Übungsblatt 3

Aufgabe 1. Gesucht ist ein Code C der Ordnung $|C| = 2^k$, der 1-fehlerkorrigierend ist und die Informationsrate $R = 0,8$ hat.
Geben Sie die kleinsten n und k an, für die es einen solchen Code gibt. Benutzen Sie dafür die Kugelpackungsgleichung.

Leider liegt ein Existenzbeweis eines solchen Codes außerhalb unserer derzeitigen Möglichkeiten, sodass wir stattdessen lediglich notwendige Bedingungen für n und k errechnen.
Sei $q := |K|$ die Größe des Alphabets. Wir erhalten durch die Gleichung (Lemma 5.5)

$$\left\lfloor \frac{d-1}{2} \right\rfloor = 1$$

für die Minimaldistanz $d \in \{3,4\}$. Die Singleton-Schranke (Satz 6.4) liefert mit der Informationsrate $0,8 = R = \frac{\log_q(|C|)}{n}$

$$d \leq n - \log_q(|C|) + 1 = n - \log_q(|C|) + 1 = 0,2n + 1.$$

D.h. wir erhalten mit $d \geq 3$

$$10 \leq \frac{d-1}{0,2} \leq n.$$

Sei nun $n = 10$, so liefert die Informationsrate

$$8 = 0,8 \cdot 10 = \log_q\left(2^k\right)$$

und somit

$$q = \sqrt[8]{2^k}.$$

Nun ist also genau dann $q \in \mathbb{N}_{\geq 2}$, wenn $k = 8m$ für ein $m \in \mathbb{N}$. Letzteres liefert somit

$$(q,k) = (2^m, 8m) \in \{(2,8),(4,16),(8,24),(16,32),(32,40),\ldots\}.$$

Die Kuglepackungsungleichung liefert nun für $n = 10$, $k = 8m$ und $q = 2^m$

$$2^{10m} = q^n \geq 2^k \sum_{j=0}^{e} \binom{n}{j}(q-1)^j = 2^{8m} \sum_{j=0}^{e} \binom{n}{j}(2^m-1)^j.$$

Also gilt

$$2^{2m} \geq \sum_{j=0}^{e} \binom{n}{j}(2^m-1)^j.$$

Wegen $4 \geq d \geq 2e+1$ erhalten wir $e \in \{0,1\}$ und damit

$$2^{2m} \geq \begin{cases} 1 & , e = 0 \\ 1 + 10(2^m - 1) & , e = 1. \end{cases}$$

Für $e = 0$ ist die Ungleichung für alle $m \in \mathbb{N}$ erfüllt, wobei für $e = 1$ sie nur für $m \geq 4$ gilt.

Definition. *Seien Γ, Γ' zwei Kanäle mit Input-Mengen I, I' und Output-Mengen J, J', so definiere einen Kanal $\Gamma \times \Gamma'$ mit Input-Menge $I \times I'$ und Output-Menge $J \times J'$ durch*

$$(\Gamma \times \Gamma')_{xx'\ yy'} = \Gamma_{xy} \cdot \Gamma'_{x'y'} = p(y \mid x)p(y' \mid x').$$

Ist $\Gamma = \Gamma'$, so schreiben wir Γ^2 für $\Gamma \times \Gamma$.

Lemma. *Sei Γ der binäre symmetrische Kanal mit Fehlerwahrscheinlichkeit e, so gilt*

$$\Gamma^n_{x,y} = e^{d(x,y)}(1-e)^{n-d(x,y)},$$

wobei $\Gamma^n_{x,y}$ der Eintrag der Matrix Γ^n mit Koordinaten $(x,y) \in \{0,1\}^n \times \{0,1\}^n$.

