Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

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

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

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

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

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

    (gerade Anzahl von Einsen in den Codewörten **c**)
  - Paritätskontrolle ist systematisch
  - kein Fehler korrigierbar, ungerade Anzahl von Fehlern erkennbar
  - Paritätskontrolle:

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel: $k = 3$

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

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

u_0	u_1	u_2	u_3			
↓	↓	↓	↓			
c_0	c_1	c_2	c_3	c_4	c_5	c_6

  - Kontrollstellen:

$$c_4 = c_0 + c_1 + c_2 \tag{3.8}$$

$$c_5 = c_0 + c_1 \qquad + c_3 \tag{3.9}$$

$$c_6 = c_0 \qquad + c_2 + c_3 \tag{3.10}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Matrix-Darstellung von Blockcodes

$$\boxed{\mathbf{x} = \mathbf{u}\,\mathbf{G}} \qquad (3.11)$$

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

- Systematische Blockcodes:

$$\boxed{\mathbf{G} = [\mathbf{I}_k\ \mathbf{P}]} \qquad (3.12)$$

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

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix}}_{\mathbf{u}} \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & | & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & | & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & | & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & | & 0 & 1 & 1 \end{pmatrix}}_{\mathbf{G}} = \underbrace{\begin{pmatrix} 1 & 0 & 0 & 1 & | & 1 & 0 & 0 \end{pmatrix}}_{\mathbf{x}}$$

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Codewort-Tabelle

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

$$
\begin{aligned}
d_{\min} &= \min\left(d_{\mathrm{H}}(\mathbf{c}_1,\mathbf{c}_2) \mid \mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C};\ \mathbf{c}_1 \neq \mathbf{c}_2\right) \\
&= \min\left(w_{\mathrm{H}}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C};\ \mathbf{c} \neq \mathbf{0}\right) = w_{\min} \qquad (3.14)
\end{aligned}
$$

  - Beweis:

$$
\begin{aligned}
d_{\min} &= \min\left(d_{\mathrm{H}}(\mathbf{c}_1,\mathbf{c}_2) \mid \mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C};\ \mathbf{c}_1 \neq \mathbf{c}_2\right) \\
&= \min\left(d_{\mathrm{H}}(\mathbf{0},\mathbf{c}_1+\mathbf{c}_2) \mid \mathbf{c}_1,\mathbf{c}_2 \in \mathcal{C};\ \mathbf{c}_1 \neq \mathbf{c}_2\right) \\
&= \min\left(d_{\mathrm{H}}(\mathbf{0},\mathbf{c}) \mid \mathbf{c} \in \mathcal{C};\ \mathbf{c} \neq \mathbf{0}\right) \\
&= \min\left(w_{\mathrm{H}}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C};\ \mathbf{c} \neq \mathbf{0}\right)
\end{aligned}
$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

$$s_0 = y_0 + y_1 + y_2 + y_4 \qquad (3.15)$$

$$s_1 = y_0 + y_1 + y_3 + y_5 \qquad (3.16)$$

$$s_2 = y_0 + y_2 + y_3 + y_6 \qquad (3.17)$$

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Nachweis der Orthogonalität:

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

Dualer Code

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

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

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

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel für duale Codes:
  - Wiederholungscode

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

  - Paritätskontrolle:

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Syndromberechnung in Matrix-Schreibweise:

$$\boxed{\mathbf{s} = \mathbf{y}\,\mathbf{H}^{\mathrm{T}}} \qquad (3.26)$$

Eigenschaften des Syndroms:

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

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

$$\mathbf{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & | & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & | & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & | & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & | & 0 & 1 & 1 \end{bmatrix} \qquad \mathbf{P} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$$

$$\mathbf{H} = (\mathbf{P}^{\mathrm{T}}\ \mathrm{I}_{n-k}) = \begin{bmatrix} 1 & 1 & 1 & 0 & | & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & | & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & | & 0 & 0 & 1 \end{bmatrix}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

Beispiel: (7,4)-Hamming-Code

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

    $$\mathbf{s} = \mathbf{f}\,\mathbf{H}^{\mathrm{T}} \qquad (3.28)$$

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Prüfmatrix eines systematischen Hamming-Codes:

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

alle möglichen Spaltenvektoren mit mehr als einer 1

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

$$\mathbf{H} = \left[\begin{array}{ccccccccccc|cccc} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \tag{3.30}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

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

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

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

    $n' < n,\quad k' < k,\quad m' = m,\quad R_C' < R_C,\quad d_{\min}' \geq d_{\min}$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fehlerkorrektur und Fehlererkennung
  - minimale Distanz zwischen Codewörtern:

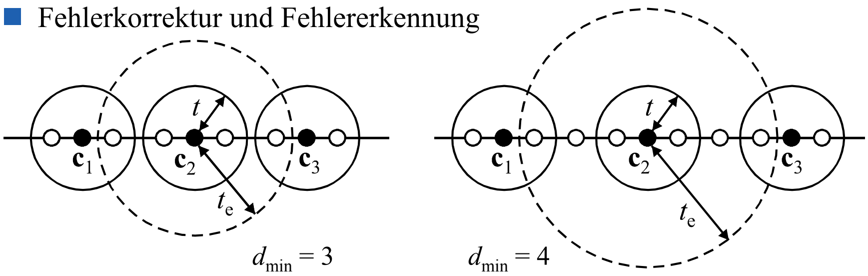
$$d_{\text{min}} = \min\left(d_{\text{H}}(\mathbf{c}_1, \mathbf{c}_2) \mid \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}\right) \qquad (3.32)$$

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fehlerkorrektur und Fehlererkennung



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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

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

  - Gesamtzahl aller Vektoren innerhalb von Decodierkugeln:

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

■

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Perfekte Codes (dichtgepackte Codes)
  - in (3.39) gilt Gleichheitszeichen
  - keine Codewörter liegen zwischen den Codierkugeln
  - nur sehr wenige bekannte Codes sind perfekt

  - Hamming-Codes sind perfekt
  - Beispiel: (7,4)-Hamming-Code
    - $d_{\min} = w_{\min} = 3 \qquad \Rightarrow \qquad t = 1$

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

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

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

  - Näherung: $d_{\min} \leq \frac{n}{2}$ für $2^k >> 1$

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

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Gilbert-Varshamov-Schranke:
  - Es existiert ein binärer (n,k)-Blockcode mit der minimalen Distanz $d_{\min}$, wenn für die Parameter n, k, $d_{\min}$ gilt:

$$\boxed{\sum_{i=0}^{d_{\min}-2} \binom{n-1}{i} < 2^{n-k}} \tag{3.42}$$

  - Schranke, die die Existenz eines Codes garantiert, aber keine Konstruktionsvorschrift liefert

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beweis: Prüfmatrix

$$\mathbf{H} = \begin{pmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,n} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k,1} & h_{n-k,2} & \cdots & h_{n-k,n} \end{pmatrix} = \begin{pmatrix} \mathbf{h}_{\mathrm{S}1} & \mathbf{h}_{\mathrm{S}2} & \ldots & \mathbf{h}_{\mathrm{S}n} \end{pmatrix}$$

  - **c** sei Codewort: $\mathbf{c}\,\mathbf{H}^{\mathrm{T}} = \mathbf{0} \quad \Rightarrow \quad \mathbf{H}\,\mathbf{c}^{\mathrm{T}} = \sum_{i=1}^{n} c_i\, \mathbf{h}_{\mathrm{S}i} = \mathbf{0}$
  - jedes Codewort besitzt mindestens $w_{\min} = d_{\min}$ Einsen
    $\Rightarrow d_{\min}$ Spalten von **H** sind linear abhängig
    $\Rightarrow (d_{\min} - 1)$ Spalten von **H** sind nicht linear abhängig

