V. Codierung

Prof. Dr.-Ing. Armin Dekorsy

University of Bremen
Institute for Telecommunications and High Frequency Techniques
Department of Communications Engineering
www.ant.uni-bremen.de

Arbeitsbereich Nachrichtentechnik

Inhalt der Vorlesung

0. Einführung (Grundbegriffe, Struktur eines Kommunikationssystems)
I. Kontinuierliche Signale und Systeme
   1. Fouriertransformation
   2. Tiefpass-Darstellung von Bandpass-Signalen
   3. Eigenschaften von Übertragungskanälen
II. Analoge Übertragung
III. Diskretisierung von Quellensignalen
   1. Abtasttheorem
   2. Pulsamplitudenmodulation
   3. Pulsdauer- und Pulsphasenmodulation, Pulscodemodulation
   4. Prinzip des Zeitmultiplex
IV. Digitale Übertragung
   1. Struktur eines Datenübertragungssystems
   2. Erste und Zweite Nyquistbedingung
   3. Rauschangepasstes Empfangsfilter
   4. Bitfehlerwahrscheinlichkeit
   5. Digitale lineare Modulationsverfahren (inkl. Offset-PSK, DPSK)

V. Codierung

V. Codierung

1. Grundbegriffe
2. Information / Entropie / Kanalkapazität
3. Quellencodierung
   - Huffman-Code
4. Kanalcodierung
   - Fehlererkennung / Fehlerkorrektur / Distanz
   - Lineare Blockcodes
   - Beschreibung durch Matrizendarstellung
   - Beispiele linearer Blockcodes
5. Weitere Kanalcodierungskonzepte

General Declarations

- Important terms:
  - Message — Amount of transmitted data or symbols by the source
  - Information — Part of message, which is new for the sink
  - Redundancy — Difference of message and information, which is unknown to the sink

Message = Information + Redundancy

- Message is also transmitted in a distinct amount of time
  - Messageflow — Amount of message per time
  - Informationflow — Amount of information per time
  - Transinformation — Amount of error-free information per time transmitted from the source to the sink

Diskrete Nachrichtenquellen

- Nachricht
  - Folge von Symbolen X_ν ; $\nu = 1, 2, \ldots, M$ (diskretes Set von Elementen)
- Statistische Interpretation einer Nachricht
  - Auftreten von Symbolen(= Ereignis) mit zugehörigen Auftrittswahrscheinlichkeiten
- Informationsgehalt einer Nachricht
  - Statistisch nicht vorhersagbarer Anteil der Nachricht (Entscheidungsgehalt)
- Es gilt: ➡ je wahrscheinlicher ein Symbol auftritt desto geringer ist die damit verbundene Information, d.h. der Informationsgehalt des Symbols ist geringer.
- Informationsgehalt eines Symbols
  - Annahme: Binäre Entscheidungen

$$I(X_\nu) = \log_2 \frac{1}{Pr\{X_\nu\}} = -\log_2 Pr\{X_\nu\}$$

[**b**inary dig**its** = bits]

  - Beispiele: $I(X_\nu) = 0$ für $Pr\{X_\nu\} = 1$ (Gewißheit = keine Information)

$$\lim_{Pr\{X_\nu\} \to 0} I(X_\nu) \to \infty$$

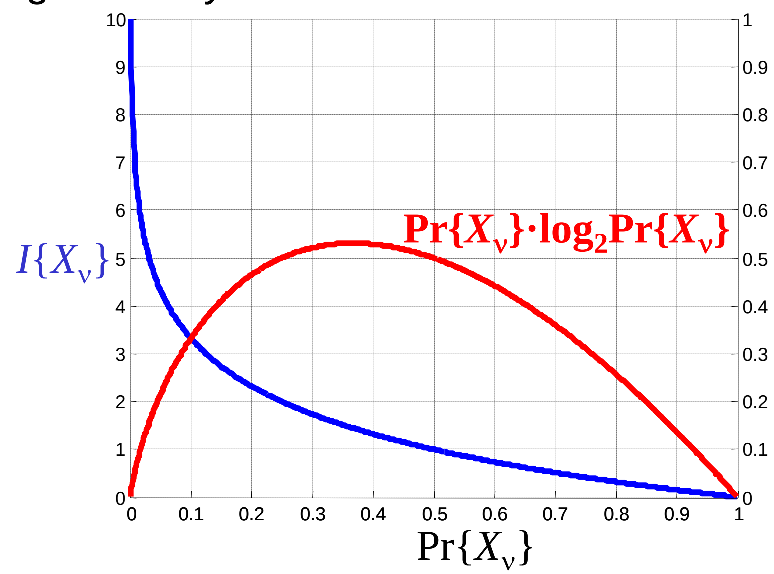
(absolute Ungewißheit = viel Information)

