Informations- und Kodierungstheorie

mit einer Einführung in Sicherheitsaspekte

IKT: Dr.-Ing. Elke Franz
elke.franz@tu-dresden.de
Foliensatz: Dr.-Ing. Dagmar Schönfeld
Sicherheit: Prof. Dr.-Ing. Thorsten Strufe

Professur
Datenschutz und Datensicherheit

SS 2019

Organisatorisches

Was Sie wissen sollten:

- Einschreibung in jExam (Vorlesung <u>und</u> Übung)
- Folienskript komplett im Netz
  Skript enthält keine Beispiellösungen!
  Beispiele werden an der Tafel vorgerechnet
- Ergänzende/Vertiefende Folienvorlagen zur Vorlesung werden im Netz bereitgestellt
- Zur Klärung von Fragen: Übung, E-Mail, APB 3069
- Begleitbuch zum Teil IKT:
  D. Schönfeld, H. Klimant, R. Piotraschke.
  Informations- und Kodierungstheorie. 4. Aufl., Springer, 2012.
  (im Anhang weiterführende Literatur zu finden)
- Klausur: **handgeschriebenes** Formelblatt einseitig A4,
  Taschenrechner

Gegenstand der Informations- und Kodierungstheorie

Informations- und Kodierungstheorie

C.E. Shannon (1948)[1] R.W. Hamming (1950)[2]

Informationstheorie setzt sich mit zwei Problemstellungen auseinander:

- Inwieweit lässt sich Information kompakt darstellen?
- Inwieweit überträgt man Information „fehlerfrei" (quasi fehlerfrei)?

$\rightarrow$ Informationstheorie begründet die Grenzen, was ist erreichbar, was nicht
(Zwei Kodierungstheoreme, SHANNON-Grenze „fehlerfreier" Übertragung)

$\rightarrow$ Kodierungstheorie konstruiert praktikable Umsetzungen
(weniger komplexe Algorithmen, die sich den Grenzen annähern)

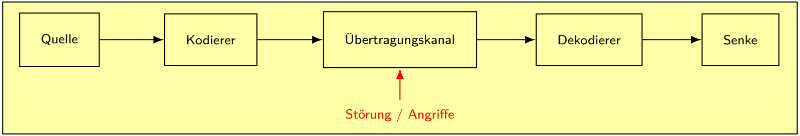
[1] C.E. Shannon. *A Mathematical Theory of Communication.* BSTJ 27(1948)379-423, 623-656

[2] R.W. Hamming. *Error Detecting and Correcting Codes.* BSTJ 29(1950)147-160

Information

- **Statistischer Aspekt**
- Semantischer Aspekt (Bedeutung der Information)
- Pragmatischer Aspekt (Nutzen für den Informationsempfänger)

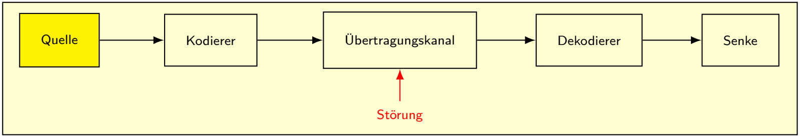
$\rightarrow$ Statistische Informationstheorie

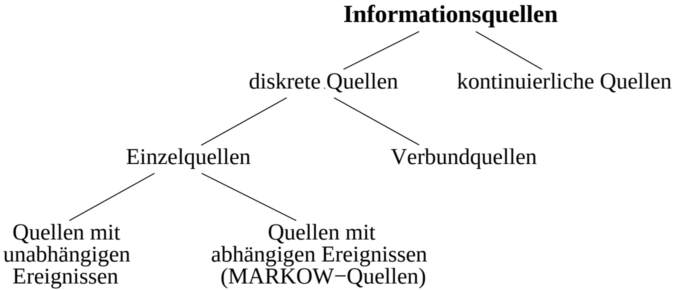


Information ist beseitigte Unbestimmtheit

Das Maß dieser Unbestimmtheit ist äquivalent der Ermittlung der Informationsmenge.

Systematisierung





Quellen mit unabhängigen Ereignissen

Definition 1.1

Eine Quelle mit dem Alphabet

$$X = \{x_1, x_2, ..., x_N\}$$

und der Verteilung der zugehörigen Auftrittswahrscheinlichkeiten

$$(p(x_i)) = (p(x_1), p(x_2), ..., p(x_N)), \quad 0 \le p(x_i) \le 1,$$

wobei

$$\sum_{i=1}^{N} p(x_i) = 1,$$

wird als **diskrete Quelle mit unabhängigen Ereignissen** bezeichnet.

Die Unbestimmtheit (der Informationsgehalt) eines Ereignisses x_i ist

$$H_i = \log \frac{1}{p(x_i)} = -\log p(x_i), \text{ im Weiteren } H_i = \text{ld}\, \frac{1}{p(x_i)} = -\text{ld}\, p(x_i).$$

(Quellen)Entropie

Für H_i $(i = 1, 2, ..., N)$ gilt dann:

$$H_1 = \text{ld}\,\frac{1}{p(x_1)}\,, \quad H_2 = \text{ld}\,\frac{1}{p(x_2)}\,, \quad \dots \quad , \quad H_N = \text{ld}\,\frac{1}{p(x_N)}\,.$$

Gewichteter Mittelwert $H_Q = H_m$:

$$\boldsymbol{H_m = \sum_{i=1}^{N} p(x_i)\, H_i = \sum_{i=1}^{N} p(x_i)\; \textbf{ld}\,\frac{1}{p(x_i)}} = -\sum_{i=1}^{N} p(x_i)\;\text{ld}\,p(x_i)$$

H_m **(Quellen)Entropie**, gleichzeitig **mittlerer Informationsgehalt** in *bit/Ereignis, bit/Messwert, bit/(Quellen-)Zeichen* = *bit/QZ* u. ä.

Beispiel $N = 2\,,\ (p(x_i)) = (p(x_1),\, p(x_2)) = (1\ \ 0)$
$\rightarrow$ sicheres, unmögliches Ereignis $\longrightarrow H_Q?$

Warum log bzw. **ld**, d. h. Anwendung des logarithm. Informationsmaßes?

Maximalwert der Entropie

Sonderfall der **Gleichverteilung:**

$$p(x_i) = \frac{1}{N} \text{ für alle } i$$

$$H_Q = H_0 = \text{ld}\, N$$

$\rightarrow$ **Maximalwert** der Entropie oder **Entscheidungsgehalt** der Quelle

$\rightarrow$ Beweis

Definition 1.2

Der Entscheidungsgehalt von zwei unabhängigen und gleichwahrscheinlichen Ereignissen einer Quelle

$$H_0 = \text{ld}\, 2 = 1 \;\; \frac{bit}{Ereignis}$$

wird als **Einheit der Informationsmenge** bezeichnet.

[Begleitbuch, S. 1 - 20]

MARKOW-Quellen

MARKOW-Quellen: diskrete Quellen mit abhängigen Ereignissen

- Das Ereignis $x^{(m+1)}$ tritt unter der Bedingung ein, dass ganz bestimmte Ereignisse $x^{(1)}, x^{(2)}, ..., x^{(m)}$ bereits eingetreten sind.
- Die Auswahl des Ereignisses $x^{(m+1)}$ erfolgt demnach mit der bedingten Wahrscheinlichkeit

$$p\left(x^{(m+1)}|x^{(m)} ... \; x^{(2)} \; x^{(1)}\right).$$

MARKOW-Quellen **erster Ordnung**:

$$p(x^{(m+1)}|x^{(m)}),$$

wofür wir im Folgenden schreiben

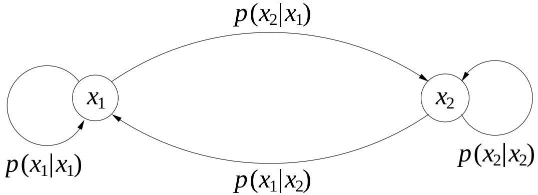
$$p(x_j|x_i) \quad (i,j = 1, 2, ..., N).$$

MARKOW-Quellen

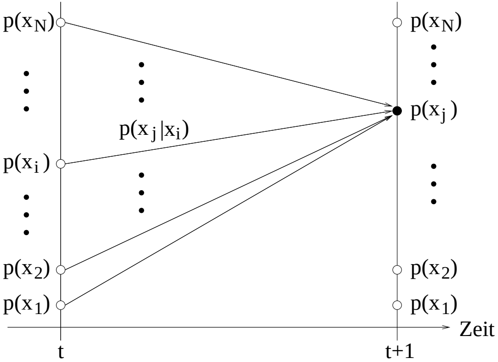
Definition 1.3

Eine **MARKOW-Quelle** ist das mathematische Modell einer Informationsquelle, bei dem die aufeinanderfolgende Auswahl von Ereignissen, d. h. die Folge der Zustände, sowohl von der momentanen Verteilung der Auftritts- bzw. Zustandswahrscheinlichkeiten als auch von der Verteilung der Übergangswahrscheinlichkeiten abhängt.

