CodT **Aufgabe 1: Wahrscheinlichkeitsmodell**

Regeln der Wahrscheinlichkeitsrechnung:

$$\sum_i p(i/j) = 1 \qquad \sum_j p(i/j) \neq 1 \qquad p(i\,j) = p(j)\cdot p(i/j) = p(i)\cdot p(j/i)$$

a) p(r)=3/8 p(g)=1/8 p(b)=4/8

b) p(w)=5/8 p(s)=3/8

c) Bedingte Wahrscheinlichkeit gezielt bezogen auf w oder s:

p(w/r)=2/3 p(w/g)=0 p(w/b)=3/4
p(s/r)=1/3 p(s/g)=1 p(s/b)=1/4

d) Verbundwahrscheinlichkeit, blind gewählt aus allen:

p(rw) = (3/8)·(2/3) =1/4 p(gw)=0 p(bw)=3/8 (Die Größen
p(rs) = (3/8)·(1/3) =1/8 p(gs)=1/8 p(bs)=1/8 sind abhängig)

CodT **Aufgabe 2: Informationsquelle Buchungsdaten**

a) Beschreibung als statistisch typische Folge: | **z z z z V z z z z V z z z z V T** |

p(z) = 12/16 = 3/4 = Wahrscheinlichkeit für irgend eine Ziffer
p = Hilfsgröße = Wahrscheinlichkeit für eine bestimmte Ziffer

$$\underbrace{\sum_{i=0}^{9} p(i) = p(z) = 10\cdot p}_{?}$$

p(V) = p(+) + p(-) = 1/4 p(z) = 5/2 p
p(T) = 1/12 p(z) = 5/6 p

Mit $\sum_{j=1}^{3} p(j) = 1$: 10 p + 5/2 p + 5/6 p = 1 ⇒ p = p(z)/10 = 3/40

b) p(V) = 2 p(+) = 2 p(-) = 5/2 p ⇒ p(+) = p(-) = 3/32

c) p(T) = 5/6 p ⇒ p(T) = 1/16

d) $$H = \sum_i p(i)\cdot \mathrm{ld}\frac{1}{p(i)} = 10\cdot\frac{3}{40}\cdot\mathrm{ld}\frac{40}{3} + 2\cdot\frac{3}{32}\cdot\mathrm{ld}\frac{32}{3} + \frac{1}{16}\cdot\mathrm{ld}16$$
Entropie

$$= \frac{3}{4}(\mathrm{ld}\,8 + \mathrm{ld}\,5 - \mathrm{ld}\,3) + \frac{3}{16}(\mathrm{ld}\,32 - \mathrm{ld}\,3) + \frac{1}{16}\mathrm{ld}16$$

= 3,693 bit/Sym ≈ 3,7 bit/Sym

CodT **Aufgabe 3: Nachrichtenquelle ohne Gedächtnis**

a) Entropie der Quelle S

$$H = \sum_{i=1}^{k} p_i\cdot\mathrm{ld}\frac{1}{p_i} \qquad H(S) = \frac{1}{2}\mathrm{ld}\,2 + 2\cdot\frac{1}{4}\mathrm{ld}\,4 = 1{,}5\ \text{bit/Sym}$$

b) Redundanz der Quelle $R_S = H_{max}(S) - H(S)$

Maximale Entropie ergibt sich dann, wenn alle drei Ereignisse gleich wahrscheinlich sind, hier mit p=1/3 :

$$H_{S\,max} = \sum_{i=1}^{3}\frac{1}{3}\mathrm{ld}\frac{1}{1/3} = 3\cdot\frac{1}{3}\mathrm{ld}\,3 = 1{,}585\ \text{bit/Sym}$$

$$H_S = \frac{1}{2}\mathrm{ld}\,2 + 2\cdot\frac{1}{4}\mathrm{ld}\,4 = \frac{1}{2}+\frac{1}{2}\cdot 2 = 1{,}5\ \text{bit/Sym}$$

$$R_S = H_{max}(S) - H(S) = 1{,}585 - 1{,}5 = 0{,}085\ \text{bit/Sym}$$

c) Erweitern der Quelle S durch Zusammenfassen zweier Symbole zur Quelle $\sigma(j)$

Symbole der erweiterten Quelle: $\sigma(j) = S(i1)S(i2)$
i1 = 1 . . 3 i2 = 1 . . 3 j = 1 .. 9

$\sigma_1 = (S_1S_1)$ $\sigma_2 = (S_1S_2)$ $\sigma_3 = (S_1S_3)$
$\sigma_4 = (S_2S_1)$ $\sigma_5 = (S_2S_2)$ $\sigma_6 = (S_2S_3)$
$\sigma_7 = (S_3S_1)$ $\sigma_8 = (S_3S_2)$ $\sigma_9 = (S_3S_3)$

d) Symbolwahrscheinlichkeiten der erweiterten Quelle. Die Quelle ist ohne Gedächtnis, ihre Zustände sind daher unabhängig: $p(\sigma_j) = p(Si_1)\cdot p(Si_2)$

$p(\sigma_1) = \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$ $p(\sigma_2) = \frac{1}{2}\cdot\frac{1}{4} = \frac{1}{8}$ $p(\sigma_3) = \frac{1}{2}\cdot\frac{1}{4} = \frac{1}{8}$

$p(\sigma_4) = \frac{1}{4}\cdot\frac{1}{2} = \frac{1}{8}$ $p(\sigma_5) = \frac{1}{4}\cdot\frac{1}{4} = \frac{1}{16}$ $p(\sigma_6) = \frac{1}{4}\cdot\frac{1}{4} = \frac{1}{16}$

$p(\sigma_7) = \frac{1}{4}\cdot\frac{1}{2} = \frac{1}{8}$ $p(\sigma_8) = \frac{1}{4}\cdot\frac{1}{4} = \frac{1}{16}$ $p(\sigma_9) = \frac{1}{4}\cdot\frac{1}{4} = \frac{1}{16}$

e) Entropie der erweiterten Quelle

$$H_\sigma = \frac{1}{4}\mathrm{ld}\,4 + 4\cdot\frac{1}{8}\mathrm{ld}\,8 + 4\cdot\frac{1}{16}\mathrm{ld}\,16 = \frac{1}{2}+\frac{3}{2}+1 = 3\text{bit/Sym}$$

Die Entropie ist gegenüber der einfachen Quelle verdoppelt: $H_\sigma = 2\cdot H_S$

f) Redundanz der erweiterten Quelle:

$$R_\sigma = 9\cdot\frac{1}{9}\mathrm{ld}\,9 - 3 = 3{,}17 - 3 = 0{,}17\ \text{bit/Sym}$$

Die Redundanz ist gegenüber der einfachen Quelle verdoppelt: $R_\sigma = 2\cdot R_S$

CodT Aufgabe 5: **Markoff-Quelle** mit zwei Symbolen

a) Ordnung m der Markoff-Quelle: Ein Zustand ist jeweils nur vom unmittelbar vorhergehenden Zustand abhängig, daher: $\underline{m = 1}$

b) Markoff-Diagramm

c) Symbolwahrscheinlichkeiten $p(S_0)$ und $p(S_1)$: $\quad p(S_0) + p(S_1) = 1$

für zulaufende Pfade: $\quad p(S_0) = p(S_0) \cdot p(S_0/S_0) + p(S_1) \cdot p(S_0/S_1)$

$p(S_1) = p(S_0) \cdot p(S_1/S_0) + p(S_1) \cdot p(S_1/S_1)$

Überbestimmung: eine Gleichung ist unnötig.

$$p(S_0) = p(S_0) \cdot \frac{3}{4} + p(S_1) \cdot \frac{1}{3} = p(S_0) \cdot \frac{3}{4} + [1 - p(S_0)] \cdot \frac{1}{3} = \frac{1}{3} \cdot \frac{12}{7} = \underline{\frac{4}{7}}$$

$p(S_1) = \underline{\frac{3}{7}}$ $\qquad$ Probe dazu: $p(S_1) = \frac{4}{7} \cdot \frac{1}{4} + \frac{3}{7} \cdot \frac{2}{3} = \frac{1}{7}(1+2) = \underline{\frac{3}{7}}$

d) **Übergangsentropien** (Zustandsentropien)

$$H(S_0) = \sum_i p(S_i/S_0) \cdot \mathrm{ld} \frac{1}{p(S_i/S_0)}$$

$$H(S_0) = \frac{3}{4} \mathrm{ld} \frac{4}{3} + \frac{1}{4} \mathrm{ld} 4 = 2 - \frac{3}{4} \mathrm{ld} 3 = \underline{0{,}8112 \text{bit/Sym}}$$

$$H(S_1) = \sum_i p(S_i/S_1) \cdot \mathrm{ld} \frac{1}{p(S_i/S_1)}$$

$$H(S_1) = \frac{1}{3} \mathrm{ld} 3 + \frac{2}{3} \mathrm{ld} \frac{3}{2} = 1 \cdot \mathrm{ld} 3 - \frac{2}{3} \mathrm{ld} 2 = \underline{0{,}9182 \text{bit/Sym}}$$

e) Entropie der Quelle $\qquad H_{MQ} = \sum_i p(S_i) \cdot H(S_i)$

$$H_{MQ} = \frac{4}{7} \cdot 0{,}8112 + \frac{3}{7} \cdot 0{,}9182 = \underline{0{,}8570 \text{bit/Sym}}$$

f) Wahrscheinlichkeit für die Folge $S_0 S_0 S_0$:

$$p(S_0 S_0 S_0) = p(S_0) \cdot p(S_0/S_0) \cdot p(S_0/S_0)$$

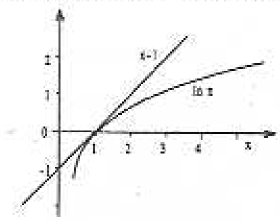
$$= \frac{4}{7} \cdot \frac{3}{4} \cdot \frac{3}{4} = \underline{0{,}3214}$$

CodT Aufgabe 4: **Quellenentropie H**

Weisen Sie unter Verwendung der Relationen $\quad \ln x \le x - 1$ und $\quad H(i) - \mathrm{ld}\, k = \Delta H$

formal nach, daß für die Quellenentropie $H(i)$ gilt: $\quad H(i) \le \hat{H}(i) = \mathrm{ld}\, k$.