Information / Entropie

- Entropie: ***Mittlerer*** Informationsgehalt einer Quelle (z.B. Nachricht)
  $X = \{X_1, \ldots, X_M\}$

$$H(X) = \mathrm{E}\{-\log_2 Pr\{X\}\} = -\sum_{\nu} \underbrace{\log_2 Pr\{X_\nu\}\, Pr\{X_\nu\}}_{\text{Informationsbeitrag eines Symbols}}$$ (stat. unabh. Symbole X_ν)

- Unsicherheit über die Nachricht X
- Zufälligkeit der Nachricht X



Information / Entropie

- Maximale Entropie, wenn alle Symbole gleichwahrscheinlich sind, $\Pr\{X_\nu\}=1/M$

$$\max_{\Pr\{X\}} H(X) = H_{\text{gleich}}(X) = \sum_{\nu=0}^{M-1} \frac{1}{M} \cdot \log_2 M = M \cdot \frac{1}{M} \cdot \log_2 M = \log_2 M \text{ bit}$$

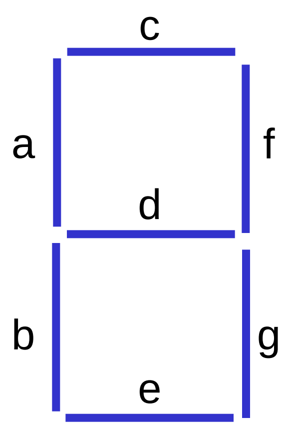
  - Treten alle Zeichen gleichwahrscheinlich auf
    → maximale Unsicherheit ≡ maximaler Informationsgehalt

    → $0 \le H(X) \le \log_2 M$

- Redundanz
  - Nachricht = Informationsgehalt + Redundanz [bits]
  - $m = H(X) + R(X)$

➡ $R(X) = m - H(X)$: (Anzahl Bits für Nachricht – Informationsgehalt)

Beispiel: LCD-Anzeige

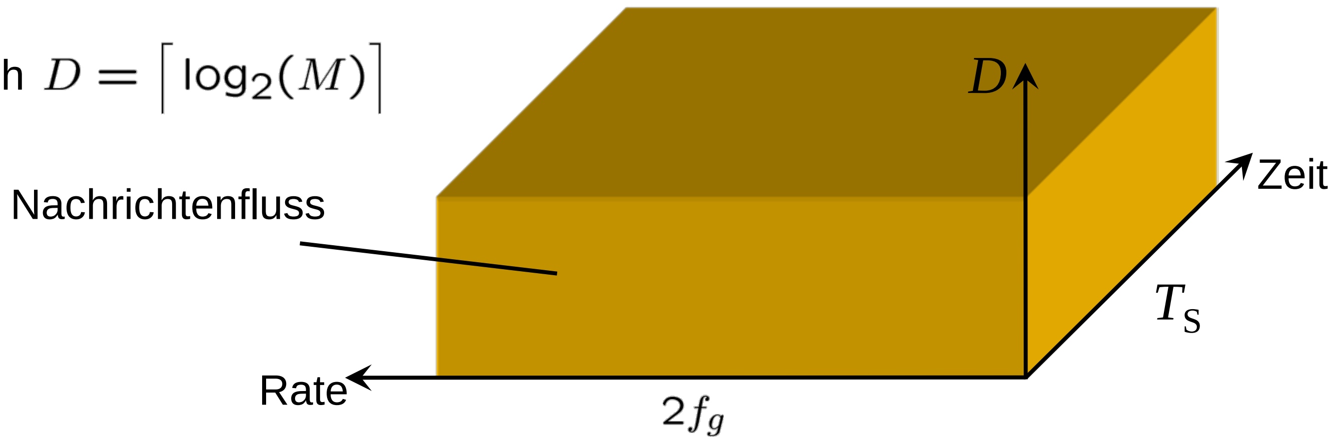


digit	0	1	2	3	4	5	6	7	8	9
a	1	0	0	0	1	1	1	0	1	1
b	1	0	1	0	0	0	1	0	1	0
c	1	0	1	1	0	1	1	1	1	1
d	0	0	1	1	1	1	1	0	1	1
e	1	0	1	1	0	1	1	0	1	1
f	1	1	1	1	1	0	0	1	1	1
g	1	1	0	1	1	1	1	1	1	1

- Alle Symbole (Zahlen 0…9) gleichwahrscheinlich: $\Pr\{X_\nu\} = 0.1$
- Menge an Information pro Zahl: $I(X_\nu) = -\log_2(\Pr\{X_\nu\}) = \log_2(10) = 3.32\text{ bit}$
- Entropie des Alphabets: $H(X) = \sum_\nu \Pr\{X_\nu\} \cdot I(X_\nu) = 3.32\text{ bit}$
- Absolute Redundanz: $R = m - H(X) = 7\text{ bit} - 3.32\text{ bit} = 3.68\text{ bit}$
- Relative Redundanz: $r = R\,/\,m = 3.68\text{ bit} / 7\text{ bit} = 52.54\%$