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Eine Spalte $\mathbf{h}_{Sj}$ und $(d_{\min} - 2)$ weitere Spalten müssen linear unabhängig sein.
- Dies ist erfüllbar, wenn Spalte $\mathbf{h}_{Sj}$ mehr unterschiedliche Spaltenvektoren erzeugen kann als unterschiedliche Linearkombinationen mit den $(d_{\min} - 2)$ weiteren Spalten möglich sind.
- Anzahl unterschiedlicher Spalten von $\mathbf{h}_{Sj}$: 2^{n-k}
- Anzahl von Linearkombinationen mit genau i Spalten in $(n-1)$ Spalten: $\binom{n-1}{i}$
- Gesamtzahl von Linearkombinationen von 1 ... $(d_{\min} - 2)$ Spalten:

$$\sum_{i=0}^{d_{\min}-2} \binom{n-1}{i} < 2^{n-k}$$

Nachrichtentechnik 4

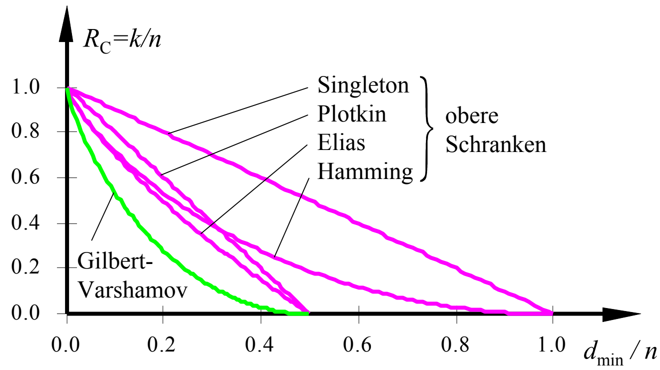
3 Kanalcodierung in der Nachrichtenübertragung

- Schranken für große Codewortlängen ($n \to \infty$):
  - Zusammenhang zwischen Coderate R_C und normierter Distanz $d_{\min}/n$
  - Singleton-Schranke: $$R_C \le 1 - \frac{d_{\min}}{n} \qquad (3.43)$$
  - Hamming-Schranke: $$R_C \le 1 - S\left(\frac{1}{2} \cdot \frac{d_{\min}}{n}\right) \qquad (3.44)$$
  - Plotkin-Schranke: $$R_C \le 1 - 2 \cdot \frac{d_{\min}}{n} \qquad (3.45)$$
  - Elias-Schranke: $$R_C \le 1 - S\left(\frac{1}{2}\left(1 - \sqrt{1 - 2\frac{d_{\min}}{n}}\right)\right) \qquad (3.46)$$
  - Gilbert-Varshamov-Schranke: $$R_C \ge 1 - S\left(\frac{d_{\min}}{n}\right) \qquad (3.47)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- asymptotische Schranken ($n \to \infty$) zwischen Coderate R_C und normierter Distanz d_{min} / n



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Gewichtsverteilung
  - Anzahl von Codewörtern, die das Gewicht i besitzen: A_i
  - Gewichtsfunktion: zwei Schreibweisen

$$\boxed{A(z) = \sum_{i=0}^{n} A_i \, z^i} \quad (3.48) \qquad \boxed{W(x,y) = \sum_{i=0}^{n} A_i \, x^{n-i} \, y^i} \quad (3.49)$$

$$= W(1, z) \qquad\qquad = x^n \, A\left(\frac{y}{x}\right)$$

  - nur für wenige Codes geschlossen berechenbar
  - Gewichtsverteilung linearer Codes:

    $A_0 = 1; \quad A_n \le 1$

    $A_i = 0$ für $0 < i < d_{min}$
  - manche Codes: symmetrische Gewichtsverteilung: $A_i = A_{n-i}$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel: (4,3)-Paritätskontrolle

Codewort	Information	Prüfstelle	Gewicht
$\mathbf{c}_0$	000	0	0
$\mathbf{c}_1$	001	1	2
$\mathbf{c}_2$	010	1	2
$\mathbf{c}_3$	011	0	2
$\mathbf{c}_4$	100	1	2
$\mathbf{c}_5$	101	0	2
$\mathbf{c}_6$	110	0	2
$\mathbf{c}_7$	111	1	4

$$A(z) = 1 + 6z^2 + z^4$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Gewichtsverteilung ermöglicht exakte Berechnung der Restfehlerwahrscheinlichkeit

- MacWilliams-Identität
  - gegeben: (n,k)-Blockcode mit Gewichtsfunktion $A(z)$
  - Gewichtsfunktion des dualen Codes:

$$\boxed{A_\mathrm{d}(z) = 2^{-k} \cdot (1+z)^n \cdot A\left(\frac{1-z}{1+z}\right)} \quad \boxed{A(z) = 2^{-(n-k)} \cdot (1+z)^n \cdot A_\mathrm{d}\left(\frac{1-z}{1+z}\right)} \tag{3.50}$$

  - bzw.:

$$\boxed{W_\mathrm{d}(x,y) = 2^{-k} \cdot W(x+y, x-y)} \quad \boxed{W(x,y) = 2^{-(n-k)} \cdot W_\mathrm{d}(x+y, x-y)} \tag{3.51}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel:
  - Code $\mathcal{C}$ = {000,011,101,110} (Paritätskontrolle)

    Generatormatrix: $\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$

    Gewichtsfunktion: $A(z) = 1 + 3\,z^2$

  - dualer Code $\mathcal{C}_\mathrm{d}$ = {000,111} (Wiederholungscode)

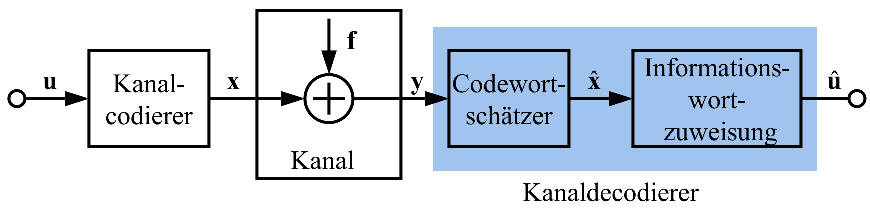
    Generatormatrix: $\mathbf{G}_\mathrm{d} = (\,1 \quad 1 \quad 1\,)$

    Gewichtsfunktion: $A_\mathrm{d}(z) = 2^{-2} \cdot (1+z)^3 \cdot \left[1 + 3\left(\frac{1-z}{1+z}\right)^2\right] = 1 + z^3$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Kanalcodierung und -decodierung



- Strategien zur Decodierung
  - Ziel: minimale Wort-Fehlerwahrscheinlichkeit

$$p_\mathrm{W} = p(\hat{\mathbf{u}} \neq \mathbf{u}) = p(\hat{\mathbf{x}} \neq \mathbf{x}) \tag{3.52}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- mögliche Ergebnisse einer Übertragung:
  - $\mathbf{y} = \mathbf{x}$ fehlerfreie Übertragung

    Decodierergebnis: $\hat{\mathbf{x}} = \mathbf{x}, \quad \hat{\mathbf{u}} = \mathbf{u}$
  - $\mathbf{y} \neq \mathbf{x}, \ \mathbf{y} \in \mathcal{C}$ Verfälschung in ein anderes Codewort, nicht korrigierbar

    Decodierergebnis: $\hat{\mathbf{x}} \neq \mathbf{x}, \quad \hat{\mathbf{u}} \neq \mathbf{u}$
  - $\mathbf{y} \neq \mathbf{x}, \ \mathbf{y} \notin \mathcal{C}$ fehlerhafte Übertragung, Fehler erkennbar, u.U. korrigierbar

    Decodierergebnis: $\hat{\mathbf{x}} \left\{ \begin{matrix} = \\ \neq \end{matrix} \right\} \mathbf{x}, \quad \hat{\mathbf{u}} \left\{ \begin{matrix} = \\ \neq \end{matrix} \right\} \mathbf{u}$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Mögliche Decodierergebnisse
  - korrekte Decodierung: $\hat{\mathbf{x}} = \mathbf{x}, \quad \hat{\mathbf{u}} = \mathbf{u}$
    - Kanal ohne Fehler
    - Fehler wurden richtig korrigiert
  - fehlerhafte Decodierung: $\hat{\mathbf{x}} \neq \mathbf{x}, \quad \hat{\mathbf{u}} \neq \mathbf{u}$
    - Fehler ist aufgetreten, wurde aber fehlerhaft korrigiert (z.B. Sende-Codewort wurde durch Fehler in anderes gültiges Codewort verändert)
  - Decodierversagen
    - Fehler ist aufgetreten, Decodierer findet keine Lösung

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Wortfehlerwahrscheinlichkeit für einen DMC

$$p_W = p(\hat{\mathbf{x}} \neq \mathbf{x}) = \sum_{\mathbf{x}\in\mathcal{C}} p(\hat{\mathbf{x}} \neq \mathbf{x} \mid \mathbf{x} \text{ gesendet}) \cdot p(\mathbf{x} \text{ gesendet}) \tag{3.53}$$

