Grundlagen der Nachrichtentechnik 4

Prof. Dr.-Ing. Andreas Czylwik

Nachrichtentechnik 4
Organisatorisches

- Vorlesung 2 SWS
- Übung 1 SWS, Betreuer: Dipl.-Ing. Lars Häring
- Folienkopien sind verfügbar
- Prüfung: schriftlich

- Neue Forschungsthemen im Fachgebiet Nachrichtentechnische Systeme
- Studien- und Diplomarbeiten

Nachrichtentechnik 4
Literatur

- Literatur zur Vorlesung:
  - B. Friedrichs: Kanalcodierung, Springer-Verlag
  - H. Schneider-Obermann: Kanalcodierung, Vieweg-Verlag
  - H. Rohling: Einführung in die Informations- und Codierungstheorie, Teubner-Verlag
  - Blahut: Theory and practice of error control codes, Addison-Wesley
  - M. Bossert: Channel coding for telecommunications, John Wiley
  - M. Bossert: Kanalcodierung, Teubner-Verlag
  - J. H. van Lint: Introduction to coding theory

Nachrichtentechnik 4
Literatur

- Literatur zur digitalen Übertragung:
  - S. Benedetto, E. Biglieri, V. Castellani: Digital transmission theory, Prentice-Hall
  - J.G. Proakis: Digital communications, McGraw-Hill
  - S. Haykin: Communication systems, John Wiley

Nachrichtentechnik 4

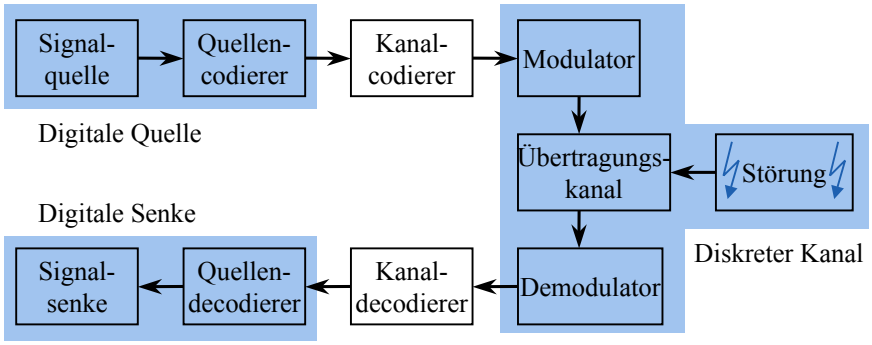
Inhalt

1. Einführung
2. Grundlagen der Informationstheorie
3. Kanalcodierung in der Nachrichtenübertragung
4. Algebraische Grundbegriffe für Codes
5. Blockcodes
6. Faltungscodes
7. Codierungstechniken
8. Ausblick

Nachrichtentechnik 4

1 Einführung

- Blockschaltbild eines Systems zur digitalen Nachrichtenübertragung



Nachrichtentechnik 4
1 Einführung

- Quellencodierung (source coding):
  - Kompression der Nachricht auf eine minimale Anzahl von Symbolen ohne Informationsverlust (Reduktion von Redundanz)
  - weitergehende Kompression, wobei toleriert wird, dass Information verloren geht (z. B. bei Bild- und Tonübertragung)
- Codierung zur Verschlüsselung (Kryptologie)
  - Schutz vor unberechtigtem Abhören
  - Entschlüsselung nur mit Kenntnis eines Code-Schlüssels

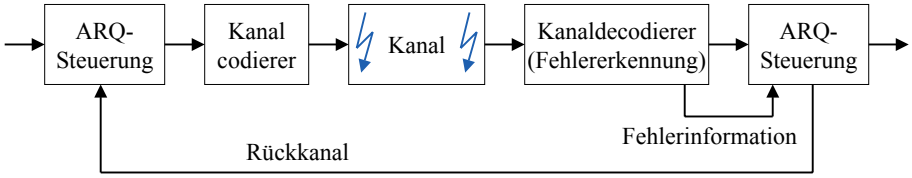
Nachrichtentechnik 4
1 Einführung

- Kanalcodierung (error control coding): kontrolliertes Hinzufügen von Redundanz zum Schutz gegen Übertragungsfehler
  - Kanalcodierung zur Fehlerkorrektur (FEC – forward error correction)
  - vereinfachtes Modell:

  - Kanalqualität bestimmt Restfehlerwahrscheinlichkeit nach Decodierung
  - Datenrate unabhängig von Kanalqualität

Nachrichtentechnik 4
1 Einführung

- Kanalcodierung zur Fehlerdetektion (CRC – cyclic redundancy check, Einsatz für ARQ-Verfahren (automatic repeat request))



- Rückkanal notwendig
- adaptives Einfügen von Redundanz (zusätzliche Redundanz nur im Fehlerfall
- Restfehlerwahrscheinlichkeit unabhängig von der Kanalqualität
- Datenrate abhängig von Kanalqualität

Nachrichtentechnik 4
1 Einführung

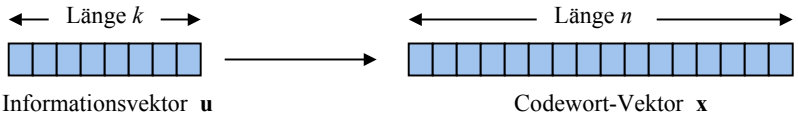
- Anwendungen: sichere Datenübertragung über Wellenleiter und Funkkanäle (insbesondere Mobilfunkkanäle), sichere Datenspeicherung
- Begründer der Informationstheorie Claude E. Shannon:

  Durch Kanalcodierung kann die Fehlerwahrscheinlichkeit beliebig reduziert werden, wenn die Datenrate kleiner als die Kanalkapazität ist.

  (Shannon gibt keine Konstruktionsvorschrift an.)

Nachrichtentechnik 4
1 Einführung

- Grundgedanke der Kanalcodierung:
  - Einfügen von Redundanz
  - Ziel: Fehlererkennung oder Fehlerkorrektur
  - Zuordnung im Codierer am Beispiel einer Block-Codierung:

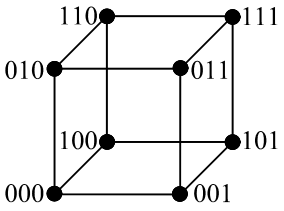


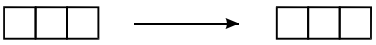
Informationsvektor **u** Codewort-Vektor **x**

  - Eingangsvektor: $\mathbf{u} = (u_1, \ldots, u_k)$
  - Ausgangsvektor: $\mathbf{x} = (x_1, \ldots, x_n)$
  - Coderate: $R_C = \frac{k}{n}$ (1.1)

Nachrichtentechnik 4
1 Einführung

- Codewürfel mit $n = 3$, $k = 3$

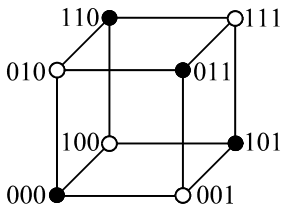


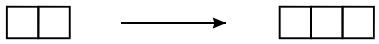


  - uncodierte Übertragung: $R_C = 1$
  - kleinstmögliche Distanz zu anderem Codewort: $d_{min} = 1$
  - keine Fehlererkennung und keine Fehlerkorrektur möglich

Nachrichtentechnik 4
1 Einführung

- Codewürfel mit $n = 3,\ k = 2$

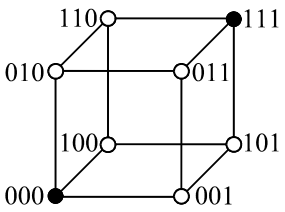


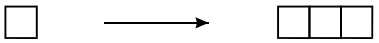


  - codierte Übertragung: $R_C = 2/3$
  - kleinstmögliche Distanz zu anderem Codewort: $d_{min} = 2$
  - Erkennung eines Fehlers möglich, keine Fehlerkorrektur möglich

Nachrichtentechnik 4
1 Einführung

- Codewürfel mit $n = 3,\ k = 1$





  - codierte Übertragung: $R_C = 1/3$
  - kleinstmögliche Distanz zu anderem Codewort: $d_{min} = 3$
  - Erkennung von zwei Fehlern und Korrektur eines Fehlers möglich

Nachrichtentechnik 4

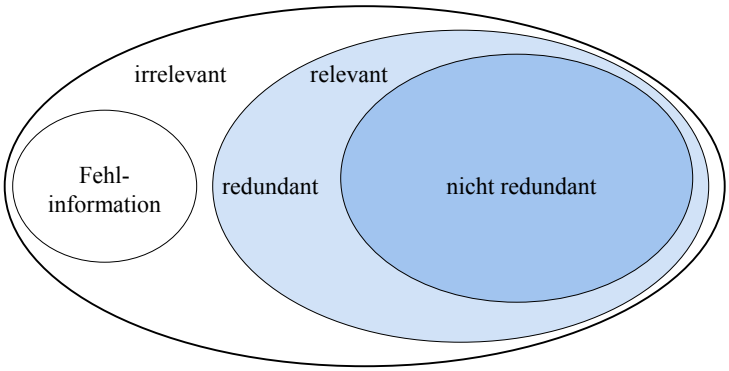
2 Grundlagen der Informationstheorie

- Informationtheorie: mathematische Beschreibung der Übertragung von Nachrichten
- zentrale Fragestellungen:
  - quantitative Berechnung des Informationsgehalts von Nachrichten
  - Bestimmung der Übertragungskapazität von Übertragungskanälen
  - Analyse und Optimierung von Quellen- und Kanalcodierung

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Nachricht aus der Sicht der Informationstheorie



Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Informationsgehalt einer Nachricht, Entropie
- qualitative Einordung von Nachrichten: Bedeutung umso größer, je weniger die Nachricht vorhersagbar ist
  - Beispiel:
    - Morgen geht die Sonne auf.
    - Morgen gibt es schlechtes Wetter.
    - Morgen gibt es ein starkes Unwetter, bei dem der Strom ausfallen wird.

- Nachrichten einer digitalen Quelle: Folge von Zeichen

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Entscheidungsgehalt H_0 einer Quelle: Anzahl der für die Auswahl der Nachricht benötigten Binärentscheidungen
  - Zeichenvorrat: N Zeichen

$$H_0 = \mathrm{ld}(N)\ \text{bit/Zeichen} \qquad (2.1)$$

mit ld(x) = logarithmus dualis

  - Einheit: bit = binary digit
  - Entscheidungsgehalt H_0 berücksichtigt nicht die Auftrittswahrscheinlichkeit

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiel: deutschsprachiger Text als Quelle
  - 26 · 2 Buchstaben, 3 · 2 Umlaute, ß, 12 Sonderzeichen einschließlich Leerzeichen „“ ()-.,;:!?
  - insgesamt 71 alphanumerischen Zeichen
  - $H_0 = \mathrm{ld}(71) = \ln(71) / \ln(2) = 6{,}15$ bit/Zeichen
- Beispiel: eine Seite deutschsprachiger Text mit 40 Zeilen und 70 Zeichen pro Zeile
  - Anzahl unterschiedlicher Seiten: $N = 71^{40 \cdot 70}$
  - Entscheidungsgehalt:

    $H_0 = \mathrm{ld}(71^{40 \cdot 70}) = 40 \cdot 70 \cdot \mathrm{ld}\,(71) = 17{,}22$ kbit/Seite

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Zeichenvorrat (Alphabet): $X = \{x_1, \ldots, x_N\}$
- Auftrittswahrscheinlichkeiten der Zeichen: $p(x_1), \ldots, p(x_N)$
- gewünschte Eigenschaften des Informationsgehalts $I = f(p)$:
  - $I(x_i) \geq 0 \quad \text{für} \quad 0 \leq p(x_i) \leq 1$
  - $I(x_i) \to 0 \quad \text{für} \quad p(x_i) \to 1$
  - $I(x_i) > I(x_j) \quad \text{für} \quad p(x_i) < p(x_j)$
  - zwei aufeinanderfolgende statistisch unabhängige Zeichen

    x_i und x_j mit $p(x_i,x_j) = p(x_i) \cdot p(x_j)$:

    $I(x_i,x_j) = I(x_i) + I(x_j)$
- allgemeine Lösung: $I(x_i) = -k \cdot \log_b(p(x_i))$ (2.2)

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Definition des Informationsgehalts:

$$I(x_i) = \mathrm{ld}\left(\frac{1}{p(x_i)}\right) \text{ bit/Zeichen} \qquad (2.3)$$

- Entropie $H(X)$ = mittlerer Informationsgehalt einer Quelle:

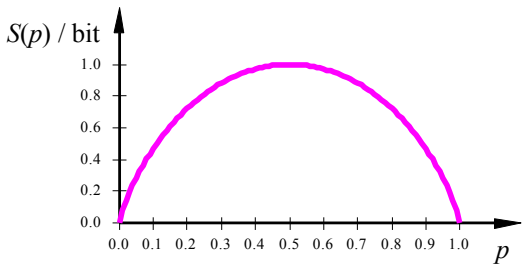
$$H(X) = \langle I(x_i) \rangle = \sum_{i=1}^{N} p(x_i) \cdot I(x_i)$$

$$= \sum_{i=1}^{N} p(x_i) \cdot \mathrm{ld}\left(\frac{1}{p(x_i)}\right) \text{ bit/Zeichen} \qquad (2.4)$$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Beispiel: binäre Quelle mit $X = \{x_1, x_2\}$
  - Auftrittswahrscheinlichkeiten: $p(x_1) = p$, $p(x_2) = 1 - p$
  - Entropie: $H(X) = -p\ \mathrm{ld}(p) - (1-p)\ \mathrm{ld}(1-p)$ (2.5)
  - Shannon-Funktion: $H(X) = S(p)$



Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

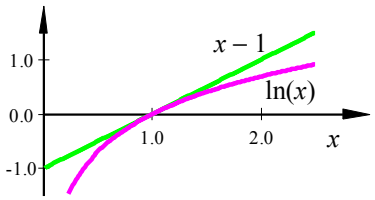
- Die Entropie wird maximal für gleichwahrscheinliche Zeichen

  $\Rightarrow \quad H(X) \le H_0 = \mathrm{ld}\, N.$ (2.6)

  - Beweis:

$$H(X) - \mathrm{ld}\, N = \sum_{i=1}^{N} p(x_i) \cdot \mathrm{ld} \frac{1}{p(x_i)} - \sum_{i=1}^{N} p(x_i) \cdot \mathrm{ld}\, N$$

$$= \sum_{i=1}^{N} p(x_i) \cdot \mathrm{ld} \frac{1}{p(x_i) \cdot N}$$



Ausnutzen der Ungleichung:

$\ln x \le x - 1$ (2.7)

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

mit $\ln x \le x - 1 \quad \Rightarrow \quad \mathrm{ld}\, x \le \frac{1}{\ln 2}(x-1)$

$$H(X) - \mathrm{ld}\, N \le \sum_{i=1}^{N} p(x_i) \cdot \frac{1}{\ln 2} \left(\frac{1}{p(x_i) \cdot N} - 1 \right)$$

$$\le \frac{1}{\ln 2} \sum_{i=1}^{N} \left(\frac{1}{N} - p(x_i) \right) = \frac{1}{\ln 2} \left(N \cdot \frac{1}{N} - 1 \right) = 0$$

■

- Redundanz einer Quelle: $R_Q = H_0 - H(X)$ (2.8)

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Übertragung über Binärkanal:

  Entwurf von Binärcodierungen für eine diskrete Quelle

- Aufgaben der Quellencodierung:
  - Zuweisung eines Binärcodes mit der Codewortlänge $L(x_i)$ zu einem Zeichen x_i
  - Minimierung der mittleren Codewortlänge $\overline{L}$

$$\overline{L} = \langle L(x_i) \rangle = \sum_{i=1}^{N} p(x_i) \cdot L(x_i) \qquad (2.9)$$

$x_1 \rightarrow 1001$

$x_2 \rightarrow 011$

$\vdots \qquad \vdots$

$x_N \rightarrow 010111$

$L(x_N)$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiele für binäre Codierungen von Zeichen:
  - ASCII-Code: feste Codewortlänge $L(x_i) = 8$ (Blockcode)
  - Morse-Code (Punkt-Strich-Alphabet mit Pause zur Trennung der Codewörter): häufig auftretende Buchstaben werden kurzen Codeworten zugeordnet
- Präfix-Eigenschaft eines Codes: kein Codewort bildet gleichzeitig den Beginn eines anderen Codewortes – „kommafreier Code“

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiel für einen Code *ohne* Präfix-Eigenschaft:

x_1	$\rightarrow$	0
x_2	$\rightarrow$	01
x_3	$\rightarrow$	10
x_4	$\rightarrow$	100

  - eindeutige Decodierung einer Bitfolge nicht möglich
  - mögliche Decodier-Ergebnisse für die Sequenz 010010:
    $x_1x_3x_2x_1$, $x_2x_1x_1x_3$, $x_1x_3x_1x_3$, $x_2x_1x_2x_1$, $x_1x_4x_3$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiel für einen Code *mit* Präfix-Eigenschaft:

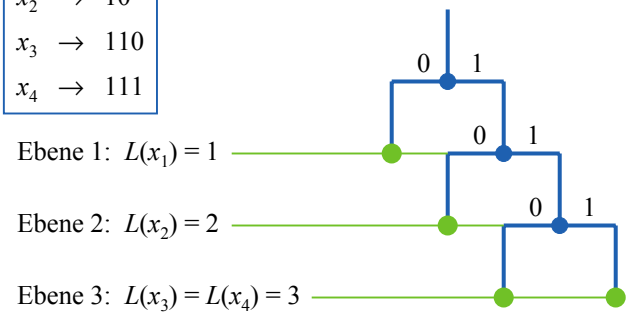
x_1	$\rightarrow$	0
x_2	$\rightarrow$	10
x_3	$\rightarrow$	110
x_4	$\rightarrow$	111

  - eindeutige Decodierung einer Bitfolge
  - Decodierung der Sequenz 010010110111100:
    $x_1x_2x_1x_2x_3x_4x_2x_1$
  - Synchronisation: Anfang der Sequenz

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Decodierung mit Hilfe eines Entscheidungsbaums

$x_1 \rightarrow 0$
$x_2 \rightarrow 10$
$x_3 \rightarrow 110$
$x_4 \rightarrow 111$



Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Kraftsche Ungleichung: Ein Binärcode mit der Präfix-Eigenschaft und den Codewortlängen $L(x_1)$, $L(x_2)$, ... , $L(x_N)$ existiert nur dann, wenn

$$\sum_{i=1}^{N} 2^{-L(x_i)} \leq 1 \qquad (2.10)$$

- Das Gleichheitszeichen gilt, wenn alle Endpunkte des Codebaums mit Codewörten besetzt sind.

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beweis:
  - Länge der Baumstruktur = maximale Codewortlänge

    $L_{\max} = \max(L(x_1), L(x_2), \ldots, L(x_N))$
  - Codewort in Ebene $L(x_i)$ eliminiert $2^{L_{\max}-L(x_i)}$ der möglichen Codeworte in der Ebene $L_{\max}$
  - Summe aller eliminierten Codeworte ≤ maximale Anzahl in der Ebene $L_{\max}$

$$\sum_{i=1}^{N} 2^{L_{\max}-L(x_i)} \le 2^{L_{\max}}$$

■

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Grenze für die mittlere Codewortlänge:

$$\bar{L} \ge H(X) \qquad (2.11)$$

  - Beispiel für den Sonderfall, dass die Auftrittswahrscheinlichkeiten Zweierpotenzen sind: $p(x_i) = \left(\frac{1}{2}\right)^{K_i}$ (2.12)
    - Zuordnung der Codeworte entsprechend der Vorschrift

      $L(x_i) = K_i$
    - Sonderfall:

      $\bar{L} = H(X) = \frac{15}{8}$

x_i	$p(x_i)$	Codeworte
x_1	1/2	1
x_2	1/4	00
x_3	1/8	010
x_4	1/16	0110
x_5	1/16	0111

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Shannon'sches Codierungstheorem: Für jede Quelle lässt sich eine Binärcodierung finden mit:

$$H(X) \le \overline{L} \le H(X)+1 \qquad (2.13)$$

  - Beweis:

    linke Seite: mittlere Codewortlänge ≥ mittlerer Informationsgehalt

    rechte Seite: Auswahl eines Codewortes mit

$$I(x_i) \le L(x_i) \le I(x_i) + 1 \qquad (2.14)$$

    Multiplikation mit $p(x_i)$ und Summation über alle i $\Rightarrow$ s.o.

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Nachweis, dass es einen Code mit Präfix-Eigenschaft (11) gibt:

  linke Seite von (2.14):

$$I(x_i) = \mathrm{ld}\left(\frac{1}{p(x_i)}\right) \le L(x_i) \quad \Rightarrow \quad p(x_i) \ge 2^{-L(x_i)}$$

  Summe über alle Symbole entspricht (2.10):

$$\sum_{i=1}^{N} 2^{-L(x_i)} \le \sum_{i=1}^{N} p(x_i) = 1$$

■

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Shannon'sche Codierung
  - Codewortlänge entsprechend (2.14): $I(x_i) \le L(x_i) \le I(x_i) + 1$
  - akkumulierte Auftrittswahrscheinlichkeiten $P_i = \sum_{j=1}^{i-1} p(x_j)$
  - Sortieren der Symbole nach Auftrittswahrscheinlichkeit
  - Codeworte sind Nachkommastellen eine Binärdarstellung von P_i

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiel
  - $H_0 = 3{,}17$ bit
  - $H(X) = 2{,}97$ bit
  - Mittlere Codewortlänge: $\overline{L} = 3.54$ bit
  - Berechnung eines Codewortes:

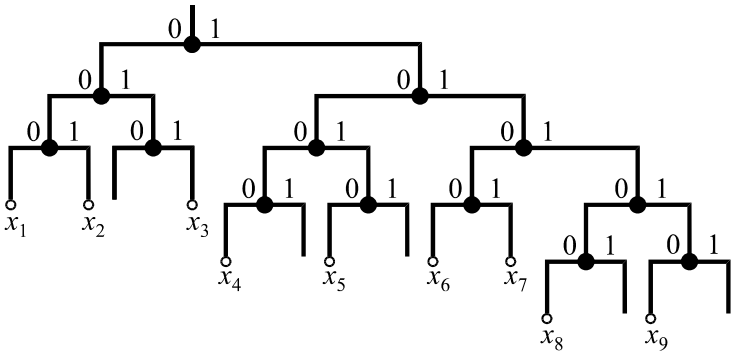
i	$p(x_i)$	$I(x_i)$	$L(x_i)$	P_i	Code
1	0,22	2,18	3	0,00	000
2	0,19	2,40	3	0,22	001
3	0,15	2,74	3	0,41	011
4	0,12	3,06	4	0,56	1000
5	0,08	3,64	4	0,68	1010
6	0,07	3,84	4	0,76	1100
7	0,07	3,84	4	0,83	1101
8	0,06	4,06	5	0,90	11100
9	0,04	4,64	5	0.96	11110

$$0{,}90 = 1\cdot2^{-1} + 1\cdot2^{-2} + 1\cdot2^{-3} + 0\cdot2^{-4} + 0\cdot2^{-5} + 1\cdot2^{-6} + 1\cdot2^{-7} + 0\cdot2^{-8} + 0\cdot2^{-9} + 1\cdot2^{-10} + \ldots$$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Baumdarstellung eines Shannon-Codes:



- Nachteil: nicht alle Endpunkte des Baums sind besetzt

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Codewortlänge kann reduziert werden $\Rightarrow$ Code ist nicht optimal
- Redundanz eines Codes: $R_C = \overline{L} - H(X)$ (2.15)
- Redundanz einer Quelle: $R_Q = H_0 - H(X)$ (2.16)