Zustandsgraph einer binären MARKOW-Quelle erster Ordnung



MARKOW-Kette



Nach dem Satz von der vollständigen Wahrscheinlichkeit gilt:

$$p(x_j)_{t+1} = \sum_{i=1}^{N} p(x_i)_t \, p(x_j|x_i) \quad (j = 1, 2, ..., N)\,.$$

Entropie von MARKOW-Quellen

Unbestimmtheit, die in den Übergangsmöglichkeiten von einem beliebigen x_i zu allen x_j $(j = 1, 2, ..., N)$ liegt:

$$H_i = \sum_{j=1}^{N} p(x_j|x_i) \,\text{ld}\, \frac{1}{p(x_j|x_i)}$$

Gewichteter Mittelwert über alle x_i $(i = 1, 2, ..., N)$:

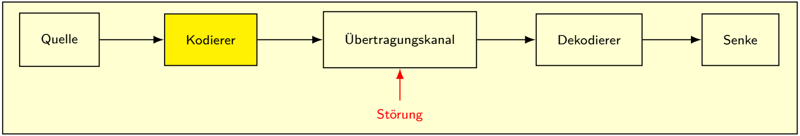
$$H_Q = \sum_{i=1}^{N} p(x_i)\, H_i$$

Die Entropie wird für den stationären Fall $p(x_i) = \overline{p(x_i)}$ als **MARKOW-Entropie** H_M bezeichnet:

$$H_Q = H_M = \sum_{i=1}^{N} \sum_{j=1}^{N} \overline{p(x_i)}\, p(x_j|x_i) \,\text{ld}\, \frac{1}{p(x_j|x_i)} \quad \text{in} \quad \frac{bit}{Zustand}\,.$$

[Begleitbuch, S. 20 - 26]

Kodierung diskreter Quellen



Unter **Kodierung** wird i. Allg. ein Vorgang verstanden, bei dem die Elemente eines Alphabets auf die Elemente eines anderen Alphabets (bzw. auf Wörter über diesem Alphabet) **eineindeutig** abgebildet werden.

Für die **Kodierung diskreter Quellen** bedeutet dies:

Jedes Element des Quellenalphabets X wird einem Element des Kanalalphabets U bzw. einem Wort über U eineindeutig zugeordnet.

Aus praktischen (technischen) Erwägungen beschränken wir uns auf die Binärkodierung, d. h.
$U = \{0, 1\}$.

Kodierung diskreter Quellen

Quellenkodierung (Optimalkodierung, Kompression)

ist die erste Stufe der Kodierung, bei der die eineindeutige Darstellung der Quelleninformation in einer realisierbaren, möglichst *redundanzfreien* oder *redundanzarmen* Form erfolgen soll.

$\rightarrow$ **verlustfreie** Quellenkodierung (Redundanzreduktion)

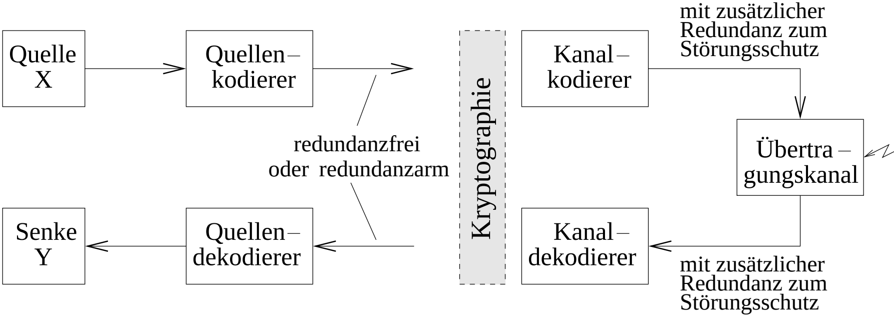
[$\rightarrow$ verlustbehaftete Quellenkodierung (Irrelevanzreduktion)]

Kanalkodierung,

die sich meistens an die Quellenkodierung anschließt, dient dem Zweck des Störungsschutzes (*Schutz gegen zufällige Veränderungen*, z. B. durch Übertragungs/Speicherungsfehler).
Sie macht erst quasi fehlerfreie Übertragung/Speicherung möglich.

Notwendig: *Hinzufügung von Redundanz* in Form von zusätzlicher Kontrollinformation (Kontrollstellen).

Kodierung diskreter Quellen

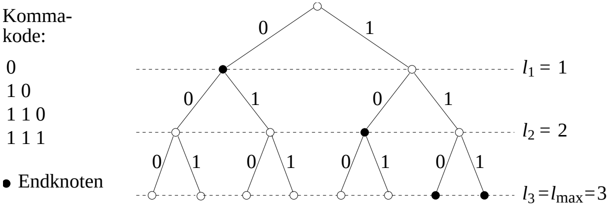


Dekodierbarkeitsbedingung

Definition 2.1

Ein ungleichmäßiger Kode, bei dem kein Kodewort den Anfang (Präfix) eines anderen Kodewortes darstellt, wird als **präfixfreier Kode** bezeichnet (**hinreichende Bedingung für Eineindeutigkeit**).

Kodebaum – Darstellungsmöglichkeit eines (Quellen-)Kodes



Von L.G. KRAFT gefundene Ungleichung $\sum_{i=1}^{N} 2^{-l_i} \leq 1$

ist eine **notwendige Bedingung für die Dekodierbarkeit**.

Kodewortlänge und Koderedundanz

Kodewortlänge

- $l = \lceil \mathrm{ld}\, N \rceil$ **gleichmäßiger** Kode (allg.: $l = \lceil \frac{\mathrm{ld}\, N}{[H_K]} \rceil$)
  H_K : Entropie am Kanaleingang des Übertragungskanals
- $l_m = \sum_{i=1}^{N} p(x_i)\, l_i$ **ungleichmäßiger** Kode

Schranken

- $l_m \geq H_m$ **dekodierbarer** Kode
- $H_m \leq l_m < H_m + 1$ **redundanzarme** Kodierung
- $l_m = H_m$ **redundanzfreie** Kodierung (Möglich?)

$p(x_i) = 2^{-l_i}$

$$\boxed{R_K = l_{(m)}\,[\cdot H_K] - H_Q \geq 0 \quad \textbf{Koderedundanz}}$$

Erstes SHANNONsches Kodierungstheorem

Das **erste SHANNONsche Kodierungstheorem** besagt:

Redundanzfreie Kodierung ist auch für $p(x_i) \neq 2^{-l_i}$ möglich.

Man nimmt eine m-fache Erweiterung der Quelle vor, d. h., die Quellenzeichen werden nicht einzeln, sondern in Blöcken von m Quellenzeichen kodiert.

$$m\,H_m \leq m\,l_m < m\,H_m + 1$$

$$H_m \leq l_m < H_m + \frac{1}{m}$$

Im Folgenden: **Verfahren der Optimalkodierung**

$\rightarrow$ Verfahren der (annähernd) redundanzfreien Kodierung

$\rightarrow$ Grundlage bilden $N, (p(x_i)), (p(x_j|x_i))$, deshalb auch **Entropiekodierung**

[Begleitbuch, S. 40 - 59]

SHANNON-FANO-Verfahren (1949)

1. **Ordnen** der zu kodierenden Quellenzeichen nach fallenden Werten der Auftrittswahrscheinlichkeiten
2. **Teilen** des geordneten Wahrscheinlichkeitsfeldes in zwei Gruppen; die Teilsummen der Wahrscheinlichkeiten in jeder Gruppe sollten möglichst gleich groß sein.
   Aufgrund dieses Teilungsprinzips enthält jeder Teilungsschritt und damit jedes Kodewortelement die größte Entropie bzw. Informationsmenge.
3. **Kodieren** nach dem Prinzip, dass der ersten Gruppe immer einheitlich das Zeichen 0 (bzw. 1) und der zweiten Gruppe immer einheitlich das Zeichen 1 (bzw. 0) zugeordnet wird.
4. **Wiederholen** der Schritte 2. und 3.; solange, bis jede Teilgruppe nur noch ein Element enthält.

Beispiel $(p(x_i)) = (0,11\ \ 0,30\ \ 0,16\ \ 0,25\ \ 0,06\ \ 0,06\ \ 0,06)$, $l_m = ?$

HUFFMAN-Verfahren (1952)

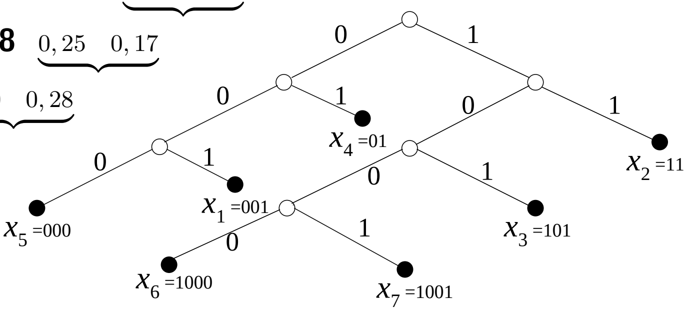
1. **Ordnen** des gegebenen Wahrscheinlichkeitsfeldes nach fallenden Werten.
2. **Zusammenfassen** der letzten zwei Wahrscheinlichkeiten (die mit den kleinsten Werten) zu einem neuen Wert.
3. **Erneutes Ordnen** des reduzierten Wahrscheinlichkeitsfeldes entsprechend Schritt 1.
4. **Wiederholen** der Schritte 2. und 3. solange, bis die Zusammenfassung der beiden letzten Elemente den Wert 1 ergibt.
5. **Aufstellen** eines Kodebaumes entsprechend dem Reduktionsschema und Zuordnung der Kodesymbole 0 und 1.