Zu beweisende Behauptung: $\quad H \le \hat{H}, \quad \hat{H} = \mathrm{ld}\, k, \quad$ wobei k = Anzahl der Symbole.



$\ln x \le x - 1$

Das Kurvenbild zeigt: $\ln x$ bleibt stets unter $x-1$.

Untersuchung zum Verhalten der Entropie-Differenz $\quad \mathbf{\Delta H = H - ld\, k}$:

$$\Delta H = \sum_{i=1}^{k} p(i) \cdot \mathrm{ld} \frac{1}{p(i)} - \mathrm{ld}\, k \quad \text{mit der Eigenschaft: } \sum_{i=1}^{k} p(i) = 1 \text{ gilt dann:}$$

?

$$\Delta H = \sum_{i=1}^{k} p(i) \left(\mathrm{ld} \frac{1}{p(i)} - \mathrm{ld} k \right)$$

$$\Delta H = \sum_{i=1}^{k} p(i) \left(\mathrm{ld} \frac{1}{p(i)} + \mathrm{ld} \frac{1}{k} \right) \quad \text{und mit } \mathrm{ld}\, x = \mathrm{ld}\, e \cdot \ln x:$$

$$\Delta H = \mathrm{ld}\, e \cdot \sum_{i=1}^{k} p(i) \cdot \underbrace{\ln \frac{1}{k \cdot p(i)}}_{\text{"}\ln x\text{"}} \le \mathrm{ld}\, e \cdot \sum_{i=1}^{k} p(i) \cdot \underbrace{\left(\frac{1}{k \cdot p(i)} - 1 \right)}_{\text{"}x - 1\text{"}}$$

Das Gleichheitszeichen gilt für den Fall

$k \cdot p(i) = 1$, $\quad$ d.h., $\quad p(i) = \frac{1}{k}$, wenn alle Quellensymbole gleich wahrscheinlich sind.

Die Summe auf der rechten Seite

$$\sum_{i=1}^{k} p(i) \cdot \left(\frac{1}{k \cdot p(i)} - 1 \right) = \sum_{i=1}^{k} \left(\frac{1}{k} - p(i) \right) = \sum_{i=1}^{k} \frac{1}{k} - \sum_{i=1}^{k} p(i)$$

verschwindet, daher muß gelten: $\quad \mathbf{\Delta H = H - ld\, k \le 0}$

und somit $\quad \mathbf{H \le ld\, k} \quad$ mit $\mathbf{ld\, k = \hat{H}}$.

CodT **Aufgabe 7: Codierung für ein Fernsehsignal**

a) Wahrscheinlichkeit für das Auftreten der Amplitudenwerte:

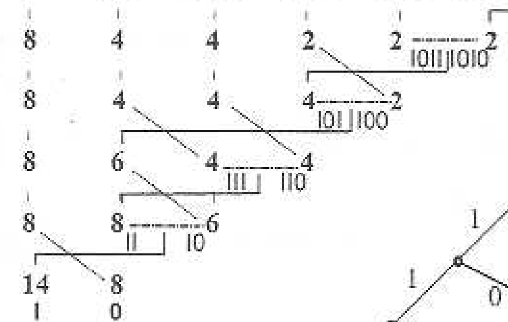
$$p(A_4)=2\cdot p(A_5)=2\cdot p(A_3)=4\cdot p(A_6)=4\cdot p(A_2)=8\cdot p(A_7)=8\cdot p(A_1)$$

$$p(A_4)+\frac{1}{2}p(A_4)\cdot 2+\frac{1}{4}p(A_4)\cdot 2+\frac{1}{8}p(A_4)\cdot 2=1$$

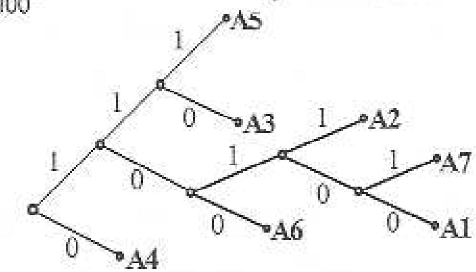
$$p(A_4)=\frac{4}{11}\qquad p(A_5)=p(A_3)=\frac{2}{11}\qquad p(A_6)=p(A_2)=\frac{1}{11}\qquad p(A_7)=p(A_1)=\frac{1}{22}$$

b) **Binärer Code,** Huffman - Codierung:

$p(A_4)$	$p(A_5)$	$p(A_3)$	$p(A_6)$	$p(A_2)$	$p(A_7)$	$p(A_1)$	
8	4	4	2	2	1	1	(x/22)
0	111	110	100	1011	10101	10100	**Code**

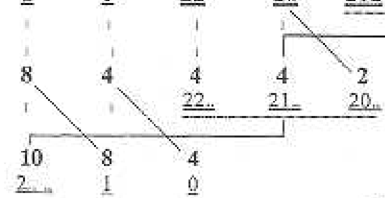


c) Codebaum

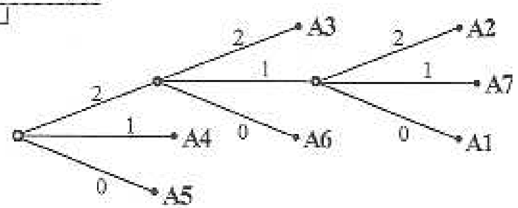


b) **Ternärer Code,** Huffman - Codierung:

$p(A_4)$	$p(A_5)$	$p(A_3)$	$p(A_6)$	$p(A_2)$	$p(A_7)$	$p(A_1)$	
8	4	4	2	2	1	1	(x/22)
1	0	22	20	212	211	210	**Code**

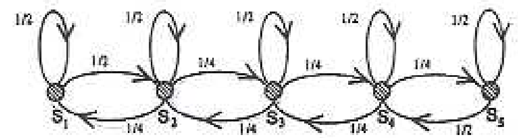


c) Codebaum



CodT Aufgabe 6: **Markoff-Quelle Temperaturfühler**

a) **Markoff-Diagramm**



b) **Übergangswahrscheinlichkeiten**

$$\underline{M}=\left(p(S_j/S_i)\right)=\begin{pmatrix} p(1/1) & p(2/1) & \cdots & p(5/1)\\ p(1/2) & p(2/2) & & \\ \vdots & & & \vdots \\ p(1/5) & & & p(5/5)\end{pmatrix}=\begin{pmatrix} 1/2 & 1/2 & 0 & 0 & 0\\ 1/4 & 1/2 & 1/4 & 0 & 0\\ 0 & 1/4 & 1/2 & 1/4 & 0\\ 0 & 0 & 1/4 & 1/2 & 1/4\\ 0 & 0 & 0 & 1/2 & 1/2\end{pmatrix}$$

Jede Zeile der Matrix bildet die ablaufenden Kanten eines Knotens ab.

c) **Ergodizität**

Die Markoff-Quelle liefert 5 verschiedene Symbole (Zustände) S_i.

Die Quelle hat die Ordnung m=1.

Zur Prüfung der Ergodizität werden hier die Kriterien herangezogen, die sich aus dem Markoff-Diagramm ablesen lassen:

- Das Markoff-Diagramm zerfällt nicht;
- alle Zustände können mit einer endlichen Wahrscheinlichkeit wieder eingenommen werden;
- der größte gemeinsame Teiler aller möglichen Zyklenlängen, d.h., Anzahl der Einschritt-Übergänge, ist gleich 1.

Die Quelle ist also ergodisch. ?

CodT **Aufgabe 8 : Codierung für einen Buchungsautomaten**

a) Huffman-Codierung

Quellensymbol	+	−	0	1	2	3	4	5	6	7	8	9	T
rel. Wkt. (/160)	15	15	12	12	12	12	12	12	12	12	12	12	10
Code	0+	−0	−−	−+	+0	+−	++	000	00−	00+	0−0	0−−	0−+

34 15 15 12 12 12 12 12 12 12 12

36 34 15 15 12 12 12 12 12

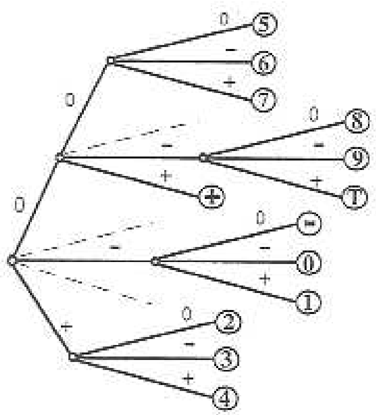
36 36 34 15 15 12 12

39 36 36 34 15

85 39 36

0 −U +U

b) Codebaum



d) Coderedundanz

$R_C = L \cdot \mathrm{ld}\, b - H_Q \qquad L = \sum_i p(i) \cdot l_i \qquad H = \sum_i p(i) \cdot \mathrm{ld}\frac{1}{p(i)}$

$$H_Q = \frac{8}{22} \cdot \mathrm{ld}\frac{22}{8} + 2 \cdot \frac{4}{22} \cdot \mathrm{ld}\frac{22}{4} + 2 \cdot \frac{2}{22} \cdot \mathrm{ld}\frac{22}{2} + 2 \cdot \frac{1}{22} \cdot \mathrm{ld}\frac{22}{1} = 2{,}4594 \text{ bit/Symbol}$$

$$L_{\text{binär}} = \frac{1}{22}[8 \cdot 1 + 4 \cdot 3 \cdot 2 + 2 \cdot 3 + 2 \cdot 4 + 1 \cdot 5 \cdot 2] = \frac{56}{22} = 2{,}5454 \text{ bit / Symbol}$$

$$L_{\text{ternär}} = \frac{1}{22}[8 \cdot 1 + 4 \cdot 1 + 4 \cdot 2 + 2 \cdot 2 + 2 \cdot 3 + 1 \cdot 3 \cdot 2] = \frac{36}{22} = 1{,}636 \text{ tt / Symbol}$$

$R_{C\text{binär}} = L_{\text{binär}} \cdot \mathrm{ld}2 - H_Q = 2{,}5454 - 2{,}4594 = \underline{0{,}0860 \text{ bit / Symbol}}$

! Beide Coderedundanzen werden mit der binären Einheit "bit/Symbol" dargestellt !