Nachrichtenfluß / Nachrichtenquader

- Für die Darstellung einer (digitalen) Nachricht von M binär codierten (Dualcode) Symbolen sind 3 Dimensionen wichtig
  - Abtastrate: Abtastung eines zeitkontinuierlichen Signals mit Grenzfrequenz $f_g \Rightarrow f_A = 2 \cdot f_g$
  - Signaldauer T_S
  - Dynamikbereich $D = \lceil \log_2(M) \rceil$



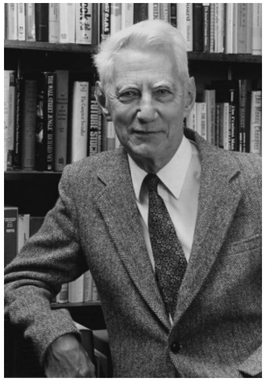
- Definitionen
  - Nachrichtenfluß $\phi = 2 \cdot f_g \cdot \lceil \log_2(M) \rceil = \dfrac{\lceil \log_2(M) \rceil}{T}$ [bit/s] mit $T = \dfrac{1}{f_A} = \dfrac{1}{2 \cdot f_g}$
  - Nachrichtenmenge $N = \phi \cdot T_S = 2 \cdot f_g T_S \lceil \log_2(M) \rceil$ [bit]
  - Informationsfluß $H'(X) = \dfrac{H(X)}{T} = 2 \cdot f_g \cdot H(X)$ [bit/s]

Kanalkapazität

- Größe abhängig vom Kanal und der zu sendenden Nachricht

- Charakteristisch für einen Kanal sind prinzipiell seine <u>Bandbreite</u> und die in ihm wirksamen <u>Störungen</u>
  - Tiefpass-Kanal mit Nyquistbandbreite $B=2f_g$

- Satz von Shannon (1949)

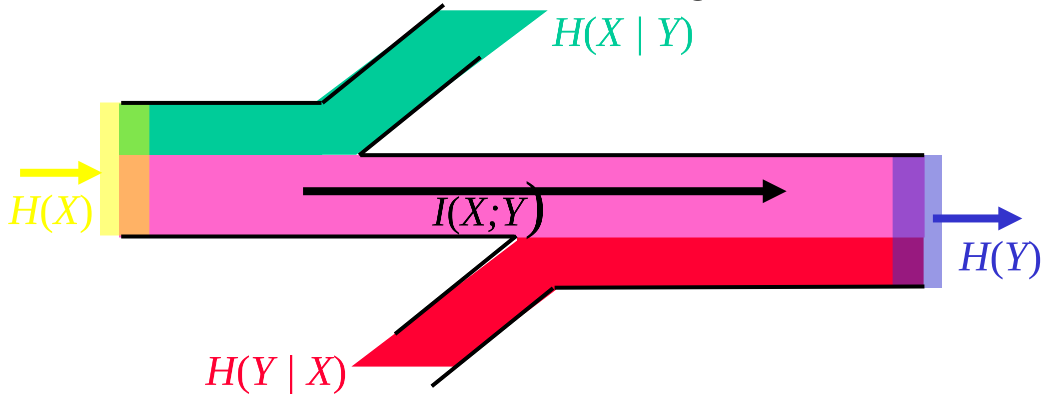


> „Wenn die Signale einer Quelle mit dem Informationsfluß $H'(X)=2f_g\,H(X)$ über einen Kanal mit Kanalkapazität C' übertragen werden, dann exis-tiert ein geeignetes Codierverfahren, so dass für $H' \leq C'$ die Fehlerwahr-scheinlichkeit beliebig klein ist."

  - Anmerkung: C' - zeitbezogene Kanalkapazität [bit/s]

Kanalkapazität (2)

- Herleitung von C' mittels Informationsfluß-Diagramm



  - $H(X)$: Entropie der Quelle/Sender
  - $H(Y)$: Entropie der Senke/Empfänger
  - $H(X \mid Y)$: **Äquivokation**: Mittlerer Informationsgehalt von X bei Kenntnis von Y
    → Informationsverlust infolge von Störungen
  - $H(Y \mid X)$: **Irrelevanz**: Informationsgehalt von Y bei Kenntnis von X
    → Fehlinformation infolge von Störungen
  - $I(X;Y)$: **Transinformation**: gegenseitige Information
- Es gilt $I(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X)$
- Beispiel: Fehlerfreiheit → $H(Y \mid X) = H(X \mid Y) = 0$ → $I(X;Y) = H(X) = H(Y)$