- Wahrscheinlichkeit eines Fehlers:

$$p(\hat{\mathbf{x}} \neq \mathbf{x} \mid \mathbf{x} \text{ gesendet}) = \sum_{\mathbf{y}|\hat{\mathbf{x}}\neq\mathbf{x}} p(\mathbf{y} \text{ empfangen} \mid \mathbf{x} \text{ gesendet}) = \sum_{\mathbf{y}|\hat{\mathbf{x}}\neq\mathbf{x}} p(\mathbf{y} \mid \mathbf{x}) \tag{3.54}$$

- Annahme: gesendete Codeworte sind gleichwahrscheinlich

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Wortfehlerwahrscheinlichkeit

$$\begin{aligned}
p_W &= \sum_{\mathbf{x}\in\mathcal{C}} \sum_{\mathbf{y}|\hat{\mathbf{x}}\neq\mathbf{x}} p(\mathbf{y} \mid \mathbf{x}) \cdot 2^{-k} \\
&= 2^{-k} \cdot \Big[\sum_{\mathbf{x}\in\mathcal{C}} \sum_{\mathbf{y}} p(\mathbf{y} \mid \mathbf{x}) - \sum_{\mathbf{x}\in\mathcal{C}} \sum_{\mathbf{y}|\hat{\mathbf{x}}=\mathbf{x}} p(\mathbf{y} \mid \mathbf{x}) \Big] \\
&= 1 - 2^{-k} \cdot \sum_{\mathbf{x}\in\mathcal{C},\mathbf{y}|\hat{\mathbf{x}}=\mathbf{x}} p(\mathbf{y} \mid \mathbf{x}) \\
&= 1 - 2^{-k} \cdot \sum_{\mathbf{y}} p(\mathbf{y} \mid \hat{\mathbf{x}})
\end{aligned} \tag{3.55}$$

- $\hat{\mathbf{x}}$ muss so gewählt werden, dass $p(\mathbf{y} \mid \hat{\mathbf{x}})$ maximal wird

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Optimale Empfangsstrategien
  - Kenntnis eines Empfängers: $\mathbf{y}$
  - Strategie eines Empfängers: maximiere die A-posteriori-Wahrscheinlichkeit $p(\mathbf{x}|\mathbf{y})$
  - **MAP(maximum a posteriori)-Decodierer:**

    Suche das Codewort $\mathbf{x} = \hat{\mathbf{x}}$, für das $p(\mathbf{x}|\mathbf{y})$ maximal wird.

$$\boxed{p(\mathbf{x} = \hat{\mathbf{x}} \mid \mathbf{y}) \geq p(\mathbf{x} \mid \mathbf{y}) \quad \text{für alle} \quad \mathbf{x} \in \mathcal{C}} \tag{3.56}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Bayes-Theorem: $p(\mathbf{x} \mid \mathbf{y}) = \dfrac{p(\mathbf{y} \mid \mathbf{x}) \cdot p(\mathbf{x})}{p(\mathbf{y})}$ (3.57)
- Annahme: gleichwahrscheinliche Informations- / Codewörter: (gleiche A-priori-Wahrscheinlichkeiten): $p(\mathbf{x}_i) = 2^{-k}$

  $\Rightarrow \quad p(\mathbf{x} \mid \mathbf{y}) = k_0(\mathbf{y}) \cdot p(\mathbf{y} \mid \mathbf{x})$
- $p(\mathbf{y}|\mathbf{x})$ = Likelihood-Funktion
- A-posteriori-Wahrscheinlichkeit und Likelihood-Funktion haben das Maximum an der gleichen Stelle $\mathbf{x} = \hat{\mathbf{x}}$
- **Maximum-Likelihood-Decodierer:**

  Suche das Codewort $\mathbf{x} = \hat{\mathbf{x}}$, für das $p(\mathbf{y}|\mathbf{x})$ maximal wird.

$$\boxed{p(\mathbf{y} \mid \mathbf{x} = \hat{\mathbf{x}}) \geq p(\mathbf{y} \mid \mathbf{x}) \quad \text{für alle} \quad \mathbf{x} \in \mathcal{C}} \tag{3.58}$$

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Maximum-Likelihood-Decoder minimiert Wortfehlerwahrscheinlichkeit
- Maximum-Likelihood-Decoder bei einem BSC:

$$p(\mathbf{y}\,|\,\mathbf{x}) = \prod_{i=0}^{n-1} p(y_i\,|\,x_i) = \prod_{i=0}^{n-1} \begin{Bmatrix} 1-p_{\mathrm{err}} & \text{für} & y_i = x_i \\ p_{\mathrm{err}} & \text{für} & y_i \neq x_i \end{Bmatrix}$$

$$= (1-p_{\mathrm{err}})^{n-d_{\mathrm{H}}(\mathbf{y},\mathbf{x})} \cdot p_{\mathrm{err}}{}^{d_{\mathrm{H}}(\mathbf{y},\mathbf{x})} = (1-p_{\mathrm{err}})^n \cdot \left(\frac{p_{\mathrm{err}}}{1-p_{\mathrm{err}}}\right)^{d_{\mathrm{H}}(\mathbf{y},\mathbf{x})} \qquad (3.59)$$

- Schätzergebnis ist Codewort mit geringster Hammingdistanz zum Empfangsvektor

$$\boxed{d_{\mathrm{H}}(\mathbf{y},\hat{\mathbf{x}}) \leq d_{\mathrm{H}}(\mathbf{y},\mathbf{x}) \quad \text{für alle} \quad \mathbf{x} \in \mathcal{C}} \qquad (3.60)$$

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel:
  - Code $\mathcal{C} = \{\mathbf{c}_1,\mathbf{c}_2,\mathbf{c}_3,\mathbf{c}_4\} = \{00000,11100,00111,11011\}$
  - $d_{\min} = 3$
  - Beispiel für Maximum-Likelihood-Decodierung:

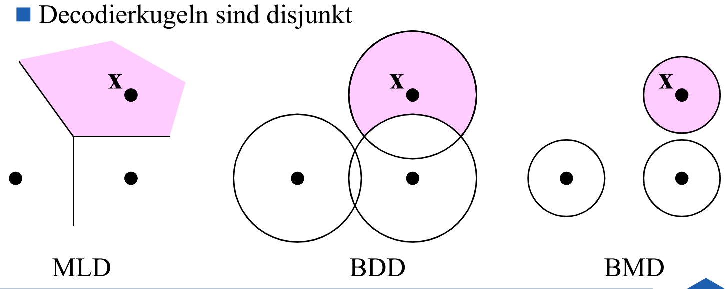
$\mathbf{y}$	$d_{\mathrm{H}}(\mathbf{y},\mathbf{c}_1)$	$d_{\mathrm{H}}(\mathbf{y},\mathbf{c}_2)$	$d_{\mathrm{H}}(\mathbf{y},\mathbf{c}_3)$	$d_{\mathrm{H}}(\mathbf{y},\mathbf{c}_4)$	$\hat{\mathbf{x}}$
00111	3	4	0	3	$\mathbf{c}_3$
10000	1	2	4	3	$\mathbf{c}_1$
11000	2	1	5	2	$\mathbf{c}_2$
10001	2	3	3	2	$\mathbf{c}_1$ oder $\mathbf{c}_4$

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- Maximum-Likelihood-Decodierung (MLD): optimales Verfahren
  - großer Decodieraufwand
  - Anzahl der notwendigen Vektorvergleiche: 2^k
  - u. U. mehr als t Fehler korrigierbar
- begrenzte Distanz-Decodierung (BDD)
  - Kugel um jedes Codewort mit Radius t_0,
  - Decodierung nur für Empfangsvektoren **y**, die in genau einer Kugel liegen
  - Empfangsvektoren **y**, die in keiner oder mehreren Kugeln liegen, werden nicht decodiert

Nachrichtentechnik 4
3 Kanalcodierung in der Nachrichtenübertragung

- **Begrenzte Mindestdistanz-Decodierung (BMD)**
  - Kugel um jedes Codewort mit Radius t,
  - Decodierung nur für Empfangsvektoren **y**, die in einer Kugel liegen
  - Decodierkugeln sind disjunkt



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- weitere suboptimale Decodierverfahren:
  - Syndrom-Decodierung
    - einfache Realisierung
    - suboptimal, da nicht sämtliche Information genutzt wird
  - Mehrheitsentscheidung