$R_{C\text{ternär}} = L_{\text{ternär}} \cdot \mathrm{ld}3 - H_Q = 1{,}636 \cdot 1{,}5849 - 2{,}4594 = 2{,}5928 - 2{,}4594 = \underline{0{,}1334 \text{ bit / Symbol}}$

Die Redundanz der ternären Codierung ist etwas größer als die des binären Codes.

Im Vergleich: Redundanz der Quelle

$$R_Q = \hat{H} - H_Q = \frac{7}{7}\mathrm{ld}7 - 2{,}4596 = \underline{0{,}3477 \text{ bit / Symbol}}$$

e) Unverzögerte und eindeutige Decodierbarkeit

Prüfung der Decodierbarkeit nach den folgenden Kriterien:
- Sind alle Codewörter gleich lang? -nein
- Sind Trennungszeichen vorhanden? -nein
- Ist kein Codewort Anfangsteil eines anderen? Bedingung ist erfüllt.
- Ist kein innerer Knoten des Codebaums besetzt? Bedingung ist erfüllt.

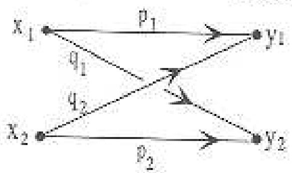
- Kriterium $\sum_{i=1}^{k} b^{-l_i} \leq 1$: mit b: Codebasis, l_i : Länge des i-ten Codesymboles
  Bedingung ist erfüllt.

Schluß: Beide Codes sind <u>unverzögert und eindeutig decodierbar</u>.

CodT **Aufgabe 9 : Kettenschaltung unsymmetrischer Kanäle**

a) **Kanalmatrix:**

Allgemein:



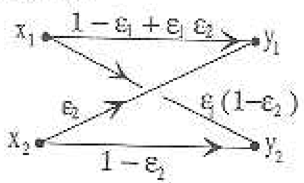
$$(K)=\begin{pmatrix} p(y_1/x_1) & p(y_2/x_1) \\ p(y_1/x_2) & p(y_2/x_2) \end{pmatrix}$$

$$(K)=\begin{pmatrix} p_1 & q_1 \\ q_2 & p_2 \end{pmatrix}=\begin{pmatrix} 1-q_1 & q_1 \\ q_2 & 1-q_2 \end{pmatrix}$$

Aus der Aufgabenstellung:

$$(p(y/x))=\begin{pmatrix} 1-\varepsilon_1 & \varepsilon_1 \\ 0 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ \varepsilon_2 & 1-\varepsilon_2 \end{pmatrix}$$

$$=\begin{pmatrix} 1-\varepsilon_1+\varepsilon_1\varepsilon_2 & \varepsilon_1\cdot(1-\varepsilon_2) \\ \varepsilon_2 & 1-\varepsilon_2 \end{pmatrix}$$



b) **Transinformation** (- im Mittel je Kanalsymbol übertragenene Information)

$T(x,y)=H(y)-H(y/x)$ Werte: $p(x_1)=p(x_2)=\frac{1}{2}$, $\varepsilon_1=\varepsilon_2=\frac{1}{2}$

$$H(y)=\sum_{i=1}^{2}p(y_i)\cdot \mathrm{ld}\frac{1}{p(y_i)}$$

mit: $p(y_1)=p(x_1)\cdot(1-\varepsilon_1+\varepsilon_1\varepsilon_2)+p(x_2)\cdot\varepsilon_2=\frac{5}{8}$

und $p(y_2)=p(x_1)\cdot(\varepsilon_1(1-\varepsilon_2))+p(x_2)\cdot(1-\varepsilon_2)=\frac{3}{8}$

$$H(y)=\frac{5}{8}\cdot\mathrm{ld}\frac{8}{5}+\frac{3}{8}\cdot\mathrm{ld}\frac{8}{3}\approx\underline{0{,}95\,\mathrm{bit/Symbol}}$$

$$H(y/x)=\sum_{i=1}^{2}p(x_i)\cdot\sum_{j=1}^{2}p(y_j/x_i)\cdot\mathrm{ld}\frac{1}{p(y_j/x_i)}$$

$$=p(x_1)\cdot\left((1-\varepsilon_1+\varepsilon_1\varepsilon_2)\cdot\mathrm{ld}\frac{1}{1-\varepsilon_1+\varepsilon_1\varepsilon_2}+\varepsilon_1\cdot(1-\varepsilon_2)\cdot\mathrm{ld}\frac{1}{\varepsilon_1\cdot(1-\varepsilon_2)}\right)$$

$$+p(x_2)\cdot\left(\varepsilon_2\cdot\mathrm{ld}\frac{1}{\varepsilon_2}+(1-\varepsilon_2)\cdot\mathrm{ld}\frac{1}{1-\varepsilon_2}\right)$$

$$=\frac{1}{2}\cdot\left(\frac{3}{4}\,\mathrm{ld}\frac{4}{3}+\frac{1}{4}\,\mathrm{ld}\,4\right)+\frac{1}{2}\cdot\left(\frac{1}{2}\,\mathrm{ld}\,2+\frac{1}{2}\,\mathrm{ld}\,2\right)\approx\underline{0{,}91\,\mathrm{bit/Symbol}}$$

30 c) : $\underline{T(x,y)}=H(y)-H(y/x)=0{,}95-0{,}91=\underline{0{,}04\ \mathrm{bit/Symbol}}$

CodT

zu Aufgabe 8

c) Wahrscheinlichkeiten der Codesymbole $p(+U)$, $p(0)$, $p(-U)$

$$p(b_v)=\frac{1}{L}\cdot\sum_{i=1}^{13}p(S_i)\cdot \ell_{iv}=\frac{L_v}{L} \qquad \text{mit} \qquad L=\sum_{i=1}^{13}p(S_i)\cdot\ell_i\ ,$$

d.h., die Anzahl der einzelnen Codesymbole wird zur Gesamtzahl der ausgegebenen Codesymbole ins Verhältnis gesetzt.

$$L=5\cdot\overset{p(0..4)}{\frac{12}{160}}\cdot2+5\cdot\overset{p(5..9)}{\frac{12}{160}}\cdot3+2\cdot\overset{p(+)=p(-)}{\frac{15}{160}}\cdot2+\overset{p(T)}{\frac{10}{160}}\cdot3=\frac{390}{160}=\underline{2{,}438\ \mathrm{tt/symbol}}$$

$$p(+U)=\frac{1}{L}\left[\frac{12}{160}\cdot(1+1+1+2+1)+\frac{10}{160}\cdot1+\frac{15}{160}\cdot1)\right]=\frac{97}{390}=\underline{0{,}249}$$

$$p(0)=\frac{1}{L}\left[\frac{12}{160}\cdot(1+3+2+2+2+1)+\frac{10}{160}\cdot1+\frac{15}{160}\cdot(1+1)\right]=\frac{172}{390}=\underline{0{,}441}$$

$$p(-U)=\frac{1}{L}\left[\frac{12}{160}\cdot(2+1+1+1+1+2)+\frac{10}{160}\cdot1+\frac{15}{160}\cdot1)\right]=\frac{121}{390}=\underline{0{,}310}$$

$\Sigma=1$

d) Decodierbarkeit

1.) Kein Codewort ist Anfangsteil eines anderen - oder

2.) Kriterium $\sum_{i=1}^{13}b^{-\ell_i}\le1$:

Probe: $\sum_{i=1}^{13}3^{-\ell_i}=7\cdot3^{-2}+6\cdot3^{-3}=\frac{7}{9}+\frac{6}{27}=\underline{1}$

Beide Kriterien bestätigen: eindeutige und unverzögerte Decodierbarkeit.

e) Coderedundanz $R_C=H_C-H_S=L\cdot\mathrm{ld}\,b-H_S$

($\underline{\mathrm{ld}\,b}$ bewirkt Umrechnung auf binäre Basis)

mit $H_Q=10\cdot\frac{3}{40}\cdot\mathrm{ld}\frac{40}{3}+2\cdot\frac{3}{32}\cdot\mathrm{ld}\frac{32}{3}+\frac{1}{16}\cdot\mathrm{ld}\,16=3{,}6923\ \mathrm{bit/Symbol}$:

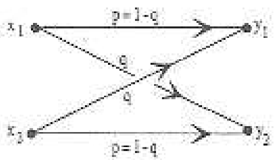
$R_{Cbin}=H_C-H_Q=\mathrm{ld}\,3\cdot L-H_Q=\underline{0{,}171\ \mathrm{bit/Symbol}}$

oder

$R_{Cter}=\qquad =L-\frac{1}{\mathrm{ld}\,3}\cdot H_Q=2{,}438-\frac{3{,}6923}{1{,}5849}=\underline{0{,}1094\ \mathrm{tt/Symbol}}$?

CodT **Aufgabe 11 : Maximale Transinformation am symmetrischen Binärkanal**

Bestimmen Sie analytisch für einen symmetrisch gestörten Binärkanal, bei welchen Wahrscheinlichkeiten der Eingangssymbole x_1, x_2 die Transinformation $T(x,y)$ am größten ist: $T = T_{max}(x,y)$ oder Symbolkapazität des Kanals.