Kanalkapazität (3)

$$C = \sup_{\Pr\{X\}} I(X;Y) = \sup_{\Pr\{X\}} \sum_{\nu} \sum_{\mu} \Pr\{Y_\mu | X_\nu\} \cdot \Pr\{X_\nu\} \cdot \log_2 \frac{\Pr\{Y_\mu | X_\nu\}}{\sum_{\ell} \Pr\{Y_\mu | X_\ell\} \cdot \Pr\{X_\ell\}}$$

bits per channel use

bits/s/Hz

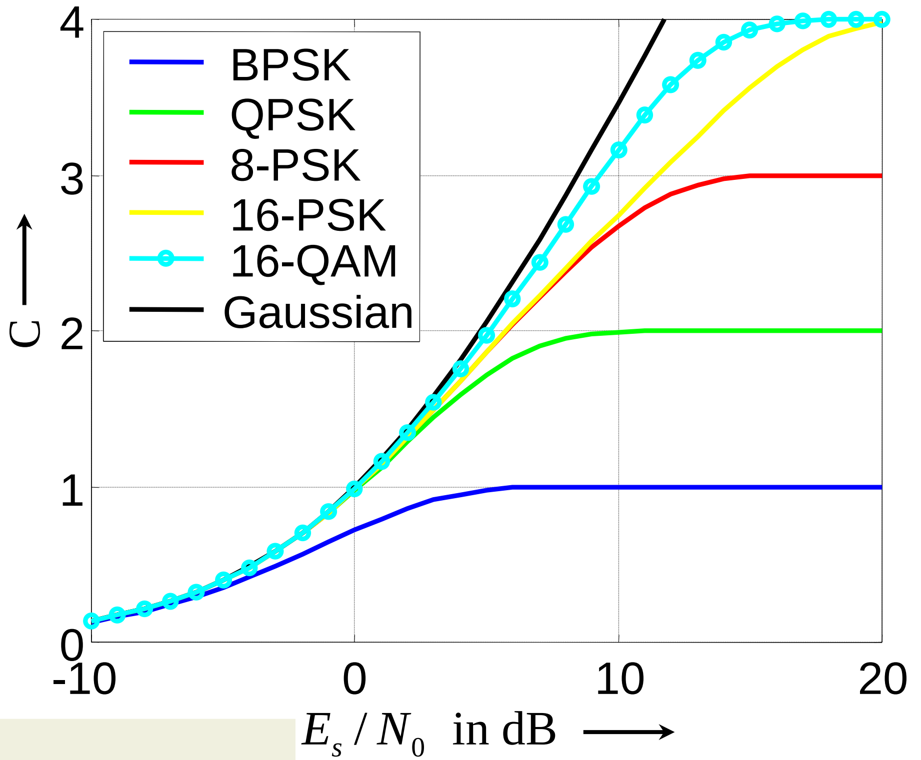
- Bsp.: AWGN-Kanal, gaußverteilte Sendesymbole, Nutz- und Störsignal voneinander unabhängig
  - Kanalkapazität (mit S/N: Signal-Rauschabstand)

$$C = \frac{1}{2}\log_2\left(1 + \frac{S}{N}\right) \qquad \text{[bit]}$$

- Gauß-Kanal: siehe oben und Bandbegrenzung des Kanals durch idealen TP mit Grenzfrequenz f_{gk} und Abtastung mit Nyquistrate $2f_{\text{gk}}$ (Nyquistfilter, fehlerfrei)

➡ max. Transinformationsfluß

$$C' = 2 \cdot f_{gk} \cdot C = f_{gk} \cdot \log_2(1 + S/N) \qquad \text{[bit/s]}$$



Basic Principles of Channel Coding

- Forward Error Correction (**FEC**)
  - Added redundancy is used to ***correct transmission errors*** at the receiver
  - Channel condition affects the quality of data transmission
    → errors after decoding occur if the error-correction capability of the code is passed
  - No feedback channel is required

  ➡ **varying reliability, constant bit throughput**

- Automatic Repeat Request (**ARQ**)
  - Small amount of redundancy is added to ***detect transmission errors***
    → retransmission of data in case of a detected error
    → feedback channel is required
  - Channel condition affects the throughput

  ➡ **constant reliability, but varying throughput**

- Hybrid FEC/ARQ: Combination to use advantages of both schemes

Codierung

Quelle — Quellen-codierung — Kanal-codierung — Kanal — Kanalde-codierung — Quellende-codierung — Senke

- <u>Codierung:</u> Darstellung von zeit- und amplitudendiskreter Signale (diskretes Sendealphabet X) durch Codewörter, z.B. Dualcode (Binärdarstellung), ASCII-Code
  - 3 Gebiete der Codierung
    - Quellencodierung
    - Kanalcodierung
    - Kryptographie

    (Quellencodierung und Kanalcodierung:) Nachrichtenübertragung
- Quellencodierung
  - Setzt analoges Signal um auf zeit- und amplitudendiskretes Signal (diskretes Sendealphabet X)
  - Codierung der Sendesymbole mit möglichst wenig Redundanz, d.h. mit der maximal notwendigen Information $H(X)$ und möglichst nicht mehr → **Ziel: Nachricht** = **Information** + **~~Redundanz~~**
- Kanalcodierung
  - Sicherung der Übertragung der Nachricht durch gezieltes Hinzufügen von „künstlicher" Redundanz → erlaubt Fehlererkennung und/oder Korrektur am Empfänger
- Kryptographie
  - Sicherung der Nachricht vor unerlaubtem Lesen durch nicht autorisierte Personen mittels Verschlüsselung (Nachricht kann nur bei Kenntnis des Schlüssels entschlüsselt werden)

