1 Diskrete Quellen

Alphabet $X = \{x_1, x_2, \dots, x_N\}$
Verteilung $(p(x_i)) = (p(x_1), p(x_2), \dots, p(x_N))$ mit $0 \le p(x_i) \le 1$.
Vereinbarung

$$\sum_i := \sum_{i=1}^{N}, \sum_j := \sum_{j=1}^{M}$$

Satz der vollständigen Wahrscheinlichkeit $\sum_i p(x_i) = 1$.
Unbestimmtheit/Entropie/Informationsgehalt

$$\boxed{H_i = \mathrm{ld}\,\frac{1}{p(x_i)}} = -\,\mathrm{ld}\,p(x_i)$$

Mittlerer Informationsgehalt

$$\boxed{H_m = \sum_i p(x_i) \frac{1}{\mathrm{ld}\,p(x_i)}}$$

Bei Gleichverteilung gilt:
$p(x_i) = \frac{1}{N}$ $H_Q = H_0 = \mathrm{ld}\,N$

1.1 Markow-Quellen

Entropie $H_Q = H_M =$

$$\boxed{\sum_{i,j} \overline{p(x_i)} p(x_j|x_i)\,\mathrm{ld}\,\frac{1}{p(x_j|x_i)}}$$

Stationärer Fall $p(x_i) = \overline{p(x_i)}$:
$\lim_{n\to\infty} (p(x_j|x_i))^n = (\overline{p(x_i)})$

1.2 Verbundquellen

Zwei diskrete Quellen X und Y mit Verbundwahrscheinlichkeiten $(p(x_i, y_j))$, $i \in \{1, 2, \dots, N\}$, $j \in \{1, 2, \dots, M\}$ bilden eine Verbundquelle (X, Y).
Verbundwahrscheinlichkeiten

$$\boxed{\begin{aligned} p(x_i, y_j) &= p(x_i) \cdot p(y_j|x_i) \\ &= p(y_j) \cdot p(x_i|y_j) \end{aligned}}$$

Verbundentropie

$$\begin{aligned} H(X, Y) &= H(X) + H(Y|X) \\ &= H(Y) + H(X|Y) \end{aligned}$$

$H(X,Y) =$

$$\boxed{\sum_{i,j} p(x_i, x_j)\,\mathrm{ld}\,\frac{1}{p(x_i, x_j)}}$$

$H(X) = \sum_i p(x_i)\,\mathrm{ld}\,\frac{1}{p(x_i)}$
$H(Y) = \sum_j p(y_j)\,\mathrm{ld}\,\frac{1}{p(y_j)}$
$H(Y|X) =$

$$\boxed{\sum_{i,j} p(x_i) p(y_j|x_i)\,\mathrm{ld}\,\frac{1}{p(y_j|x_i)}}$$

$H(Y|X) =$

$$\boxed{\sum_{j,i} p(y_j) p(x_i|y_j)\,\mathrm{ld}\,\frac{1}{p(x_i|y_j)}}$$

In den Matrix-Darstellungen $(p(x_i, y_j))$, $(p(x_i|y_j))$ und $(p(y_j|x_i))$ läuft i zeilenweise und j spaltenweise.

2 Quellkodierung

Mittlere Kodewortlänge

$$\boxed{l_m = \sum_i p(x_i) l_i}$$

Gleichmäßiger Kode $l = \lceil \mathrm{ld}\,N \rceil$

dekodierbar $l_m \ge H_m$ oder auch $\sum_i 2^{-l_i} \le 1$

annähernd redundanzfrei $H_m \le l_m < H_m + 1$

$2^{-l_i} \le p(x_i) < 2^{-l_i + 1}$

redundanzfrei $l_m = H_m \Leftrightarrow p(x_i) = 2^{-l_i}$

Koderedundanz

$$\boxed{R_K = l_m\,[\cdot H_K] - H_Q \ge 0}$$

3 Kanäle

3.1 Diskrete Kanäle

Quelle X, Senke Y
Transinformation

$$\begin{aligned} H_T &= H(X) + H(Y) - H(X, Y) \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \end{aligned}$$