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Wahrscheinlichkeit von Fehlern in Codeworten
  - Übertragungskanal: symmetrischer Binärkanal mit Fehlerwahrscheinlichkeit p_{err}
  - mittlere Fehlerzahl in einem Codewort: $\langle n_{\text{Fehler}} \rangle = n \cdot p_{\text{err}}$
  - Wahrscheinlichkeit keines Fehlers:

$$p(\mathbf{f} = \mathbf{0}) = \underbrace{(1 - p_{\text{err}}) \cdot (1 - p_{\text{err}}) \cdot \ldots \cdot (1 - p_{\text{err}})}_{n \text{ Faktoren}} = (1 - p_{\text{err}})^n \qquad (3.61)$$

  - Wahrscheinlichkeit eines einzelnen Fehlers an einer bestimmten Stelle ($\mathbf{f} = \mathbf{f}_1$, $w_{\text{H}}(\mathbf{f}_1) = 1$):

$$p(\mathbf{f} = \mathbf{f}_1) = p_{\text{err}} \cdot (1 - p_{\text{err}})^{n-1} \qquad (3.62)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Wahrscheinlichkeit eines einzelnen Fehlers an einer beliebigen Stelle ($\mathbf{f} = \mathbf{f}_1$, $w_\mathrm{H}(\mathbf{f}_1) = 1$):

$$p(\mathbf{f} = \mathbf{f}_1) = n \cdot p_\mathrm{err} \cdot (1 - p_\mathrm{err})^{n-1} \tag{3.63}$$

- Wahrscheinlichkeit von n_e Fehlern an beliebigen Stellen ($\mathbf{f} = \mathbf{f}_{n_\mathrm{e}}$, $w_\mathrm{H}(\mathbf{f}_{n_\mathrm{e}}) = n_\mathrm{e}$):

$$\boxed{p(\mathbf{f} = \mathbf{f}_{n_\mathrm{e}}) = \binom{n}{n_\mathrm{e}} \cdot p_\mathrm{err}{}^{n_\mathrm{e}} \cdot (1 - p_\mathrm{err})^{n-n_\mathrm{e}}} \tag{3.64}$$

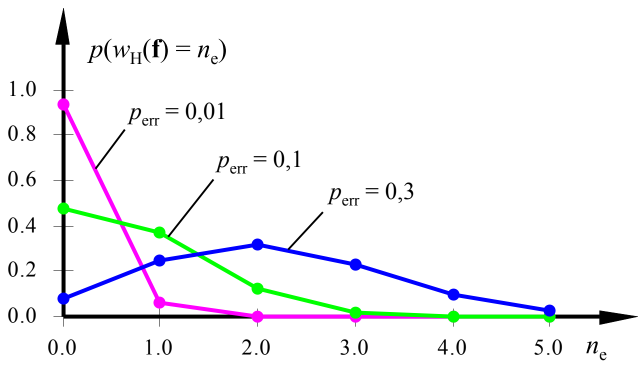
- Binomial-koeffizienten: $\binom{n}{k} = \dfrac{n!}{k! \cdot (n-k)!} = \binom{n}{n-k} \quad ; \quad \binom{n}{0} = \binom{n}{n} = 1$ (3.65)

- binomische Formel: $\sum\limits_{k=0}^{n} \binom{n}{k} a^k\, b^{n-k} = (a+b)^n \quad ; \quad \sum\limits_{k=0}^{n} \binom{n}{k} = 2^n$ (3.66)

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Binomialverteilung der Bitfehler je Codewort für $n = 7$



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Fehlererkennung: unerkannte Fehler
  - linearer Blockcode $\mathcal{C} = \{\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{2^k-1}\}$
    mit $\mathbf{c}_\nu = (c_{\nu,0}, c_{\nu,1}, \ldots, c_{\nu,n-1})$ und $\mathbf{c}_0 = \mathbf{0}$
  - Fehler bleibt nur dann unerkannt, wenn $\mathbf{f} \in \mathcal{C}$ und $\mathbf{f} \neq \mathbf{0}$
  - Wahrscheinlichkeit unerkannter Fehler p_{ue} (ue = undetected error):

$$p_{\text{ue}} = p(\mathbf{f} \in \mathcal{C} \cap \mathbf{f} \neq \mathbf{0}) = \sum_{\nu=1}^{2^k-1} p(\mathbf{f} = \mathbf{c}_\nu) \qquad (3.67)$$

  - unerkannter Fehler: $\mathbf{f} = \mathbf{c}_\nu$

$\Rightarrow\ f_j = c_{\nu,j} = 0$ an $n - w_{\text{H}}(\mathbf{c}_\nu)$ Stellen mit $p(f_j = 0) = 1 - p_{\text{err}}$

$\Rightarrow\ f_j = c_{\nu,j} = 1$ an $w_{\text{H}}(\mathbf{c}_\nu)$ Stellen mit $p(f_j = 1) = p_{\text{err}}$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Wahrscheinlichkeit unerkannter Fehler p_{ue}:

$$p_{\text{ue}} = \sum_{\nu=1}^{2^k-1} p(\mathbf{f} = \mathbf{c}_\nu) = \sum_{\nu=1}^{2^k-1} (1 - p_{\text{err}})^{n - w_{\text{H}}(\mathbf{c}_\nu)} \cdot p_{\text{err}}{}^{w_{\text{H}}(\mathbf{c}_\nu)} \qquad (3.68)$$

- Summation über das Gewicht der Codeworte:

$$p_{\text{ue}} = \sum_{i=d_{\min}}^{n} A_i \cdot (1 - p_{\text{err}})^{n-i} \cdot p_{\text{err}}{}^{i} \qquad (3.69)$$

- mit $A\left(\dfrac{p_{\text{err}}}{1 - p_{\text{err}}}\right) = 1 + \sum_{i=d_{\min}}^{n} A_i \cdot p_{\text{err}}{}^{i} \cdot (1 - p_{\text{err}})^{-i}$ erhält man:

$$\boxed{p_{\text{ue}} = (1 - p_{\text{err}})^n \left[A\left(\frac{p_{\text{err}}}{1 - p_{\text{err}}}\right) - 1 \right]} \qquad (3.70)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Näherung für kleine Fehlerwahrscheinlichkeiten:

$$p_{\text{ue}} \approx \sum_{i=d_{\min}}^{n} A_i \cdot p_{\text{err}}{}^{i} = A(p_{\text{err}}) - 1 \approx A_{d_{\min}} \cdot p_{\text{err}}{}^{d_{\min}} \qquad (3.71)$$

- Beispiel: (7,4)-Hamming-Code
  - Gewichtsfunktion: $A(z) = 1 + 7\,z^3 + 7\,z^4 + z^7$
  - $d_{\min} = 3$
  - $p_{\text{ue}} = 7\,(1 - p_{\text{err}})^4\, p_{\text{err}}{}^3 + 7\,(1 - p_{\text{err}})^3\, p_{\text{err}}{}^4 + p_{\text{err}}{}^7$
    $= 7\,p_{\text{err}}{}^3 - 21\,p_{\text{err}}{}^4 + 21\,p_{\text{err}}{}^5 - 7\,p_{\text{err}}{}^6 + p_{\text{err}}{}^7 \approx 7\,p_{\text{err}}{}^3$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Restfehlerwahrscheinlichkeit
  - linearer Blockcode $\mathcal{C} = \{\mathbf{c}_0, \mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_{2^k-1}\}$ mit Korrekturfähigkeit t
  - Annahme: begrenzte Mindestdistanz-Decodierung (BMD)
  - Wortfehlerwahrscheinlichkeit:

$$\begin{aligned} p_{\text{W,BMD}} &= 1 - p(\text{richtige Decodierung}) \\ &= 1 - p(w_{\text{H}}(\mathbf{f}) \le t) = p(w_{\text{H}}(\mathbf{f}) \ge t+1) \\ &= 1 - \sum_{i=0}^{t} p(w_{\text{H}}(\mathbf{f}) = i) = \sum_{i=t+1}^{n} p(w_{\text{H}}(\mathbf{f}) = i) \end{aligned} \qquad (3.72)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Wahrscheinlichkeit von Fehlervektoren mit Gewicht $w_{\mathrm{H}}(\mathbf{f}) = i$ (Gl. (3.64)):

$$p(w_{\mathrm{H}}(\mathbf{f}) = i) = \binom{n}{i} \cdot p_{\mathrm{err}}{}^{i} \cdot (1 - p_{\mathrm{err}})^{n-i} \qquad (3.73)$$

