Formelsammlung für IKT Prüfung

1. Diskrete Informationsquellen

mittlerer Informationsgehalt: $H_m = \sum_i p(x_i) \cdot \log_2 \frac{1}{p(x_i)} = \frac{bit}{Zustand}$

Informationsgehalt bei gleichwahrscheinlichen N Zuständen: $H_0 = \lceil log_2 N \rceil = \frac{bit}{Zustand}$

Unbestimmtheit eines Ereignisses : $H_i = log_2 \frac{1}{p(x_i)} = \frac{bit}{Ereignis}$

Einsparung durch bessere Kodierung: $(1 - \frac{l_m}{l}) \cdot 100$

Markov-Kette:

- $p(y_j) = \sum p(x_i) \cdot p(y_j|x_i)$
- $p(x_i) = \sum p(y_j) \cdot p(x_i|y_j)$

Einzelwahrscheinlichkeiten: $p(x_i) = \sum_{j=1}^{M} p(x_i, y_j)$ => Summe einer Zeile ,

$p(y_j) = \sum_{i=1}^{N} p(x_i, y_j)$ => Summe einer Spalte

Übergangswahrscheinlichkeiten:

$$p(y_j|x_i) = \begin{pmatrix} p(y_0|x_0) & p(y_1|x_0) & \dots & p(y_N|x_0) \\ p(y_0|x_1) & p(y_1|x_1) & \dots & p(y_N|x_1) \\ \dots & \dots & \dots & \dots \\ p(y_0|x_N) & p(y_1|x_N) & \dots & p(y_N|x_N) \end{pmatrix}$$

$$p(x_i|y_j) = \begin{pmatrix} p(x_0|y_0) & p(x_0|y_1) & \dots & p(x_0|y_{M-1}) \\ p(x_1|y_0) & p(x_1|y_1) & \dots & p(x_1|y_{M-1})) \\ \dots & \dots & \dots & \dots \\ p(x_{N-1}|y_0) & p(x_{N-1}|y_1) & \dots & p(x_{N-1}|y_{M-1}) \end{pmatrix}$$

Verbundwahrscheinlichkeiten

$$p(x_i, y_j) = \begin{pmatrix} p(x_0, y_0) & p(x_0, y_1) & \dots & p(x_0, y_M) \\ p(x_1, y_0) & p(x_1, y_1) & \dots & p(x_1, y_M) \\ \dots & \dots & \dots & \dots \\ p(x_N, y_0) & p(x_N, y_1) & \dots & p(x_N, y_M) \end{pmatrix}$$

bedingte Wahrscheinlichkeit: $p(x_i, y_j) = p(x_i) \cdot p(y_j|x_i) = p(y_j) \cdot p(x_i|y_j)$

$p(y_j|x_i) = \frac{p(x_i, y_j)}{p(x_i)}$

$p(x_i|y_j) = \frac{p(x_i, y_j)}{p(y_j)}$

stationäre Zustände einer binären Quelle:

$\bar{p}_1 = \frac{p(x_1|x_2)}{p(x_2|x_1)+p(x_1|x_2)}$

$\bar{p}_2 = \frac{p(x_2|x_1)}{p(x_2|x_1)+p(x_1|x_2)}$

Markov-Entropie: $H_m = \sum_j \sum_i \bar{p}(x_i) * p(x_j, x_i) * \log_2 \frac{1}{p(x_j,x_i)}$ (es kann $\bar{p}(x_i)$ aus der Gleichung immer ausgeklammert werden)

$=>$ zweistufiger Prozess: $H_m = \sum_{i=1}^{N} p_i \cdot (log_2 \frac{1}{p_i} + log_2 M)$ (M - Anzahl der Unterelemente in der 2ten Stufe)

Entropien:

$H(X) = \sum_{i=1}^{N} p(x_i) \cdot log_2 \frac{1}{p(x_i)} \frac{bit}{KZ}$,

$H(Y) = \sum_{j=1}^{M} p(y_j) \cdot log_2 \frac{1}{p(y_j)} \frac{bit}{KZ}$,

$H(Y|X) = \sum_i p(x_i) \cdot (\sum_j p(y_j|x_i) \cdot log_2 \frac{1}{p(y_j|x_i)}) \frac{bit}{KZ}$

$H(X|Y) = \sum_j p(y_j) \cdot \sum_i p(x_i|y_j) \cdot log_2 \frac{1}{p(x_i|y_j)}$

Verbundsentropie: $H(X,Y) = H(X) + H(Y|X)$

vollständige Abhängigkeit: $H(X,Y) = H(Y)$

vollständig Unabhängigkeit: $H(X,Y) = H(X) * H(Y)$ oder $H(Y|X) = H(Y)$

Koderedundanz: $R_k = l_m \cdot H_k - H_m$ (H_k wird im Normalfall mit 1 angenommen)

mittlere Kodewortlänge: $l_m = \sum p_i \cdot l_i$ (ungleichmäßiger Kode) , $l = \lceil \log_2 N \rceil$ (gleichmäßiger Kode)

Kraft-Ungleichung: $\sum_{i=1}^{N} 2^{-l_i} \leq 1$ (notwendige aber nicht hinreichende Bedingung)

Schranken der Minimierung: $H_m \leq l_m < H_m + 1$--> mit Erweiterung: $m \cdot H_m \leqslant m \cdot l_m < m \cdot H_m + 1$

2.Übertragungskanal

Transinformation: $H_T = H(X) - H(X|Y) = H(Y) - H(Y|X)$

symmetrisch gestörter Binärkanal ($p_s = \delta = \epsilon$):