Beispiel

$$(p(x_i)) = (0,11 \;\; 0,30 \;\; 0,16 \;\; 0,25 \;\; 0,06 \;\; 0,06 \;\; 0,06)\,, \; l_m = ?$$

HUFFMAN-Verfahren: Ablauf

x_2	x_4	x_3	x_1	x_5	x_6	x_7
0,30	0,25	0,16	0,11	0,06	$\underbrace{0,06 \quad 0,06}$	
0,30	0,25	0,16	**0,12**	$\underbrace{0,11 \quad 0,06}$		
0,30	0,25	**0,17**	$\underbrace{0,16 \quad 0,12}$			
0,30	**0,28**	$\underbrace{0,25 \quad 0,17}$				
0,42	$\underbrace{0,30 \quad 0,28}$					
$\underbrace{\mathbf{0,58} \quad 0,42}$						
1						



$l_m = 2,57 \, \frac{KZ}{QZ}$

Erweiterte Quelle

Beispiel **m-fache Erweiterung der Quelle**

Eine Binärquelle sei mit $p(0) = 0,8$ gegeben.
Aufzeigen der Reduzierung von R_K mit Erhöhung der Blocklänge von $m = 1$ auf $m = 2, 3$ (Grundlage: SHANNON-FANO)!

Berücksichtigung von $(p(x_j|x_i))$?

Beispiel **Beispiel aus Abschnitt zu MARKOW-Quellen**

$$(\overline{p(x_i)}) = (0,25 \;\; 0,25 \;\; 0,5)\,,\; (p(x_j|x_i)) \;\rightarrow\; H_M = 1,27\,\frac{bit}{QZ}$$

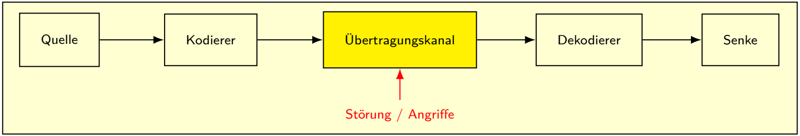
$$(p(x_j|x_i)) = \begin{pmatrix} 0,5 & 0,2 & 0,3 \\ 0,1 & 0,6 & 0,3 \\ 0,2 & 0,1 & 0,7 \end{pmatrix} \begin{matrix} A_1^* = \{0, 11, 10\}, l_{m,1} = 1,5\,\frac{KZ}{QZ}, H_{Q,1} = 1,48\,\frac{bit}{QZ} \\ A_2^* = \{11, 0, 10\}, l_{m,2} = 1,4\,\frac{KZ}{QZ}, H_{Q,2} = 1,30\,\frac{bit}{QZ} \\ A_3^* = \{10, 11, 0\}, l_{m,3} = 1,3\,\frac{KZ}{QZ}, H_{Q,3} = 1,16\,\frac{bit}{QZ} \end{matrix}$$

$$H_Q = H_M = \sum_i \overline{p(x_i)}\, H_{Q,i}\,;\; l_M = \sum_i \overline{p(x_i)}\, l_{m,i} = 1,37\,\frac{KZ}{QZ} \;\rightarrow\; \underline{R_K = 0,10\,\frac{bit}{QZ}}$$

Andere Möglichkeiten

- LEMPEL-ZIV(-WELCH) (1977)
- Arithmetische Kodierung (1979)

Übertragungskanäle: Störungen

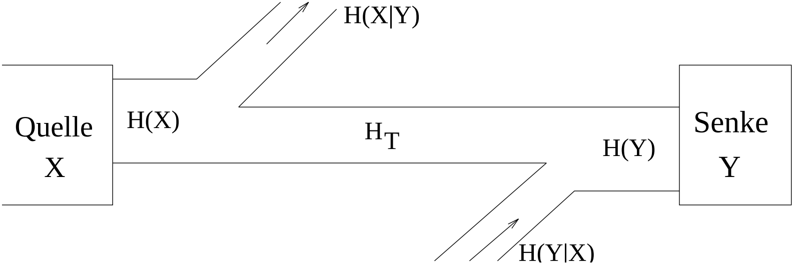


Störungen

- Störungen durch Betriebsmittel (z. B. Unterbrechungen durch Vermittlungseinrichtungen)
- Störungen aus dem Umfeld (z. B. Beeinflussungen durch Starkstromleitungen, magnetische Streufelder)
- thermisches Rauschen der Bauelemente des Übertragungskanals
- Funkkanäle: Mehrwegeausbreitung (reflektierende Objekte), kurzzeitige Abschattungen, Nachbarkanalbeeinflussungen

Trotzdem: Quasi fehlerfreie Übertragung

BERGERsches Entropiemodell des Übertragungskanals



$H(X)$	Entropie am Kanaleingang
$H(Y)$	Entropie am Kanalausgang
H_T	Transinformation
$H(X\|Y)$	Äquivokation (Rückschlussentropie)
$H(Y\|X)$	Irrelevanz (Störentropie)

Im Idealfall, d. h., der Kanal ist ungestört, gilt $H(X) = H(Y) = H_T$.

Transinformation

Die **Transinformation** H_T ist die Informationsmenge, die im Mittel durch ein Kanalzeichen vom Sender zum Empfänger übertragen werden kann:

$$\begin{aligned} H_T &= H(X) + H(Y) - H(X,Y) \\ &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \qquad \text{in } bit/KZ\,. \end{aligned}$$

Notwendig: Kenntnisse über das Stör-(Übergangs-)verhalten

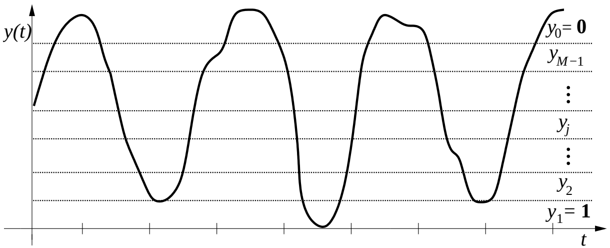
– Statistische Untersuchungen

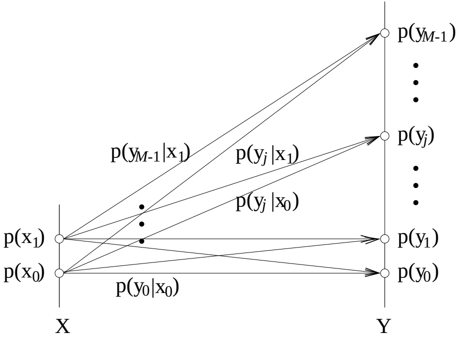
– Übertragungsweg (Kabel, Funk) widerspiegelt typische Fehlerstrukturen

$\rightarrow$ Nachbildung des Störverhaltens (z. B. Binär-, AWGN-Kanalmodell)

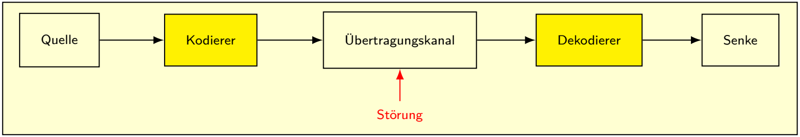
Annahme: $(p(y_j|x_i))$ bekannt, $N \leq M$

Binärkanal mit Störerkennung





Möglichkeiten der Fehlerkorrektur



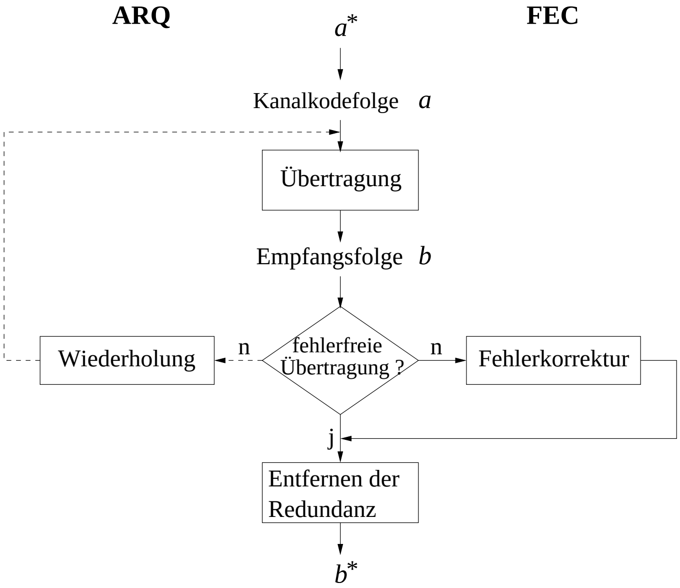
Fehlerkorrektur

durch Wiederholung
ARQ [Automatic Repeat reQuest]
"Fehlererkennung" (FE)

durch Rekonstruktion
FEC [Forward Error Correction]
"Fehlerkorrektur" (FK)

- mit Maximum–Likelihood
- mit begrenzter Mindestdistanz

Allgemeiner Ablauf mit ARQ bzw. FEC



Redundanz und Rekonstruktionsergebnisse

Fehlerkorrektur durch Wiederholung (FE)