- Wortfehlerwahrscheinlichkeit bei BMD:

$$\boxed{p_{\mathrm{W,BMD}} = 1 - \sum_{i=1}^{t} \binom{n}{i} p_{\mathrm{err}}^{i} \, (1 - p_{\mathrm{err}})^{n-i} = \sum_{i=t+1}^{n} \binom{n}{i} p_{\mathrm{err}}^{i} \, (1 - p_{\mathrm{err}})^{n-i}} \qquad (3.74)$$

- Näherung für kleine Fehlerwahrscheinlichkeiten:

$$p_{\mathrm{W,BMD}} \approx \binom{n}{t+1} p_{\mathrm{err}}^{t+1} \qquad (3.75)$$

- Wortfehlerwahrscheinlichkeit bei MLD:

$$p_{\mathrm{W,MLD}} \leq p_{\mathrm{W,BMD}} \qquad (3.76)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Abschätzung der Bitfehlerwahrscheinlichkeit

$$p_{\mathrm{bit}} = \frac{1}{k} \langle \text{Anzahl der Bitfehler pro decodiertem Wort} \rangle$$

$$= \frac{1}{k} \sum_{i=0}^{n} \langle \text{Anz. d. Bitfehler pro decod. Wort} \mid w_{\mathrm{H}}(\mathbf{f}) = i \rangle \cdot p(w_{\mathrm{H}}(\mathbf{f}) = i) \qquad (3.77)$$

- Anzahl der Bitfehler ist begrenzt auf die Anzahl der Informationsbits k und $i + t$:

$$d_{\mathrm{H}}(\mathbf{x}, \hat{\mathbf{x}}) \leq \underbrace{d_{\mathrm{H}}(\mathbf{x}, \mathbf{y})}_{= i} + \underbrace{d_{\mathrm{H}}(\mathbf{y}, \hat{\mathbf{x}})}_{\leq t} \qquad (3.78)$$

- $\Rightarrow \quad p_{\mathrm{bit}} \leq \frac{1}{k} \sum_{i=t+1}^{n} \min(k, i+t) \cdot p(w_{\mathrm{H}}(\mathbf{f}) = i) \qquad (3.79)$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Abschätzung der Bitfehlerwahrscheinlichkeit:

$$\boxed{p_{\text{bit}} \leq \sum_{i=t+1}^{n} \min\left(1, \frac{i+t}{k}\right) \cdot \binom{n}{i} \cdot p_{\text{err}}^{i} \cdot (1-p_{\text{err}})^{n-i}} \qquad (3.80)$$

- Näherung für kleine Fehlerwahrscheinlichkeiten:

$$p_{\text{bit}} \approx \min\left(1, \frac{d_{\min}}{k}\right) \cdot \binom{n}{t+1} \cdot p_{\text{err}}^{t+1} \qquad (3.81)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

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

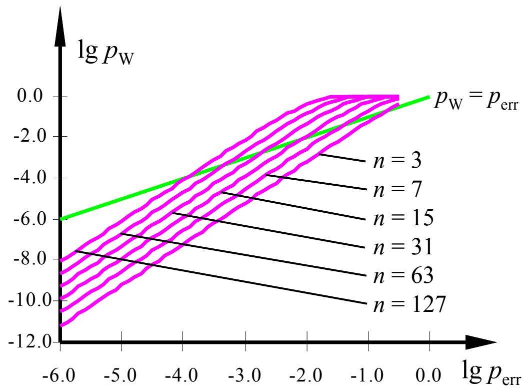
$$\begin{aligned} p_{\text{W}} &= 1 - \binom{7}{0} p_{\text{err}}^{0} \, (1-p_{\text{err}})^{7} - \binom{7}{1} p_{\text{err}}^{1} \, (1-p_{\text{err}})^{6} \\ &= 1 - (1-p_{\text{err}})^{7} - 7\, p_{\text{err}} \, (1-p_{\text{err}})^{6} \\ &= 1 - (1 - 7\, p_{\text{err}} + 21\, p_{\text{err}}^{2} - p_{\text{err}}^{3} \ldots) - 7\, p_{\text{err}} \, (1 - 6\, p_{\text{err}} + p_{\text{err}}^{2} \ldots) \\ &\approx 21\, p_{\text{err}}^{2} = \binom{7}{2} p_{\text{err}}^{2} \end{aligned} \qquad (3.82)$$

- Gleichheitszeichen, da Code perfekt

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

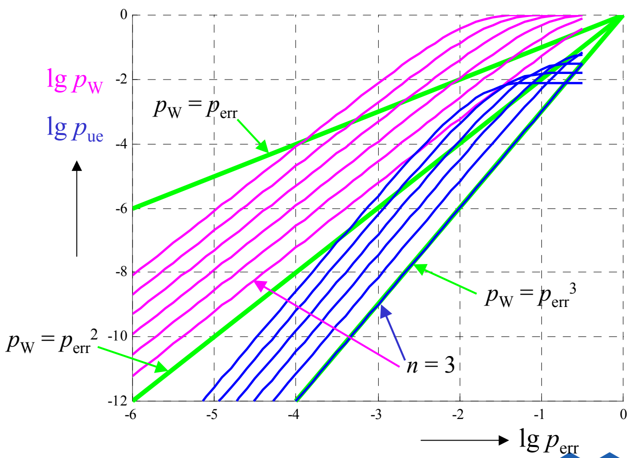
- Wortfehlerwahrscheinlichkeit von Hamming-Codes:



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Wortfehlerwahrscheinlichkeit und Wahrscheinlichkeit unerkannter Fehler von Hamming-Codes:



Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- minimale Distanz allgemeiner Hamming-Codes
- alle Spalten der Prüfmatrix unterscheiden sich

  $\Rightarrow$ zwei Spalten sind linear unabhängig
- drei Spalten sind linear abhängig,
  z. B. 100000...., 010000.... und 110000....
- $\Rightarrow d_{\min} = 3, \quad t = 1$
- Gewichtsfunktion:

$$A(z) = \frac{1}{n+1}\left[(1+z)^n + n \cdot (1+z)^{\frac{n-1}{2}} \cdot (1-z)^{\frac{n+1}{2}}\right] \qquad (3.83)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Produkte zweier Vektoren

  $\mathbf{x} = (x_0, x_1, x_2, \ldots, x_{n-1}) \quad , \quad \mathbf{y} = (y_0, y_1, y_2, \ldots, y_{n-1})$

  - Skalarprodukt

$$\mathbf{x} \cdot \mathbf{y}^{\mathrm{T}} = x_0 \cdot y_0 + x_1 \cdot y_1 + x_2 \cdot y_2 + \ldots + x_{n-1} \cdot y_{n-1} \qquad (3.84)$$

  - Vektorprodukt

$$\mathbf{x} \times \mathbf{y} = (x_0 y_0, x_1 y_1, x_2 y_2, \ldots, x_{n-1} y_{n-1}) \qquad (3.85)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Summenkonstruktion von Codes
  - linearer $(n,k_1,d_{\min,1})$-Blockcode $\mathcal{C}_1$ und
    linearer $(n,k_2,d_{\min,2})$-Blockcode $\mathcal{C}_2$
  - Summenkonstruktion: linearer $(2n,k_1+k_2,d_{\min})$-Blockcode $\mathcal{C}$

    $\mathcal{C} = \mathcal{C}_1 \,\&\, \mathcal{C}_2 = \{(\mathbf{c}_1, \mathbf{c}_1 + \mathbf{c}_2)\}$ mit $\mathbf{c}_1 \in \mathcal{C}_1$ und $\mathbf{c}_2 \in \mathcal{C}_2$
  - Generatormatrix:

$$\boxed{\mathbf{G} = \begin{pmatrix} \mathbf{G}_1 & \mathbf{G}_1 \\ \mathbf{0} & \mathbf{G}_2 \end{pmatrix}} \qquad (3.86)$$

  - Distanz:

$$\boxed{d_{\min} = \min(2d_{\min,1}, d_{\min,2})} \qquad (3.87)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beweis:

$(\mathbf{c}_1, \mathbf{c}_1) \in \mathcal{C}$ und $(0, \mathbf{c}_2) \in \mathcal{C}$

