10. Übung aus Informations- und Codierungstheorie SS 2016

1. Man zeige, dass eine maßtreue Transformation T auf einem Wahrscheinlichkeitsraum $(\Omega, \mathfrak{S}, P)$ genau dann ergodisch ist, wenn gilt

$$A \in \mathfrak{S} \wedge P(A) > 0 \;\Rightarrow\; P\left(\limsup_n T^{-n}(A)\right) = 1. \tag{0.1}$$

Hinweis: Zeigen Sie, dass $B_n := \bigcup\limits_{k \geq n} T^{-k}(A) \quad \forall\, n \in \mathbb{N}_0$ P–fs invariant ist.

Beweis: $\Leftarrow$: Ist A invariant, so gilt $A = \limsup\limits_n T^{-n}(A)$. Gilt $P(A) > 0$, so folgt aus (0.1) $P(A) = 1$, d.h. $P(A) \in \{0,1\} \quad \forall\, A \in \mathfrak{I}$. Somit ist T ergodisch.
$\Rightarrow$: Für $B_n := \bigcup\limits_{k \geq n} T^{-k}(A),\ n \in \mathbb{N}_0$ gilt $T^{-1}(B_n) = \bigcup\limits_{k > n} T^{-k}(A) \subseteq B_n$.
Nun gilt $0 = P(B_n) - P\left(T^{-1}(B_n)\right) = P\left(B \setminus T^{-1}(B_n)\right) = P\left(B \triangle T^{-1}(B_n)\right)$, da T maßtreu ist. Somit sind alle B_n P–fs invariant $\Rightarrow\ P(B_n) \in \{0,1\}$.
Daraus, aus $T^{-n}(A) \subseteq B_n$ und aus $0 < P(A) = P\left(T^{-n}(A)\right) \leq P(B_n)$ folgt $P(B_n) = 1 \quad \forall\, n \in \mathbb{N}_0 \;\Rightarrow\; P\left(\limsup\limits_n T^{-n}(A)\right) = P\left(\bigcap\limits_n B_n\right) = 1$.

2. Ist $(X_n)_{n \in \mathbb{Z}}$ eine stationäre, ergodische Quelle mit $P(X_0 = a) > 0$, so zeige man, dass für $\tau := \min\{n \geq 1 :\ X_n = a\}$ gilt

$$\int\limits_{[X_0 = a]} \tau \, dP = 1 \quad \text{bzw.} \quad \mathbb{E}(\tau | X_0 = a) = \frac{1}{P(X_0 = a)}. \tag{0.2}$$

Hinweis: Nach Beispiel 1 ist $\nu := \min\{n \geq 0 :\ X_n = a\}$ P–fs endlich, sodass gilt $1 = \sum\limits_{n=0}^{\infty} P(\nu = n)$. Außerdem kann man $[\nu = n]$ darstellen in der Form $[\nu = n] = \bigcup\limits_{k=1}^{\infty} [X_{-k} = a, X_{-k+1} \neq a, \ldots, X_{n-1} \neq a, X_n = a]$.

Beweis: Mit $A_{n,k} := [X_{-k} = a, X_{-k+1} \neq a, \ldots, X_{n-1} \neq a, X_n = a]$ gilt

$$\begin{aligned}
1 &= \sum_{n=0}^{\infty} P(\nu = n) = \sum_{n=0}^{\infty} \sum_{k=1}^{\infty} P(A_{n,k}) = \sum_{n=0}^{\infty} \sum_{k=1}^{\infty} P(A_{0,n+k}) \\
&= \sum_{n=0}^{\infty} \sum_{m \geq n+1} P(A_{0,m}) = \sum_{m=1}^{\infty} P(A_{0,m}) \sum_{n=0}^{m-1} 1 = \sum_{m=1}^{\infty} m\, P(A_{0,m}) \\
&= \sum_{m=1}^{\infty} m\, P\left([X_0 = a] \cap [\tau = m]\right) = \int\limits_{[X_0 = a]} \tau \, dP.
\end{aligned}$$

Die linke Summe in der letzten Zeile oben kann man umformen zu

$$1=\sum_{m=1}^{\infty} m\,P\left([X_0=a]\cap[\tau=m]\right)=P(X_0=a)\sum_{m=1}^{\infty} m\,P\left(\tau=m|X_0=a\right)$$
$$=P(X_0=a)\,\mathbb{E}(\tau|X_0=a)\;\Rightarrow\;\mathbb{E}(\tau|X_0=a)=\frac{1}{P(X_0=a)}.$$

Da $\mathbb{E}(\tau|X_0=a)$ auf $[X_0=a]$ konstant ist, folgt dies auch aus

$$1=\int\limits_{[X_0=a]}\tau\,dP=\int\limits_{[X_0=a]}\mathbb{E}(\tau|X_0=a)\,dP=\mathbb{E}(\tau|X_0=a)\,P(X_0=a).$$