$\rightarrow$ hinzugefügte redundante Stellen **nur** zur **Erkennung** eines Fehlers

Fehlerkorrektur durch Rekonstruktion (FK)

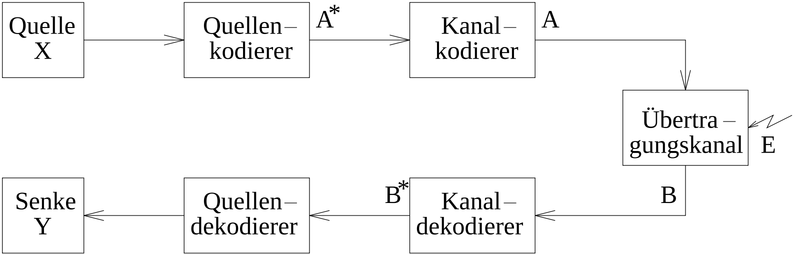
$\rightarrow$ hinzugefügte redundante Stellen zur **Erkennung** eines Fehlers **und Lokalisierung** der Fehlerpositionen

$\rightarrow k_{\text{FEC}} > k_{\text{ARQ}}$

Rekonstruktionsergebnisse

- korrekte Rekonstruktion
- falsche Rekonstruktion
- Versagen der Rekonstruktion

Allgemeine Kenngrößen von Kanalkodes



$X = \{x_1, x_2, ..., x_L\}$

$A^* = \{a_1^*, a_2^*, ..., a_L^*\}$

$A = \{a_1, a_2, ..., a_L\}$

$E = \{e_1, e_2, ..., e_N\}$

$B = \{b_1, b_2, ..., b_N\}$ $\rightarrow (n, l, d_{min})$, auch (n, l)Kode

Beispiel $(n, 1, n)$Wiederholungskode

HAMMING-Distanz

Definition 4.1

Die Anzahl der Stellen, in denen sich zwei Kodewörter

$a_i = (u_{i1}\, u_{i2} \ldots u_{in})$ und $a_j = (u_{j1}\, u_{j2} \ldots u_{jn})$

unterscheiden, bezeichnet man als **HAMMING-Distanz** $d(a_i, a_j)$:

$d(a_i, a_j) = |\{g \in \mathbb{Z}_n \,|\, u_{ig} \neq u_{jg}\}|$ mit $g \in \mathbb{Z}_n = \{1, 2, \ldots, n\}$.

Binärkode:

HAMMING-Distanz: $$d(a_i, a_j) = \sum_{g=1}^{n} (u_{ig} \oplus u_{jg})$$

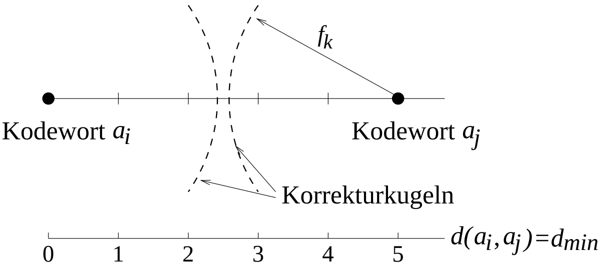
HAMMING-Gewicht: $$w(a_i) = \sum_{g=1}^{n} u_{ig} = d(\mathbf{0}, a_i)$$

$$\rightarrow d_{min} = \min_{a_i, a_j \in A, a_i \neq a_j} d(a_i, a_j) = \min_{a_i \in A \setminus \mathbf{0}} d(\mathbf{0}, a_i) = \min_{a_i \in A \setminus \mathbf{0}} w(a_i) = w_{min}$$

Beispiel min. HAMMING-Distanz d_{min} (auch Mindestdistanz)

$(4, 1, d_{min} = ?\,)$Wiederholungskode; $(4, 3, d_{min} = ?\,)$Paritätskode

Geometrische Deutung der minimalen HAMMING-Distanz



$\boxed{d_{min} = f_e + f_k + 1}$ FE: $f_e = d_{min} - 1\,,\ f_k = 0$

FK: $f_e = \lfloor \frac{d_{min}}{2} \rfloor\,,\ f_k = \lfloor \frac{d_{min}-1}{2} \rfloor$ (d_{min} geradzahlig?)

$\rightarrow$ Dekodierungsprinzip *Rekonstruktion mit begrenzter Mindestdistanz*

Beispiel Fortsetzung: f_e, f_k bei Anwendung von FE oder FK?

HAMMING-Schranke

Berechnung der redundanten Stellen k (bekannt: d_{min}; l oder n)

$$2^n = 2^l\,2^k \quad \geq \quad 2^l \left(1 + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{f_k}\right)$$

$$2^k \quad \geq \quad \sum_{i=0}^{f_k} \binom{n}{i} \qquad\qquad \binom{n}{i} = \frac{n!}{i!\,(n-i)!} = \frac{n(n-1)\cdot\ldots\cdot(n-i+1)}{1\cdot 2\cdot\ldots\cdot i}$$

$$k \quad \geq \quad \mathrm{ld} \sum_{i=0}^{f_k} \binom{n}{i} = \mathrm{ld} \sum_{i=0}^{f_k} \binom{l+k}{i}$$

→ *untere* Schranke für k bei vorgegebenem l
obere Schranke für l bei vorgegebenem n; $l = n - k$

→ **HAMMING-Schranke**

→ „=“: Entsprechende Kodes heißen **dichtgepackt** oder **perfekt**.

Beispiel Berechnung von k

$l = 4\,,\ d_{min} = 5$

Zweites SHANNONsches Kodierungstheorem

Weitere Kodekenngrößen

relative Redundanz $r_k = \frac{n-l}{n} = \frac{k}{n}$

Koderate $R = \frac{l}{n}$

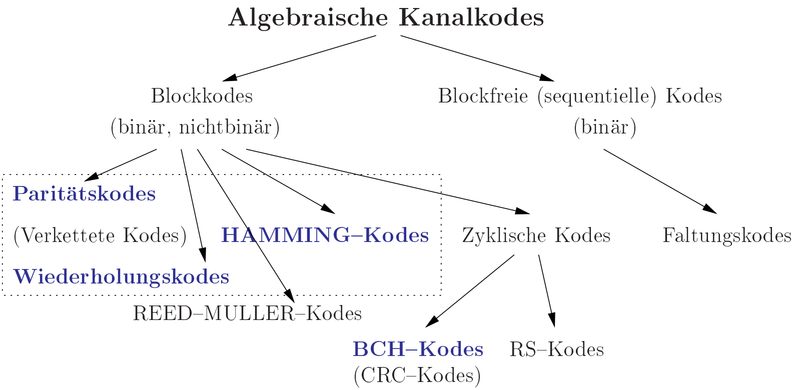
Zweites SHANNONsches Kodierungstheorem

Die **Restfehlerwahrscheinlichkeit** p_R kann beliebig klein gehalten werden, solange die Koderate R den Wert der maximalen Transinformation H_T nicht überschreitet.

Darüber hinaus hat SHANNON theoretisch nachgewiesen, dass auch bei beliebig kleiner Restfehlerwahrscheinlichkeit immer noch eine Koderate größer als Null möglich ist [SHA 48].

[Begleitbuch, S. 125 - 137]

Klassifizierung von Kanalkodes



„Neu“: Turbokodes, LDPC-Kodes
(einfache, auch verkettete Blockkodes mit iterativer Dekodierung)

[Begleitbuch, S. 138 - 141]

Lineare Blockkodes

Definition 4.2

Ein Kode heißt *linearer* Blockkode, oder kurz Linearkode, wenn der Kanalkodierer für die Transformation von Quellenkodewörtern der Länge l aus dem Alphabet A^* (Quellenkode) in Kanalkodewörter der Länge n des Alphabetes A (Kanalkode) *eine* Verknüpfungsoperation verwendet, die in der *algebraischen Struktur einer Gruppe* definiert ist.

Darstellung von Linearkodes als Gruppen

Axiom G1: Abgeschlossenheit

Axiom G2: Assoziatives Gesetz

Axiom G3: Neutrales Element

Axiom G4: Inverses Element

Kommutativgesetz $\rightarrow$ **abelsche Gruppe**

Beispiel $(5, 1, 5)$Wiederholungskod : $A = \{00000, 11111\}$

$(3, 2, 2)$Paritätskode : $A = \{00\underline{0}, 01\underline{1}, 10\underline{1}, 11\underline{0}\}$

Wichtig für algebraische Kodes

- lineare Verknüpfung von Kanalkodewörtern führt wieder zu einem Kanalkodewort
- Nullwort ist immer auch Kanalkodewort
- Axiome stellen Kodebildungs- und Fehlererkennungsvorschrift dar
- (n, l, d_{min})Kanalkode:
  $A \subset \{0,1\}^n$ mit $L = 2^l$ Kanalkodewörtern, $k = n - l$
- d_{min} des Kanalkodes bestimmt Leistungsfähigkeit
  Bei einem Linearkode ist die minimale HAMMING-Distanz gleich dem minimalen Gewicht der Kodewörter (außer dem Nullwort).
  FE: $f_e = d_{min} - 1 = w_{min} - 1$
  FK: $f_k = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{w_{min}-1}{2} \right\rfloor, \; f_e = \left\lfloor \frac{d_{min}}{2} \right\rfloor = \left\lfloor \frac{w_{min}}{2} \right\rfloor$