$\Rightarrow \quad d_{\min} \le \min(2d_{\min,1}, d_{\min,2})$

für $\mathbf{c}_2 = \mathbf{0}$ und $\mathbf{c}_1 \ne \mathbf{0}$ gilt: $\quad w_{\mathrm{H}}((\mathbf{c}_1, \mathbf{c}_1)) = 2\, w_{\mathrm{H}}(\mathbf{c}_1) \ge 2\, d_1$

für $\mathbf{c}_2 \ne \mathbf{0}$ und $\mathbf{c}_1 \ne \mathbf{0}$ gilt:

$$w_{\mathrm{H}}((\mathbf{c}_1, \mathbf{c}_1 + \mathbf{c}_2)) = w_{\mathrm{H}}(\mathbf{c}_1) + w_{\mathrm{H}}(\mathbf{c}_1 + \mathbf{c}_2)$$
$$\ge w_{\mathrm{H}}(\mathbf{c}_1 + (\mathbf{c}_1 + \mathbf{c}_2)) = w_{\mathrm{H}}(\mathbf{c}_2) \ge d_2$$

$\Rightarrow \quad d_{\min} \ge \min(2d_{\min,1}, d_{\min,2})$ ■

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Reed-Muller-Codes
  - Summenkonstruktion
  - Parameter: r, m mit $0 \le r \le m$
  - $(n,k,d_{\min})$-Reed-Muller-Code $\mathcal{RM}(r,m)$ mit

$$n = 2^m \quad , \quad k = \sum_{i=0}^{r} \binom{m}{i} \quad , \quad d_{\min} = 2^{m-r} \qquad (3.88)$$

  - Rekursionsvorschrift:

$$\boxed{\mathcal{RM}(r+1, m+1) = \mathcal{RM}(r+1, m) \,\&\, \mathcal{RM}(r, m)} \qquad (3.89)$$

  - Anfangswerte: $\mathcal{RM}(0, m) = (2^m, 1, 2^m)$-Wiederholungscode

    $\mathcal{RM}(m, m) = (2^m, 2^m, 1)$-uncodiert

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel für die Konstruktion der Generatormatrix des Reed-Muller-Codes $\mathcal{RM}(r,m)$:

  $\mathcal{RM}(1, 2) = \mathcal{RM}(1, 1) \,\&\, \mathcal{RM}(0, 1)$

$$\mathbf{G}_{01} = \begin{pmatrix} 1 & 1 \end{pmatrix} \qquad \mathbf{G}_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \mathbf{G}_{12} = \left(\begin{array}{cc:cc} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hdashline 0 & 0 & 1 & 1 \end{array}\right) \qquad (3.90)$$

- Alternative Konstruktion:

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \\ \vdots \\ \mathbf{G}_r \end{pmatrix} \qquad (3.91)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- $\mathbf{G}_0$ = 1-Vektor der Länge $n = 2^m$: $\mathbf{G}_0 = (1\ 1\ 1\ 1\ \ldots\ 1)$
- $\mathbf{G}_1$ = $m \times 2^m$-Matrix : Spalten enthalten alle möglichen Binärwörter der Länge m
- $\mathbf{G}_l$: Vektorprodukte aller möglichen Kombinationen von l Zeilenvektoren von $\mathbf{G}_1$
- Jeder Zeile von $\mathbf{G}$ entspricht eine Informationsstelle

$\Rightarrow$

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r} = \sum_{i=0}^{r} \binom{m}{i} \qquad (3.92)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel: $m = 4, \quad r = 3 \quad \Rightarrow \quad n = 16$

$$\mathbf{G}_0 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \qquad (3.93)$$

$$\mathbf{G}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{g}_{Z1} \\ \mathbf{g}_{Z2} \\ \mathbf{g}_{Z3} \\ \mathbf{g}_{Z4} \end{pmatrix} \qquad (3.94)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

$$\mathbf{G}_2 = \begin{pmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1 \\ 0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1 \end{pmatrix} = \begin{pmatrix} \mathbf{g}_{Z1}\times\mathbf{g}_{Z2} \\ \mathbf{g}_{Z1}\times\mathbf{g}_{Z3} \\ \mathbf{g}_{Z1}\times\mathbf{g}_{Z4} \\ \mathbf{g}_{Z2}\times\mathbf{g}_{Z3} \\ \mathbf{g}_{Z2}\times\mathbf{g}_{Z4} \\ \mathbf{g}_{Z3}\times\mathbf{g}_{Z4} \end{pmatrix} \tag{3.95}$$

$$\mathbf{G}_3 = \begin{pmatrix} 0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1 \end{pmatrix} = \begin{pmatrix} \mathbf{g}_{Z1}\times\mathbf{g}_{Z2}\times\mathbf{g}_{Z3} \\ \mathbf{g}_{Z1}\times\mathbf{g}_{Z2}\times\mathbf{g}_{Z4} \\ \mathbf{g}_{Z1}\times\mathbf{g}_{Z3}\times\mathbf{g}_{Z4} \\ \mathbf{g}_{Z2}\times\mathbf{g}_{Z3}\times\mathbf{g}_{Z4} \end{pmatrix} \tag{3.96}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Alternative Konstruktion des Beispiels: $m = 2, \quad r = 1 \quad \Rightarrow \quad n = 4$

$$\mathbf{G}_{12} = \begin{pmatrix} 1&1&1&1 \\ 0&0&1&1 \\ 0&1&0&1 \end{pmatrix} \qquad\qquad \mathbf{G}_{12} = \begin{pmatrix} 1&0&1&0 \\ 0&1&0&1 \\ 0&0&1&1 \end{pmatrix}$$

$$\begin{pmatrix} 0&0&0 \\ 0&0&1 \\ 0&1&0 \\ 0&1&1 \\ 1&0&0 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix}\begin{pmatrix} 0&0&0&0 \\ 0&0&1&1 \\ 0&1&0&1 \\ 0&1&1&0 \\ 1&0&1&0 \\ 1&0&0&1 \\ 1&1&1&1 \\ 1&1&0&0 \end{pmatrix} \qquad\qquad \begin{pmatrix} 0&0&0 \\ 0&0&1 \\ 0&1&0 \\ 0&1&1 \\ 1&0&0 \\ 1&0&1 \\ 1&1&0 \\ 1&1&1 \end{pmatrix}\begin{pmatrix} 0&0&0&0 \\ 0&1&0&1 \\ 0&0&1&1 \\ 0&1&1&0 \\ 1&1&1&1 \\ 1&0&1&0 \\ 1&1&0&0 \\ 1&0&0&1 \end{pmatrix}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Minimale Distanz: Berechnung mit Hilfe des Ergebnisses der Summenkonstruktion

  $d_{\min} = \min(2d_{\min,1}, d_{\min,2})$

$$\boxed{d_{\min}\,(\mathcal{RM}(r+1, m+1)) = \min(2\, d_{\min}(\mathcal{RM}(r+1, m)),\, d_{\min,2}(\mathcal{RM}(r, m)))} \tag{3.97}$$

Tabelle: $d_{\min}\,(\mathcal{RM}(r, m)) = 2^{m-r}$ (3.98)

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

m	r / n	0	1	2	3	4	5
0	1	$k = 1$ $d_{min} = 1$					
1	2	$k = 1$ $d_{min} = 2$	$k = 2$ $d_{min} = 1$				
2	4	$k = 1$ $d_{min} = 4$	$k = 3$ $d_{min} = 2$	$k = 4$ $d_{min} = 1$			
3	8	$k = 1$ $d_{min} = 8$	$k = 4$ $d_{min} = 4$	$k = 7$ $d_{min} = 2$	$k = 8$ $d_{min} = 1$		
4	16	$k = 1$ $d_{min} = 16$	$k = 5$ $d_{min} = 8$	$k = 11$ $d_{min} = 4$	$k = 15$ $d_{min} = 2$	$k = 16$ $d_{min} = 1$	
5	32	$k = 1$ $d_{min} = 32$	$k = 6$ $d_{min} = 16$	$k = 16$ $d_{min} = 8$	$k = 26$ $d_{min} = 4$	$k = 31$ $d_{min} = 2$	$k = 32$ $d_{min} = 1$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Decodierung durch Mehrheitsentscheid: Beispiel $m = 4, \quad r = 1$
  $\Rightarrow \quad n = 16, \; d_{\min} = 8 \quad \Rightarrow \quad t = 3$

$$\mathbf{G} = \begin{pmatrix} \mathbf{G}_0 \\ \mathbf{G}_1 \end{pmatrix} = \begin{pmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