- Huffman-Codierung
  - rekursives Vorgehen
  - Startpunkt: Symbole mit den kleinsten Wahrscheinlichkeiten
  - gleiche Codewortlänge für die beiden Symbole mit der kleinsten Wahrscheinlichkeit
  - andernfalls: Reduzierung der Codewortlänge möglich

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Algorithmus:
  - Schritt 1: Ordnen der Symbole entsprechend ihrer Wahrscheinlichkeit
  - Schritt 2: Zuordnung von 0 und 1 zu den beiden Symbolen mit der kleinsten Wahrscheinlichkeit
  - Schritt 3: Zusammenfassen der beiden Symbole mit der kleinsten Wahrscheinlichkeit x_{N-1} und x_N zu einem neuen Symbol mit der Wahrscheinlichkeit $p(x_{N-1}) + p(x_N)$
  - Schritt 4: Wiederholung der Schritte 1 - 3, bis nur noch ein Symbol übrig bleibt
- Beispiel

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9
0,22	0,19	0,15	0,12	0,08	0,07	0,07	0,06	0,04
							0	1

x_1	x_2	x_3	x_4	x_8	x_9	x_5	x_6	x_7
0,22	0,19	0,15	0,12	0,10		0,08	0,07	0,07
				0	1		0	1

x_1	x_2	x_3	x_6	x_7	x_4	x_8	x_9	x_5
0,22	0,19	0,15	0,14		0,12	0,10		0,08
			0	1		00	01	1

x_1	x_2	x_8	x_9	x_5	x_3	x_6	x_7	x_4
0,22	0,19	0,18			0,15	0,14		0,12
		00	01	1		00	01	1

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

x_6	x_7	x_4	x_1	x_2	x_8	x_9	x_5	x_3
0,26			0,22	0,19	0,18			0,15
00	01	1			000	001	01	1

x_8	x_9	x_5	x_3	x_6	x_7	x_4	x_1	x_2
0,33				0,26			0,22	0,19
000	001	01	1	00	01	1	0	1

x_1	x_2	x_8	x_9	x_5	x_3	x_6	x_7	x_4
0,41		0,33				0,26		
0	1	0000	0001	001	01	100	101	11

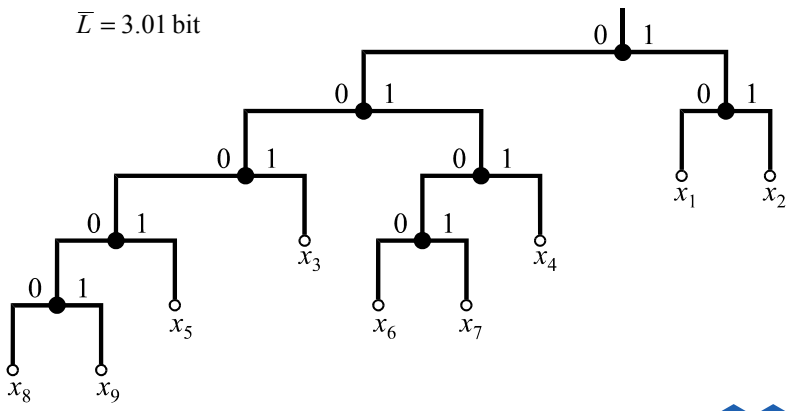
x_8	x_9	x_5	x_3	x_6	x_7	x_4	x_1	x_2
0,59							0,41	
00000	00001	0001	001	0100	0101	011	10	11

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Baumstruktur des Huffman-Code-Beispiels

$\overline{L} = 3.01$ bit



Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Diskrete Quelle ohne Gedächtnis
  - Verbundentropie von Zeichenketten
    - zwei unabhängige Zeichen: $p(x_i,y_k) = p(x_i) \cdot p(y_k)$

$$H(X,Y) = -\sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i,y_k)\,\mathrm{ld}(p(x_i,y_k)) \qquad (2.17)$$

$$= -\sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i)\cdot p(y_k)\cdot[\mathrm{ld}(p(x_i)) + \mathrm{ld}(p(y_k))]$$

$$= -\sum_{k=1}^{N} p(y_k)\cdot\sum_{i=1}^{N} p(x_i)\cdot\mathrm{ld}(p(x_i)) - \sum_{i=1}^{N} p(x_i)\cdot\sum_{k=1}^{N} p(y_k)\cdot\mathrm{ld}(p(y_k))$$

$$H(X,Y) = H(X) + H(Y) \qquad (2.18)$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- M unabhängige Zeichen der gleichen Quelle:

$$H(X_1, X_2, \ldots, X_M) = M \cdot H(X) \qquad (2.19)$$

- Effizienteres Codieren durch Codieren von Zeichenketten
  - Shannon'sches Codierungstheorem:

$$\begin{aligned} H(X_1,\ldots,X_M) \le \overline{L_M}(X_1,\ldots,X_M) &\le H(X_1,\ldots,X_M) + 1 \\ M\cdot H(X) \le M\cdot\overline{L} &\le M\cdot H(X) + 1 \\ H(X) \le \overline{L} &\le H(X) + 1/M \end{aligned} \qquad (2.20)$$

  - Nachteil beim Codieren von Zeichenketten: stark ansteigender Codierungsaufwand (exponentielle Zunahme der Zahl der möglichen Zeichen)

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiel: Codierung von Zeichenfolgen
  - binäre Quelle mit $X = \{x_1, x_2\}$
  - Auftrittswahrscheinlichkeiten: $p(x_1) = 0{,}2, \quad p(x_2) = 0{,}8$
  - Entropie: $H(X) = 0{,}7219$ bit/Zeichen
  - Codierung von Einzelzeichen:

Zeichen	$p(x_i)$	Code	$L(x_i)$	$p(x_i)\cdot L(x_i)$
x_1	0,2	0	1	0,2
x_2	0,8	1	1	0,8
				$\Sigma = 1$

  - mittlere Codewortlänge: $\overline{L} = 1$ bit/Zeichen

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Codierung von Zeichenpaaren:

Zeichen-paar	$p(x_i)$	Code	$L(x_i)$	$p(x_i)\cdot L(x_i)$
x_1x_1	0,04	101	3	0,12
x_1x_2	0,16	11	2	0,32
x_2x_1	0,16	100	3	0,48
x_2x_2	0,64	0	1	0,64
				$\Sigma = 1{,}56$

- mittlere Codewortlänge: $\overline{L} = 0{,}78$ bit/Zeichen

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Codierung von Zeichentripeln:

Zeichen-tripel	$p(x_i)$	Code	$L(x_i)$	$p(x_i)\cdot L(x_i)$
$x_1x_1x_1$	0,008	11111	5	0,040
$x_1x_1x_2$	0,032	11100	5	0,160
$x_1x_2x_1$	0,032	11101	5	0,160
$x_1x_2x_2$	0,128	100	3	0,384
$x_2x_1x_1$	0,032	11110	5	0,160
$x_2x_1x_2$	0,128	101	3	0,384
$x_2x_2x_1$	0,128	110	3	0,384
$x_2x_2x_2$	0,512	0	1	0,512
				$\Sigma = 2{,}184$

- mittlere Codewortlänge: $\overline{L} = 0{,}728$ bit/Zeichen

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Diskrete Quelle mit Gedächtnis
  - reale Quellen: Korrelation zwischen den Einzelzeichen
  - zwei abhängige Zeichen: $p(x_i,y_k) = p(x_i)\cdot p(y_k|x_i) = p(y_k)\cdot p(x_i|y_k)$

$$H(X,Y) = -\sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i,y_k)\,\mathrm{ld}(p(x_i,y_k))$$

$$= -\sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i)\cdot p(y_k\,|\,x_i)\cdot[\mathrm{ld}(p(x_i)) + \mathrm{ld}(p(y_k\,|\,x_i))]$$

$$= -\sum_{i=1}^{N}\sum_{k=1}^{N} p(y_k\,|\,x_i)\cdot p(x_i)\cdot \mathrm{ld}(p(x_i)) - \sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i,y_k)\cdot \mathrm{ld}(p(y_k\,|\,x_i))$$

$$\boxed{H(X,Y) = H(X) + H(Y\,|\,X)} \qquad (2.21)$$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- $H(Y \mid X)$ = bedingte Entropie

$$H(Y \mid X) = -\sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i, y_k) \cdot \mathrm{ld}(p(y_k \mid x_i)) \qquad (2.22)$$

- Entropie einer Quelle $\geq$ bedingte Entropie

$$\boxed{H(Y) \geq H(Y \mid X)} \qquad (2.23)$$

  - Beweis:

$$H(Y) = -\sum_{k=1}^{N} p(y_k) \cdot \mathrm{ld}(p(y_k)) = -\sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i, y_k) \cdot \mathrm{ld}(p(y_k))$$

$$H(Y \mid X) - H(Y) = \sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i, y_k) \cdot \mathrm{ld}\left(\frac{p(y_k)}{p(y_k \mid x_i)}\right)$$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Abschätzung mit: $\ln x \leq x - 1 \quad \Rightarrow \quad \mathrm{ld}\, x \leq \frac{1}{\ln 2}(x-1)$

$$H(Y \mid X) - H(Y) \leq \sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i, y_k) \cdot \frac{1}{\ln 2} \cdot \left(\frac{p(y_k)}{p(y_k \mid x_i)} - 1\right)$$

- mit $p(x_i, y_k) = p(x_i) \cdot p(y_k \mid x_i)$

$$H(Y \mid X) - H(Y) \leq \frac{1}{\ln 2}\left[\underbrace{\sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i)p(y_k)}_{=1} - \underbrace{\sum_{i=1}^{N}\sum_{k=1}^{N} p(x_i, y_k)}_{=1}\right] = 0$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- gleichwahrscheinliche Einzelzeichen: Entropie einer Quelle mit Gedächtnis < Entropie einer Quelle ohne Gedächtnis
- besonders effiziente Quellencodierung durch Codierung von Zeichenfolgen bei Quellen mit Gedächtnis

- allgemeine Beschreibung einer diskreten Quelle mit Gedächtnis als Markoff-Quelle
  - Markoff-Prozesse:
    - Folge von Zufallsvariablen $z_0, z_1, z_2, \ldots, z_n$, ($n$ = Zeitachse)
    - z_i und z_j sind statistisch unabhängig:

$$f_{z_n|z_{n-1},z_{n-2},\ldots,z_0}(z_n \mid z_{n-1},z_{n-2},\ldots,z_0) = f_{z_n}(z_n) \qquad (2.24)$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- z_i und z_j sind stat. abhängig (Markoff-Prozess m-ter Ordnung):

$$f_{z_n|z_{n-1},z_{n-2},\ldots,z_0}(z_n \mid z_{n-1},z_{n-2},\ldots,z_0) = f_{z_n|z_{n-1},\ldots,z_{n-m}}(z_n \mid z_{n-1},\ldots,z_{n-m})$$

- Häufig: Markoff-Prozess erster Ordnung (m = 1): (2.25)

$$f_{z_n|z_{n-1},z_{n-2},\ldots,z_0}(z_n \mid z_{n-1},z_{n-2},\ldots,z_0) = f_{z_n|z_{n-1}}(z_n \mid z_{n-1}) \qquad (2.26)$$

- z_i nehmen endlich viele diskrete Werte an: $z_i \in \{x_1, \ldots, x_N\}$

  $\Rightarrow$ Markoff-Kette

- vollständige Beschreibung einer Markoff-Kette durch Übergangswahrscheinlichkeiten

$$p(z_n = x_j \mid z_{n-1} = x_{i_{n-1}},\ldots,z_0 = x_{i_0}) = p(z_n = x_j \mid z_{n-1} = x_{i_{n-1}},\ldots,z_{n-m} = x_{i_{n-m}}) \qquad (2.27)$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- homogene Markoff-Kette: Übergangswahrscheinlichkeiten hängen nicht von der absoluten Zeit ab:

$$p(z_n = x_j \mid z_{n-1} = x_{i_1}, \ldots, z_{n-m} = x_{i_m}) = p(z_k = x_j \mid z_{k-1} = x_{i_1}, \ldots, z_{k-m} = x_{i_m}) \tag{2.28}$$