Quellencodierung

- Ziel: Codierung des diskreten Sendealphabets derart, dass gilt
  - Mittlere Codewortlänge ≈ Entropie der Quelle
- Mittlere Codewortlänge:
  - Bsp.: LCD – 7 bit pro Zeichen

$$H_C = \sum_{\nu} S_{\nu} \cdot Pr\{X_{\nu}\}$$

S_{ν}: Anzahl Stellen (Bit) eines Zeichens

- Entropie:

$$H(X) = \sum_{\nu} \log_2 (Pr\{X_{\nu}\}) \cdot Pr\{X_{\nu}\}$$

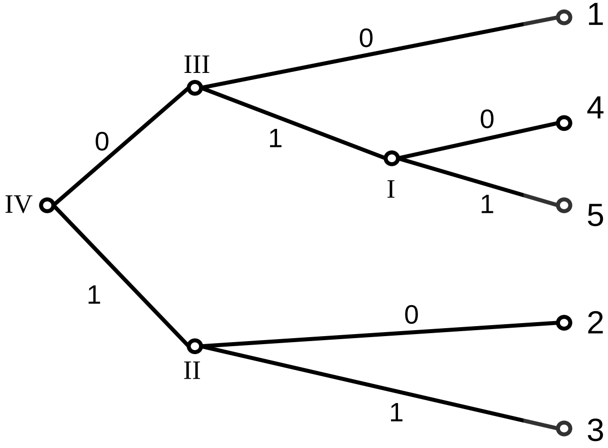
- Verbleibende Redundanz:

$$R = H_C - H(X)$$

- Optimaler Code:
  - Minimierung der mittleren Codewortlänge (und damit der Redundanz) unter Beobachtung der unterschiedlichen Auftrittswahrscheinlichkeiten der Symbole → je häufiger ein Symbol auftritt desto geringer sein Informationsgehalt, desto geringer die Anzahl Bits für dieses Zeichen
- Beispiele:
  - Huffman-Code / Fano-Code
  - Gray-Code: Benachbarte Symbole (z.B. beim Lesen einer Tonspur oder Digitale Modulation) unterscheiden sich nur durch ein Bit

Beispiel: Huffman-Code

➢ Codebaum:



Zeichen	Bitfolge
1	0 0
4	0 1 0
5	0 1 1
2	1 0
3	1 1

Zeichen	$Pr\{X_\nu\}$	1. Summation	2. Summation	3. Summation	4. Summation
1	0,30	0,30	0,44	0,56	1,0
2	0,24	0,26	0,30	0,44	
3	0,20	0,24	0,26		
4	0,15	0,20			
5	0,11				

Hier im Beispiel willkürlich gewählt für den Codebaum:

- Höhere Wahrscheinlichkeit: „0“
- Geringere Wahrscheinlichkeit „1“

Für dieses Beispiel ergibt sich:

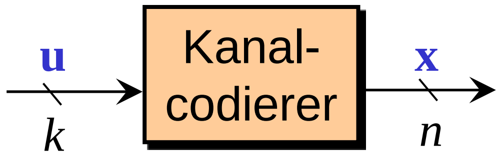
- H_0 = 2,32 bit
- H_C = 2,26 bit
- H = 2,24 bit

➡ Damit reduziert sich die Redundanz von 0,08 bit auf 0,02 bit!

Kanalcodierung

Fehlerkorrigierende Codes – Lineare Blockcodes

- Ziel: Detektion oder Korrektur von Fehlern verursacht durch Störungen auf dem Kanal
- Allgemein gilt:



$$\mathbf{u} = [u_0\ u_1 \dots u_{k-1}]$$

$$\mathbf{x} = [x_0\ x_1 \dots x_{n-1}]$$

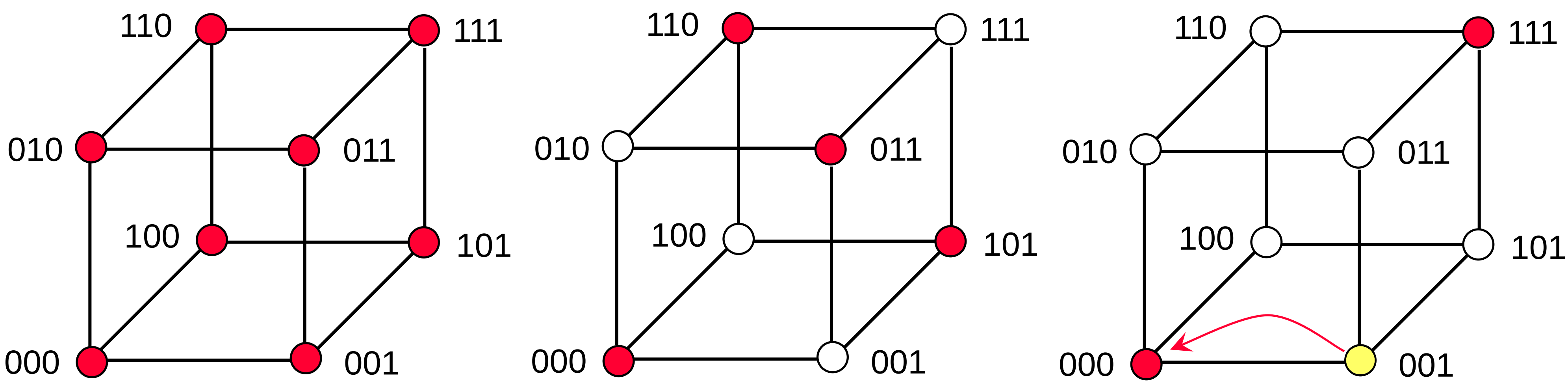
- Kanalcodierer
  - Abbildung der 2^k möglichen Informationswörter auf 2^n Codewörter
- Es gilt:
  - Werden nur alle bei k bit pro Informationswort möglichen 2^k Worte als Codewörter zugelassen ($n = k$), dann ist weder Fehlererkennung noch Fehlerkorrektur möglich → bijektive Abbildung mit $n > k$ (Redundanz beifügen)

Coderate $R_C = \frac{k}{n} < 1$

- Anmerkung
  - Wegen $n > k$ steigt die zu übertragende Nachrichtenmenge. Bei gegebener Zeit T → Anpassung der Dynamik bzw. Leistung (und/oder Anpassung der Bandbreite (siehe **Nachrichtenquader**))
- Lineare Codes
  - Sind $\boldsymbol{x}_1$ und $\boldsymbol{x}_2$ Codewörter ($\boldsymbol{x}_1, \boldsymbol{x}_2 \in \Gamma$) → Summe ist wieder ein Codewort ($\mathbf{y} = \mathbf{x}_1 \oplus \mathbf{x}_2 \in \Gamma$)
    Nullwort ist Codewort; $\mathbf{0} \in \Gamma$

Darstellung der Distanzeigenschaften

$\mathbf{x} = [x_0\ x_1\ x_2]$



$d_{\min} = 1$ $d_{\min} = 2$ $d_{\min} = 3$

- Coderate $R_c = 1$ (n=r)
- Keine Fehlerkorrektur
- Keine Fehlererkennung

- Coderate $R_c = 2/3$, n=3, k=2
- Keine Fehlerkorrektur
- Erkennung von einem Fehler

- Coderate $R_c = 1/3$, n=3, k=1
- Korrektur eines Fehlers
- Erkennung von zwei Fehlern

Distanz-Eigenschaften von $(n,k,d_{\min})_2$-Codes

- Definitionen:
  - Hamming-Gewicht $w_H(\mathbf{x}_1)$: Anzahl Elemente ungleich Null eines Codewortes
  - Hamming-Distanz $d_H(\mathbf{x}_1, \mathbf{x}_2) = w_H(\mathbf{x}_1 - \mathbf{x}_2)$: Gewicht des Differenzwortes = Anzahl der Stellen in denen sich Codeworte $\mathbf{x}_1$ und $\mathbf{x}_2$ unterscheiden

- Minimale Hamming-Distanz $d_{\min}$: Minimale Distanz zweier Codewörter

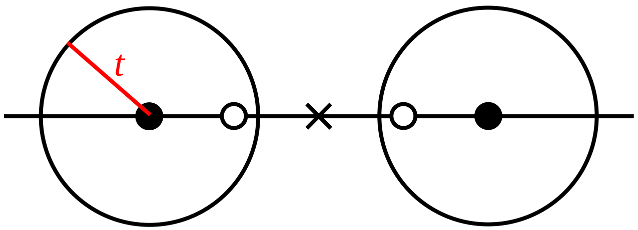
$$d_{\min} = \min_{\mathbf{x}_1,\mathbf{x}_2 \in \Gamma, \mathbf{x}_1 \neq \mathbf{x}_2} d_H(\mathbf{x}_1, \mathbf{x}_2)$$

Γ: Coderaum

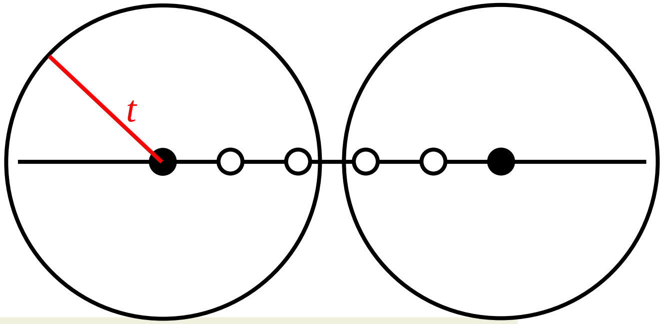
- Für lineare Codes: $d_{\min} = \min_{\mathbf{x} \in \Gamma, \mathbf{x} \neq \mathbf{0}} w_H(\mathbf{x})$: minimales Gewicht aller Codewörter