$q = q_1 = q_2 \qquad p(x_2) = 1 - p(x_1)$

kürzende Schreibweise:
$p(x_1) = \chi \quad p(x_2) = 1 - \chi$

Lösung:

Geeignete Beziehungen zur Berechnung der **Transinformation** $T(x,y)$:

(20 a) $\quad T(x,y) = H(x) + H(y) - H(xy)$
(30 b) $\quad T(x,y) = H(x) - H(x/y)$
(30 c) $\quad T(x,y) = H(y) - H(y/x)$

Für die Bestimmung des Maximums von T(x) wird die Beziehung (30 b) gewählt.

$$H(x) = \chi \cdot \mathrm{ld}\frac{1}{\chi} + (1-\chi) \cdot \mathrm{ld}\frac{1}{(1-\chi)}$$

$$H(x/y) = \sum_{j=1}^{2} p(y_j) \cdot \sum_{i=1}^{2} p(x_i/y_j) \cdot \mathrm{ld}\frac{1}{p(x_i/y_j)}$$

mit $\quad p(y_1) = \chi(1-q) + (1-\chi) \cdot q \;, \quad p(y_2) = \chi \cdot q + (1-\chi) \cdot (1-q)$

und $\quad p(x/y) \cdot p(y) = p(y/x) \cdot p(x) \Rightarrow p(x/y) = \frac{p(x) \cdot p(y/x)}{p(y)}$

$$p(x_1/y_1) = \frac{\chi(1-q)}{p(y_1)} \; p(x_2/y_1) = \frac{(1-\chi) \cdot q}{p(y_1)} \qquad p(x_1/y_2) = \frac{\chi \cdot q}{p(y_2)} \; p(x_2/y_2) = \frac{(1-\chi) \cdot (1-q)}{p(y_2)}$$

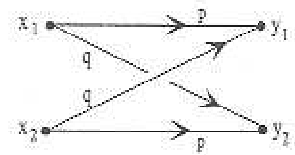
$$H(x/y) = p(y_1) \cdot \left[\frac{\chi(1-q)}{p(y_1)} \cdot \mathrm{ld}\frac{p(y_1)}{\chi(1-q)} + \frac{(1-\chi) \cdot q}{p(y_1)} \cdot \mathrm{ld}\frac{p(y_1)}{(1-\chi) \cdot q}\right]$$
$$+ p(y_2) \cdot \left[\frac{\chi \cdot q}{p(y_2)} \cdot \mathrm{ld}\frac{p(y_2)}{\chi \cdot q} + \frac{(1-\chi) \cdot (1-q)}{p(y_2)} \cdot \mathrm{ld}\frac{p(y_2)}{(1-\chi) \cdot (1-q)}\right]$$

$$H(x/y) = [\chi \cdot (1-q) + (1-\chi) \cdot q] \cdot \mathrm{ld}\, p(y_1) - \chi(1-q) \cdot \mathrm{ld}(\chi(1-q)) - (1-\chi) \cdot q \cdot \mathrm{ld}((1-\chi) \cdot q)$$
$$+ [\chi \cdot q + (1-\chi) \cdot (1-q)] \cdot \mathrm{ld}\, p(y_2) - \chi \cdot q \cdot \mathrm{ld}(\chi \cdot q) - (1-\chi)(1-q) \cdot \mathrm{ld}((1-\chi)(1-q))$$

$$T(x/y) = -\chi \cdot \mathrm{ld}\chi - (1-\chi) \cdot \mathrm{ld}(1-\chi)$$
$$- [p(y_1)] \cdot \mathrm{ld}p(y_1) + \chi(1-q) \cdot \mathrm{ld}(\chi(1-q)) + (1-\chi) \cdot q \cdot \mathrm{ld}((1-\chi) \cdot q)$$
$$- [p(y_2)] \cdot \mathrm{ld}p(y_2) + \chi \cdot q \cdot \mathrm{ld}(\chi \cdot q) + (1-\chi)(1-q) \cdot \mathrm{ld}((1-\chi)(1-q))$$

CodT **Aufgabe 10 : Kettenschaltung symmetrischer Binärkanäle (SBK)**

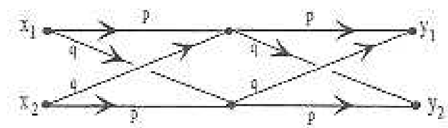
Allgemein:



$$(K) = \begin{pmatrix} p(y_1/x_1) & p(y_2/x_1) \\ p(y_1/x_2) & p(y_2/x_2) \end{pmatrix}$$

$$(K) = \begin{pmatrix} p & q \\ q & p \end{pmatrix} = \begin{pmatrix} 1-q & q \\ q & 1-q \end{pmatrix}$$

a) Kettenschaltung zweier Kanäle:



$$(K_{Ersatz}) = \begin{pmatrix} p & q \\ q & p \end{pmatrix} \cdot \begin{pmatrix} p & q \\ q & p \end{pmatrix} = \begin{pmatrix} p^2+q^2 & 2pq \\ 2pq & p^2+q^2 \end{pmatrix} = \begin{pmatrix} 1-q_{Ers} & q_{Ers} \\ q_{Ers} & 1-q_{Ers} \end{pmatrix}$$

$\Rightarrow$ Der Ersatzkanal ist ebenfalls ein symmetrischer Binärkanal.

$$q_{Ers} = 2 \cdot p \cdot q = 2 \cdot (1-q) \cdot q$$
$$= 2q - 2q^2$$

$$(K_{Ers}) = \begin{pmatrix} 1-2q+2q^2 & 2q-2q^2 \\ 2q-2q^2 & 1-2q+2q^2 \end{pmatrix}$$

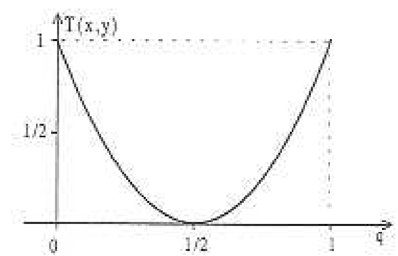
Allgemein: bei m-facher Kaskadierung folgt für symmetrische Binärkanäle: $\quad q_{m\,Ers} = \frac{1}{2} \cdot \left[1 - (2q-1)^m\right]$

b) Für gleichwahrscheinliche Eingangssymbole x_1, x_2 gilt (sh. Studienhilfe Gl. (37)):

Maximale Transinformation: auch Symbolkapazität, Kanalweite, mit zwei Gliedern

$$T(x,y) = T_{max}(x,y) = 1 - [1 - q_{Ers}] \cdot \mathrm{ld}\frac{1}{1-q_{Ers}} - q_{Ers} \cdot \mathrm{ld}\frac{1}{q_{Ers}}$$

$$= 1 - \left[(1-q)^2 + q^2\right] \cdot \mathrm{ld}\frac{1}{\left[(1-q)^2 + q^2\right]} - \left[2q(1-q)\right] \cdot \mathrm{ld}\frac{1}{\left[2q(1-q)\right]}$$



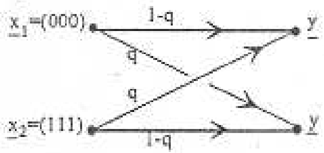
CodT **Aufgabe 12 : Fehlerwahrscheinlichkeit am symmetrischen Binärkanal**

Bestimmen Sie die Fehlerwahrscheinlichkeit q_C bei der Symbolübertragung über einen symmetrischen Binärkanal der Bitfehlerwahrscheinlichkeit q, wenn am Eingang die Codeworte $\underline{x}_1 = (000)$ und $\underline{x}_2 = (111)$ gleich wahrscheinlich eingegeben werden:

a) allgemein $q_C = f(q)$ und b) q_C für $q = 10^{-2}$

Der Decoder kann alle Ein-Bit-Fehler erkennen. Die Decodierung am Ausgang erfolgt nach der Vorschrift: max $p(\underline{y}/\underline{x}_i)$ (Maximum-Likelihood-Regel).

Symmetrischer Binärkanal:



Decodiervorschrift nach der Maximum-Likelihood-Regel.
Mögliche Empfangs - Ereignisse:

$$\left.\begin{array}{l} \underline{b}_0 = (000) \\ \underline{b}_1 = (001) \\ \underline{b}_2 = (010) \\ \underline{b}_4 = (100) \end{array}\right\} \Rightarrow \underline{y}_1 = \underline{x}_1 \qquad \left.\begin{array}{l} \underline{b}_3 = (011) \\ \underline{b}_5 = (101) \\ \underline{b}_6 = (110) \\ \underline{b}_7 = (111) \end{array}\right\} \Rightarrow \underline{y}_2 = \underline{x}_2$$

Allgemein ist die n-fache Wiederholung des Eingangs-Codesymbols möglich.

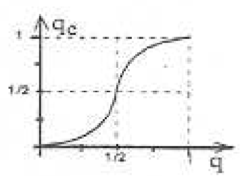
a) q_C **allgemein:** mögliche Fehler bei der Maximum-Likelihood-Entscheidung:

$$q_C = p(\underline{y} = \underline{b}_3, \underline{b}_5, \underline{b}_6, \underline{b}_7/x_1) + p(\underline{y} = \underline{b}_0, \underline{b}_1, \underline{b}_2, \underline{b}_4/x_2)$$

$\Downarrow$ x_2 $\quad$ **Entscheidung des Decoders** $\quad$ $\Downarrow$ x_1

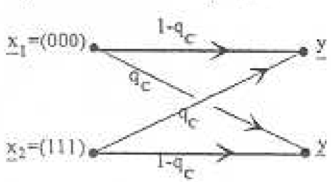
Bei einem symmetrischen Binärkanal und mit $p(x_1) = p(x_2) = 1/2$ gilt für die Restfehlerwahrscheinlichkeit q_C nach der Korrektur:

$$q_C = p(x_1)\cdot[(1-q)qq + q(1-q)q + qq(1-q) + qqq]$$
$$+ p(x_2)\cdot[qqq + qq(1-q) + q(1-q)q + (1-q)qq]$$
$$q_C = 3\cdot(1-q)q^2 + q^3 = 3\cdot q^2 - 2\cdot q^3, \quad \Rightarrow \text{für } q \ll 1: \quad q_C \approx 3\cdot q^2$$



Beispiel.: Für q=1/2 ergibt sich $q_C = 1/2$,
d.h., es ist keine sinnvolle Entscheidung möglich.

b) **Restfehler für q=0,01:**



$q_C = 10^{-4}(3 - 2\cdot 10^{-2}) = 2{,}98\cdot 10^{-4}$

Das Ergebnis entspricht rund **3% von q** .