- stationäre Markoff-Kette: eingeschwungener Zustand hängt nicht von den Anfangswahrscheinlichkeiten ab

$$\lim_{n\to\infty} p(z_{k+n} = x_j \mid z_k = x_i) = \lim_{n\to\infty} p(z_{k+n} = x_j) = p(x_j) = w_j \tag{2.29}$$

- homogene und stationäre Markoff-Kette erster Ordnung: $m = 1$

$$p(z_n = x_j \mid z_{n-1} = x_i) = p_{ij} \tag{2.30}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Übergangsmatrix:

$$\mathbf{P} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1N} \\ p_{21} & p_{22} & \cdots & p_{2N} \\ \cdots & \cdots & \ddots & \cdots \\ p_{N1} & p_{N2} & \cdots & p_{NN} \end{pmatrix} \tag{2.31}$$

- Eigenschaften der Übergangsmatrix:

$$\sum_{j=1}^{N} p_{ij} = 1 \tag{2.32}$$

- Wahrscheinlichkeitsvektor:

$$\mathbf{w} = (w_1 \quad w_2 \quad \cdots \quad w_N) = (p(x_1) \quad p(x_2) \quad \cdots \quad p(x_N)) \tag{2.33}$$

- Bestimmung von $\mathbf{w}$ mit Hilfe des eingeschwungenen Zustands:

$$\mathbf{w} = \mathbf{w}\,\mathbf{P} \tag{2.34}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- stationäre Markoff-Quelle: Markoff-Kette erster Ordnung
  - Entropie einer stationären Markoff-Quelle = Entropie im eingeschwungenen Zustand:

$$H_\infty(Z) = \lim_{n\to\infty} H(z_n \mid z_{n-1}, z_{n-2}, \ldots, z_0) = H(z_n \mid z_{n-1}) \tag{2.35}$$

$$= -\sum_{i=1}^{N}\sum_{j=1}^{N} p(z_n = x_j, z_{n-1} = x_i) \cdot \mathrm{ld}(p(z_n = x_j \mid z_{n-1} = x_i)) \tag{2.36}$$

$$= -\sum_{i=1}^{N} w_i \cdot \sum_{j=1}^{N} p(z_n = x_j \mid z_{n-1} = x_i) \cdot \mathrm{ld}(p(z_n = x_j \mid z_{n-1} = x_i)) \tag{2.37}$$

$$H_\infty(Z) = \sum_{i=1}^{N} w_i \cdot H(z_n \mid z_{n-1} = x_i) = \langle H(z_n \mid z_{n-1} = x_i) \rangle_i \tag{2.38}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- $\Rightarrow$ Entropie $H_\infty(Z)$ = bedingte Entropie, da Zeichen aus der Vergangenheit bereits bekannt sind

$$H_\infty(Z) = H(z_n \mid z_{n-1}) \le H(z_n) \le H_0(z_n) \tag{2.39}$$

- Codierung einer Markoff-Quelle:
  - Berücksichtigung des Gedächtnisses
  - z. B. Huffman-Codierung unter Berücksichtigung des momentanen Zustands der Quelle

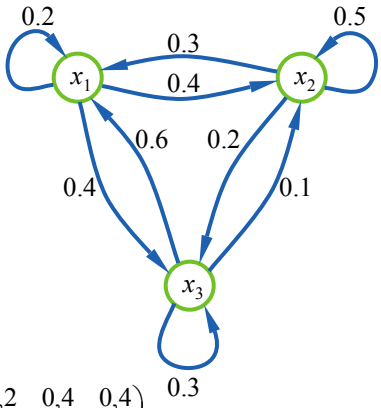
- grundsätzliches Problem bei Quellencodes mit variabler Länge: katastrophale Fehlerfortpflanzung

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Beispiel einer Markoff-Quelle:
  - Zustände = gesendete Zeichen
    $z_n \in \{x_1, x_2, x_3\}$
  - Übergangswahrscheinlichkeiten:

z_{n-1} \ z_n	x_1	x_2	x_3
x_1	0,2	0,4	0,4
x_2	0,3	0,5	0,2
x_3	0,6	0,1	0,3



$$\left(p(z_n = x_j \mid z_{n-1} = x_i)\right) = \left(p_{ij}\right) = \mathbf{P} = \begin{pmatrix} 0{,}2 & 0{,}4 & 0{,}4 \\ 0{,}3 & 0{,}5 & 0{,}2 \\ 0{,}6 & 0{,}1 & 0{,}3 \end{pmatrix}$$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Berechnung der stationären Wahrscheinlichkeiten mit:

$$\mathbf{w} = \mathbf{w}\,\mathbf{P} \quad \text{und} \quad \sum_{i=1}^{N} w_i = 1 \tag{2.40}$$

$$w_1 = 0{,}2\,w_1 + 0{,}3\,w_2 + 0{,}6\,w_3$$
$$w_2 = 0{,}4\,w_1 + 0{,}5\,w_2 + 0{,}1\,w_3$$
$$w_3 = 0{,}4\,w_1 + 0{,}2\,w_2 + 0{,}3\,w_3$$
$$1 = w_1 + w_2 + w_3$$

- lineare Abhängigkeit !
- Lösung:

$$w_1 = \frac{33}{93} \approx 0{,}3548 \qquad w_2 = \frac{32}{93} \approx 0{,}3441 \qquad w_3 = \frac{28}{93} \approx 0{,}3011$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Berechnung der Entropie mit (35):

$$H_\infty(Z) = \sum_{i=1}^{N} w_i \cdot H(z_n \mid z_{n-1} = x_i)$$
$$= -\sum_{i=1}^{N} w_i \cdot \sum_{j=1}^{N} p_{ij} \cdot \mathrm{ld}(p_{ij}) \qquad (2.41)$$

- Zahlenwerte einsetzen:

$$H(z_n \mid z_{n-1} = x_1) = 0{,}2 \cdot \mathrm{ld}\frac{1}{0{,}2} + 0{,}4 \cdot \mathrm{ld}\frac{1}{0{,}4} + 0{,}4 \cdot \mathrm{ld}\frac{1}{0{,}4} \cong 1{,}5219 \text{ bit / Zeichen}$$
$$H(z_n \mid z_{n-1} = x_2) = 0{,}3 \cdot \mathrm{ld}\frac{1}{0{,}3} + 0{,}5 \cdot \mathrm{ld}\frac{1}{0{,}5} + 0{,}2 \cdot \mathrm{ld}\frac{1}{0{,}2} \cong 1{,}4855 \text{ bit / Zeichen}$$
$$H(z_n \mid z_{n-1} = x_3) = 0{,}6 \cdot \mathrm{ld}\frac{1}{0{,}6} + 0{,}1 \cdot \mathrm{ld}\frac{1}{0{,}1} + 0{,}3 \cdot \mathrm{ld}\frac{1}{0{,}3} \cong 1{,}2955 \text{ bit / Zeichen}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Entropie:

$$H_\infty(Z) = w_1 H(z_n \mid z_{n-1} = x_1) + w_2 H(z_n \mid z_{n-1} = x_2) + w_3 H(z_n \mid z_{n-1} = x_3)$$
$$\cong 1{,}441 \text{ bit / Zeichen} \qquad (2.42)$$

- zum Vergleich: statistisch unabhängige Zeichen

$$H(Z) = \lim_{n\to\infty} H(z_n) = \sum_{i=1}^{N} w_i \cdot \mathrm{ld}\frac{1}{w_i} \cong 1{,}5814 \text{ bit / Zeichen}$$

$$H_0 = \mathrm{ld}3 \cong 1{,}5850 \text{ bit / Zeichen}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- zustandsabhängige Huffman-Codierung für das Beispiel: unterschiedliche Codierungen für jeden Zustand z_{n-1}

p_{ij}

z_{n-1} \ z_n	x_1	x_2	x_3
x_1	0,2	0,4	0,4
x_2	0,3	0,5	0,2
x_3	0,6	0,1	0,3

Codewörter

z_{n-1} \ z_n	x_1	x_2	x_3	$\langle L \rangle \vert z_{n-1}$
x_1	11	10	0	1,6
x_2	10	0	11	1,5
x_3	0	11	10	1,4

mittlere Codewortlänge:

$$\bar{L} = \left\langle L(z_n = x_j \mid z_{n-1} = x_i) \right\rangle = \sum_{i=1}^{N} \sum_{j=1}^{N} w_i \cdot p_{ij} \cdot L(z_n = x_j \mid z_{n-1} = x_i) \quad (2.43)$$

$\cong 1{,}5054$ bit / Zeichen

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Quellencodierung ohne Kenntnis der statistischen Parameter der Quelle
  - Lauflängencodierung (run-length coding)
    - Substitution eines wiederholten Symbols durch ein einzelnes Symbole und die Anzahl der Wiederholungen
    - Beispiel:
      - Ausgangssequenz der Quelle:

        aaaabbbccccccccddddeeeeeaaaaaaabddddd.....
      - codierte Sequenz:

        4a3b8c5d5e7a1b5d.....

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

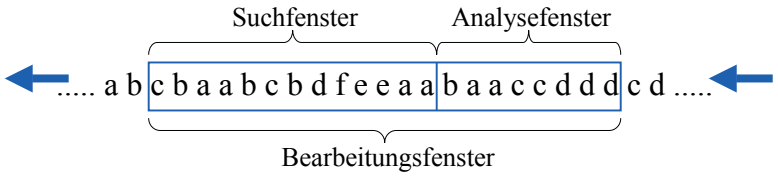
- Codierung mit Wörterbüchern
  - Idee: Wiederholungen in der Datensequenz werden durch (kürzere) Referezierungen in das Wörterbuch ersetzt
  - Statisches Wörterbuch:
    - schlechte Anpassung des Wörterbuchs an bestimmte zu codierende Daten
    - geringe Kompression für die meisten Datenquellen

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- halbadaptives Wörterbuch
  - Das Wörterbuch ist für die zu codierenden Daten zugeschnitten.
  - Das Wörterbuch muss über den Kanal übertragen werden.
  - Zwei Durchläufe über die Daten notwendig:
    - » für den Aufbau des Wörterbuchs
    - » für die Codierung der Daten
- Adaptives Wörterbuch
  - Einfacher Durchlauf für den gleichzeitigen Aufbau des Wörterbuchs und der Codierung
  - Lempel-Ziv-Algorithmus: *.zip *.gzip Dateien

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Lempel-Ziv-Algorithmus (LZ77)



- Suche nach der längsten Übereinstimmung zwischen den ersten Symbolen des Analysefensters und dem Suchfenster
- Ausgabe: Codewörter mit fester Länge
  - Position der Übereinstimmung (Zählanfang = 0)
  - Länge der Übereinstimmung
  - nächstes Symbol im Analysefenster

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

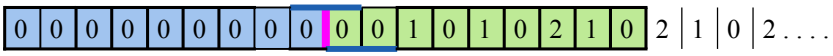
- Parameter:
  - Symbolalphabet: $\{x_0, x_1, x_2, \ldots, x_{\alpha-1}\}$
  - Eingangssequenz: $\mathbf{S} = \{S_1, S_2, S_3, S_4, \ldots\}$
  - Länge des Analysefensters: L_S
  - Länge des Bearbeitungsfensters: n

- Codewörter: $\mathbf{C}_i = \{p_i, l_i, S_i\}$
  - Position der Übereinstimmung: p_i
  - Länge der Übereinstimmung: l_i
  - nächstes Symbol: S_i
  - Länge der Codewörter: $L_C = \log_\alpha(n - L_S) + \log_\alpha(L_S) + 1$

Nachrichtentechnik 4

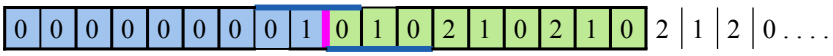
2 Grundlagen der Informationstheorie

- Beispiel:
  - Symbolalphabet: {0,1,2}
  - Eingangssequenz:
    S = {00101021021021202102120012 0.....}
  - Länge des Analysefensters: $L_S = 9$
  - Länge des Bearbeitungsfensters: $n = 18$
  - Schritt 1:



$\mathbf{C}_1 = \{22\ 02\ 1\}$

  - Schritt 2:

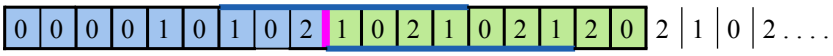


$\mathbf{C}_2 = \{21\ 10\ 2\}$

Nachrichtentechnik 4

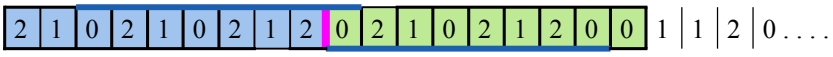
2 Grundlagen der Informationstheorie

  - Schritt 3:



$\mathbf{C}_3 = \{20\ 21\ 2\}$

  - Schritt 4:

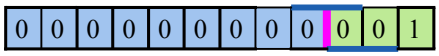


$\mathbf{C}_4 = \{02\ 22\ 0\}$

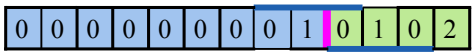
  - Anzahl codierter Quellensymbole nach 4 Schritten:
    $3 + 4 + 8 + 9 = 24$
  - Anzahl von Codewortsymbolen nach 4 Schritten:
    $4 \times 5 = 20$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Decodierung:
  - Schritt 1: $\mathbf{C}_1 = \{22\ 02\ 1\}$



  - Schritt 2: $\mathbf{C}_2 = \{21\ 10\ 2\}$



  - Schritt 3: $\mathbf{C}_3 = \{20\ 21\ 2\}$

  - Schritt 4: $\mathbf{C}_4 = \{02\ 22\ 0\}$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Nachrichtenübertragung über einen diskreten gedächtnislosen Kanal
  - störungsfreier Kanal:

    Information am Ausgang = Information am Eingang

    $\Rightarrow$ übertragene Information = Entropie der Quelle
  - gestörter Kanal:

    Information am Ausgang < Information am Eingang

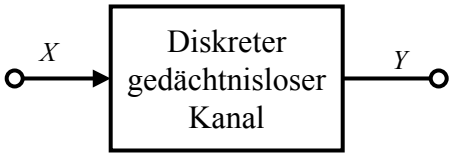
    $\Rightarrow$ übertragene Information < Entropie der Quelle
  - Definition:

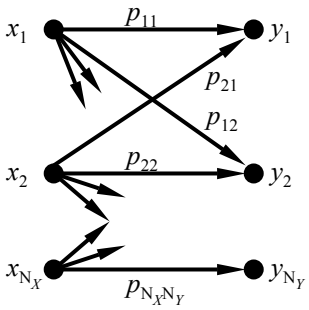
    Transinformation = tatsächlich übertragene Information

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Diskreter gedächtnisloser Kanal
  (discrete memoryless channel – DMC)





- Eingangssignal: $X \in \{x_1, x_2, ..., x_{N_X}\}$
- Ausgangssignal: $Y \in \{y_1, y_2, ..., y_{N_Y}\}$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Übergangsmatrix:

$$\mathbf{P} = \left(p(Y = y_j \mid X = x_i)\right) = \left(p_{ij}\right) = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1N_Y} \\ p_{21} & p_{22} & \cdots & p_{2N_Y} \\ \cdots & \cdots & \ddots & \cdots \\ p_{N_X 1} & p_{N_X 2} & \cdots & p_{N_X N_Y} \end{pmatrix} \quad (2.44)$$

mit $\sum_{j=1}^{N} p_{ij} = 1$ (2.45)

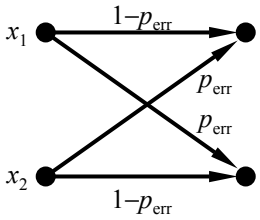
- Binärkanal: $\mathbf{P} = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix}$ (2.46)
- Fehlerwahrscheinlichkeit eines Binärkanals:

$$p(\text{Fehler}) = p(x_1) \cdot p(y_2 \mid x_1) + p(x_2) \cdot p(y_1 \mid x_2)$$
$$= p(x_1) \cdot p_{12} + p(x_2) \cdot p_{21} \quad (2.47)$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Symmetrischer Binärkanal (binary symmetric channel - BSC)

$$\mathbf{P} = \begin{pmatrix} 1-p_{\mathrm{err}} & p_{\mathrm{err}} \\ p_{\mathrm{err}} & 1-p_{\mathrm{err}} \end{pmatrix} \qquad (2.48)$$



  - Fehlerwahrscheinlichkeit:

$$p(\text{Fehler}) = p(x_1)\cdot p_{12} + p(x_2)\cdot p_{21}$$
$$= [p(x_1) + p(x_2)]\cdot p_{\mathrm{err}} = p_{\mathrm{err}}$$

(2.49)

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiel zur Transinformation – qualitative Betrachtung:
  - Übertragung von 1000 binären, statistisch unabhängigen und gleichwahrscheinlichen Symbolen ($p(0) = p(1) = 0{,}5$)
  - symmetrischer Binärkanal mit $p_{\mathrm{err}} = 0{,}01$
  - mittlere Anzahl der richtig übertragenen Symbole: 990
  - aber: $T(X,Y) < 0{,}99$ bit/Zeichen
  - Ursache: genaue Lage der Fehler ist nicht bekannt

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Definitionen der Entropien an einem diskreten gedächtnislosen Kanal:
- **Eingangsentropie** = mittlerer Informationsgehalt der Eingangssymbole:

$$H(X) = \sum_{i=1}^{N_X} p(x_i) \cdot \mathrm{ld} \frac{1}{p(x_i)} \qquad (2.50)$$

- **Ausgangsentropie** = mittlerer Informationsgehalt der Ausgangssymbole:

$$H(Y) = \sum_{j=1}^{N_Y} p(y_j) \cdot \mathrm{ld} \frac{1}{p(y_j)} \qquad (2.51)$$

- **Verbundentropie** = mittlere Unsicherheit des gesamten Übertragungssystems:

$$H(X,Y) = \sum_{i=1}^{N_X} \sum_{j=1}^{N_Y} p(x_i, y_j) \cdot \mathrm{ld} \frac{1}{p(x_i, y_j)} \qquad (2.52)$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- bedingte Entropie $H(Y|X)$ = mittlerer Informationsgehalt am Ausgang bei bekanntem Eingangssymbol = **Entropie der Irrelevanz**

$$H(Y \mid X) = \sum_{i=1}^{N_X} \sum_{j=1}^{N_Y} p(x_i, y_j) \cdot \mathrm{ld} \frac{1}{p(y_j \mid x_i)} \qquad (2.53)$$

- bedingte Entropie $H(X|Y)$ = mittlerer Informationsgehalt am Eingang bei bekanntem Ausgangssymbol = Entropie der Information, die auf dem Kanal verloren geht = **Entropie der Äquivokation**

$$H(X \mid Y) = \sum_{i=1}^{N_X} \sum_{j=1}^{N_Y} p(x_i, y_j) \cdot \mathrm{ld} \frac{1}{p(x_i \mid y_j)} \qquad (2.54)$$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Beziehungen zwischen den Entropien:

$$H(X,Y) = H(Y,X) = H(X) + H(Y \mid X) = H(Y) + H(X \mid Y) \quad (2.55)$$

$$H(X \mid Y) \le H(X) \quad (2.56)$$

$$H(Y \mid X) \le H(Y) \quad (2.57)$$

- mittlere Transinformation:

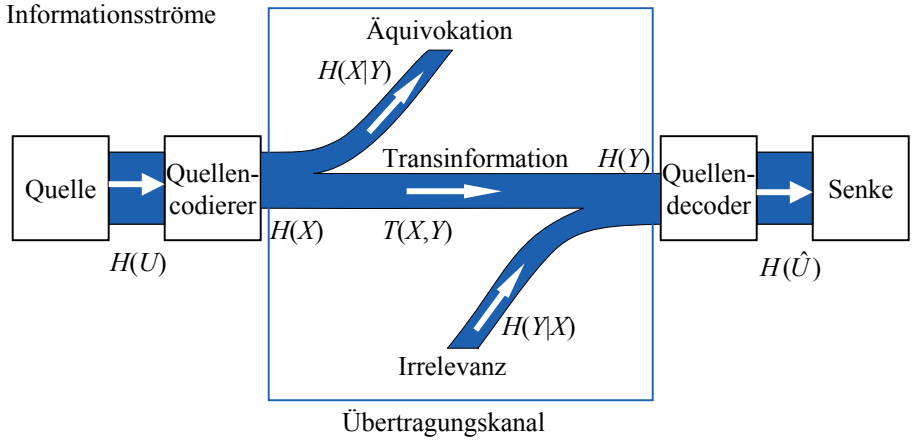
$$T(X,Y) = H(X) - H(X \mid Y) \quad (2.58)$$

$$= H(Y) - H(Y \mid X) \quad (2.59)$$

$$= H(X) + H(Y) - H(X,Y) \quad (2.60)$$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie



Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- spezielle Beispiele zur Transinformation:
  - idealer ungestörter Kanal:

$$p_{ij} = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases} \tag{2.61}$$

- Entropien: $H(X|Y) = 0, \quad H(Y|X) = 0,$ (2.62)

$$H(X,Y) = H(X) = H(Y) \tag{2.63}$$

$$T(X,Y) = H(X) = H(Y) \tag{2.64}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- nutzloser, vollständig gestörter Kanal:

$$p(x_i,y_j) = p(x_i) \cdot p(y_j) = p(y_j|x_i) \cdot p(x_i) \tag{2.65}$$

$$\Rightarrow p(y_j|x_i) = p(y_j) \quad \Rightarrow p_{ij} = p_{kj} \tag{2.66}$$

- Entropien: $H(X|Y) = H(X), \quad H(Y|X) = H(Y),$ (2.67)

$$H(X,Y) = H(X) + H(Y) \tag{2.68}$$

$$T(X,Y) = 0 \tag{2.69}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiel zur Transinformation – quantitative Betrachtung:
  - Übertragung von 1000 binären, statistisch unabhängigen und gleichwahrscheinlichen Symbolen ($p(0) = p(1) = 0{,}5$)
  - symmetrischer Binärkanal mit $p_{\mathrm{err}} = 0{,}01$

$$T(X,Y) = H(Y) - H(Y \mid X)$$

$$= \sum_{j=1}^{N_Y} p(y_j) \cdot \mathrm{ld} \frac{1}{p(y_j)} - \sum_{i=1}^{N_X} \sum_{j=1}^{N_Y} p(x_i) \cdot p(y_j \mid x_i) \cdot \mathrm{ld} \frac{1}{p(y_j \mid x_i)}$$

$$= 1 - (p(0) + p(1)) \left[(1 - p_{\mathrm{err}}) \mathrm{ld} \frac{1}{1 - p_{\mathrm{err}}} + p_{\mathrm{err}} \mathrm{ld} \frac{1}{p_{\mathrm{err}}} \right] = 1 - S(p_{\mathrm{err}})$$

$$\cong 0{,}9192 \text{ bit/Zeichen}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Kanalkapazität
  - Transinformation hängt von der Wahrscheinlichkeitsdichte der Quellensymbole ab
  - Definition der Kanalkapazität:

$$C = \frac{1}{\Delta T} \max_{p(x_i)} T(X,Y) \qquad (2.70)$$

  - Kanalkapazität = Maximum des Transinformationsflusses
  - ΔT = Periode der Zeichen
  - Dimension der Kanalkapazität: bit/s
  - C hängt von den Kanaleigenschaften ab, nicht von der Quelle!