Quelleninformationsfluß

$$\boxed{I_Q = f_Q H_Q}$$

Quellenkodeinformationsfluß

$$\boxed{I_{KQ} = f_Q l H_K}$$

Kanalkodeinformationsfluß

$$\boxed{I_{KK} = f_Q (l + \Delta l) H_K = f_Q n H_K}$$

Kanalsymbolfrequenz f_K
Schrittgeschwindigkeit v_s

$$\boxed{f_K = v_s}$$

Übertragungsgeschwindigkeit

$$\boxed{v_{ü} = I_K = v_s H_K}$$

Transinformationsfluß

$$\boxed{I_T = v_s H_T}$$

Kanalkapzität
$C = \max\{I_T\} = 2B \max H_T$

Ungesicherte Übertragung

$$\boxed{I_K = I_{KQ}}, \boxed{v_s = \frac{I_{KQ}}{H_K} = f_Q l}$$

Gesicherte Übertragung

$$\boxed{I_K = I_{KK} = f_Q n H_K} \text{ bzw.}$$

$$\boxed{I_T = I_{KQ}}$$

$$\boxed{v_s = \frac{I_{KQ}}{H_T} = f_Q l \frac{H_K}{H_T} = f_Q n}$$

$$\boxed{\begin{aligned} I_{KK} &= f_Q \left(l \frac{H_K}{H_T} \right) H_K \\ &= f_Q n H_K \end{aligned}}$$

3.2 Analoge Kanäle

$H(X) = \int_{-\infty}^{+\infty} f(x)\,\mathrm{ld}\,\frac{1}{f(x)}\mathrm{d}x - \mathrm{ld}\,\Delta x$

3.2.1 Normalverteilung

$f(x) = \frac{1}{\sqrt{2\pi P}} \exp -\frac{x^2}{2P}$
$P_x \dots$ mittlere Nutzsignalleistung
$p_z \dots$ mittlere Störsignalleistung
$H(X) = \frac{1}{2}\,\mathrm{ld}(2\pi \mathrm{e} P_x)$
$H(Y|X) = \frac{1}{2}\,\mathrm{ld}(2\pi \mathrm{e} P_z)$
$H(Y) = \frac{1}{2}\,\mathrm{ld}(2\pi \mathrm{e}(P_x + P_z))$
$H_T = \frac{1}{2}\,\mathrm{ld}\left(1 + \frac{P_x}{P_z}\right)$
Rauschabstand $r = 10 \log \frac{P_x}{P_z}$
$C = 2B\frac{1}{2}\,\mathrm{ld}\left(1 + \frac{P_x}{P_z}\right)$
Für $\frac{P_x}{P_z} \gg 1$ gilt:

$$\boxed{H_T \approx 0{,}166 r}$$

$$\boxed{C \approx 0{,}332 B r}$$

3.2.2 Zeitquantisierung

Abtastfrequenz $\boxed{f_A \ge 2 f_g}$
Abstand der Abtastwerte

$$\boxed{t_A \le \frac{1}{2 f_g} = \frac{1}{f_A}}$$

Umsetzzeit $t_u \le \frac{1}{2 f_g}$
$l = \lceil 0{,}166 r \rceil \to m = 2^l$
$C \ge I_{KQ} = 2 f_g l H_K = f_A l H_K$

4 Kanalkodierung

Die Anzahl an Stellen an der sich zwei Kodewörter $a_i = (u_{i1} u_{i2} \dots u_{in})$ und $a_j = (u_{j1} u_{j2} \dots u_{jn})$ unterscheiden heißt Hamming-Distanz $d(a_i, a_j) = \sum_{g=1}^{n} (u_{ig} \oplus u_{jg})$
Hamming-Gewicht $w(a_i) = \sum_{g=1}^{n} u_{ig} = d(\mathbf{0}, a_i)$

Hamming-Schranke

$$\boxed{2^k \ge \sum_{i=0}^{f_k} \binom{l + k}{i}}$$

Relative Redundanz $r_k = \frac{k}{n}$
Koderate $R = \frac{l}{n}$

4.1 Eigenschaften

$(n, l, d_{\min})$
allgemein $d_{\min} = f_e + f_k + 1$
Fehlererkennungskode

$$\boxed{f_e = d_{\min} - 1}$$

Fehlerkorrekturkode

$$\boxed{f_k = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor}$$

4.2 Lineare Gruppenkodes

4.2.1 Eigenschaften

Erfüllen Gruppenaxiome:

1. Neutrales Element
2. Inverses Element
3. Abgeschlossenheit

4.2.2 Erzeugung

Können eindeutig durch eine Generatormatrix $G_{l\times n}$ beschrieben werden.
Bildung Kanalkodewort

$$\boxed{(a_i) = (a_i^*) \cdot G_{l\times n}}$$

Kanonische/reduzierte Form der Generatormatrix $G_{l\times n} = (I_l C)$, mit I_l als $l \times l$-Einheitsmatrix

4.2.3 Fehlererkennung

Systematischer Kode Quellkodewort kann durch Streichen redundanter Stellen aus dem Kanalkodewort entnommen werden.
Kontrollmatrix

$$\boxed{H_{k\times n} = (C^\mathsf{T} I_k)}$$

Fehlersyndrom von Kanalwort b

$$\boxed{s = H \cdot b^\mathsf{T}}$$

$s = \mathbf{0} \Rightarrow$ kein Fehler.