Beispiel Kanalkodealphabet A

Beispiel: Kanalkodealphabet A

Kanalkodealphabet A:

$$
\begin{array}{llll}
a_0 = & (0\,0\,0\,0\,0\,0\,0) & a_8 = & (1\,0\,0\,0\,1\,0\,1) \\
a_1 = & (0\,0\,0\,1\,0\,1\,1) & a_9 = & (1\,0\,0\,1\,1\,1\,0) \\
a_2 = & (0\,0\,1\,0\,1\,1\,0) & a_{10} = & (1\,0\,1\,0\,0\,1\,1) \\
a_3 = & (0\,0\,1\,1\,1\,0\,1) & a_{11} = & (1\,0\,1\,1\,0\,0\,0) \\
a_4 = & (0\,1\,0\,0\,1\,1\,1) & a_{12} = & (1\,1\,0\,0\,0\,1\,0) \\
a_5 = & (0\,1\,0\,1\,1\,0\,0) & a_{13} = & (1\,1\,0\,1\,0\,0\,1) \\
a_6 = & (0\,1\,1\,0\,0\,0\,1) & a_{14} = & (1\,1\,1\,0\,1\,0\,0) \\
a_7 = & (0\,1\,1\,1\,0\,1\,0) & a_{15} = & (1\,1\,1\,1\,1\,1\,1)
\end{array}
$$

$\rightarrow$ Überprüfen der Eigenschaften!

$\rightarrow$ (n, l, d_{min})Linearkode

Darstellung von Linearkodes durch Matrizen

Definition 4.3

Ein Linearkode A mit $L = 2^l$ Kanalkodewörtern ist durch seine **Generatormatrix** G mit l *linear unabhängigen* Kanalkodewörtern (Basiswörtern) eindeutig beschrieben:

$$G_{l \times n} = \begin{pmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ u_{21} & u_{22} & \dots & u_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ u_{l1} & u_{l2} & \dots & u_{ln} \end{pmatrix} ; \; u_{i,j} \in \{0, 1\} \, .$$

$\rightarrow$ Mit einer Einheitsmatrix über den ersten l Spalten der Generatormatrix sind die zugehörigen Kanalkodewörter mit Sicherheit linear unabhängig.

Darstellung der Generatormatrix

Kanonische oder **reduzierte Staffelform**

$$G_{l\times n} = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & u_{1,l+1} & u_{1,l+2} & \dots & u_{1n} \\ 0 & 1 & 0 & \dots & 0 & u_{2,l+1} & u_{2,l+2} & \dots & u_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & u_{l,l+1} & u_{l,l+2} & \dots & u_{ln} \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & c_{11} & c_{12} & \dots & c_{1k} \\ 0 & 1 & 0 & \dots & 0 & c_{21} & c_{22} & \dots & c_{2k} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & c_{l1} & c_{l2} & \dots & c_{lk} \end{pmatrix} = [\, I_l \; C \,]$$

Beispiel Fortsetzung: $A \rightarrow G_{l\times n}$

Systematischer Kode

Definition 4.4

Ein Linearkode heißt **systematischer Kode**, wenn aus einem Kanalkodewort $a_i \in A$ durch Streichen redundanter Stellen das Quellenkodewort $a_i^* \in A^*$ unmittelbar entnommen werden kann.

Bildung eines Kanalkodewortes – Kanalkodierung

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

$$(u_{i1} u_{i2} \ldots u_{in}) = (u_{i1} u_{i2} \ldots u_{il}) \begin{pmatrix} 1 & 0 & 0 \ldots 0 & c_{11} & c_{12} & \ldots & c_{1k} \\ 0 & 1 & 0 \ldots 0 & c_{21} & c_{22} & \ldots & c_{2k} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 \ldots 1 & c_{l1} & c_{l2} & \ldots & c_{lk} \end{pmatrix}$$

Beispiel Fortsetzung: $a^* = (0101) \to a = ?$

Kontrollmatrix

Aufbau einer Kontrollmatrix (aus der Generatormatrix):

Ein zu A **orthogonal**er Unterraum A' ist dadurch gekennzeichnet, dass das Skalarprodukt eines beliebigen Vektors aus A mit jedem beliebigen Vektor aus A' Null ist.

Es sei

$a_i = (u_{i1}\, u_{i2} \ldots u_{in})$ mit $a_i \in A$ und

$a'_j = (u_{j1}\, u_{j2} \ldots u_{jn})$ mit $a'_j \in A'$.

Dann gilt

$$a_i \cdot a'_j = u_{i1} \cdot u_{j1} \oplus u_{i2} \cdot u_{j2} \oplus \ldots \oplus u_{in} \cdot u_{jn} = 0 \qquad \text{für alle} \quad i,\, j\,.$$

▷ Ist $G = [\, I_l\, C\,]$ dann ist der zu A orthogonale Unterraum A' durch $H = [\, C^T\, I_k\,]$ beschrieben.

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

Beispiel Fortsetzung: $G_{l \times n} \;\rightarrow\; H_{k \times n}$

Kontrollmatrix: Bestimmungsgleichungen

Kontroll(auch **Prüf-**)**matrix** liefert auch Vorschrift zur Bildung der Kontrollstellen k_j (Bestimmungsgleichungen):

$$a_i \cdot a_1'^T = u_{i1} \cdot c_{11} \oplus u_{i2} \cdot c_{21} \oplus ... \oplus u_{il} \cdot c_{l1} \oplus u_{i,l+1} \cdot 1 \oplus u_{i,l+2} \cdot 0 \oplus ... \oplus u_{in} \cdot 0$$
$$= 0 \,.$$

Erstes Kontrollelement $u_{i,l+1} = k_{[i,]1}$ des Kanalkodewortes a_i:

$$u_{i,l+1} = k_{[i,]1} = u_{i1} \cdot c_{11} \oplus u_{i2} \cdot c_{21} \oplus ... \oplus u_{il} \cdot c_{l1}$$

Allgemein:

$$u_{i,l+j} = \mathbf{k_{[i,]j}} = u_{i1} \cdot c_{1j} \oplus u_{i2} \cdot c_{2j} \oplus ... \oplus u_{il} \cdot c_{lj} \quad (j = 1, 2, ..., k)$$

für $a_i = (u_{i1} u_{i2} \dots u_{il} \; u_{i,l+1} u_{i,l+2} \dots u_{i,l+k}) = (l_1 \, l_2 \dots l_l \, k_1 \, k_2 \dots k_k)$

Beispiel Fortsetzung: Bestimmungsgleichungen für k_j $(j = 1, 2, ..., k)$

$a^* = (0101) \rightarrow a = ?$

[Begleitbuch, S. 142 - 151]

Fehlererkennung und Fehlerkorrektur – Kanaldekodierung

- Die Empfangsfolge b kann als Überlagerung eines Kanalkodewortes a_i mit einem Fehlerwort e aufgefasst werden:

  $$b = a_i \oplus e\,.$$

  Damit gilt für das **Fehlersyndrom** (auch Prüfvektor)

  $$s = H \cdot b^T = H \cdot (a_i \oplus e)^T = \underbrace{H \cdot a_i^T}_{\mathbf{0}} \oplus H \cdot e^T = H \cdot e^T\,.$$

- Alle Fehlermuster, deren Gewicht $w(e) \leq d_{min} - 1$ ist, sind mit Sicherheit erkennbar.
- Alle Fehlermuster, deren Gewicht $w(e) \leq \lfloor \frac{d_{min}-1}{2} \rfloor$ ist, sind mit Sicherheit korrigierbar.
- Darüber hinaus sind nur Fehlermuster erkennbar, die nicht in A definiert sind, d. h. $e \notin A$.
- Ist $e \notin A$ und $w(e) > \lfloor \frac{d_{min}-1}{2} \rfloor$ erfolgt eine Falschkorrektur oder Rekonstruktionsversagen.

Fehlererkennung und Fehlerkorrektur – Kanaldekodierung

- Empfangsfolge $b \in A$?

  $s = H_{k \times n} \cdot b^T$ (auch: Kontrollgleichungen für s_j $(j = 1, 2, ..., k)$)

  $s = \mathbf{0}$: $b \in A$

  $\rightarrow$ fehlerfreie Übertragung oder

  $\rightarrow$ kein erkennbarer Fehler

  $s \neq \mathbf{0}$: $b \notin A$ $\rightarrow$ Fehlererkennung, Korrektur?

- Jedem Fehlersyndrom ist maximal ein Fehlermuster zugeordnet, solange $w(e) \leq \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$.
- Die Syndrome sind k-stellige Vektoren. Also können $(2^k - 1)$ verschiedene Fehlermuster korrigiert werden.

Beispiel Fortsetzung: $b = (1100101) \in A$?

Kontrollgleichungen für s_j $(j = 1, 2, ..., k)$

[Begleitbuch, S. 152 - 154]

„Einfachster“ Linearkode: Paritätskode

Paritätskode

$$a_i^* = (u_{i1}\, u_{i2} \ldots u_{il}) \;\;\rightarrow\;\; a_i = (u_{i1}\, u_{i2} \ldots u_{il}\, u_{i,l+1})$$

$u_{i,l+1}$ – Paritätselement:

$$u_{i,l+1} = \sum_{j=1}^{l} u_{ij} \bmod 2 \quad \text{(Ergänzung auf geradzahlige Anzahl Eins)}$$

d_{min} ?