Der Preis für eine hohe Fehlersicherheit ist hier die Verminderung der Übertragungsrate auf ein Drittel.

Mit der Beziehung $\dfrac{dT(x,y)}{d\chi} = 0$ Bestimmung der **maximalen Transinformation:**

beachte: $p(y_1),\ p(y_2) = F(q,\chi)$

$$\frac{dT(x,y)}{d\chi} = -1\cdot \mathrm{ld}\,\chi - \frac{\chi}{\chi\cdot\ln 2} - (-1)\cdot\mathrm{ld}(1-x) - \frac{(1-\chi)}{(1-\chi)\cdot\ln 2}\cdot(-1)$$
$$-(1-2q)\cdot\mathrm{ld}p(y_1) - \frac{p(y_1)}{p(y_1)\cdot\ln 2}\cdot(1-2q) + (1-q)\cdot\mathrm{ld}(\chi(1-q)) + \frac{\chi(1-q)}{\chi(1-q)\cdot\ln 2}(1-q)$$
$$+(-q)\cdot\mathrm{ld}((1-\chi)\cdot q) + \frac{(1-\chi)\cdot q}{(1-\chi)\cdot q\cdot\ln 2}(-q)$$
$$-(2q-1)\cdot\mathrm{ld}p(y_2) + \frac{p(y_2)}{p(y_2)\cdot\ln 2}\cdot(2q-1) + q\cdot\mathrm{ld}(\chi q) + \frac{(\chi\cdot q)}{(\chi\cdot q)\cdot\ln 2}\cdot q$$
$$+(q-1)\cdot\mathrm{ld}((1-\chi)(1-q)) + \frac{(1-\chi)(1-q)}{(1-\chi)(1-q)\cdot\ln 2}\cdot(q-1)$$

$$\frac{dT(x,y)}{d\chi} = -\mathrm{ld}\,\chi + \mathrm{ld}(1-\chi) - (1-2q)\cdot\mathrm{ld}p(y_1) + (1-q)\cdot\mathrm{ld}(\chi(1-q)) - q\cdot\mathrm{ld}((1-\chi)\cdot q)$$
$$-(2q-1)\cdot\mathrm{ld}p(y_2) + q\cdot\mathrm{ld}(\chi\cdot q) + (q-1)\cdot\mathrm{ld}((1-\chi)(q-1))$$

$$\frac{dT(x,y)}{d\chi} = -\mathrm{ld}\,\chi + \mathrm{ld}(1-\chi) + (2q-1)\cdot[\mathrm{ld}\,p(y_1) - \mathrm{ld}p(y_2)]$$
$$+\mathrm{ld}\,\chi + \mathrm{ld}(1-q) - q\cdot\mathrm{ld}\,\chi - q\cdot\mathrm{ld}(1-q) - q\cdot\mathrm{ld}(1-\chi) - q\cdot\mathrm{ld}\,q$$
$$+q\cdot\mathrm{ld}\,\chi + q\cdot\mathrm{ld}q + q\cdot\mathrm{ld}(1-\chi) + q\cdot\mathrm{ld}(1-q) - \mathrm{ld}(1-\chi) - \mathrm{ld}(1-q)$$

$$\frac{dT(x,y)}{d\chi} = -\mathrm{ld}\,\chi + \mathrm{ld}(1-\chi) + (2q-1)\cdot[\mathrm{ld}(\chi+q-2q\chi) - \mathrm{ld}(1-x-q+2q\chi)]$$
$$+\mathrm{ld}\,\chi - \mathrm{ld}(1-\chi)$$

Bedingung für Extremwert: $\dfrac{dT(x,y)}{d\chi} = 0$: $\quad \chi + q - 2q\chi = 1 - \chi - q + 2q\chi$

$$\chi\cdot 2\cdot(1-2q) = (1-2q) \quad \Rightarrow \chi = \tfrac{1}{2}$$

Für $\chi = 0{,}5$ findet man $\dfrac{d^2T(x,y)}{d\chi^2} < 0$, d.h., es liegt tatsächlich ein **Maximum** vor.

Mit $p(x_1) = \chi = 0{,}5$ und mit $p(x_2) = 1-\chi = 0{,}5$ bestimmt man $T_{max}(x,y)$:

$$T_{max}(x,y) = \tfrac{1}{2}\cdot\mathrm{ld}\frac{1}{\frac{1}{2}} + \tfrac{1}{2}\cdot\mathrm{ld}\frac{1}{\frac{1}{2}} - \tfrac{1}{2}\cdot\mathrm{ld}\tfrac{1}{2} + \tfrac{1}{2}(1-q)\cdot\mathrm{ld}(\tfrac{1}{2}(1-q)) + \tfrac{1}{2}q\cdot\mathrm{ld}(\tfrac{1}{2}q)$$
$$-\tfrac{1}{2}\cdot\mathrm{ld}\tfrac{1}{2} + \tfrac{1}{2}q\cdot\mathrm{ld}(\tfrac{1}{2}q) \qquad + \tfrac{1}{2}(1-q)\cdot\mathrm{ld}(\tfrac{1}{2}(1-q))$$

$$T_{max}(x,y) = 1 + 1\cdot(1-q)\cdot\mathrm{ld}(1-q) + 1\cdot q\cdot\mathrm{ld}\,q + 1 - 1\cdot(1-q)\cdot\mathrm{ld}\,2 - 1\cdot q\cdot\mathrm{ld}\,2$$

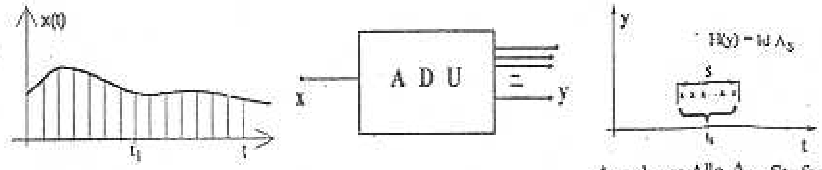
$$T_{max}(x,y) = 1 - (1-q)\cdot\mathrm{ld}\frac{1}{(1-q)} - q\cdot\mathrm{ld}\frac{1}{q}$$

CodT Aufgabe 13 : Analog-Digital-Umsetzer: Anzahl der Amplitudenstufen

Störabstand: $SNR_X = 10 \cdot \lg \frac{P_X}{P_N} |dB$

a) **Abschätzung nach dem Informationsfluß**

Informationsfluß an x und y:



Annahme: Alle A_S Stufen (Symbole) treten gleich wahrscheinlich auf:

$$H(y) = A_S \cdot \frac{1}{A_S} \cdot \mathrm{ld} \frac{1}{\frac{1}{A_S}} = \mathrm{ld}\, A_S$$

Vorgabe: $C_x \approx C_y$

$C_x = B_x \cdot \mathrm{ld}(1 + P_X/P_N)$
Shannon'sche Kanalkapazität

$C_y = f_S \cdot H(y)$
Symbolfrequenz, Abtastfrequenz nach Abtasttheorem: $\boxed{2 \cdot B_x \le f_S}$

$\le$!

$$B_x \cdot \mathrm{ld}(1 + P_X/P_N) \le 2 \cdot B_x \cdot \mathrm{ld}\, A_S$$

$\ge$

Annahme: $P_X >> P_N$

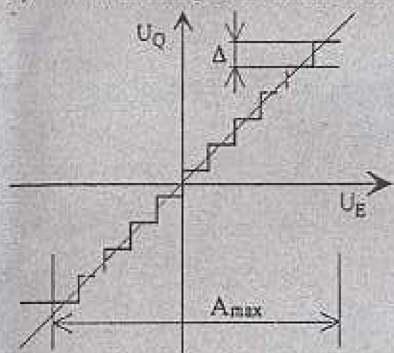
$$\mathrm{ld}\, P_X/P_N \le 2 \cdot \mathrm{ld}\, A_S$$

$$\sqrt{P_X/P_N} \le A_S$$

Mit $P_X/P_N = 10^{\frac{SNR_X}{10}}$: $10^{\frac{SNR_X}{20}} \le A_S$

$A_S \ge 10^{\frac{40}{20}} = 100$ ist für $A_S = 128$: $\underline{S = 7\ \text{bit}}$

b) **Abschätzung nach dem Quantisierungsrauschen**



$A_{max} = A_S \cdot \Delta = 2^S \cdot \Delta$

Die Quantisierungs-Rauschleistung

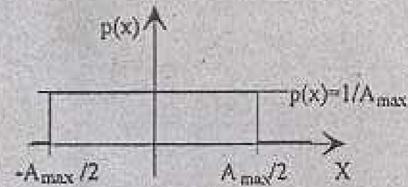
$$\bar{P}_Q = \bar{P}_N = \frac{\Delta^2}{12}$$

ist ins Verhältnis zu setzen zur mittleren Signalleistung

$$\bar{P}_X = \frac{A_{max}^2}{12} = \frac{1}{12}\left(2^S \cdot \Delta\right)^2 .$$

$$\frac{P_X}{P_Q} = \frac{2^{2S} \cdot \Delta^2}{\Delta^2} = \underline{2^{2S}}$$