Beweis. Sei $(x,y) \in \{0,1\}^n \times \{0,1\}^n$, so folgt aus obiger Definition $\Gamma^n_{x,y} = e^{d(x,y)}(1-e)^{n-d(x,y)}$ (Bernoulli-Verteilung). □

Aufgabe 2. Es sei Γ der binäre symmetrische Kanal mit Fehlerwahrscheinlichkeit e und Eingabe- und Ausgabemenge $K = \{0,1\}$. Es sei $C \subseteq K^n$ und $\widetilde{\Gamma} = \Gamma^n$. Weiter sei p die Wahrscheinlichkeitsverteilung auf der Eingabemenge K^n und $q = p\widetilde{\Gamma}$ die Wahrscheinlichkeitsverteilung auf der Ausgabemenge K^n. Es wurden bereits berechnet, dass

$$H(q \mid p) = H(T) - H(p) = nh(e)$$

ist. Zeigen Sie, dass für die Kapazitäten κ von $\widetilde{\Gamma}$ gilt

$$\kappa(\widetilde{\Gamma}) = n(1-h(e)).$$

Beweis. In der Vorlesung wurden die folgenden Größen definiert

$$H(q \mid p) \coloneqq H(T) - H(p) \text{ und } H(p \mid q) \coloneqq H(T) - H(q),$$

wobei p eine Wahrscheinlichkeitsverteilung auf $\{0,1\}^n$, $q = p\Gamma^n$ die entsprechende Wahrscheinlichkeitsverteilung auf der Ausgabemenge $\{0,1\}^n$ und T die Wahrscheinlichkeitsverteilung auf $\{0,1\}^n \times \{0,1\}^n$ mit $T(xy) = \Gamma^n_{xy}p(x)$, d.h. p und $q = p\Gamma^n$ sind Randverteilungen von T. Die Kapazität ist nun definiert durch

$$\kappa(\Gamma^n) = \max_p \left(H(p) - H(p \mid q)\right) = \max_p \left(H(q) - H(q \mid p)\right).$$

Wir erhalten also mit $H(q \mid p) = nh(e)$ und Blatt 2 Aufgabe 4

$$\kappa(\Gamma^n) = \max_p \left(H(q) - nh(e)\right) \leq \log_2(2^n) - nh(e) = n(1-h(e)).$$

Das Maximum der linken Seite wird angenommen, wenn q die Gleichverteilung auf $\{0,1\}^n$ ist. Sei nun p die Gleichverteilung auf $\{0,1\}^n$, so gilt für die Verteilung q

$$q(y) = \sum_{x \in \{0,1\}^n} p(x)\Gamma^n_{xy} = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \Gamma^n_{xy},$$

wobei $\Gamma^n_{x,y}$ der Eintrag der Matrix Γ^n mit Koordinaten $(x,y) \in \{0,1\}^n \times \{0,1\}^n$ ist. Nun ist die Matrix wegen $\Gamma^n_{xy} = e^{d(x,y)}(1-e)^{n-d(x,y)}$ symmetrisch (siehe obiges Lemma) und wir erhalten mit Lemma 4.5

$$q(y) = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \Gamma^n_{yx} = \frac{1}{2^n},$$

d.h. q ist die Gleichverteilung auf $\{0,1\}^n$. □

Aufgabe 3. Ein binärer Code mit Informationsrate $R(C) = 0,9$ wurde durch den Kanal Γ^2 geschickt, wobei Γ der binäre symmetrische Kanal mit Fehlerwahrscheinlichkeit $0,03$ ist.

(a) Übersteigt die Rate die Kapazität?

(b) Wenn jedes Codewort gleichwahrscheinlich ist, was können wir dann über die Unsicherheit aus Sicht des Empfängers sagen?

Mit Aufgabe 2 und den Parametern $e = 0,3$ und $n = 2$ erhalten wir

$$\kappa(\Gamma^n) = n(1 - h(e)) = 2(1 - h(0,3)) \geq 1,6 > 0,9 = R(C).$$

Die Kapazität überschreitet also nicht die Rate.
Gesucht ist die konditionelle Entropie $H(p \mid q) = H(T) - H(q)$. Da p nach Voraussetzung die Gleichverteilung auf $\{0,1\}^2$ ist, so ist auch $q = p\Gamma^2$ die Gleichverteilung (siehe im Beweis von Aufgabe 2). Somit erhalten wir $H(q) = \log_2(2^2) = 2$.
Es bleibt also $H(T)$ zu bestimmen. Es gilt

