C}_1$ und $\mathcal{C}_2$ ergibt sich ein dritter Code $\mathcal{C}_3$, definiert durch die Codiervorschrift $\mathbf{c}_3 = g_3(\mathbf{d}_3) = g_2\big(g_1(\mathbf{d}_3)\big)$.
Bearbeiten Sie die nachfolgenden Punkte jeweils für alle drei Codes $\mathcal{C}_i$, $i \in \{1, 2, 3\}$.

(a) Wie viele Codewörter besitzt der Code $\mathcal{C}_i$? Geben Sie alle Codewörter an.

(b) Bestimmen Sie Codewortlänge n_i, die Datenwortlänge k_i und die Coderate R_i.

(c) Bestimmen Sie das minimale Hamming-Gewicht $w_{\min}$.

(d) Handelt es sich um einen systematischen Code?

(e) Ist der Code linear? *Falls Ja*, geben Sie eine Generator- und eine Checkmatrix an. *Falls Nein*, finden Sie Datenwörter $\mathbf{d}_i, \mathbf{d}'_i \in \mathrm{GF}(2)^{k_i}$ mit $g_i(\mathbf{d}_i + \mathbf{d}'_i) \neq g_i(\mathbf{d}_i) + g_i(\mathbf{d}'_i)$.

(f) Bestimmen Sie die minimale Hamming-Distanz $d_{\min}$. Gilt hier $d_{\min} = w_{\min}$?

Beispiel 7 — Maximale Entropie

Eine Zufallsvariable $\mathsf{X} \in \mathcal{X} = \{1, 2, 3, \ldots, n\}$ sei gemäß der Verteilung p verteilt. Die Entropie von X ist gegeben durch

$$H(\mathsf{X}) \triangleq H(p) \triangleq -\sum_{i=1}^{n} p(i) \log_2\big(p(i)\big).$$

Zeigen Sie, dass $0 \leq H(\mathsf{X}) \leq \log_2(n)$, d.h., die Entropie $H(\mathsf{X})$ ist nicht-negativ und kleiner als $\log(n)$. Finden Sie ausserdem Wahrscheinlichkeitsverteilungen $\hat{p}_1$ und $\hat{p}_2$ sodass $H(\hat{p}_1) = 0$ und $H(\hat{p}_2) = \log_2(n)$. Sind die Verteilungen $\hat{p}_1$ und $\hat{p}_2$ eindeutig?
Hinweis: Sie können z.B. die Jensensche Ungleichung verwenden und die Tatsache dass $\log_2$ *eine konkave Funktion ist.*

Beispiel 8 — 8 Punkte
Gegeben sei die Matrix

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

(a) Ist $\mathbf{G}'$ eine gültige Generatormatrix eines linearen Blockcodes? Entfernen Sie möglichst wenige Zeilen von $\mathbf{G}'$ um zu einer gültigen Generatormatrix $\mathbf{G}$ zu gelangen.[2] Begründen Sie Ihre Antwort.

Es sei nun $\mathcal{C}$ der von $\mathbf{G}$ erzeugte lineare Blockcode.

(b) Geben Sie alle Codewörter von $\mathcal{C}$ an.

(c) Berechnen Sie n, k und die Coderate R.

(d) Geben Sie d_{min} und w_{min} an. Wie viele Fehler können erkannt bzw. korrigiert werden?

(e) Geben Sie eine Generatormatrix $\widetilde{\mathbf{G}}$ und eine Checkmatrix $\widetilde{\mathbf{H}}$ für den Code $\mathcal{C}$ in Standardform an.

(f) Ein Code $\mathcal{C}$ heißt *selbst-orthogonal* wenn für jedes Codewort $\mathbf{c} \in \mathcal{C}$ gilt: $\mathbf{c}^{\mathrm{T}}\mathbf{c} = 0$. Ist der Code $\mathcal{C}$ selbst-orthogonal?

Literatur

[1] Thomas M. Cover und Joy A. Thomas. *Elements of Information Theory.* 2^{nd}. Wiley-Interscience, 2006.

[2] Falls $\mathbf{G}'$ bereits eine gültige Generatormatrix ist, so müssen keine Zeilen entfernt werden und es gilt $\mathbf{G} = \mathbf{G}'$.