Mittlere Leistung bei Gleichverteilung über alle Amplitudenstufen:



$$\bar{P}_X = \int_{-A_{max}/2}^{A_{max}/2} x^2 \cdot p(x)\,dx$$

$$\bar{P}_X = \frac{1}{A_{max}} \cdot \frac{x^3}{3} \Bigg|_{-A_{max}/2}^{A_{max}/2}$$

$$\bar{P}_X = \frac{1}{A_{max}} \cdot 2 \cdot \left(\frac{A_{max}}{2}\right)^3 \cdot \frac{1}{3} = \underline{\frac{A_{max}^2}{12}}$$

$$SNR_x = 10 \cdot \lg \frac{P_x}{P_Q}\Big|_{dB} = 10 \cdot \lg 2^{2 \cdot S}\Big|_{dB} = 10 \cdot 2 \cdot S \cdot \lg 2 \approx \underline{S \cdot 6\,dB = SNR_x}$$

$\Rightarrow$ $S \cdot 6\,dB = 40\,dB$, damit erforderlich $S = 6{,}6$ bit $\Rightarrow$ $\underline{7\ \text{bit}}$

Dieses Ergebnis korrespondiert mit dem des Teiles a)

c) **Praktisch notwendige Bitbreite**

Damit ein ausreichender Dynamikbereich zur Verfügung steht, kann die Amplitude A_{max} in der Regel nicht völlig ausgenutzt werden. Beispielsweise bei Tonsignalen müssen auch die leisesten Stellen noch ausreichenden Störabstand zum Quantisierungsrauschen haben (footroom). Im oberen Dynamikbereich ist eine Übersteuerungsreserve nötig (head).
S muß daher praktisch größer sein als durch a) und b) ermittelt, z.B. S=16 bit.
Eine Verbesserung ist auch mit einer nichtlinearen Quantisierungskennlinie zu erreichen.

CodT Aufgabe 15 : Galois Felder und Polynome

Stellen Sie die Additions- und Multiplikationstafeln in einem Rechenbereich

a) mod 4 , b) mod 5 auf.

Warum erhält man im Fall a) keinen endlichen Körper und
im Fall b) ein Galois Feld ?

Lösung:

Ring der ganzen Zahlen mod 4

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0*	2
3	0	3	2	1

0*: Nullteiler
2: Mehrdeutigkeit

$2 \cdot 1 = 2 \bmod 4$
$2 \cdot 3 = 2 \bmod 4$
$2 \cdot 2 = 4 \bmod 4 = 0$

-keine uneingeschränkte Division der Elemente möglich, Unterschied zu GF(5) und GF(2^2)

Galoisfeld GF(5)

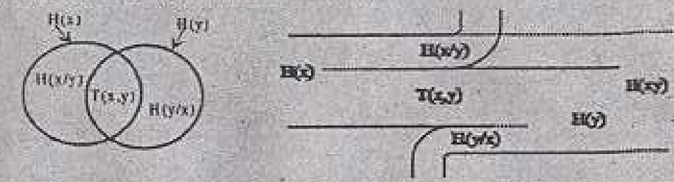
+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

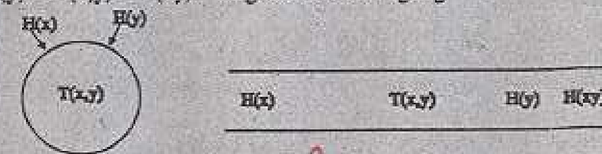
Alle Gruppen-Axiome sind erfüllt, z.B.: $3 \cdot 3 = 9 = 4 \bmod 5$.
Jedes Element $\neq 0$ hat ein inverses: $1 \cdot 1 = 1$
$2 \cdot 3 = 6 = 1 \bmod 5$ und $3 \cdot 2 = 6 = 1 \bmod 5$,
$4 \cdot 4 = 16 = 1 \bmod 5$

CodT Aufgabe 14 Entropiebilanz - Diagramm

Allgemeine Darstellung der gesamten Bilanz:



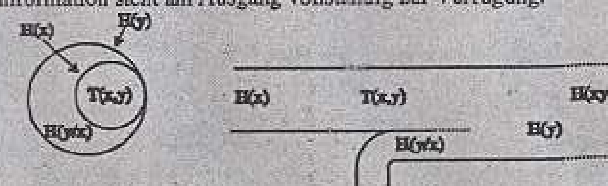
a) $H(x) = H(y) = T(x,y) = H(xy)$: Ungestörte Übertragung



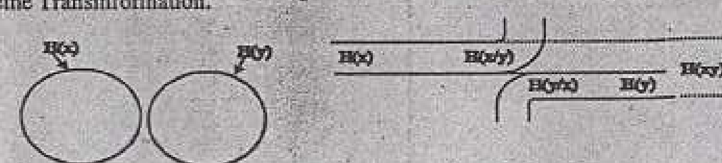
?

oder: $H(x) = H(y)$ wegen $H(x/y) = H(y/x) \neq 0$ Bild s. Allgemeine Darstellung.

b) $H(x) = T(x,y) < H(y) = H(xy)$ Die gesamte Quelleninformation gelangt zum Ausgang; sie wird aber durch Streuung überlagert.
Die Quelleninformation steht am Ausgang vollständig zur Verfügung.



c) $T(x,y) = 0$ Vollständig gestörter Kanal. Die Quelleninformation geht vollständig in die Äquivokation ein; die gesamte Senkeninformation stammt aus der Streuung; keine Transinformation.



Gegeben sind folgende Polynome über G(2):

a) $f_a = x^4 + x^2 + 1$ b) $f_b = x^4 + x^3 + 1$

Ermitteln Sie, ob es sich dabei um irreduzible und primitive Polynome handelt!

Irreduzibilität:
liegt vor, wenn das Polynom f(x) nicht mehr in Polynomfaktoren zerlegbar ist:

$f(x) \neq f_1(x) \cdot f_2(x)$ (Grad der Polynome >0)

Primitiv ist das Polynom $f(x) \in F(p)$ genau dann, p = Primzahl

wenn $(x^N - 1) : f(x)$ teilbar ist für $N = p^n - 1$ n = Grad von f(x)

und nicht teilbar ist für $1 \le N < p^n - 1$.

d.h., es ist $f(x) \cdot h(x) \neq x^N - 1$ für $1 \le N < p^n - 1$

a) Polynom $f_a = x^4 + x^2 + 1$

Test auf Irreduzibilität: Ausreichend ist die Probe mit den Polynomfaktoren $(x^2 + x + 1)$, $(x^2 + x)$, $(x^2 + 1)$, $(x + 1)$, (x), weil eine Teilbarkeit mit den übrigen Faktoren wieder einen dieser Faktoren ergäbe.

Versuch: $(x^4 + x^2 + 1) : (x^2 + x + 1) = x^2 + x + 1$ (teilbar ohne Rest).

d.h., $f_a = (x^2 + x + 1) \cdot (x^2 + x + 1)$; das Polynom ist **reduzibel**.
Primitiv können nur irreduzible Polynome sein, daher erübrigt sich nach Feststellung der Reduzibilität die Prüfung des Polynoms auf Primitivität.

Primitiv → irreduzible

Eine solche Prüfung ergäbe hier:

$(x - 1) : (x^4 + x^2 + 1) = 0 +$ Rest,
$(x^2 - 1) : (x^4 + x^2 + 1) = 0 +$ Rest
$(x^3 - 1) : (x^4 + x^2 + 1) = 0 +$ Rest
$(x^4 - 1) : (x^4 + x^2 + 1) = 1 +$ Rest
$(x^5 - 1) : (x^4 + x^2 + 1) = x +$ Rest
$(x^6 - 1) : (x^4 + x^2 + 1) = x^2 + 1$. d.h., Teilbarkeit ist für $N = 6 < 15 = 2^n - 1$ gegeben.
Das Polynom ist folglich auch **nicht primitiv**.

b) Polynom $f_b = x^4 + x^3 + 1$

Test auf **Irreduzibilität**: Ausreichend ist die Probe mit den Polynomfaktoren (x^2+x+1), (x^2+x), (x^2+1), $(x+1)$, (x), weil die Teilbarkeit mit den übrigen möglichen Faktoren wieder einen dieser Faktoren ergäbe.

$(x^4 + x^3 + 1) : (x^2 + x + 1) = x^2 + 1$ + *Rest* $\neq 0$
$\underline{x^4 + x^3 + x^2}$
$- \;\; - \;\; x^2 + 1$
$\underline{x^2 + x + 1}$
$- \;\; x$

$(x^4 + x^3 + 1) : (x^2 + x) = x^2$ + *Rest* $\neq 0$
$\underline{x^4 + x^3}$
$- \;\; - \;\; 1$

$(x^4 + x^3 + 1) : (x^2 + 1) = x^2 + x$ + *Rest* $\neq 0$
$\underline{x^4 + x^2}$
$x^3 + x^2 + 1$
$\underline{x^3 + x}$
$- \;\; x^2 + x + 1$

$(x^4 + x^3 + 1) : (x + 1) = x^3$ + *Rest* $\neq 0$
$\underline{x^4 + x^3}$
$- \;\; - \;\; 1$

$(x^4 + x^3 + 1) : x = x^3 + x^2$ + *Rest* $\neq 0$
$\underline{x^4}$
$- \;\; x^3 + 1$
$\underline{x^3}$
$- \;\; 1$

Es kann kein Polynomfaktor gefunden werden, das Polynom f_b ist also **irreduzibel**.