$$\Gamma^2 = \begin{pmatrix} (1-e)^2 & e(1-e) & e(1-e) & e^2 \\ e(1-e) & (1-e)^2 & e^2 & e(1-e) \\ e(1-e) & e^2 & (1-e)^2 & e(1-e) \\ e^2 & e(1-e) & e(1-e) & (1-e)^2 \end{pmatrix},$$

wobei wir die Anordnung der Zeilen und Spalten wie folgt gewählt haben: 00, 01, 10, 11. Die Verteilung T ist wie folgt definiert

$$T(xy) = \Gamma^2_{xy} p(x)$$

und somit gilt

$$\begin{aligned} H(T) &= \sum_{x,y \in \{0,1\}^2} T(xy) \log_2\left(\frac{1}{T(xy)}\right) \\ &= \frac{1}{2^2}\left(4(1-e)^2 \log_2\left(\frac{2^2}{(1-e)^2}\right) + 8e(1-e)\log_2\left(\frac{2^2}{e(1-e)}\right) + 4e^2 \log_2\left(\frac{2^2}{e^2}\right)\right). \end{aligned}$$

Die konditionelle Entropie lautet somit

$$\begin{aligned} H(p \mid q) &= H(T) - H(q) \\ &= \frac{1}{2^2}\left(4(1-e)^2 \log_2\left(\frac{2^2}{(1-e)^2}\right) + 8e(1-e)\log_2\left(\frac{2^2}{e(1-e)}\right) + 4e^2 \log_2\left(\frac{2^2}{e^2}\right)\right) - 2. \end{aligned}$$

Alternativ mit Aufgabe 2 kann man die konditionelle Entropie auch wie folgt errechnen. Es gilt

$$H(p \mid q) + H(q) = H(q \mid p) + H(p).$$

Da p die Gleichverteilung ist, ist $q = p\Gamma^2$ auch gleichverteilt und somit erhalten wir nach Aufgabe 2 $H(p \mid q) = H(q \mid p) = 2h(0,03) = 2 \cdot \left(0,03 \cdot \log_2\left(\frac{1}{0,03}\right) + (1 - 0,03) \cdot \log_2\left(\frac{1}{1-0,03}\right)\right) \approx 0,39$.

Aufgabe 4. Betrachten Sie den Code $C = \{0,1\}$ als eine Eingabe eines symmetrischen binären Kanals mit Fehlerwahrscheinlichkeit $e = 0,2$. Zeigen Sie:

(a) Die Maximum-Likelihood Decodierung decodiert 0 zu 0 und 1 zu 1.

(b) Die Wahrscheinlichkeit einer falschen Decodierung ist $0,2$ für alle Wahrscheinlichkeitsverteilungen p auf C.

Beweis. (a) Mit $e = 0,2$ erhalten wir den Kanal $\Gamma = \begin{pmatrix} p(0|0) & p(1|0) \\ p(0|1) & p(1|1) \end{pmatrix} = \begin{pmatrix} 0,8 & 0,2 \\ 0,2 & 0,8 \end{pmatrix}$. Die Maximum-Likelihood Decodierung decodiert 0 zu 0, denn

$$\max_{c \in C} p(0|c) = \max\{p(0|0), p(0|1)\} = p(0|0) = 0,8$$

und 1 zu 1, denn

$$\max_{c \in C} p(1|c) = \max\{p(1|0), p(1|1)\} = p(1|1) = 0,8.$$

Nach der Vorlesung sucht die Maximum-Likelihood Decodierung die Codewörter, deren Hammingabstand minimal zum empfangenen Wort sind. Hieraus kann man direkt die obige Decodierung folgern.

(b) Sei p eine Wahrscheinlichkeitsverteilung auf $C = \{0, 1\}$, so ist die Wahrscheinlichkeit einer falschen Decodierung

$$p(0 \mid 1)p(1) + p(1 \mid 0)p(0) = ep(1) + ep(0) = e.$$

□