$\mathbf{x} = \mathbf{u}\,\mathbf{G} \qquad \Rightarrow$

$$\left.\begin{array}{l} x_0 = u_0 \\ x_1 = u_0 + u_4 \end{array}\right\} u_4 = x_0 + x_1$$

$$\left.\begin{array}{l} x_2 = u_0 + u_3 \\ x_3 = u_0 + u_3 + u_4 \end{array}\right\} u_4 = x_2 + x_3$$

$$\left.\begin{array}{l} x_4 = u_0 + u_2 \\ x_5 = u_0 + u_2 + u_4 \end{array}\right\} u_4 = x_4 + x_5$$

$$\vdots \qquad\qquad \vdots$$

$$\left.\begin{array}{l} x_{14} = u_0 + u_1 + u_2 + u_3 \\ x_{15} = u_0 + u_1 + u_2 + u_3 + u_4 \end{array}\right\} u_4 = x_{14} + x_{15}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Gleichungen für weitere Nachrichtenstellen:
- $u_3 = x_0 + x_2 = x_1 + x_3 = x_4 + x_6 = x_5 + x_7 = x_8 + x_{10} = x_9 + x_{11} = x_{12} + x_{14} = x_{13} + x_{15}$
- $u_2 = x_0 + x_4 = x_1 + x_5 = x_2 + x_6 = x_3 + x_7 = x_8 + x_{12} = x_9 + x_{13} = x_{10} + x_{14} = x_{11} + x_{15}$
- $u_1 = x_0 + x_8 = x_1 + x_9 = x_2 + x_{10} = x_3 + x_{11} = x_4 + x_{12} = x_5 + x_{13} = x_6 + x_{14} = x_7 + x_{15}$
- u_0: Mehrheitsentscheid für den Vektor:
- $\mathbf{v}_1 = \mathbf{x} + (0, u_1, u_2, u_3, u_4)\,\mathbf{G}$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Nebenklassen (Restklassen, Cosets)
  - Voraussetzung: (n,k)-Blockcode $\mathcal{C}$ mit Prüfmatrix $\mathbf{H}$

    Syndrom: $\mathbf{s} = \mathbf{y}\,\mathbf{H}^{\mathrm{T}} = (\mathbf{x} + \mathbf{f})\,\mathbf{H}^{\mathrm{T}} = \mathbf{f}\,\mathbf{H}^{\mathrm{T}}$ (3.99)

    Anzahl verschiedener Fehlermuster $\mathbf{f}$: $2^n - 2^k$

    Anzahl möglicher Syndrome: 2^{n-k}

    Bezeichnung der Syndrome als $\mathbf{s}_\mu$ für $0 \leq \mu \leq 2^{n-k}$

    Definition:

    Nebenklasse = Menge $\mathcal{M}_\mu$ aller Fehlermuster $\mathbf{f}$, die das gleiche Syndrom $\mathbf{s}_\mu$ liefern: $\mathcal{M}_\mu = \{\mathbf{f} \mid \mathbf{f}\,\mathbf{H}^{\mathrm{T}} = \mathbf{s}_\mu\}$ (3.100)

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Anführer der Nebenklasse (coset leader) = Fehlervektor $\mathbf{f}_\mu$ mit dem geringsten Hamming-Gewicht
- Anführer nicht unbedingt eindeutig bestimmbar
- Eigenschaft der Vektoren aus einem Coset $\mathcal{M}_\mu$:
  - für $\mathbf{f}_1, \mathbf{f}_2 \in \mathcal{M}_\mu$ ist auch $\mathbf{f}_1 + \mathbf{f}_2 \in \mathcal{C}$,
    denn $\mathbf{s} = \mathbf{y}\,\mathbf{H}^T = (\mathbf{f}_1 + \mathbf{f}_2)\,\mathbf{H}^T = \mathbf{f}_1\,\mathbf{H}^T + \mathbf{f}_2\,\mathbf{H}^T = \mathbf{s}_\mu + \mathbf{s}_\mu = \mathbf{0}$
- $\mathcal{M}_\mu$ kann erzeugt werden aus:

$$\mathcal{M}_\mu = \{(\mathbf{c} + \mathbf{f}_\mu)\} \qquad \text{mit} \qquad \mathbf{c} \in \mathcal{C} \tag{3.101}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel: (5,2)-Code $\mathcal{C}$ = {00000,10110,01011,11101}

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad \mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

μ	$\mathbf{f}_\mu$	$\mathcal{M}_\mu$				$\mathbf{s}_\mu$
0	00000	00000	10110	01011	11101	000
1	00001	00001	10111	01010	11100	001
2	00010	00010	10100	01001	11111	010
3	00100	00100	10010	01111	11001	100
4	01000	01000	11110	00011	10101	011
5	10000	10000	00110	11011	01101	110
6	11000	11000	01110	10011	00101	101
7	01100	01100	11010	00111	10001	111

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Zyklische Codes
  - Teilmenge linearer Blockcodes
  - Definition: ein linearer (n,k)-Blockcode heißt zyklisch, wenn jede zyklische Verschiebung eines Codewortes wieder ein Codewort ist:

$$\boxed{(c_0, c_1, c_2, \ldots, c_{n-1}) \in \mathcal{C} \quad \Rightarrow \quad (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}} \qquad (3.102)$$

  - Beispiel:

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

Codewörter:

u	x
0000	0000000
1000	1101000
0100	0110100
0010	0011010
0001	0001101
1110	1000110
0111	0100011
1101	1010001

u	x
1011	1111111
1010	1110010
0101	0111001
1100	1011100
0110	0101110
0011	0010111
1111	1001011
1001	1100101

- Alle zyklischen Codes besitzen zumindest eine Generatormatrix mit Bandstruktur.

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Generatormatrizen mit Bandstruktur beschreiben nicht notwendig zyklische Codes

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad \mathcal{C} = \{00000, 11010, 01101, 10111\}$$

- eine Zeile charakterisiert Generatormatrix vollständig
- Beschreibung eines Vektors durch ein Polynom:

$$\boxed{c = (c_0 \quad c_1 \quad \ldots \quad c_{n-1}) \quad \Leftrightarrow \quad c(x) = \sum_{i=0}^{n-1} c_i\, x^i} \qquad (3.103)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel für Polynome von Codewörtern der Länge n:

c	$c(x)$
0000 ... 0	0
1000 ... 0	1
0100 ... 0	x
0010 ... 0	x^2
000 ... 01	x^{n-1}
1111 ... 1	$1 + x + x^2 + \ldots + x^{n-1}$
1010 ... 0	$1 + x^2$

- Addition von Vektoren entspricht Addition von Polynomen:

$$\mathbf{c}_1 + \mathbf{c}_2 \quad \Leftrightarrow \quad c_1(x) + c_2(x) \qquad (3.104)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Zyklische Codes sind im Allgemeinen nicht systematisch.
- Beschreibung eines zyklischen Codes mit einer Generatormatrix:

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & & & & & & & \vdots \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 \\ 0 & 0 & \cdots & 0 & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} \end{pmatrix} \tag{3.105}$$

$n-k+1$ von 0 verschiedene Einträge: $g_0, g_1, g_2, \dots, g_{n-k}$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Nachrichtenworte: $\mathbf{u} = (u_0, u_1, u_2, \dots, u_{k-1})$
- Codeworte: $\mathbf{c} = (c_0, c_1, c_2, \dots, c_{n-1})$
- Bestimmung der Codeworte mit Hilfe der Generatormatrix:

$$\boxed{\mathbf{c} = \mathbf{u}\,\mathbf{G}} \tag{3.106}$$

$$c_0 = u_0\, g_0 \tag{3.107}$$

$$c_1 = u_0\, g_1 + u_1\, g_0 \tag{3.108}$$

$$c_2 = u_0\, g_2 + u_1\, g_1 + u_2\, g_0 \tag{3.109}$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- vereinfachte Beschreibung von Generatormatrix, Nachrichten- und Codevektor mit Polynomen:

$$u(x) = u_0 + u_1\,x + u_2\,x^2 + \ldots + u_{k-1}\,x^{k-1} \tag{3.110}$$

$$c(x) = c_0 + c_1\,x + c_2\,x^2 + \ldots + c_{n-1}\,x^{n-1} \tag{3.111}$$

$$g(x) = g_0 + g_1\,x + g_2\,x^2 + \ldots + g_{n-k}\,x^{n-k} \tag{3.112}$$

- Codierungsvorschrift: $\boxed{c(x) = u(x) \cdot g(x)}$ (3.113)

$$c_0 = u_0\,g_0 \tag{3.114}$$

$$c_1 = u_0\,g_1 + u_1\,g_0 \tag{3.115}$$

$$c_2 = u_0\,g_2 + u_1\,g_1 + u_2\,g_0 \tag{3.116}$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

> Satz: Jedes Codewortpolynom $c(x)$ ist ohne Rest durch $g(x)$ teilbar.