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Definition von Informationsfluss ...
  - Informationsfluss = Entropie / Zeit:

$$H'(X) = H(X) / \Delta T \tag{2.71}$$

  - Transinformationsfluss = Transinformation / Zeit:

$$T'(X,Y) = T(X,Y) / \Delta T \tag{2.72}$$

  - Entscheidungsfluss = Entscheidungsgehalt / Zeit:

$$H_0'(X) = H_0(X) / \Delta T \tag{2.73}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

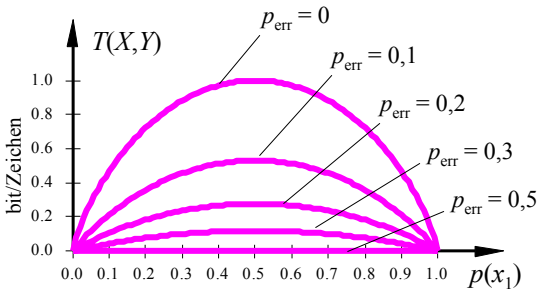
- Beispiel: symmetrischer Binärkanal (binary symmetric channel – BSC):

$$\begin{aligned} T(X,Y) &= H(Y) - H(Y \mid X) \\ &= (p_1 + p_{err} - 2p_1p_{err}) \operatorname{ld} \frac{1}{p_1 + p_{err} - 2p_1p_{err}} \\ &\quad + (1 - p_1 - p_{err} + 2p_1p_{err}) \operatorname{ld} \frac{1}{1 - p_1 - p_{err} + 2p_1p_{err}} \\ &\quad - \left[p_{err} \operatorname{ld} \frac{1}{p_{err}} + (1 - p_{err}) \operatorname{ld} \frac{1}{1 - p_{err}} \right] \end{aligned} \tag{2.74}$$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Transinformation

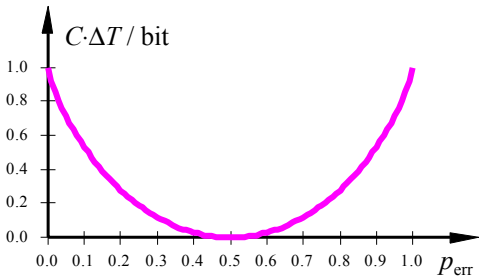


- Maximum für $p_1 = p(x_1) = 0{,}5$

Nachrichtentechnik 4

2 Grundlagen der Informationstheorie

- Kanalkapazität

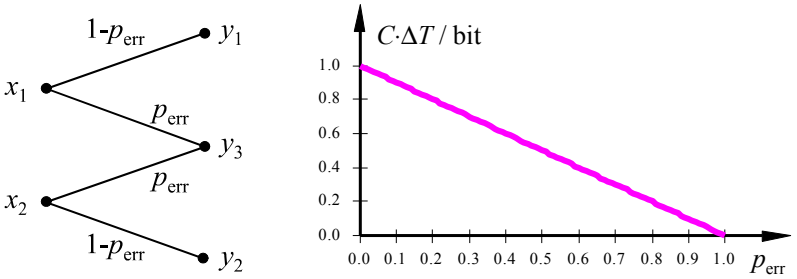


$$C \cdot \Delta T = \max_{p(x_i)} T(X,Y) = 1 - \left[p_{\mathrm{err}} \,\mathrm{ld}\frac{1}{p_{\mathrm{err}}} + (1-p_{\mathrm{err}}) \,\mathrm{ld}\frac{1}{1-p_{\mathrm{err}}} \right] = 1 - S(p_{\mathrm{err}}) \tag{2.75}$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beispiel: binärer Auslöschungskanal (binary erasure channel – BEC)

$$\mathbf{P} = \begin{pmatrix} 1-p_{\text{err}} & 0 & p_{\text{err}} \\ 0 & 1-p_{\text{err}} & p_{\text{err}} \end{pmatrix} \quad (2.76) \qquad C \cdot \Delta T = 1 - p_{\text{err}} \quad (2.77)$$



Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Satz von der Kanalkapazität (Shannon 1948):
  - Für jedes ε > 0 und jeden Informationsfluss einer Quelle R kleiner als die Kanalkapazität C ($R < C$) existiert ein binärer Blockcode der Länge n (n hinreichend groß), so dass die Restfehlerwahrscheinlichkeit nach der Decodierung im Empfänger kleiner ε ist.
  - Umkehrung: Für $R > C$ kann die Restfehlerwahrscheinlichkeit eine gewisse Grenze auch bei größtem Aufwand nicht unterschreiten.

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Beweisführung mit zufälligen Blockcodes (random coding argument):
  - Beweis für das Mittel über alle Codes
  - Alle bekannten Codes sind schlechte Codes
- keine Konstruktionsvorschrift für Codes
- Kanalkapazität: Optimum für unendliche Codewortlänge ⇒ unendliche Verzögerungszeit, unendliche Komplexität

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Verfeinerung des Satzes von der Kanalkapazität mit dem Fehlerexponent nach Gallager für einen DMC mit N_X Eingangssymbolen:

$$E_G(R_C) = \max_{0 \le s \le 1} \max_{p(x_i)} \left[-s \cdot R_C - \mathrm{ld} \sum_{j=1}^{N_Y} \left(\sum_{i=1}^{N_X} p(x_i) \cdot p(y_j \mid x_i)^{\frac{1}{1+s}} \right)^{1+s} \right] \quad (2.78)$$

Es existiert immer ein (n,k)-Blockcode mit $R_C = k/n \; \mathrm{ld}\, N_X < C - \Delta T$, so dass für die Wort-Fehlerwahrscheinlichkeit gilt:

$$P_W < 2^{-n \cdot E_G(R_C)} \quad (2.79)$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

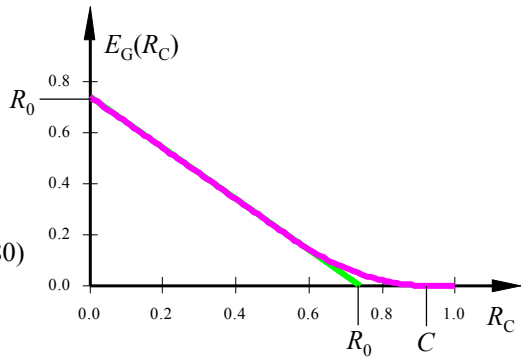
- Fehlerexponent nach Gallager
  - Eigenschaften:

    $E_G(R_C) > 0$ für $R_C < C$

    $E_G(R_C) = 0$ für $R_C \geq C$

    Definition R_0-Wert:

    $$\boxed{R_0 = E_G(R_C = 0)} \quad (2.80)$$



Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- R_0-Wert (auch: computational cut-off rate)
  - Maximum von $E_G(R_C = 0)$ liegt bei $s = 1$

$$R_0 = E_G(R_C = 0) = \max_{p(x_i)} \left[-\mathrm{ld} \sum_{j=1}^{N_Y} \left(\sum_{i=1}^{N_X} p(x_i) \cdot \sqrt{p(y_j \mid x_i)} \right)^2 \right] \quad (2.81)$$

- Vergleich für $s = 1$:

$$E_G(R_C) \geq \max_{p(x_i)} \left[-R_C - \mathrm{ld} \sum_{j=1}^{N_Y} \left(\sum_{i=1}^{N_X} p(x_i) \cdot \sqrt{p(y_j \mid x_i)} \right)^2 \right] = R_0 - R_C \quad (2.82)$$

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- R_0-Theorem:
  - Es existiert immer ein (n,k)-Blockcode mit $R_C = k / n$ ld $N_X < C\,\Delta T$, so dass für die Wort-Fehlerwahrscheinlichkeit (bei Maximum-Likelihood-Decodierung) gilt:

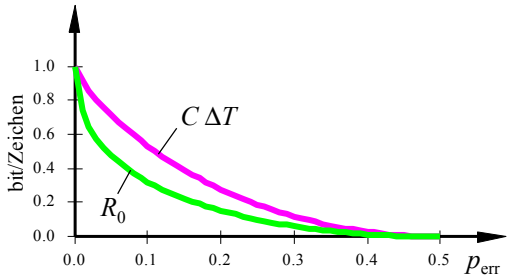
$$P_W < 2^{-n\,(R_0 - R_C)} \qquad (2.83)$$

  - keine Konstruktionsvorschrift für gute Codes
  - Wertebereiche für die Coderate

$0 \le R_C \le R_0$	Abschätzung von P_W mit (2.83)
$R_0 \le R_C \le C\,\Delta T$	Abschätzung von P_W schwierig zu berechnen
$R_C > C\,\Delta T$	P_W kann nicht beliebig klein werden

Nachrichtentechnik 4
2 Grundlagen der Informationstheorie

- Vergleich von Kanalkapazität und R_0-Wert für einen BSC:



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Ziele: Grundbegriffe und Codebeispiele für Blockcodes
- Konstruktion von Codewörtern
  - binäre Codewörter
  - redundante Codes
  - Code $\mathcal{C}$ = Menge aller Codewörter
  - Codewort $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ mit $\mathbf{c} \in \mathcal{C}$
  - Codierung ist gedächtnislose Zuweisung:

Informationswort → Codewort

$$\mathbf{u} = \underbrace{(u_0, u_1, \ldots, u_{k-1})}_{k \text{ Informationsstellen}} \rightarrow \mathbf{c} = \underbrace{(c_0, c_1, \ldots, c_{n-1})}_{n \text{ Codewortstellen}} \qquad n \geq k$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- identische Codes: Codes mit den gleichen Codewörtern
- äquivalente Codes: Codes, die nach Vertauschung von Stellen identisch werden
- allgemeine Bezeichnung: $(n,k,d_{\min})_q$-Blockcode

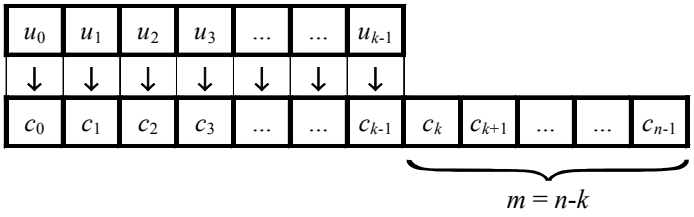
  q = Anzahl bzw. Stufenzahl der Symbole

- Coderate: $R_C = \frac{k}{n} \leq 1$ (3.1)
- Anzahl von Codewörtern: $N = 2^k$ (3.2)

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- systematische Codes:
  - Codewort $\mathbf{c} = (\mathbf{u}, \mathbf{p})$ (3.3)



- nicht-systematische Codes: Informations- und Prüfstellen nicht trennbar
- Blockcodes sind immer in äquivalente systematische Codes umformbar

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Addition und Multiplikation im binären Zahlensystem (modulo 2):

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

- zwei Binärvektoren gleicher Länge **x** und **y**
- Hamming-Distanz:

$d_H(\mathbf{x},\mathbf{y})$ = Anzahl der Abweichungen zwischen den Stellen von **x** und **y**

- Beispiel: $d_H($ 0 1 1 1 0 1 0 1, 1 0 1 0 0 1 0 1 $) = 3$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- (Hamming-)Gewicht eines Vektors **x**:

$$w_H(\mathbf{x}) = \sum_{i=0}^{n-1} x_i = \text{Anzahl der von 0 verschiedenen Stellen} \qquad (3.4)$$

- Beispiel: $w_H(0\ 1\ 1\ 1\ 0\ 1\ 0\ 1) = 5$
- Hamming-Distanz: $d_H(\mathbf{x},\mathbf{y}) = w_H(\mathbf{x}+\mathbf{y})$ (3.5)
- Beispiel: $\mathbf{x} = (\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ )$

$\mathbf{y} = (\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ )$

$\mathbf{x}+\mathbf{y} = (\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ )$

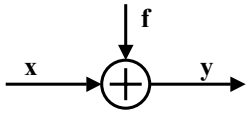
$w_H(\mathbf{x}+\mathbf{y}) = 3$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Übertragung über Binärkanal:

$$\mathbf{y} = \mathbf{x} + \mathbf{f} \qquad (3.6)$$



$\mathbf{f}$ = Fehlervektor

- Der Wiederholungscode (repetition code)
  - $k = 1$ Informationsbit $\rightarrow$ $n-1$ Wiederholungen
  - $2^k = 2$ Codewörter: $\mathbf{c}_1 = (0\ 0\ 0\ \ldots\ 0)$ und $\mathbf{c}_2 = (1\ 1\ 1\ \ldots\ 1)$
  - Wiederholungscode ist systematisch
  - einfache Decodierung durch Mehrheitsentscheid, wenn n ungerade ist
  - $(n-1)/2$ Fehler sind korrigierbar, $n-1$ Fehler sind erkennbar