Generatormatrix $G_{(n-1)\times n}$?

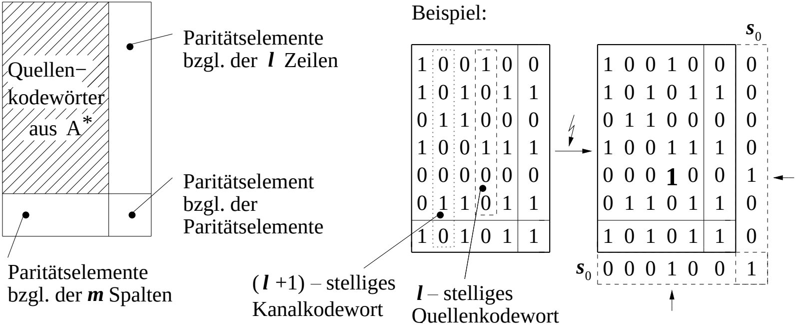
Kontrollmatrix $H_{1\times n}$?

Fehlererkennung: $s = H \cdot b^T = \sum_{j=1}^{n} u_j \bmod 2\,,\; s \neq 0 :\; b \notin A$

Anwendung: DÜ in Rechnern, Erweiterung von Kodes, RAID5

Verkettung von zwei Paritätskodes

$\rightarrow \quad (n_1 \cdot n_2, l_1 \cdot l_2, d_{min,1} \cdot d_{min,2})$Produktkode



$\rightarrow \; (6 \cdot 7, 5 \cdot 6, 2 \cdot 2) = (42, 30, 4)$Produktkode, $R = \frac{30}{42} = 0,71$

Zum Vergleich: $(4, 1, 4)$Wiederholungskode, $R = \frac{1}{4} = 0,25$

Fehlerkorrigierender HAMMING-Kode

Fehlerkorrigierender HAMMING-Kode

Definition 4.5

Der fehlerkorrigierende HAMMING-Kode ist ein spezieller linearer Gruppenkode und bzgl. der HAMMING-Schranke ein dichtgepackter Kode. Er hat einen minimalen HAMMING-Abstand von $d_{min} = 3$ und eine Kodewortlänge von $n = 2^k - 1$.

- Man bezeichnet diesen Kode auch als *einfehlerkorrigierenden* HAMMING-Kode.
- **Geschickte Vertauschung der Spalten von** H, so dass die i-te Spalte von H der Dualdarstellung von i entspricht. Das Fehlersyndrom s liefert dann unmittelbar die dual dargestellte Position des fehlerhaften Elementes in b.

Fehlerkorrigierender HAMMING-Kode: Kontrollmatrix

- Kontrollmatrix eines $(7,4)$HAMMING-Kodes:

$$H_{3\times 7} = \begin{array}{c} \begin{array}{ccccccc} n_7 & n_6 & n_5 & n_4 & n_3 & n_2 & n_1 \end{array} \\ \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \\ \begin{array}{ccccccc} l_4 & l_3 & l_2 & k_3 & l_1 & k_2 & k_1 \end{array} \end{array}$$

$\rightarrow$ Kontrollstellen an Positionen n_{2^i} $(i = 0, 1, ...)$ $\rightarrow$ systematisch!

$\rightarrow$ Berechnen der Kontrollstellen mittels den Bestimmungsgleichungen k_j $(j = 1, 2, ..., k)$ aus H $\rightarrow$ $a = ([...]l_4 l_3 l_2 k_3 l_1 k_2 k_1)$

- $s = H \cdot b^T$ bzw. Kontrollgleichungen s_j $(j = 1, 2, ..., k)$ aus H
  Ein Fehler wird durch $s = (s_k s_{k-1} ... s_1)^T$ lokalisiert und damit korrigiert.

Beispiel $a^* = (1001) \rightarrow a =? \rightarrow b = a \oplus (0010000) \rightarrow b^* =?$

Verkürzter HAMMING-Kode

Für k Kontrollstellen sind maximal $n = 2^k - 1$ verschiedene Syndrome möglich und damit maximal $n = 2^k - 1$ Stellen bzgl. Einfachfehler korrigierbar.

$l = 2^k - 1 - k$ liefert einen dichtgepackten Kode
(HAMMING-Schranke mit „=“ erfüllt),

$l < 2^k - 1 - k$ einen verkürzten Kode mit $n < 2^k - 1$.

Das Korrekturschema des einfehlerkorrigierenden HAMMING-Kodes lässt sich auch dann anwenden.

Beispiel

$(7,4)$HAMMING-Kode $\rightarrow$ verkürzter $(6,3)$HAMMING-Kode

Überprüfe mit HAMMING-Schranke!

Erweiterter HAMMING-Kode

- Jedem Kanalkodewort wird ein weiteres Kontrollelement k_0 hinzugefügt.
- Dieses Kontrollelement wird durch eine zusätzliche Bestimmungsgleichung berechnet, die sämtliche Kodewortelemente einbezieht:

  $a = ([...]l_4 l_3 l_2 k_3 l_1 k_2 k_1 k_0) = ([...]n_7 n_6 n_5 n_4 n_3 n_2 n_1 n_0)$ mit

  $n_0 = \sum_{i=1}^{n} n_i \bmod 2$; zusätzl. Kontrollgleichung: $s_0 = \sum_{i=0}^{n} n_i \bmod 2$.

  → Paritätsbit

  → Erzeugt Kanalkode mit geradzahliger Parität
- Die Anzahl der Kontrollelemente beträgt damit $k+1$, die Kodewortlänge erhöht sich auf $n \leq 2^k$. Der Minimalabstand ist $d_{min} = 4$.
- Die Anzahl der Informationselemente ist unverändert.

Beispiel $a^* = (1001) \rightarrow a = ?$

$b = (11011001) \in A$? → Auswertung von s und s_0

[Begleitbuch, S. 156 - 161]

Zyklische Kodes

Zyklische Kodes $\rightarrow$ Binäre primitive BCH-Kodes

Definition 4.6

Ein Kode heißt **zyklisch**, wenn für jedes Kanalkodewort

$a_i = (u_{i,n-1}\, u_{i,n-2} \ldots u_{i1}\, u_{i0})$

durch zyklische Verschiebung der Elemente mit

$a_j = (u_{i,n-2}\, u_{i,n-3} \ldots u_{i0}\, u_{i,n-1})$

wieder ein Kanalkodewort entsteht. [a]

[a] $a_j(x) = a_i(x)\, x^z \bmod (x^n + 1)$ ersetzt Exponenten $r \geq n$ durch $r \bmod n$.

Ein zyklischer Kode ist ein **spezieller Linearkode**, der sowohl algebraische Gruppenaxiome als auch Ring- und Körperaxiome erfüllt.

Das **Generatorpolynom** $g(x)$ ist i. Allg. ein Produkt von Minimalpolynomen $m_i(x)$, das den zyklischen Kode vollständig beschreibt. $g \in A$!

Hinweis: Schreibweise von Polynomen

$P(x) = u_r x^r + u_{r-1} x^{r-1} + \ldots + u_0$ mit $u_i \in \{0, 1\}$

Ausgewählte algebraische Grundlagen

- Eigenschaften eines Modularpolynoms über $GF(2)$

1. Das Modularpolynom muss irreduzibel sein.

- ▷ Ein Polynom ist **irreduzibel**, wenn es nicht in ein Produkt von Polynomen zerlegbar ist.
- ▷ Das Modularpolynom $M(x)$ vom Grad $k_1 = \text{grad}\, M(x)$ bestimmt den Kodeparameter n mit

  $n \leq 2^{k_1} - 1\,.$
- ▷ Der tatsächliche Wert von n berechnet sich aus dem **Zyklus der Polynomreste** über $GF(2)$ mit

  $x^i \bmod M(x) \quad (i = 0, 1, ..., p)$

  und bestimmt $\; n = p \,|\, 2^{k_1} - 1\,.$

Beispiel $M(x) = x^3 + x^2 + 1$

Ausgewählte algebraische Grundlagen

2. Ist

$$n = p = 2^{k_1} - 1\,,$$

dann besitzt das **irreduzible Polynom** $M(x)$ **auch** die Eigenschaft, **primitiv** zu sein.

- **Erweiterungskörper und Minimalpolynome**

  Die Leistungsfähigkeit eines BCH-Kodes hängt von der **Anzahl aufeinanderfolgender Nullstellen in** $g(x)$ ab. $\rightarrow$ Nullstellen?

Beispiel

$P(x) = x^4 + x + 1$ über $GF(2)$, primitiv:

$P(x=1) = 1\,;\;\; P(x=0) = 1$

Das Polynom $P(x)$ hat über $GF(2)$ keine Nullstelle.

Fundamentalsatz der Algebra

Jedes Polynom hat mindestens eine Nullstelle, gegebenenfalls in einem anderen Körper, und jedes Polynom r-ten Grades lässt sich in genau r Teilpolynome ersten Grades, d. h. in r Linearfaktoren, zerlegen, i. Allg. unter Zuhilfenahme von Erweiterungselementen α_i:

$$\begin{aligned} P(x) &= u_r x^r + u_{r-1} x^{r-1} + ... + u_1 x + u_0 \\ &= (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_r). \end{aligned}$$

Ein neues Element α wird als Nullstelle eines irreduziblen Polynoms über $GF(2)$ hinzugefügt, welches einem Erweiterungskörper angehört.