3. Man zeige, dass für die Wartezeit $\tau:=\min\{n\geq 1:\; X_n=X_0\}$ einer stationären, ergodischen Quelle $(X_n)_{n\in\mathbb{Z}}$ mit $X(\Omega)=\{1,\ldots,m\}$ gilt

$$\mathbb{E}\tau=m\quad\text{und}\quad\mathbb{E}\log\tau\leq H(X_0).\tag{0.3}$$

Beweis: Mit $\tau_i:=\min\{n\geq 1:\; X_n=i\}$ folgt aus Beispiel 2

$$\mathbb{E}\tau=\mathbb{E}(\tau|X_0)=\sum_{i=1}^{m}p_i\,\mathbb{E}(\tau|X_0=i)=\sum_{i=1}^{m}p_i\,\mathbb{E}(\tau_i|X_0=i)=\sum_{i=1}^{m}p_i\,\frac{1}{p_i}=m.$$

Aus Beispiel 2 und der Ungleichung von Jensen folgt weiters

$$\mathbb{E}\log\tau=\mathbb{E}(\log\tau|X_0)=\sum_{i=1}^{m}p_i\,\mathbb{E}(\log\tau_i|X_0=i)\leq\sum_{i=1}^{m}p_i\,\log\left(\mathbb{E}(\tau_i|X_0=i)\right)$$
$$=\sum_{i=1}^{m}p_i\,\log\frac{1}{p_i}=H(X_0).$$

4. Man kann ein beliebiges $n\in\mathbb{N}$ mit einem Codealphabet der Größe $r\geq 2$ codieren, indem man zunächst $k:=k(n):=\lfloor\log_r n\rfloor+1$ und $m:=m(n):=\min\{j\;:\;k\leq\frac{j\,(j+1)}{2}\}$ bestimmt. Dann schreibt man n als $\frac{m(m+1)}{2}$-stellige Zahl im Zahlensystem zur Basis r an, wobei überflüssige führende Stellen mit Nullen besetzt werden. Nun bildet man ein Codewort aus insgesamt $\frac{m(m+1)}{2}+m$ Codebuchstaben. In die Stellen $h_i:=\sum_{j=1}^{i}j+i=\frac{i\,(i+1)}{2}+i,\quad i\geq 1$ schreibt man Prüfbits b_i mit $b_i:=0$ für $\frac{i\,(i+1)}{2}<k$ und $b_i:=1$ sonst. Auf die anderen Stellen kommen die Ziffern von n. Man zeige, dass dieser Code präfixfrei ist und dass für die Codewortlängen l_n gilt $l_n=\log_r n+o(\log_r n)$.
Lösung: Aus $\frac{m(m-1)}{2}<k$ folgt $m<\sqrt{2\,k}+1\leq\sqrt{2+2\,\log_r n}+1$, aber auch $\frac{m(m+1)}{2}+m=\frac{m\,(m-1)}{2}+2\,m\leq\log_r n+1+2\,\sqrt{2+2\,\log_r n}+2$, d.h. $l_n=\frac{m(m+1)}{2}+m=\log_r n+o(\log_r n)$.

Gilt $m(n_1) = m(n_2)$, so haben die zu n_1 und n_2 gehörigen Codeworte gleiche Länge, sodass eines nur dann Präfix des anderen sein kann, wenn sie übereinstimmen. Aber das geht nicht, da nicht alle Ziffern von n_1 und n_2 gleich sein können.

Gilt $m(n_1) < m(n_2)$, so hat n_1 an der Stelle $\frac{m(n_1)\,(m(n_1)+1)}{2} + m(n_1)$ eine 1 als Prüfbit, das Prüfbit für n_2 an dieser Stelle ist jedoch 0. Somit ist das Codewort von n_1 kein Präfix des Wortes von n_2.

5. Das Alphabet einer Nachrichtenquelle besteht aus den 4 Buchstaben $\{a, b, c, d\}$, und das Codealphabet ist binär.
   a) Codieren Sie die Folge $bbcbadadcdcb$ mit dem Lempel-Ziv-Verfahren.
   b) Dekodieren Sie die folgende mit dem Lempel-Ziv-Verfahren erzeugte Codefolge: $(0000, 00), (0001, 01), (0010, 01), (0000, 0010), (0000, 11), (0101, 11), (0100, 11), (0000, 01), (0001, 00), (1000, 01)$.

   Lösung: Die LZ-Teilung ist:

   $b|\ bc|\ ba|\ d|\ a|\ dc|\ dcb$

   $1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7$

   Mit $c(a) = (0, 0), c(b) = (01), c(c) = (10)$, $c(d) = (1, 1)$ ergibt das $(0, 01), (1, 10), (1, 00), (0, 11), (0, 00)$, $(4, 10), (6, 01)$.

   $a|\ ab|\ abb|\ c|\ d|\ dd|\ cd|\ b|\ aa|\ bb$

   $1\ \ 2\ \ 3\ \ 4\ \ 5\ \ 6\ \ 7\ \ 8\ \ 9\ \ 10$