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel für einen Wiederholungscode:
  - $n = 5 \Rightarrow R_C = 1/5$

    $\mathbf{u}_1 = (0) \rightarrow \mathbf{c}_1 = (0\ 0\ 0\ 0\ 0)$ und

    $\mathbf{u}_2 = (1) \rightarrow \mathbf{c}_2 = (1\ 1\ 1\ 1\ 1)$
  - gestörte Empfangsfolgen:

    $\mathbf{f}_1 = (0\ 1\ 0\ 0\ 1)$ und $\mathbf{x}_1 = (1\ 1\ 1\ 1\ 1)$

    $\mathbf{y}_1 = \mathbf{x}_1 + \mathbf{f}_1 = (1\ 0\ 1\ 1\ 0) \rightarrow$

    $\mathbf{f}_2 = (1\ 1\ 0\ 1\ 0)$ und $\mathbf{x}_2 = (0\ 0\ 0\ 0\ 0)$

    $\mathbf{y}_2 = \mathbf{x}_2 + \mathbf{f}_2 = (1\ 1\ 0\ 1\ 0) \rightarrow$
  - zwei Fehler korrigierbar, vier Fehler erkennbar

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Paritätskontrolle (parity check code)
  - k Informationsbits, eine Prüfstelle ($m = 1$) $\rightarrow$ $n = k + 1$
  - 2^k Codewörter
  - $\mathbf{c} = (\mathbf{u}\ p)$ mit $p = u_0 + u_1 + u_2 + \ldots + u_{k-1}$ (3.7)

    (gerade Anzahl von Einsen in den Codewörten $\mathbf{c}$)
  - Paritätskontrolle ist systematisch
  - kein Fehler korrigierbar, ungerade Anzahl von Fehlern erkennbar
  - Paritätskontrolle:

    $s_0 = y_0 + y_1 + y_2 + \ldots + y_{n-1} = 0 \rightarrow$ kein Fehler

    $s_0 = y_0 + y_1 + y_2 + \ldots + y_{n-1} = 1 \rightarrow$ Fehler

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel: $k = 3$

Codewort	Information	Prüfstelle
$\mathbf{c}_0$	000	0
$\mathbf{c}_1$	001	1
$\mathbf{c}_2$	010	1
$\mathbf{c}_3$	011	0
$\mathbf{c}_4$	100	1
$\mathbf{c}_5$	101	0
$\mathbf{c}_6$	110	0
$\mathbf{c}_7$	111	1

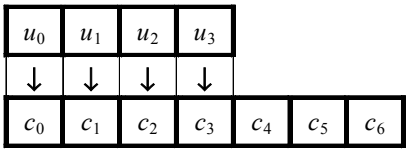
$\mathbf{y}_1 = (0\ 1\ 1\ 0) \rightarrow$ kein Fehler

$\mathbf{y}_2 = (1\ 1\ 1\ 0) \rightarrow$ Fehler

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Hamming-Code
  - Korrektur eines einzelnen Fehlers in einem Codewort
  - Beispiel: (7,4)-Hamming-Code



  - Kontrollstellen:

$$c_4 = c_0 + c_1 + c_2 \quad (3.8)$$

$$c_5 = c_0 + c_1 + c_3 \quad (3.9)$$

$$c_6 = c_0 + c_2 + c_3 \quad (3.10)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Matrix-Darstellung von Blockcodes

$$\mathbf{x} = \mathbf{u}\,\mathbf{G} \tag{3.11}$$

$\mathbf{G}$ = Generator-Matrix ($k \times n$ -Matrix)

  - Systematische Blockcodes:

$$\mathbf{G} = [\mathbf{I}_k\ \mathbf{P}] \tag{3.12}$$

$\mathbf{I}_k$ = Einheitsmatrix $k \times k$, $\mathbf{P}$ = Prüfstellenmatrix $k \times (n-k)$

  - Beispiel: (7,4)-Hamming-Code

$$\mathbf{G} = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \tag{3.13}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fortsetzung: (7,4)-Hamming-Code
- Berechnung von Codewörtern durch Matrixmultiplikation

$$\underbrace{(1\ 0\ 0\ 1)}_{\mathbf{u}}\ \underbrace{\left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right)}_{\mathbf{G}} = \underbrace{(1\ 0\ 0\ 1\ |\ 1\ 0\ 0)}_{\mathbf{x}}$$

- Anzahl von Codewörtern: $2^k = 16$
- Anzahl möglicher Empfangswörter: $2^n = 128$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Codewort-Tabelle

Codewort	Information	Prüfstellen
$\mathbf{c}_0$	0000	000
$\mathbf{c}_1$	0001	011
$\mathbf{c}_2$	0010	101
$\mathbf{c}_3$	0011	110
$\mathbf{c}_4$	0100	110
$\mathbf{c}_5$	0101	101
$\mathbf{c}_6$	0110	011
$\mathbf{c}_7$	0111	000

Codewort	Information	Prüfstellen
$\mathbf{c}_8$	1000	111
$\mathbf{c}_9$	1001	100
$\mathbf{c}_{10}$	1010	010
$\mathbf{c}_{11}$	1011	001
$\mathbf{c}_{12}$	1100	001
$\mathbf{c}_{13}$	1101	010
$\mathbf{c}_{14}$	1110	100
$\mathbf{c}_{15}$	1111	111

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Eigenschaften von linearen Blockcodes:
  - Jedes Codewort ist eine Linearkombination von Zeilen von **G**.
  - Der Code setzt sich aus allen Linearkombinationen von **G** zusammen.
  - Die Summe von Codewörtern ist wieder ein Codewort.
  - Im Code ist der Nullvektor (0 0 0 ... 0) enthalten.
  - $\Rightarrow$ Ein Code ist linear, wenn er als Matrixmultiplikation $\mathbf{x} = \mathbf{u}\,\mathbf{G}$ beschrieben werden kann ($\mathbf{u}$ beliebig).
  - Generatormatrix: Zeilen müssen linear unabhängig sein

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- elementare Zeilenoperationen ändern einen Code nicht
  - Vertauschung zweier Zeilen
  - Multiplikation einer Zeile mit einem Skalar ungleich 0
  - Addition einer Zeile zu einer anderen
- Die minimale Distanz zweier Codewörter entspricht dem minimalen Gewicht:

$$d_{\min} = \min\left(d_H(\mathbf{c}_1,\mathbf{c}_2) \mid \mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C}; \mathbf{c}_1 \neq \mathbf{c}_2\right)$$
$$= \min\left(w_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}; \mathbf{c} \neq \mathbf{0}\right) = w_{\min} \qquad (3.14)$$

  - Beweis:

$$d_{\min} = \min\left(d_H(\mathbf{c}_1,\mathbf{c}_2) \mid \mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C}; \mathbf{c}_1 \neq \mathbf{c}_2\right)$$
$$= \min\left(d_H(\mathbf{0},\mathbf{c}_1+\mathbf{c}_2) \mid \mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C}; \mathbf{c}_1 \neq \mathbf{c}_2\right)$$
$$= \min\left(d_H(\mathbf{0},\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}; \mathbf{c} \neq \mathbf{0}\right)$$
$$= \min\left(w_H(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}; \mathbf{c} \neq \mathbf{0}\right)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fehlerkorrektur mit dem (7,4)-Hamming-Code:
- Auswertung der Prüfgleichungen:

$$s_0 = y_0 + y_1 + y_2 + y_4 \qquad (3.15)$$
$$s_1 = y_0 + y_1 + y_3 + y_5 \qquad (3.16)$$
$$s_2 = y_0 + y_2 + y_3 + y_6 \qquad (3.17)$$

- Syndrom : $\mathbf{s} = (s_0\, s_1\, s_2)$
- Symdrom hängt nicht vom Codewort ab, nur vom Fehler
- Zuordnung der Fehlerposition

	Syndrom		
Fehlerposition	s_0	s_1	s_2
kein Fehler	0	0	0
Fehler in 0. Stelle	1	1	1
Fehler in 1. Stelle	1	1	0
Fehler in 2. Stelle	1	0	1
Fehler in 3. Stelle	0	1	1
Fehler in 4. Stelle	1	0	0
Fehler in 5. Stelle	0	1	0
Fehler in 6. Stelle	0	0	1

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Decodierung von Hamming-Codes:
  - Auswertung der Prüfgleichungen → Syndrom
  - Fehlerposition aus Syndromtabelle
  - Fehlerkorrektur: „1“ an der Fehlerposition addieren
- $m = n - k$ Kontrollstellen adressieren $2^m - 1$ Positionen (Nullvektor)
- Blocklänge: $n = 2^m - 1$ (3.18)
- mögliche Parameter für Hamming-Codes:

m	2	3	4	5	6	7	8
n	3	7	15	31	63	127	255
k	1	4	11	26	57	120	247

- $(2^m - 1, 2^m - 1 - m)$-Blockcode

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Prüfmatrix
  - Definition: $\mathbf{c}\,\mathbf{H}^T = \mathbf{0}$ für alle $\mathbf{c} \in \mathcal{C}$ (3.19)
    und $\mathbf{x}\,\mathbf{H}^T \neq \mathbf{0}$ für alle $\mathbf{x} \notin \mathcal{C}$
  - Eigenschaften der Prüfmatrix:
  - $\mathbf{0} = \mathbf{c}\,\mathbf{H}^T = (\mathbf{u}\,\mathbf{G})\,\mathbf{H}^T = \mathbf{u}\,(\mathbf{G}\,\mathbf{H}^T) \rightarrow \boxed{\mathbf{G}\,\mathbf{H}^T = \mathbf{0}}$ (3.20)
    → Generatormatrix und Prüfmatrix sind orthogonal
  - elementare Zeilenoperationen für $\mathbf{H}$ sind erlaubt
  - Prüfmatrix: $\boxed{\mathbf{H} = (\mathbf{P}^T\ \mathbf{I}_{n-k})}$ (3.21)
    mit $\mathbf{G} = [\mathbf{I}_k\ \mathbf{P}]$
  - $\mathbf{H}$ ist $(n - k) \times n$ -Matrix

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Nachweis der Orthogonalität:

$$\mathbf{G}\,\mathbf{H}^{\mathrm{T}} = (\mathbf{I}_k \quad \mathbf{P})\begin{pmatrix}\mathbf{P}\\ \mathbf{I}_{n-k}\end{pmatrix} = \mathbf{I}_k\,\mathbf{P} + \mathbf{P}\,\mathbf{I}_{n-k} = \mathbf{P} + \mathbf{P} = \mathbf{0} \qquad (3.22)$$

- Dualer Code
  - Code $\mathcal{C}$: Generatormatrix $\mathbf{G}$, Prüfmatrix $\mathbf{H}$
  - dualer Code $\mathcal{C}_{\mathrm{d}}$: Generatormatrix $\mathbf{G}_{\mathrm{d}} = \mathbf{H}$, Prüfmatrix $\mathbf{H}_{\mathrm{d}} = \mathbf{G}$
  - Codewörter der beiden Codes sind orthogonal:

    mit $\mathbf{c} = \mathbf{u}\,\mathbf{G} \in \mathcal{C}$ und $\mathbf{c}_{\mathrm{d}} = \mathbf{v}\,\mathbf{H} \in \mathcal{C}_{\mathrm{d}}$ gilt:

$$\mathbf{c}\,\mathbf{c}_{\mathrm{d}}^{\mathrm{T}} = (\mathbf{u}\,\mathbf{G})(\mathbf{v}\,\mathbf{H})^{\mathrm{T}} = \mathbf{u}\,\mathbf{G}\,\mathbf{H}^{\mathrm{T}}\,\mathbf{v}^{\mathrm{T}} = \mathbf{u}\,\mathbf{0}\,\mathbf{v}^{\mathrm{T}} = 0 \qquad (3.23)$$