- Beispiel:

$g(x) = 1 + x + x^3$, $u(x) = 1 + x^2 + x^3$

$\Rightarrow \quad c(x) = u(x) \cdot g(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \;\Leftrightarrow\; \mathbf{c} = (1111111)$

- Definition: Periode r eines Generatorpolynoms = kleinster Exponent, mit dem

$$\boxed{x^r + 1 = 0 \quad \bmod g(x)} \tag{3.117}$$

- zyklische Eigenschaft nur für Codewortlänge $n = r$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beweis: es soll gelten:
  - $\mathbf{c} = (c_0, c_1, c_2, \dots, c_{n-1}) \in \mathcal{C} \quad \Rightarrow \quad \mathbf{d} = (c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in \mathcal{C}$

    $$c(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1} \tag{3.118}$$
  - $c(x)$ ist ohne Rest durch $g(x)$ teilbar:
  - $$c(x) = 0 \mod g(x) \quad \Rightarrow \quad x \cdot c(x) = 0 \mod g(x) \tag{3.119}$$
  - $$\begin{aligned} d(x) &= c_{n-1} + c_0 x + c_1 x^2 + \dots + c_{n-2} x^{n-1} \\ &= c_{n-1} + x \underbrace{(c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1})}_{=\,c(x)} + c_{n-1} x^n \\ &= x \cdot c(x) + c_{n-1} (1 + x^n) \end{aligned} \tag{3.120}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

  - $\mathbf{d}$ ist nur Codewort, wenn $d(x)$ ohne Rest durch $g(x)$ teilbar ist:

    $$\Rightarrow \quad 1 + x^n = 0 \mod g(x) \tag{3.121}$$

    ■

- nur wenn das Generatorpolynom die Bedingung (3.117/3.121) erfüllt, entsteht ein zyklischer Code
- Eigenschaften des Generatorpolynoms:
  - Für die Koeffizienten des Generatorpolynoms muss gelten:

    $g_0 = g_{n-k} = 1$

    $$\Rightarrow \boxed{g(x) = 1 + g_1 x + g_2 x^2 + \dots + x^{n-k}} \tag{3.122}$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Bestimmung eines Generatorpolynoms:
  - Zerlegung von $1 + x^n$ in Faktoren, jeder Faktor kann als Generatorpolynom verwendet werden
  - Beispiel: $x^7 + 1 = (1 + x) \cdot (1 + x + x^3) \cdot (1 + x^2 + x^3)$
- Berechnung der Periode eines gegebenen Generatorpolynoms: Umkehrung des Gauß'schen Divisionsalgorithmus:
  - Beispiel: $(x^3 + x + 1) \cdot p(x) = x^n + 1$

$$
\begin{array}{r}
x^3 + 0 + x + 1 \\
x^4 + 0 + x^2 + x \phantom{{}+1} \\
x^5 + 0 + x^3 + x^2 \phantom{{}+x+1} \\
\underline{x^7 + 0 + x^5 + x^4 \phantom{{}+x^3+x^2+x+1}} \\
x^7 + 0 + 0 + 0 + 0 + 0 + 0 + 1
\end{array}
\quad \Rightarrow \quad n = 7
$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Allgemeine Darstellung eines Codewortpolynoms:

$$c(x) = (u_0 + u_1\, x + u_2\, x^2 + \ldots + u_{k-1}\, x^{k-1}) \cdot g(x) \qquad (3.123)$$

$\Rightarrow$ $g(x)$ ist das Codewortpolynom mit geringstem Grad

- Systematische Codierung
  - Multiplikation des Nachrichtenpolynoms

$u(x) = u_0 + u_1\, x + u_2\, x^2 + \ldots + u_{k-1}\, x^{k-1}$ mit x^{n-k} :

$$u(x) \cdot x^{n-k} = u_0\, x^{n-k} + u_1\, x^{n-k+1} + u_2\, x^{n-k+2} + \ldots + u_{k-1}\, x^{n-1} \qquad (3.124)$$

(entspricht Verschiebung der Nachrichtenstellen zu den höchsten Koeffizienten hin)

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Division des Polynoms $u(x) \cdot x^{n-k}$ durch $g(x)$:

$$\boxed{\frac{u(x)\cdot x^{n-k}}{g(x)} = q(x) + \frac{r(x)}{g(x)}} \qquad (3.125)$$

$$u(x) \cdot x^{n-k} = q(x) \cdot g(x) + r(x) \qquad (3.126)$$

mit $q(x)$ = ganzzahliges Divisionsergebnis

$r(x)$ = Divisionsrest, im Allgemeinen: $r(x) \neq 0$

$$r(x) = r_0 + r_1\, x + r_2\, x^2 + \ldots + r_{n-k-1}\, x^{n-k-1} \qquad (3.127)$$

- Erzwingen der ganzzahligen Dividierbarkeit:

$$\boxed{u(x) \cdot x^{n-k} + r(x) = q(x) \cdot g(x) = c(x)} \qquad (3.128)$$

- Codewort: $\mathbf{c} = (r_0, r_1, r_2, \ldots, r_{n-k-1}, u_0, u_1, u_2, \ldots, u_{k-1})$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Beispiel einer systematischen Codierung:
  - $g(x) = x^3 + x + 1$, $\mathbf{u} = (1\ 0\ 0\ 1)$, $u(x) = x^3 + 1$
  - $n = 7, \quad k = 4, \quad n - k = 3$
  - $u(x) \cdot x^{n-k} = x^6 + x^3$
  - Division des Polynoms $u(x) \cdot x^{n-k}$ durch $g(x)$:

$$(x^6 + 0 + 0 + x^3) : (x^3 + 0 + x + 1) = x^3 + x + \frac{x^2 + x}{x^3 + x + 1}$$

$$\begin{array}{l} + (x^6 + 0 + x^4 + x^3) \\ \hline (0 + 0 + x^4 + 0 + 0 + 0) \\ \quad + (x^4 + 0 + x^2 + x) \\ \hline \quad (0 + 0 + x^2 + x) = r(x) \end{array}$$

$$c(x) = u(x) \cdot x^{n-k} + r(x) = x^6 + x^3 + x^2 + x \quad \Rightarrow \quad \mathbf{c} = (0\ 1\ 1\ 1\ 0\ 0\ 1)$$

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Prüfmatrix und Prüfpolynom
  - Generatorpolynom: $x^n + 1 = g(x) \cdot h(x)$ (3.129)
  - $h(x)$ hat den Grad k:

    $h(x) = h_0 + h_1\, x + h_2\, x^2 + \ldots + h_k\, x^k$ (3.130)

    mit $h_0 = h_k = 1$
  - $h(x)$ ist das Prüfpolynom
  - Prüfmatrix $\mathbf{H}$ ist $(n-k) \times n$ -Matrix

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Prüfmatrix

$$\mathbf{H} = \begin{pmatrix} h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & & & & & & & & & \vdots \\ \vdots & & & & & & & & & \vdots \\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & 0 \\ 0 & 0 & \dots & 0 & 0 & h_k & h_{k-1} & h_{k-2} & \dots & h_0 \end{pmatrix}$$

(3.131)

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Decodierung des Empfangsvektors $\mathbf{y} = \mathbf{c} + \mathbf{f} \;\;\Leftrightarrow\;\; y(x) = c(x) + f(x)$
  - Codewörter sind ohne Rest durch das Generatorpolynom teilbar
  - Division durch Generatorpolynom = Berechnung des Informationsworts und Test, ob Empfangswort = Codewort

$$\frac{y(x)}{g(x)} = q(x) + \frac{s(x)}{g(x)} \qquad (3.132)$$

  - $s(x)$ = Syndrom: $y(x) = q(x) \cdot g(x) + s(x)$
  - Wenn $s(x) \neq \mathbf{0}$, dann Fehlerkorrektur mit Hilfe Syndrom-Tabelle
  - Realisierung der Polynomdivision durch Schieberegister-Schaltung
  - keine Matrix-Multiplikationen bei Codierung und Decodierung notwendig

Nachrichtentechnik 4

3 Kanalcodierung in der Nachrichtenübertragung

- Realisierung von Codierung und Decodierung durch Schieberegister-Schaltungen
  - Grundschaltungen
    - Schieberegister: jede Speicherzelle verzögert um einen Takt
    - Bezeichnung: $S_j(i)$ = Inhalt der Speicherzelle j zum Zeitpunkt i
    - $S_{j+1}(i+1) = S_j(i)$