Test auf **Primitivität**:

$(x - 1) : (x^4 + x^3 + 1) = 0$ + *Rest* $(x - 1)$
$(x^2 - 1) : (x^4 + x^3 + 1) = 0$ + *Rest* $(x^2 - 1)$
$(x^3 - 1) : (x^4 + x^3 + 1) = 0$ + *Rest* $(x^3 - 1)$
$(x^4 - 1) : (x^4 + x^3 + 1) = 1$ + *Rest* (x^3)
$(x^5 - 1) : (x^4 + x^3 + 1) = x + 1$ + *Rest* $(x^3 + x)$
$(x^6 - 1) : (x^4 + x^3 + 1) = x^2 + x + 1$ + *Rest* $(x^3 + x^2 + 1)$
$(x^7 - 1) : (x^4 + x^3 + 1) = x^3 + x^2 + x + 1$ + *Rest* (x^2)
$(x^8 - 1) : (x^4 + x^3 + 1) = x^4 + x^3 + x^2 + x$ + *Rest* $(x^3 + x^2 + x + 1)$
$(x^9 - 1) : (x^4 + x^3 + 1) = x^5 + x^4 + x^3 + x^2 + 1$ + *Rest* (x^2)
$(x^{10} - 1) : (x^4 + x^3 + 1) = x^6 + x^5 + x^4 + x^3 + x$ + *Rest* $(x^3 + x + 1)$
$(x^{11} - 1) : (x^4 + x^3 + 1) = x^7 + x^6 + x^5 + x^4 + x^2 + 1$ + *Rest* $(x^3 + x^2)$
$(x^{12} - 1) : (x^4 + x^3 + 1) = x^8 + x^7 + x^6 + x^5 + x^3 + x + 1$ + *Rest* (x)
$(x^{13} - 1) : (x^4 + x^3 + 1) = x^9 + x^8 + x^7 + x^6 + x^4 + x^2 + x$ + *Rest* $(x^2 + x + 1)$
$(x^{14} - 1) : (x^4 + x^3 + 1) = x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2$ + *Rest* $(x^3 + x^2 + 1)$

$(x^{15} - 1) : (x^4 + x^3 + 1) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$ ohne Rest

Die Kriterien für die Primitivität bei N=1..14 (Rest) und bei N=15 (kein Rest) sind erfüllt.
Das Polynom ist **primitiv**.

b) **Hamming-Distanz**

$$d_{min} = w_{min} = 3$$

c) **Codebasis**

Versuch: $(1\,1\,0\,0\,1\,1)$
$\oplus$ $\underline{(0\,1\,1\,0\,0\,1)}$
$(1\,0\,1\,0\,1\,0)$

Das 3. Codewort ist modulo-2-Summe der beiden anderen. Diese drei Codeworte können daher nicht als Codebasis dienen.

d) **Fehler-Erkennbarkeit** $d_{min} \geq d_E + 1$

Fall f_1: $d_E = 2$, mit $d_{min} = 3$ $\Rightarrow$ Fehlervektoren mit dem Gewicht w=1 und w= können toleriert werden; der Fehler ist erkennbar.

Fall f_2: $d_E = 3$ $\Rightarrow$ Fehlervektor mit dem Gewicht w=3 erfüllt die Grenzbedingung nicht. Er führt auf ein anderes erlaubtes Codewort, d.h., zu einem nicht erkenn- baren Fehler.

Fall f_3: $d_E = 3$ $\Rightarrow$ Wie Fall 2, also nicht erkennbarer Fehler.

e) **Zuordnung eines Sender-Wortes**

Untersuchung mittels einer Distanztabelle: $d\{\underline{b}_i \oplus (100010)\}$:

(1.): 3 (2.): 2 (3.): 4 (4.): 1 (5.): 4 (6.): 5 (7.): 3

Prinzip der Ähnlichkeits-Decodierung: Als korrigiertes Codewort wird das mit dem kleinsten Abstand, hier (4.): (101010) mit dem Abstand 1, ausgewählt.

f) **Korrigierbarkeit**

Untersuchung mittels einer Distanztabelle: $d\{\underline{b}_i \oplus (101001)\}$:

(1): 2 (2): 3 (3): 3 (4): 2 (5): 3 (6): 2 (7): 6

Wegen $d_{min} \geq 2 \cdot d_K + 1$ beträgt mit $d_{min} = 3$ die Korrekturfähigkeit nur $d_K = 1$.
Es ist keine eindeutige Zuordnung des empfangenene Wortes zu einem erlaubten Codewort möglich.

a) Bilden die folgenden Codeworte (n = 6, k = 3) einen Gruppencode?

1 (100101) **2** (110011) **3** (111100) **4** (101010)
5 (001111) **6** (011001) **7** (010110)

b) Wie groß ist die Hamming-Distanz o.g. Codes?

c) Können folgende Codeworte als Basisvektoren (Generatormatrix) dieses Codes dienen ?: (110011) (011001) (101010)

d) Welcher der angegebenen Fehlervektoren charakterisiert einen nicht erkennbaren Fehler ?

f_1 (011000), f_2 (011001), f_3 (101001).

e) Durch einen Einfachfehler wurde ein Codewort zu (100010) verfälscht.
Welches Codewort wurde gesendet?

f) Läßt sich beim Empfang des Wortes (101001) auf das gesendete Codewort schließen?

a) **Gruppeneigenschaften des Codes mit n=6, k=3**

Die Codewörter sind Teilmenge aus der Menge der 2^6 6-stelligen Binärwörter.
Sie lassen sich als Vektoren eines 6-dimensionalen Vektorraumes auffassen.
Falls sie Elemente einer Gruppe sind, ist zu ihrer Beschreibung eine Untermenge von Basisvektoren, d.h., Basiscodewörtern ausreichend.

Versuche:

(1): $(1\,0\,0\,1\,0\,1)$
(2): $(1\,1\,0\,0\,1\,1)$ $(1) \oplus (2) = (7)$
(3): $(1\,1\,1\,1\,0\,0)$ $(1) \oplus (3) = (6)$
(4): $(1\,0\,1\,0\,1\,0)$ $(1) \oplus (4) = (5)$
(5): $(0\,0\,1\,1\,1\,1)$ $(1) \oplus (5) = (4)$
(6): $(0\,1\,1\,0\,0\,1)$ $(1) \oplus (6) = (3)$
(7): $(0\,1\,0\,1\,1\,0)$ $(1) \oplus (7) = (2)$

<u>Lösung:</u>
Basiscodewörter: (1), (2), (3)

mit $(1) \oplus (2) = (7)$
$(1) \oplus (3) = (6)$
$(2) \oplus (3) = (5)$
$(1) \oplus (2) \oplus (3) = (4)$

<u>andere Lösung:</u>
Basiscodewörter: (1), (5), (7)

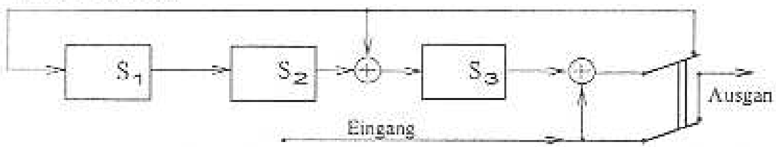
mit $(1) \oplus (5) = (4)$
$(1) \oplus (7) = (2)$
$(5) \oplus (7) = (6)$
$(1) \oplus (5) \oplus (7) = (3)$

In beiden Fällen wurden je drei Basiscodewörter gefunden, aus deren Kombinationen sich die übrigen Codewörter (einschließlich eines Nullwortes) ergeben.
Es liegt ein systematischer linearer <u>Gruppencode</u> vor.

Zyklischer (7,4)-Code:

n=7, k=4, n-k=3 $\qquad g(x) = x^3 + x^2 + 1 = g_3x^3 + g_2x^2 + g_1x + g_0$

a) **Codierschaltung**



b) **Kontrollschritte und Prüfgleichungen**

Vertauschung und mod - 2 - Addition von Zeilen:

$$\begin{array}{c} \\ \underline{G} = \end{array}\begin{array}{c} b_6\ b_5\ b_4\ b_3\ b_2\ b_1\ b_0 \\ \begin{bmatrix} 0&0&0&1&1&0&1 \\ 0&0&1&1&0&1&0 \\ 0&1&1&0&1&0&0 \\ 1&1&0&1&0&0&0 \end{bmatrix}\end{array} \begin{array}{c} \\ (1) \\ (2) \\ (3) \\ (4) \end{array} \Rightarrow \underline{G}^* = \begin{bmatrix} 1&0&0&0&1&1&0 \\ 0&1&0&0&0&1&1 \\ 0&0&1&0&1&1&1 \\ 0&0&0&1&1&0&1 \end{bmatrix} \begin{array}{c} (2)\oplus(3)\oplus(4) \\ (1)\oplus(2)\oplus(3) \\ (1)\oplus(2) \\ (1) \end{array}$$

Prüfmatrix $\underline{H}^*$:

$$\underline{H}^* = \left(\underline{A}^T, \underline{I}_3\right) = \begin{array}{c} b_6\ b_5\ b_4\ b_3\ |\ b_2\ b_1\ b_0 \\ \begin{bmatrix} 1&0&1&1&1&0&0 \\ 1&1&1&0&0&1&0 \\ 0&1&1&1&0&0&1 \end{bmatrix}\end{array}$$

Prüfgleichungen:

$$\Rightarrow \quad \begin{aligned} b_2 &= b_6 \oplus b_4 \oplus b_3 \\ b_1 &= b_6 \oplus b_5 \oplus b_4 \\ b_0 &= b_5 \oplus b_4 \oplus b_3 \end{aligned}$$