4.2.4 Hamming-Kodesi

Spezieller dichtgepackter, einfach-fehlerkorrigierender Gruppenkode mit $d_{\min} = 3$ und Kode-wort-länge $n = 2^k - 1$. Redundante Stelle k_i steht an Position 2^i im Kodewort $\Rightarrow$ Syndrom s liefert die Position des fehlerhaften Elements.

In Kontrollmatrix $H_{k\times n}$ steht in der i-ten Spalte der Wert $n - i + 1$ binär kodiert.

Verkürzter Hamming-Kode Bestimmen der minimal notwendigen Anzahl an Kontrollstellen k und Streichen der überflüssigen Informationsstellen l.

Erweiterter Hamming-Kode Ein weiteres Kontrollelement k_0 (Paritätsbit) wird hinzugefügt. $d_{\min} = 4$, $n \le 2^k$. Kontrollmatrix H erhält eine zusätzliche mit Einsen besetze Zeile und eine zusätzliche Spalte.

4.3 Zyklische Kodes

- Ein Kode heißt *zyklisch*, wenn für jedes Kanalkodewort durch zyklische Verschiebung der Elemente wieder ein Kanalkodewort entsteht. Ein zyklischer Kode ist ein spezieller Linearkode, der die Gruppen- und Körperaxiome erfüllt.
- Ein zyklischer Kode wird vollständig durch ein Produkt von *irreduziblen* Minimalpolynomen, *Generatorpolynom* $g(x)$ genannt, beschrieben.
- Ein Polynom ist *irreduzibel*, wenn es nicht in ein Produkt von Polynomen zerlegbar ist.
- Das Modularpolynom $M(x)$ vom Grad $k_1 = \operatorname{grad} M(x)$ bestimmt den Kodeparameter $n \le 2^{k_1} - 1$.
- Der tatsächliche Wert von n berechnet sich aus dem *Zyklus der Polynomreste* über $GF(2)$ mit $x_i \mod M(x)$ $(i \in \{0, 1, \dots, p\})$ und bestimmt $n = p | 2^{k_1} - 1$
- Ist $n = p = 2^{k_1} - 1$ dann ist $M(x)$ *primitiv*.
- BCH-Kodes können zusätzlich Bündelfehler $f_b \le k$ erkennen.

4.3.1 Kodeparamter

$n = 2^{k_1} - 1$
$k_1 = \operatorname{grad} M(x)$
$k = \operatorname{grad} g(x)$
$l = n - k$
$d_{\min} = z + 1$, mit z Anzahl aufeinander folgender Nullstellen

4.3.2 Bildungsverfahren

Multiplikationsverfahren
$a(x) = a^*(x) g(x)$
Divisionsverfahren
$a(x) = a^*(x) x^k + r(x)$ mit $r(x) = a^*(x) x^k \mod g(x)$ (Rest bei Divison). Erzeugt immer *systematischen* Kode
Generatormatrix

4.3.3 Fehlererkennung

$a(x) \mod g(x) = 0 \Rightarrow$ kein Fehler.

4.3.4 Kode-Konstruktion

Entwurfsabstand d_E
$g(x) = \mathrm{kgV}\{m_\mu(x), m_{\mu+1}(x), \dots, m_{\mu+d_\mathrm{E}-2}(x)\}$
Typischerweise $\mu \in \{0, 1\}$
$d_{\min} \ge d_\mathrm{E}$

Verkürzter Kode $(n, l, d_{\min}) \to (n - u, l - u, d_{\min})$, k konstant.

Erweiterter Kode $g(x)$ mit $(x + 1) = m_0(x)$ multiplizieren. $(n, l, d_{\min}) \to (n + 1, l, d_{\min} + 1)$

Zyklischer Hamming-Kode $g(x) = M(x) = m_1(x) \to d_{\min} = 3$

Abramson-Kode $g(x) = m_0(x) m_1(x) = (x + 1) M(x) \to d_{\min} = 4$