$H_T = H(Y) + (1 - p_s) \cdot \log_2(1 - p_s) + p_s \cdot \log_2 p_s$

$p(y_0) = (1 - \epsilon) \cdot p(x_0) + \delta \cdot p(x_1)$

$p(y_1) = \epsilon \cdot p(x_0) + (1 - \delta) \cdot p(x_1)$

Zeichenwahrscheinlichkeiten (allgmein):

$p(y_0) = p(x_0) \cdot p(y_0|x_0) + p(x_1) \cdot p(y_0|x_1)\ldots$
$p(y_1) = p(x_0) \cdot p(y_1|x_0) + p(x_1) \cdot p(y_1|x_1)\ldots$

allgemeine Übertragung (siehe Übertragungskanal.png):

- Quelleninformationsfluss : $I_Q = f_Q \cdot H_Q \frac{bit}{s}$
- Anzahl der Kanalzeichen : $l \geq \lceil \frac{H_0}{H_K} \rceil $
- Quellenkodeinformationsfluss : $I_{KQ} = f_Q \cdot l \cdot H_K$ => Bedingung: $I_{KQ} \geq I_Q$
- Kanalinformationsfluss: $I_K = v_ü = v_s \cdot H_K \frac{bit}{s}$
- Transinformationsfluss: $I_T = v_s \cdot H_T \ \frac{bit}{s}$
- Kanalkapazität (maximalwert des Trnasinformationsflusses): $C = max\{I_T\} = max\{v_s \cdot H_T\}$ mit der Nebenbedingung:
  - $v_{smax} = 2B$
  - $I_{KQ} \leq C$
- Kapazitätsauslastung: $A = \frac{I_T}{C} \cdot 100\% = \frac{v_s \cdot H_T}{2B \cdot H_T} \cdot 100\% = \frac{v_s}{2B} \cdot 100\%$

ungesicherte Übertragung (alles von der allgemeinen Übertragung mit den ein paar Änderungen):

- Kanalinformationsfluss: $I_K = I_{KQ}$
- Schrittgeschwindigkeit: $v_s = \frac{I_{KQ}}{H_K} = f_q \cdot l \ \frac{KZ}{s}$
- Transinformationsfluss Bedingung: $I_T < I_{KQ}$

gesicherte Übertragung (alles von der allgemeinen Übertragung mit den zusätzlichen Berechnungen):

- Länge der Kodewörter mit Redundanz: $n = l + \Delta l = l + (\frac{H_K}{H_T} - 1) \cdot l$
- Kanalinformationsfluss: $I_K = I_{KK} = f_Q \cdot n \cdot H_K$
- $I_{KK} = f_Q \cdot n \cdot H_K$ mit der Bedingung: $I_{KK} > I_{KQ}$
- Schrittgeschwindigkeit: $v_s = f_q \cdot l \cdot \frac{H_K}{H_T} = f_q \cdot n \ \frac{KZ}{s}$
- Transinformationsfluss Bedingung: $I_T = I_{KQ} \ \frac{bit}{s}$

Kanalkodierung

Grad Fehlererkennung: $d_{min} = f_e + 1 \rightarrow$ Korrektur: $f_e = \lfloor \frac{d_{min}}{2} \rfloor$

verfälschte Stellen: $d_{min} = 2 \cdot f_k + 1 \rightarrow$ Korrektur: $f_k = \lfloor \frac{d_{min}-1}{2} \rfloor$

Bündelungsfehler = $f_b \leq k$

Schranken:

- $f_k = 1 \rightarrow 2^k \geq 1 + n$
- $f_k = 2 \rightarrow 2^k \geq 1 + n + \frac{n \cdot (n-1)}{2}$
- $k \geq log_2 \sum_0^{f_k} \binom{n}{i}$

Generatormatrix: $G_{l \times n} = [I_l C]$

- Anfang bildet die Einheitsmatrix
- jede Zeile beinhaltet ein Codewort

- mittels der Matrix kann ein Codewort codiert werden

Kontrollmatrix: $H_{k\times n} = [C^T I_K]$

- Transponierung der Codewört + auffüllen mit der Einheitsmatrix
- Ziel: Testen ob ein Fehler bei Übertragen aufgetreten ist $\rightarrow$ wenn s gleich 0 dann ist er nicht erkennbar oder nicht da

Orthogonalitätsbedingung: $G \cdot H^T = (H \cdot G^T)^T = 0$

Anzahl Stellen: $n = l + k$

zyklische Codes

- $k_1 = \text{grad M(x)}$ (Hamming Code: $M(x) = m_1(x) = g(x)$)
- $n \leq 2^{k_1} - 1$ (wenn $n < 2^{k_1} - 1$ dann ist der Code verkürzt, bei Gleichheit ist er dicht gepackt)
- $g(x) = kgV\{m_\mu(x), m_{\mu+1}(x), m_{\mu+d_E-2}(x)\}$
- n = l + k
- k = grad g(x)

zyklischer Hammingcode Parameter:

- $(2^{k_1} - 1, 2^{k_1} - 1 - k_1, d_{min} = 3)$
- $f_e = 2$
- $f_k = 1$

Abrahamson Code:

- $g(x) = m_0(x), m_1(x)$
- $(2^{k_1} - 1, 2^{k_1} - 1 - (k_1 + 1), d_{min} = 4)$

Multiplikationsverfahren: $a(x) = a^*(x) \cdot g(x)$

Divisionsverfahren:

- $a(x) = a^*(x) \cdot x^k + r(x)$
- $r(x) = a^*(x) \cdot x^k \mod g(x)$