- Minimale Distanz bestimmt Fehlerdetektion- bzw. Fehlerkorrektureigenschaft:

$d_{\min} = 4 \rightarrow t = 1,\ t' = 3$



$d_{\min} = 5 \rightarrow t = 2,\ t' = 4$



Beispiel eines linearen Blockcodes

- Single-Parity-Check-Code
  - Prinzip: Ergänzung jeder Zeile (Infowort) durch ein Prüfbit auf gerade oder ungerade Quersumme
  - Codeeigenschaften: k=2, n=3, m=n-k=1, R_c =2/3, d_{min}=2

			Paritätsbit	Quersumme
X_1	0	0	0	⇨ 0
X_2	0	1	1	0
X_3	1	0	1	0
X_4	1	1	0	0

1 Fehler erkennbar

0 Fehler korrigierbar

Beschreibung linearer Blockcodes durch Matrizen

- Informationswort $\mathbf{u} = [u_0\ u_1 \ldots u_{k-1}]$ und Codewort $\mathbf{x} = [x_0\ x_1 \ldots x_{n-1}]$
- Generatormatrix der Dimension k x n:

$$\mathbf{G} = \begin{bmatrix} g_{0,0} & \cdots & g_{0,n-1} \\ \vdots & \ddots & \vdots \\ g_{k-1,0} & \cdots & g_{k-1,n-1} \end{bmatrix} \qquad g_{i,j} \in \mathrm{GF}(2)$$

- jede Zeile = gültiges Codewort
- Zeilen sind linear unabhängig und spannen Coderaum auf
- Coderaum $\Gamma \subset \mathrm{GF}(2)^n$ mit $\dim(\Gamma) = k < n$

- Codierung: $\mathbf{x} = \mathbf{u} \cdot \mathbf{G} \bmod 2$ →Linearkombination der Zeilen von $\mathbf{G}$ mit Koeffizienten u_i
- Code: $\Gamma = \left\{ \mathbf{x} \middle| \mathbf{x} = \mathbf{u} \cdot \mathbf{G} \bmod 2; \mathbf{u} \in \mathrm{GF}(2)^k \right\}$
- Prüfmatrix der Dimension

$$\mathbf{H} = \begin{bmatrix} h_{0,0} & \cdots & h_{0,n-1} \\ \vdots & \ddots & \vdots \\ h_{n-k-1,0} & \cdots & h_{n-k-1,n-1} \end{bmatrix} \qquad h_{i,j} \in \mathrm{GF}(2)$$

- Zeilen sind linear unabhängig
- Zeilen spannen den zu $\mathbf{G}$ orthogonalen Vektorraum auf
- $\Gamma^{\perp} \subset \mathrm{GF}(2)^n$ mit $\dim(\Gamma^{\perp}) = n - k = m$

Es gilt: $\mathbf{G} \cdot \mathbf{H}^T = \mathbf{0}$

Beschreibung linearer Blockcodes durch Matrizen (II)

- Syndromdecodierung
  - Annahme: $\mathbf{y} = \mathbf{x} + \mathbf{e} \pmod 2$ ist empfangener Vektor; $\mathbf{e}$: Fehlervektor
- Decodierung durch Berechnung des Syndroms $\mathbf{s} = [s_0\ s_1\ \ldots\ s_{n-k-1}]$

$$\mathbf{s} = \mathbf{y}\cdot\mathbf{H}^T = (\mathbf{x}+\mathbf{e})\cdot\mathbf{H}^T = \underbrace{\mathbf{x}\cdot\mathbf{H}^T}_{\mathbf{uGH}^T = \mathbf{0}} + \mathbf{e}\cdot\mathbf{H}^T = \mathbf{e}\cdot\mathbf{H}^T$$

→ Syndrom $\mathbf{s}$ wird nur durch Fehlervektor $\mathbf{e}$ bestimmt, nicht durch $\mathbf{x}$

- Fehlererkennung
  - $\mathbf{s} \neq \mathbf{0}$ → Fehler erkannt
  - $\mathbf{s} = \mathbf{0}$ → Fehler nicht erkannt, z.B. wenn $\mathbf{e} \in \Gamma$ da $\mathbf{x} + \mathbf{e}$ = Codewort
- Fehlerdetektion
  - Es existieren $2^n - 2^k$ Fehlervektoren aber nur 2^{n-k} Syndrome → verschiedene Fehlervektoren führen auf dasselbe Syndrom → nicht jeder Fehler korrigierbar
- Syndromdecodierung / Standard-Array-Decodierung
  - Wenn $\mathbf{s} \neq \mathbf{0}$, dann Zuweisung eines wahrscheinlichen Fehlervektors $\hat{\mathbf{e}}$ (Fehlervektor mit kleinster Anzahl an Übertragungsfehlern) zu Syndrom und Subtraktion des zugewiesenen Fehlervektors vom Empfangsvektor: $\hat{\mathbf{x}} = \mathbf{y} - \hat{\mathbf{e}}$

Hamming-Schranke

- **Frage:** Wieviele redundante Korrekturstellen $m = n - k$ braucht man für k Infobits um e Bitfehler je Codewort korrigieren zu können?