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel für duale Codes:
  - Wiederholungscode

$$\mathbf{G} = (1 \mid 1 \;\; 1 \;\; \cdots \;\; 1) \qquad \mathbf{H} = \begin{pmatrix} 1 & | & 1 & 0 & \cdots & 0 \\ 1 & | & 0 & 1 & 0 & \vdots \\ \vdots & | & \vdots & 0 & \ddots & 0 \\ 1 & | & 0 & \cdots & 0 & 1 \end{pmatrix} \qquad (3.24)$$

  - Paritätskontrolle:

$$\mathbf{G} = \begin{pmatrix} 1 & | & 1 & 0 & \cdots & 0 \\ 1 & | & 0 & 1 & 0 & \vdots \\ \vdots & | & \vdots & 0 & \ddots & 0 \\ 1 & | & 0 & \cdots & 0 & 1 \end{pmatrix} \qquad \mathbf{H} = (1 \mid 1 \;\; 1 \;\; \cdots \;\; 1) \qquad (3.25)$$

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Syndromberechnung in Matrix-Schreibweise:

$$\mathbf{s} = \mathbf{y}\,\mathbf{H}^T \tag{3.26}$$

Eigenschaften des Syndroms:

- Syndrom ist Nullvektor nur dann, wenn **y** ein Codewort ist
- Syndrom ist unabhängig vom Codewort:

$$\mathbf{s} = \mathbf{y}\,\mathbf{H}^T = (\mathbf{x} + \mathbf{f})\,\mathbf{H}^T = \mathbf{f}\,\mathbf{H}^T \tag{3.27}$$

- alle Fehlervektoren **f** werden erkannt, die nicht Codewörter sind

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel: (7,4)-Hamming-Code

$$\mathbf{G} = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right] \qquad \mathbf{P} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\mathbf{H} = (\mathbf{P}^T\ \mathrm{I}_{n-k}) = \left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

Beispiel: (7,4)-Hamming-Code

$$\mathbf{s} = \mathbf{y}\,\mathbf{H}^T$$

$$\mathbf{s} = (y_0 \quad y_1 \quad \dots \quad y_6) \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ - & - & - \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \Leftrightarrow \quad \begin{aligned} s_0 &= y_0 + y_1 + y_2 + y_4 \\ s_1 &= y_0 + y_1 + y_3 + y_5 \\ s_2 &= y_0 + y_2 + y_3 + y_6 \end{aligned}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Konstruktionsvorschrift für Hamming-Codes
  - Syndrom hängt nur von Fehlervektor ab:

$$\mathbf{s} = \mathbf{f}\,\mathbf{H}^T \tag{3.28}$$

  - ein Einzelfehler an der Stelle i ($f_i = 1$) führt zu einem Syndrom, das der entsprechenden Zeile von $\mathbf{H}^T$ entspricht
  - alle Zeilen von $\mathbf{H}^T$ müssen sich unterscheiden, damit die Fehlerposition eindeutig bestimmt werden kann
  - keine Zeile von $\mathbf{H}^T$ darf ein Nullvektor sein
  - $\Rightarrow$ Die Zeilen von $\mathbf{H}^T$ / Spalten von $\mathbf{H}$ werden durch alle möglichen Sequenzen bis auf den Nullvektor gebildet

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Prüfmatrix eines systematischen Hamming-Codes:

$$\mathbf{H} = (\mathbf{P}^{\mathrm{T}}\ \mathrm{I}_{n-k}) = \left[\begin{array}{cccc|cccc} 1 & 0 & \cdots & \cdots & 1 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & \cdots & 0 & 1 & 0 & \vdots \\ \vdots & \vdots & \cdots & \cdots & \vdots & 0 & \ddots & 0 \\ 1 & 1 & \cdots & \cdots & 0 & \cdots & 0 & 1 \end{array}\right] \qquad (3.29)$$

alle möglichen Spaltenvektoren mit mehr als einer 1

- Beispiel: (15,11)-Hamming-Code

$$\mathbf{H} = \left[\begin{array}{cccccccccccc|cccc} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \qquad (3.30)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Modifikationen linearer Codes
  - Expandieren (extending): Anhängen zusätzlicher Prüfstellen

    $n' > n,\quad k' = k,\quad m' > m,\quad R_{\mathrm{C}}' < R_{\mathrm{C}},\quad d_{\min}' \geq d_{\min}$
  - Punktieren (puncturing): Reduktion von Prüfstellen

    $n' < n,\quad k' = k,\quad m' < m,\quad R_{\mathrm{C}}' > R_{\mathrm{C}},\quad d_{\min}' \leq d_{\min}$
  - Verlängern (lengthening): Anhängen zusätzlicher Informationsstellen

    $n' > n,\quad k' > k,\quad m' = m,\quad R_{\mathrm{C}}' > R_{\mathrm{C}},\quad d_{\min}' \leq d_{\min}$
  - Verkürzen (shortening): Reduktion von Informationsstellen

    $n' < n,\quad k' < k,\quad m' = m,\quad R_{\mathrm{C}}' < R_{\mathrm{C}},\quad d_{\min}' \geq d_{\min}$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel: Hamming-Code:
  - ein Fehler korrigierbar durch Syndrom-Auswertung
  - zwei Fehler führen ebenfalls auf $\mathbf{s} \neq \mathbf{0}$
- erweiterter (expandierter) Hamming-Code:
  - Unterscheidung zwischen 1- und 2-Fehlersituation durch zusätzliche Prüfstelle
  - $(2^m, 2^m - 1 - m)$-Blockcode
  - Generatormatrix des erweiterten Hamming-Codes:

$$\mathbf{G}_{\mathrm{H,ext}} = \left[\begin{array}{c:c} \mathbf{G}_{\mathrm{H}} & \begin{matrix}1\\1\\\vdots\\1\end{matrix} \end{array}\right] \qquad (3.31)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fehlerereignisse:
  - kein Fehler: $\mathbf{s} = \mathbf{0}$
  - ein Fehler: $\mathbf{s} \neq \mathbf{0}$, $s_{m+1} = 1$
  - zwei Fehler: $\mathbf{s} \neq \mathbf{0}$, $s_{m+1} = 0$
- Decodierung:
  - $\mathbf{s} = \mathbf{0}$: Empfangsvektor = Codewort
  - $\mathbf{s} \neq \mathbf{0}$, $s_{m+1} = 1$: ungerade Anzahl von Fehlern $\Rightarrow$ ein Fehler angenommen und durch Syndrom-Auswertung korrigiert
  - $\mathbf{s} \neq \mathbf{0}$, $s_{m+1} = 0$: gerade Anzahl von Fehlern $\Rightarrow$ Fehler können nicht korrigiert werden

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fehlerkorrektur und Fehlererkennung
  - minimale Distanz zwischen Codewörtern:

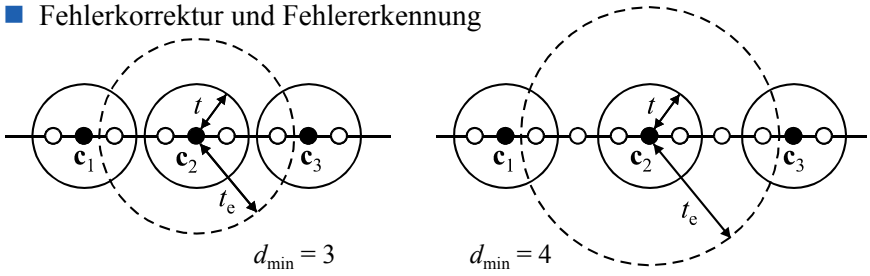
$$d_{\min} = \min\left(d_H(\mathbf{c}_1,\mathbf{c}_2) \,|\, \mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C}\right) \tag{3.32}$$

  - $d_{\min} = 1$: einzelner Fehler kann dazu führen, dass Fehler weder erkennbar noch korrigierbar ist
  - $d_{\min} = 2$: mindestens ein einzelner Fehler kann erkannt werden
  - $d_{\min} = 3$: mindestens ein einzelner Fehler kann korrigiert werden
    mindestens zwei Fehler können erkannt werden

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fehlerkorrektur und Fehlererkennung



  - Anzahl erkennbarer Fehler: $t_e = d_{\min} - 1$ (3.33)
  - Anzahl korrigierbarer Fehler
    - $d_{\min}$ ist gerade: $t = (d_{\min} - 2)/2$ (3.34)
    - $d_{\min}$ ist ungerade: $t = (d_{\min} - 1)/2$ (3.35)

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Singleton-Schranke: Mindestdistanz und Mindestgewicht eines linearen Codes sind beschränkt durch:

$$d_{\min} = w_{\min} \le 1 + n - k = 1 + m \qquad (3.36)$$

  - Beweis: systematisches Codewort mit einer Informationsstelle ungleich 0
    - Gewicht / Distanz in Informationsstellen: $d_{\mathrm{H,Information}} = 1$
    - Gewicht / Distanz in Prüfstellen: $d_{\mathrm{H,Prüf}} \le m = n - k$ ■
  - Ein Code, für den das Gleichheitszeichen in (3.36) gilt, heißt maximum distance separable (MDS)

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fehlererkennung:
  - (3.33): $t_e + 1 = d_{\min} \le 1 + m \quad \Rightarrow \quad \boxed{m \ge t_e}$ (3.37)
  - mindestens 1 Prüfstelle pro erkennbarem Fehler notwendig
- Fehlerkorrektur:
  - (3.34, 3.35): $(d_{\min} - 1) / 2 \ge t \ge (d_{\min} - 2) / 2$
  - $2t + 1 \le d_{\min} \le 1 + m \quad \Rightarrow \quad \boxed{m \ge 2t}$ (3.38)
  - mindestens 2 Prüfstellen pro korrigierbarem Fehler notwendig

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Decodierkugel:
  - n-dimensionale Kugel um Codewort mit Radius t – alle Vektoren im Innern der Decodierkugeln werden als zugehöriges Codewort decodiert
  - Gesamtzahl aller Vektoren innerhalb von Decodierkugeln ≤ Gesamtzahl aller möglichen Vektoren $\Rightarrow$
- Hamming-Schranke:
  - Für einen binären (n,k)-Blockcode mit der Korrekturfähigkeit t gilt:

$$2^k \sum_{i=0}^{t} \binom{n}{i} \leq 2^n \qquad (3.39)$$

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Beweis:
  - Anzahl von Vektoren um ein Codewort mit $d_H = 1$: $\binom{n}{1}$
  - Anzahl von Vektoren um ein Codewort mit $d_H = 2$: $\binom{n}{2}$
  - Anzahl von Vektoren um ein Codewort mit $d_H = t$: $\binom{n}{t}$

  mit $$\binom{n}{t} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-(t-1))}{t \cdot (t-1) \cdot \ldots \cdot 1} \qquad (3.40)$$

  - Gesamtzahl aller Vektoren innerhalb von Decodierkugeln:

$$2^k \left[\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{t} \right] \leq 2^n$$

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Perfekte Codes (dichtgepackte Codes)
  - in (3.39) gilt Gleichheitszeichen
  - keine Codewörter liegen zwischen den Codierkugeln
  - nur sehr wenige bekannte Codes sind perfekt
  - Beispiel: (7,4)-Hamming-Code
    - $d_{\min} = w_{\min} = 3 \quad \Rightarrow \quad t = 1$

$$2^4 \cdot \left[\binom{7}{0} + \binom{7}{1}\right] \leq 2^7$$

$$16 \cdot (1+7) = 128 = 2^7$$

  - Hamming-Codes sind perfekt

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Plotkin-Schranke:
  - Für einen binären (n,k)-Blockcode mit der minimalen Distanz $d_{\min}$ gilt:

$$d_{\min} \leq n \cdot \frac{2^{k-1}}{2^k - 1} \qquad (3.41)$$

  - Näherung: $d_{\min} \leq \frac{n}{2}$ für $2^k >> 1$
  - Beweis: minimales Gewicht ≤ mittlerem Gewicht
    - mittleres Gewicht einer Stelle eines Codeworts: 1/2
    - mittleres Gewicht eines Codeworts der Länge n: $n/2$
    - mittleres Gewicht ohne Nullvektor: $\frac{n}{2} \cdot \frac{2^k}{2^k - 1}$