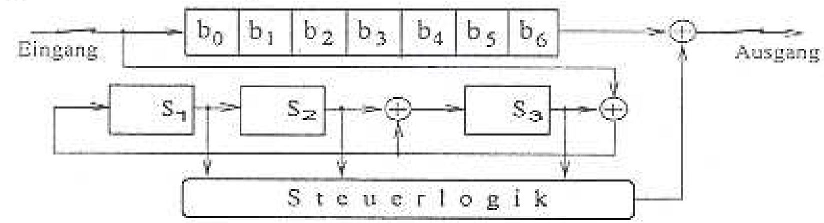
Codepolynom:

$$b(x) = b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$$

Belegungen des Eingangs, des Ausgangs und der Speicherstellen:

i	Eingang	$S_1(i)$	$S_2(i)$	$S_3(i)$	Ausgang
0	b_6	0	0	0	b_6
1	b_5	b_6	0	b_6	b_5
2	b_4	b_5+b_6	b_6	b_5+b_6	b_4
3	b_3	$b_4+b_5+b_6$	b_5+b_6	b_4+b_5	b_3
4	0	$b_3+b_4+b_5$	$b_4+b_5+b_6$	$b_3+b_4+b_6$	$b_3+b_4+b_6$
5	0	0	$b_3+b_4+b_5$	$b_4+b_5+b_6$	$b_4+b_5+b_6$
6	0	0	0	$b_3+b_4+b_5$	$b_3+b_4+b_5$
7	b_6^*	0	0	0	b_6^*

c) **Decodierschaltung**



i	Eingang	$S_1(i)$	$S_2(i)$	$S_3(i)$
4'	b_2	$b_3+b_4+b_5$	$b_4+b_5+b_6$	$b_3+b_4+b_6$
5'	b_1	$b_2+b_3+b_4+b_6$	$b_3+b_4+b_5$	$b_2+b_3+b_5$
6'	b_0	$b_1+b_2+b_3+b_5$	$b_2+b_3+b_4+b_6$	$b_1+b_2+b_4$
7'	-	$b_0+b_1+b_2+b_4$	$b_1+b_2+b_3+b_5$	$b_0+b_1+b_3+b_6$

Für die Schieberegister-Inhalte muß nach dem Einlesen des Empfangsvektors lt. Prüfgleichung gelten: $S_1(i) = S_2(i) = S_3(i) = 0 \bmod 2$

$$S_1(i) = b_0 + b_1 + b_2 + b_4 = b_5 + b_4 + b_3 + b_6 + b_5 + b_4 + b_6 + b_4 + b_3 + b_4 = 0 \bmod 2$$
$$S_2(i) = b_1 + b_2 + b_3 + b_5 = b_6 + b_5 + b_4 + b_6 + b_4 + b_3 + b_3 + b_5 = 0 \bmod 2$$
$$S_3(i) = b_0 + b_1 + b_3 + b_6 = b_5 + b_4 + b_3 + b_6 + b_5 + b_4 + b_3 + b_6 = 0 \bmod 2$$

d) **Fehler-Syndrome**

Der Inhalt des Schieberegisters stellt das Syndrom dar.

Fehler $b_i' = 1 \oplus b_i \quad \Rightarrow$ Syndrom: $(S_1\ S_2\ S_3)$

$$\left.\begin{array}{ll} b'_6 = 1\oplus b_6 & (0\ 0\ 1) \\ b'_5 = 1\oplus b_5 & (0\ 1\ 0) \\ b'_4 = 1\oplus b_4 & (1\ 0\ 0) \\ b'_3 = 1\oplus b_3 & (0\ 1\ 1) \\ b'_2 = 1\oplus b_2 & (1\ 1\ 0) \\ b'_1 = 1\oplus b_1 & (1\ 1\ 1) \\ b'_0 = 1\oplus b_0 & (1\ 0\ 1) \end{array}\right\} \Rightarrow \left\{\begin{array}{l} \text{Steuerlogik zur automatischen Korrektur aller Einfachfehler.} \\ \text{Die Korrektur aller Einzelfehler ist damit möglich.} \end{array}\right.$$

e) **Fehler-Erkennbarkeit**

$\underline{e} = (0110100) \quad \Longrightarrow \quad \underline{b}_E = (b_6\ \overline{b_5}\ \overline{b_4}\ b_3\ \overline{b_2}\ b_1\ b_0)$

$\underline{e}$ gleicht der dritten Zeile der $\underline{G}$-Matrix und damit einem erlaubten Codewort, d.h., $\underline{b} \oplus \underline{e} = \underline{b}_E$ ist wieder ein erlaubtes Codewort auf Grund der Gruppeneigenschaft und daher nicht als fehlerhaft erkennbar.

Oder:
$$\begin{aligned} s_1 &= b_0 + b_1 + (1+b_2) + (1+b_4) = 0 \\ s_2 &= b_1 + (1+b_2) + b_3 + (1+b_5) = 0 \quad \text{s.o.} \\ s_3 &= b_0 + b_1 + b_3 + b_6 = 0 \end{aligned}$$

CodT **Aufgabe 20 : Fehlererkennung mit zyklischem Code**

Ein zyklischer Code mit $k = 10$, $n = 15$ soll mit dem Generatorpolynom
$g(x) = x^5 + x^4 + x^2 + 1$ gebildet werden.

a) Leiten Sie aus der Generatormatrix die Größe der Hamming-Distanz ab!

b) Zeigen Sie am Beispiel, daß beim zyklischen Code Fehler mit einer Länge $\ell \leq n\text{-}k$ (ℓ = Länge der Fehlerfolge $\underline{e}$) erkennbar sein müssen!

c) Zeigen Sie am Beispiel, daß der Anteil der nicht erkennbaren Fehler der Länge $\ell = n\text{-}k + 1$ nur $2^{-(\ell-2)}$ ist!

Lösung: Generatorpolynom: $g(x) = x^5 + x^4 + x^2 + 1$ $k=10$, $n=15$

a) **Hamming-Distanz**

Generatormatrix $\underline{G}$ des zyklischen Codes (Der Code hat $n - k = 5$ Prüfsymbole.):

$$\underline{G} = \begin{bmatrix} 0&0&0&0&0&0&0&0&0&1&1&0&1&0&1 \\ 0&0&0&0&0&0&0&0&1&1&0&1&0&1&0 \\ 0&0&0&0&0&0&0&1&1&0&1&0&1&0&0 \\ 0&0&0&0&0&0&1&1&0&1&0&1&0&0&0 \\ &&&&&\vdots&&&&&&&&& \\ 1&1&0&1&0&1&0&0&0&0&0&0&0&0&0 \end{bmatrix} \qquad d_{min} = w_{min} = 4$$

Bemerkung: Zerlegung in Faktoren ergibt: $(x^5 + x^4 + x^2 + 1):(x+1) = x^4 + x + 1$

Der Code ist ein Abramson-Code mit $d_{min} = 4$ $\Rightarrow$ $g(x) = (x^4 + x + 1)\cdot(x+1)$

b) **Fehlererkennbarkeit**

$\underline{e} \Rightarrow e(x) = x^j \cdot e_0(x)$ für $j < n$

Beispiel: $\underline{e} = (\,0\,0\,0\,0\,\underline{1\,1\,0\,1\,1}\,0\,0\,0\,0\,0\,0\,)$ Länge des Fehlerbündels $\ell = 5$

$\Rightarrow e(x) = x^{10} + x^9 + x^7 + x^6 = x^6 \cdot (x^4 + x^3 + x + 1)$

$\Rightarrow e_0(x) = x^4 + x^3 + x + 1$

$\text{Grad}\{g(x)\} > \text{Grad}\{e_0(x)\}$

$g(x)$ ist ein Teiler von $(x^n + 1)$, wegen $g(x)\cdot h(x) = x^n + 1$

und kein Teiler von x^j, $j < n$ $\Rightarrow$ $x^n = 1 + g(x)\cdot h(x)$, $x^j \neq g(x)\cdot h(x)$

$g(x)$ ist nicht Teiler von $e_0(x)$, weil der Grad von $g(x)$ höher ist als der Grad von $e_0(x)$. Bei der Division des Empfangspolynoms $b_E(x) = b(x) + e(x)$ bleibt daher für alle Fehlerbündel der Länge $\ell \leq n\text{-}k$ ein von Null verschiedener Rest, so daß solche Fehler stets erkannt werden.

c) **Nicht erkennbare Fehler**

Gegeben: $\ell = n\text{-}k+1$ Fehler der Länge ℓ:

$$\ldots\; 0\;0\;\underbrace{X\;\overbrace{X\;0\;\ldots}^{\ell-2}\;X}_{\ell}\;0\;0\;0\;\ldots$$

Mögliche Fehler: In einer Folge der Länge $\ell = n - k + 1$ sind $\ell - 2 = n - k - 1$ bit noch als als beliebige Fehler kombinierbar. Damit sind $2^{\ell-2} = 2^{n-k-1}$ verschiedene Fehler der Länge $\ell = n\text{-}k+1$ möglich.

Von allen möglichen Fehlern hat genau einer die Form $e(x) = c^j \cdot g(x)$, d.h., $e_0(x) = g(x)$

Daher ist dieser eine Fehler nicht erkennbar (vgl. Aufg. 19 e).
Die Fehlerrate, d.h. der Anteil nicht erkennbarer Fehler R_E, ist damit

$$R_E = \frac{1}{2^{n-k-1}} = \frac{1}{2^{\ell-2}} = \underline{2^{-(\ell-2)}}.$$

Zur Kontrolle: $\underline{G}^*$, die systematische Form der Generatormatrix, die aus $\underline{G}$ durch Addition und Vertauschen von Zeilen entsteht.:

$$\underline{G}^* = \left[\begin{array}{cccccccccc|ccccc} 1&0&0&0&0&0&0&0&0&0&1&1&0&1&0 \\ 0&1&0&0&0&0&0&0&0&0&0&1&1&0&1 \\ 0&0&1&0&0&0&0&0&0&0&1&1&1&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&1&1&1&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&1&1&1 \\ 0&0&0&0&0&1&0&0&0&0&1&1&0&0&1 \\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&0 \\ 0&0&0&0&0&0&0&1&0&0&0&1&0&1&1 \\ 0&0&0&0&0&0&0&0&1&0&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&1&1&0&1&0&1 \end{array}\right]$$

$\underline{I_k}$ $\underline{A_{n-k}}$