Auf der Grundlage eines irreduziblen Modularpolynoms $M(x)$ vom Grad $k_1 = \text{grad}\, M(x)$ über $GF(2)$ entsteht durch Hinzunahme einer Nullstelle α ein endlicher Erweiterungskörper $GF(2^{k_1})$, d. h., α ist Nullstelle von $M(x)$ und ein (Erweiterungs-)Element in $GF(2^{k_1})$.

Erweiterungskörper $GF(2^{k_1})$

Zum Erweiterungskörper $GF(2^{k_1})$ gehören neben dem Nullelement die Elemente $\alpha^i \;\; (i = 0, 1, ..., (2^{k_1} - 2))$.

Beispiel $M(x) = x^3 + x^2 + 1$ über $GF(2)$

Bestimmung des Erweiterungskörpers $GF(2^3)$:

Elemente des $GF(2^3)$	Polynomreste α^i mod $M(x = \alpha)$	Koeffizienten der Polynomreste
Nullelement	0	0 0 0
α^0	1	0 0 1
α^1	α	0 1 0
α^2	α^2	1 0 0
α^3	$\alpha^2 + 1$	1 0 1
α^4	$\alpha^2 + \alpha + 1$	1 1 1
α^5	$\alpha + 1$	0 1 1
α^6	$\alpha^2 + \alpha$	1 1 0
α^7	1	0 0 1

$\rightarrow$ isomorph dem Zyklus der Polynomreste über $GF(2)$

Erweiterungskörper $GF(2^{k_1})$

Berechnungsbeispiele für Addition und Multiplikation im $GF(2^3)/x^3+x^2+1$:

- $\alpha^i + \alpha^j = \alpha^i \,\mathsf{mod}\, M(\alpha) + \alpha^j \,\mathsf{mod}\, M(\alpha) = \alpha^k$

  $i = j: \quad \alpha^i + \alpha^j = 0$

  Z. B. $\alpha^5 + \alpha^2 = \alpha + 1 + \alpha^2 = \alpha^4$ bzw.
  $\alpha^5 + \alpha^2 = (011) \oplus (100) = (111) = \alpha^4$
  $\alpha^2 + \alpha^2 = (100) \oplus (100) = 0$

  $\alpha^3 + \alpha^4 = ? \qquad \alpha + \alpha^6 = ?$

- $\alpha^i \cdot \alpha^j = \alpha^{(i+j)\,\mathsf{mod}\,p}$

  Z. B. $\alpha^4 \cdot \alpha^5 = \alpha^{9\,\mathsf{mod}\,7} = \alpha^2$

  $\alpha^2 \cdot \alpha^6 = ? \qquad \alpha^5 \cdot \alpha^6 \cdot \alpha^4 = ?$

Erweiterungskörper $GF(2^{k_1})$

Beispiel $M(x) = x^3 + x^2 + 1$

α Nullstelle von $M(x)$ und Erweiterungselement:

$M(x = \alpha) = \alpha^3 + \alpha^2 + 1 = (\alpha^2 + 1) + \alpha^2 + 1 = 0$

Fundamentalsatz der Algebra:

$M(x) = x^3 + x^2 + 1 = (x + \alpha_1)(x + \alpha_2)(x + \alpha_3)$ im $GF(2)$,

d. h., $\alpha_1 = \alpha^1$, α_2 und α_3 sind Nullstellen im $GF(2^3)$.

Zuordnung α_j zu den Elementen von $GF(2^{k_1})$:

$\alpha_j = \alpha^{2^{j-1} i \,\mathbf{mod}\, p}$ $\quad (j = 1, 2, \ldots, k_1 (= \text{grad}\, M(x)))$

- ▷ Die Elemente $\alpha^{2^0 i}, \alpha^{2^1 i}, \ldots, \alpha^{2^{k_1 - 1} i \bmod p}$ sind im Zyklus i $(i = 0, 1, \ldots, 2^{k_1} - 2)$ zueinander konjugiert.
- ▷ Konjugierte Elemente befinden sich in einem **Zyklus**.

Erweiterungskörper $GF(2^{k_1})$

Die Nullstellen von $M(x)$ sind damit die im Zyklus $i = 1$ stehenden zu α^1 konjugierten Elemente $\alpha_2 = \alpha^2$ und $\alpha_3 = \alpha^4$.

$i = 2$ und $i = 4$ liefern demzufolge den gleichen Zyklus.

- ▷ Die Anzahl der Elemente in einem Zyklus wird durch $k_1 = \mathrm{grad}\, M(x)$ begrenzt und ist für $p = 2^{k_1} - 1 \in \mathbb{P}$ für alle Zyklen gleich (ausgenommen: $i = 0$).

Beispiel Zyklen im $GF(2^3)$:

α^0

$\alpha^1, \alpha^2, \alpha^4$

$\alpha^3, \alpha^6, \alpha^5$

Minimalpolynome

Jedem α^i aus $GF(2^{k_1})$ ist ein **Minimalpolynom** $m_i(x)$ zugeordnet:

- ▷ Das Minimalpolynom eines beliebigen Elementes α^i ist irreduzibel und vom Grad $r \leq k_1$.
- ▷ Zu jedem Element α^i existiert genau ein Minimalpolynom $m_i(x)$.
- ▷ Das Minimalpolynom des Elementes α^i ist gleichzeitig das Minimalpolynom der Elemente $\alpha^{2^1 i}$, $\alpha^{2^2 i}$, ..., $\alpha^{2^{r-1} i \bmod p}$.
- ▷ Ist α^i eine Nullstelle des Minimalpolynoms $m_i(x)$, dann sind die r zueinander konjugierten Elemente α^i, $\alpha^{2^1 i}$, $\alpha^{2^2 i}$, ..., $\alpha^{2^{r-1} i}$ die sämtlichen Nullstellen von $m_i(x)$:

  $$m_i(x) = (x + \alpha^i)(x + \alpha^{2^1 i})(x + \alpha^{2^2 i})...(x + \alpha^{2^{r-1} i}) \text{ im } GF(2)\,.$$
- ▷ Das Modularpolynom $M(x)$ ist wegen $M(x = \alpha^1) = 0$ das Minimalpolynom $m_1(x)$ des Elementes α^1.

Beispiel $m_0(x)$, $m_1(x)$, $m_3(x)$ im $GF(2^3)/M(x) = x^3 + x^2 + 1$?

[Begleitbuch, S. 162 - 169]

Generatorpolynom primitiver BCH-Kodes

$\rightarrow$ zur Kodierung und Fehlererkennung

$\rightarrow g(x) = f(d_E, M(x))$; auch: $g(x) = f(d_E, l)$, $M(x) = ?$

Entwurfsabstand d_E und $M(x)$ bestimmen Wahl der Kodeparameter!

Notwendig:

- **Erweiterungskörper** $GF(2^{k_1})$:
  Wenn $M(x)$ **primitiv** ist und α als Nullstelle hat, dann gilt
  $GF(2^{k_1}) = \{0, \alpha^0, \alpha^1, \alpha^2, ..., \alpha^{2^{k_1}-2}\}$.
- Ein **Minimalpolynom** $m_i(x)$ hat $\alpha^i, \alpha^{2i}, \alpha^{4i}, ...$ als Nullstellen:
  $m_i(x) = (x + \alpha^i)(x + \alpha^{2i})(x + \alpha^{4i}) ...$ im $GF(2)$.
  Daraus folgt: $m_i(x) = m_{2i}(x) = m_{4i}(x) = ... = m_{2^{r-1}i \bmod p}$, $r \leq k_1$.
- Das Generatorpolynom $g(x)$ hat die **Aufeinanderfolge von** $\alpha^\mu, \alpha^{\mu+1}, \alpha^{\mu+2}, ..., \alpha^{\mu+d_E-2}$ als **Nullstellen**, so auch $\forall i. a_i \in A \setminus \mathbf{0}$.

Generatorpolynom primitiver BCH-Kodes

Damit ein BCH-Kode *die* aufeinanderfolgenden Elemente α^i $(i = \mu, \mu+1, ..., \mu+d_E-2)$ als Nullstellen enthält, wird $g(x)$ i. Allg. ein Produkt von Minimalpolynomen sein:

$$g(x) = \textbf{kgV}\,\{m_\mu(x), m_{\mu+1}(x), ..., m_{\mu+d_E-2}(x)\}$$

(in praktischen Anwendungsfällen ist μ meist 0 oder 1).