Syndrom: Prüfwörter mit $n - k$ Stellen → 2^{n-k} unterschiedliche Syndrome

Hamming Schranke:

$$2^{n-k} \geq \sum_{i=0}^{e} \binom{n}{i} = \sum_{i=0}^{e} \frac{n!}{i!\,(n-i)!}$$

Werte für e: $e = 0$ → $2^m \geq 1$ → $m = 0$

- $e = 1$ (1-Bit-Fehler)

$$2^m \geq \frac{n!}{0!n!} + \frac{n!}{1!\,(n-1)!} = 1 + n = 1 + m + k$$

- Perfekte Codes
  - Gleichheitszeichen der Hamming-Schranke gilt, $2^{n-k} = \sum_{i=0}^{e} \binom{n}{i}$
  - → Anzahl 2^{n-k} an Syndromen ist gleich der Anzahl aller bis zu e Fehler auftretenden Fehlerfolgen
  - Beispiel eines perfekten Codes: $(7,4,3)_2$- Hamming-Code

Beispiele linearer Blockcodes

- Systematischer Code
  - Informationswort ist in Codewort enthalten: $\mathbf{x} = [\mathbf{u}\ \mathbf{p}]$

Infobits

Paritätsbits

$$\mathbf{G} = \left[\mathbf{I}_{k\times k} \,\middle|\, \mathbf{P}_{k\times n-k}\right] = \left[\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & \mathbf{P}_{k\times n-k} \\ 0 & & 1 & \end{array}\right]$$

- Single-Partiy-Check-Code

$$\mathbf{G} = \left.\left[\begin{array}{ccc|c} 1 & & 0 & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & 1 \end{array}\right]\right\} n-1 \qquad \mathbf{H} = \underbrace{\left[\begin{array}{ccc|c} 1 & 1 & 1 & 1 \end{array}\right]}_{n}$$

$$R_c = \tfrac{n-1}{n} \quad \text{and} \quad d_{\min} = 2$$

- Wiederholungscode

$$\mathbf{G} = \underbrace{\left[\begin{array}{c|ccc} 1 & 1 & 1 & 1 \end{array}\right]}_{n} \qquad \mathbf{H} = \left.\left[\begin{array}{c|ccc} 1 & 1 & & 0 \\ \vdots & & \ddots & \\ 1 & 0 & & 1 \end{array}\right]\right\} n-1$$

$$R_c = \tfrac{1}{n} \quad \text{and} \quad d_{\min} = n$$

$$\Gamma = \left\{[0\ldots0],[1\ldots1]\right\}$$

Beispiele linearer Blockcodes (II)

- $(7,4,3)_2$-Hamming Code, systematischer Code
  - 1 Fehler korrigierbar

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

$R_c = \frac{4}{7}$ and $d_{\min} = 3$

Perfekter Code

- Spalten von H repräsentieren alle 2^{n-k} Syndrome: Da $\mathbf{s} = \mathbf{e}\,\mathbf{H}^T$ => Spalte von $\mathbf{H}$

  → $\mathbf{e}$ ist 1-Bit Fehlervektor und Position des Syndroms als Spalte von $\mathbf{H}$ ist Stelle des 1-Bit-Fehlers

  → 1 Fehler korrigierbar

Weitere Kanalcodierungskonzepte

- Zyklische Codes
  - Fehlererkennung (Cyclic Redundancy Check)
  - Häufig in Verbindung mit ARQ-Verfahren (Rückkanal erforderlich)
  - Darstellung von Bitfolgen als Polynom
  - Bsp.: $\left.\begin{array}{cccc} 1 & 0 & 1 & 1 \\ X^3 & X^2 & X^1 & X^0 \end{array}\right\} X^3 + X^1 + X = P(X)$
  - Decodierung mathematisch beschreibbar durch Polynomdivision mittels eines Prüfpolynoms
  - Einfache Realisierung durch Schieberegister

- Faltungs-Codes
  - Schieberegisterstruktur mit $L_c \cdot k$ Speicherelementen
  - In jedem Zyklus erfolgt Shift um k Bits
    → jedes Infobit beeinflußt das Ausgangswort L_c-mal
    - L_c: Einflußlänge ; Gedächtnistiefe: L_c-1
  - Codewort besitzt eine Länge n → $R_C = \frac{k}{n}$
  - Decodierung: Viterbi-Algorithmus
  - Anwendung: Mobilkommunikation