Kodeparameter

$n = 2^{k_1} - 1$, weil $M(x)$ primitiv

$k = \text{grad}\, g(x)$

$l = n - k$

$d_{min[,tatsächlich]} \geq d_E$

Über die Zyklendarstellung kann die tatsächliche Aufeinanderfolge der Nullstellen bestimmt und damit der **tatsächliche Abstand** d_{min} ermittelt werden:

$d_{min} = (\text{tatsächliche Anzahl aufeinanderfolgender Nullstellen}) + 1$

Generatorpolynom primitiver BCH-Kodes

Beispiel $M(x) = x^4 + x + 1$, primitiv

Bildung von $g(x)$

- Bestimmen möglicher Generatorpolynome $g(x)$ aus den Zyklen der Exponenten von α für $\mu = 1$ bzw. 0!
- $g(x)$ für $d_E = 4\,?$

Analysiere $g(x)$ bzgl. d_{min} und den Kodeparametern

- $g(x) = x^8 + x^7 + x^6 + x^4 + 1$
- $(31, 21)$BCH-Kode (grad $M(x) = ?$)

[Begleitbuch, S. 175 - 179]

Spezielle BCH-Kodes: CRC[cyclic redundancy check]-Kodes

Zyklischer HAMMING-Kode

$g(x) = M(x) = m_1(x) \quad \rightarrow d_{min} = 3:$

mit Sicherheit Erkennen von Ein- und Zweifachfehlern $(f_e = 2)$

UND

Erkennen von Bündelfehlern der Länge $f_b \leq k = k_1 = \text{grad}\, M(x)$

Kodeparameter?

$(n, l, d_{min}) = (2^{k_1} - 1, 2^{k_1} - 1 - k_1, d_{min} = 3)$BCH-Kode

ABRAMSON-Kode

$g(x) = m_0(x)\, m_1(x)$ mit $m_0(x) = (x + 1)$

$\rightarrow d_{min} = 4$ mit $f_e = 3,\ f_b \leq k = k_1 + 1$

$\rightarrow (2^{k_1} - 1, 2^{k_1} - 1 - (k_1 + 1), d_{min} = 4)$BCH-Kode

Beispiel Kodeparameter im $GF(2^5)$ für obige Kodes

(Kanal-)Kodierung: Bildungsverfahren für $a \in A$

- **Multiplikationsverfahren**

  Ein zyklischer Kode A der Länge n ist durch $g(x)$ beschrieben. Das Kodepolynom $a(x)$ des Kanalkodewortes a entsteht aus der Multiplikation des zu kodierenden Polynoms $a^*(x)$ mit dem Generatorpolynom $g(x)$:

  $$a(x) = a^*(x)\, g(x)\,.$$

  Beispiel $g(x) = x^3 + x^2 + 1\,,\; a^* = (1011)\,,\; a = ?\,,\; a(x) = ?$

- **Divisionsverfahren**

  Ein zyklischer Kode A der Länge n ist durch $g(x)$ (vom Grad k) beschrieben. Das Kodepolynom $a(x)$ des Kodewortes a entsteht aus der Multiplikation des zu kodierenden Polynoms $a^*(x)$ mit x^k und der Subtraktion eines Restpolynoms $r(x)$ (bedeutet im $GF(2)$ Addition):

  $$a(x) = a^*(x)\, x^k + r(x)\,,\quad r(x) = (a^*(x)\, x^k) \bmod g(x)\,.$$

(Kanal-)Kodierung: Bildungsverfahren für $a \in A$

- **Generatormatrix**

  Auf der Grundlage des Generatorpolynoms $g(x) = x^k + u_{k-1}x^{k-1} + \ldots + u_0x^0$ ist eine Generatormatrix definiert:

$$G_{l \times n} = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 & u_{k-1} & \ldots & u_1 & u_0 \\ 0 & 0 & \ldots & 1 & u_{k-1} & u_{k-2} & \ldots & u_0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 1 & u_{k-1} & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & 0 \end{pmatrix}.$$

  Das Kanalkodewort $a \in A$ bildet sich dann wie folgt:

  $a = a^* \cdot G\,.$

▷ Die Bildungsverfahren führen auf das gleiche Kanalkodealphabet. Die Zuordnung der Quellenkodewörter zu den Kanalkodewörtern ist jedoch eine andere.

▷ Die Anwendung des **Divisionsverfahrens liefert immer einen systematischen Kode**.

▷ Das Bildungsverfahren muss dem Dekodierer bekannt sein.

(Kanal-)Dekodierung: Fehlererkennung

Jedes Kanalkodewort a muss in seiner Polynomdarstellung durch $g(x)$ teilbar sein.

Ist eine Empfangsfolge $b(x)$ durch $g(x)$ teilbar, dann ist $b \in A$ definiert, sonst gilt $b \notin A$ und damit Fehlererkennung.

▷ Fehlerpolynom (auch Prüfpolynom): $s(x) = b(x) \bmod g(x) = 0\,?$

Beispiel $a = (1011100)\,,\; e = (0011010)\,,\; b \in A\,?$

Mit Sicherheit erkennbar:

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

$\rightarrow f_b \leq k$

Erkennen aller **Bündelfehler** f_b, bei denen der Abstand zwischen dem ersten und dem letzten fehlerhaften Element (einschließlich dieser) im Fehlermuster kleiner oder gleich dem Grad k des Generatorpolynoms ist.

(Kanal-)Dekodierung: Fehlererkennung

Struktur des Bündelfehlers:

$$e(x) = 0\,x^{n-1} + 0\,x^{n-2} + ... + \mathbf{1}\,x^{i-1} + ... + \mathbf{1}\,x^{i-f_b} + 0\,x^{i-f_b-1} + ... + 0\,x^0$$
$$= x^{i-f_b}(\mathbf{1}\,x^{f_b-1} + u_{f_b-2}x^{f_b-2} + ... + u_1x^1 + \mathbf{1})$$

Sind darüber hinaus **weitere Fehler erkennbar?**

$$\frac{2^n - 2^l}{2^n} = 1 - 2^{-k} \quad \rightarrow \quad p_{FE} = (1 - 2^{-k}) \cdot 100\%$$

Beispiel: $k = 5: \; p_{FE} = 96,88\%$

$k = 8: \; p_{FE} = 99,61\%$

Typische Fehlererkennungs- = CRC-Kodes:

Zyklischer HAMMING-Kode: $g(x) = m_1(x)$

ABRAMSON-Kode: $g(x) = m_1(x)(x+1)$

[Begleitbuch, S. 169 - 175]

Verkürzte und erweiterte BCH-Kodes

Ein Kanalkode heißt **verkürzter Kode**, wenn gilt:
$(n, l, d_{min}) \rightarrow (n-?, l-?, d_{min})$, $k =$const.
Diese Kodes verlieren ihre zyklische Eigenschaft.
Fehlererkennung und Fehlerkorrektur bleiben erhalten.

Beispiel BCH-Kode für $l = 12$, $d_E = 5$?

Ein Kanalkode heißt **erweiterter Kode**, wenn

- das Generatorpolynom $g(x)$ mit $m_0(x) = (x + 1)$ erweitert wird:
  $(n < 2^{k_1} - 1, l, d_{min}) \rightarrow (n + 1, l, d_{min} + 1)$,
  $(n = 2^{k_1} - 1, l, d_{min}) \rightarrow (n, l - 1, d_{min} + 1)$.
- über $n = 2^{k_1} - 1$ ein Paritätsbit gesetzt wird.
  Vergleiche mit dem erweiterten HAMMING-Kode!

Die zyklische Eigenschaft geht mit $n \neq 2^{k_1} - 1$ verloren.

Beispiel Fortsetzung: Erweiterung mit $(x + 1)$

Anwendung zyklischer Kodes

- **Fehlererkennung** $\rightarrow$ CRC-Kodes
  z. B. in Protokollen auf der Sicherungsschicht:
  CRC-5 in USB ($g(x) = m_1(x)$), in Bluetooth $\left(g(x) = m_0(x)\, m_1(x)\right)$;
  CRC-CCITT (CRC-16, $g(x) = m_0(x)\, m_1(x)$) in HDLC, X.25, ... ;
  Ethernet benutzt CRC-32 für Standard-Frames $= 1518\, Byte$,
  Jumbo-Frames $\approx\ 9000\, Byte$ (extended Ethernet Frames) sind nicht standardisiert aber bieten vergleichbaren Schutz, warum:
  $g(x) = m_1^*(x) = m_7(x)$, primitiv, $a_i(x) = x^{91639} + x^{41678} + 1$,
  im Bereich $n < 91639\, Bit \approx 11545\, Byte$ nur $w(a_i) \geq 4$
  z. B. beim Mobilfunk: CRC-3 in Kodeverkettung zur Fehlerverdeckung
- **Fehlerkorrektur** ($\rightarrow$ LV Kanalkodierung)
  Sinnvoll bei der Satellitenkommunikation wegen der Laufzeiten oder in Speicher-Anwendungen, wenn einzelne Bereiche systematisch und unwiderruflich unbrauchbar sind.

[Begleitbuch, S. 182 - 184]

Zusammenfassung IKT

IKT-Teil begonnen mit

Informationstheorie beschäftigt sich mit zwei Problemstellungen
Praktikable Umsetzung mittels Kodierung

- Inwieweit lässt sich Information kompakt darstellen?
  - ▷ Quellenkodierung (verlustfreie QK: gleichmäßige Kodierung, SHANNON-FANO, HUFFMAN, Erweiterte Quellen, ...)
  - ▷ $R_K = l_{(m)} [\cdot H_K] - H_Q \to 0$
- Inwieweit überträgt man Information quasi fehlerfrei?
  - ▷ Kanalkodierung, abhängig vom Störverhalten des Übertragungskanals
    - ▷ Dimensionierung des Kanalkodes $R \leq H_T\,!$

□