Vorlesung am 23.06.06

9.V

IC
SS-06

2.2: Der Hammingraum (Fort.)

Die Kanalcodierung kann wie folgt formuliert werden: Für einen Block aus k Nachrichtenbits konstruiert man einen Codewort aus n-Bits, mit $n > k$. Die Anzahl der möglichen Knoten im n-dimensionalen Hammingraum 2^n ist größer als die Anzahl der möglichen Blöcke aus k-Nachrichtenbits 2^k. Die Codewörter werden dann so verteilt, daß der Abstand dazwischen maximiert wird. Dies führt zur Minimierung des Decodierungsfehlers. Der Abstand zwischen den Knoten des n-dimensionalen Hammingraum wird Hammingdistanz genannt

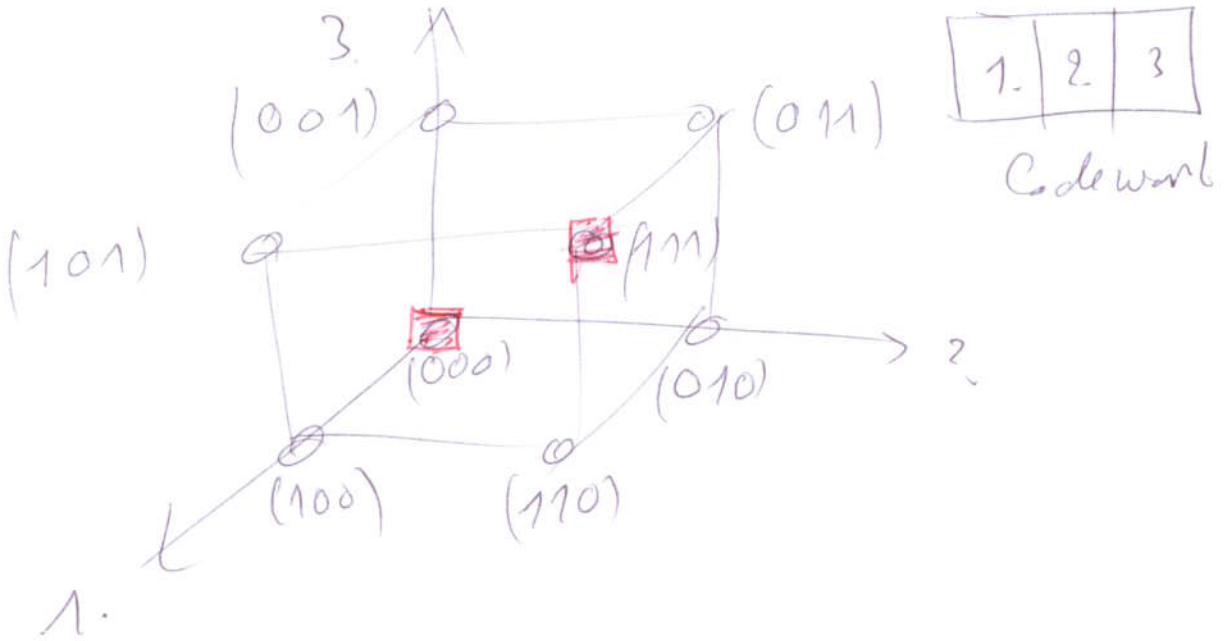
Definition: Die Hammingdistanz ist die

Anzahl der unterschiedlichen Stellen (Bits) zwischen zwei Codewörtern (Kmale)

$$d_{12} = d(W_1, W_2)$$

= Anzahl der unterschiedlichen Stellen z. W_1 u. W_2

Beispiele: 1-) Wiederholungscode ($n=3$, $k=1$)



1.	2.	3

Codewörter

$W_0 = (000)$ $\quad W_1 = (111)$

$d(W_0, W_1) = 3$

Anzahl der gültigen Codewörter $= 2^k = 2$

Hammingdistanz zwischen diesen Codewörtern = 3

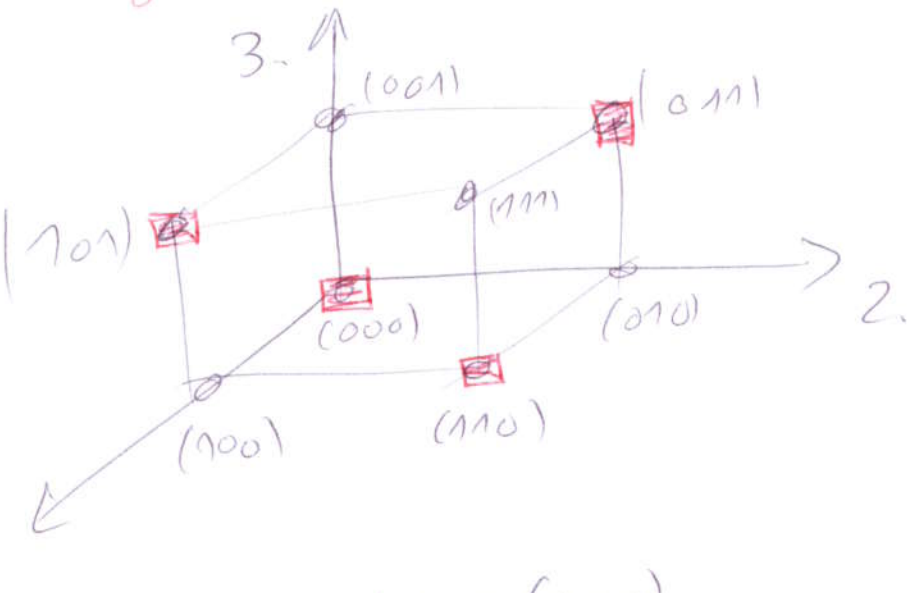
Bemerkung: Wir haben bereits gezeigt, daß hier,
bis zweibitfehler erkennbar ist u.
der Einbitfehler korrigierbar ist.

2- Paritätskontrolle ($n=3$, $k=2$)

1	2	3

Anzahl der Codewörter $= 2^n = 8$

" " gültigen Codewörter $= 2^k = 4$



Gültige Codewörter

$W_0 = (000)$
$W_1 = (011)$
$W_2 = (101)$
$W_3 = (110)$

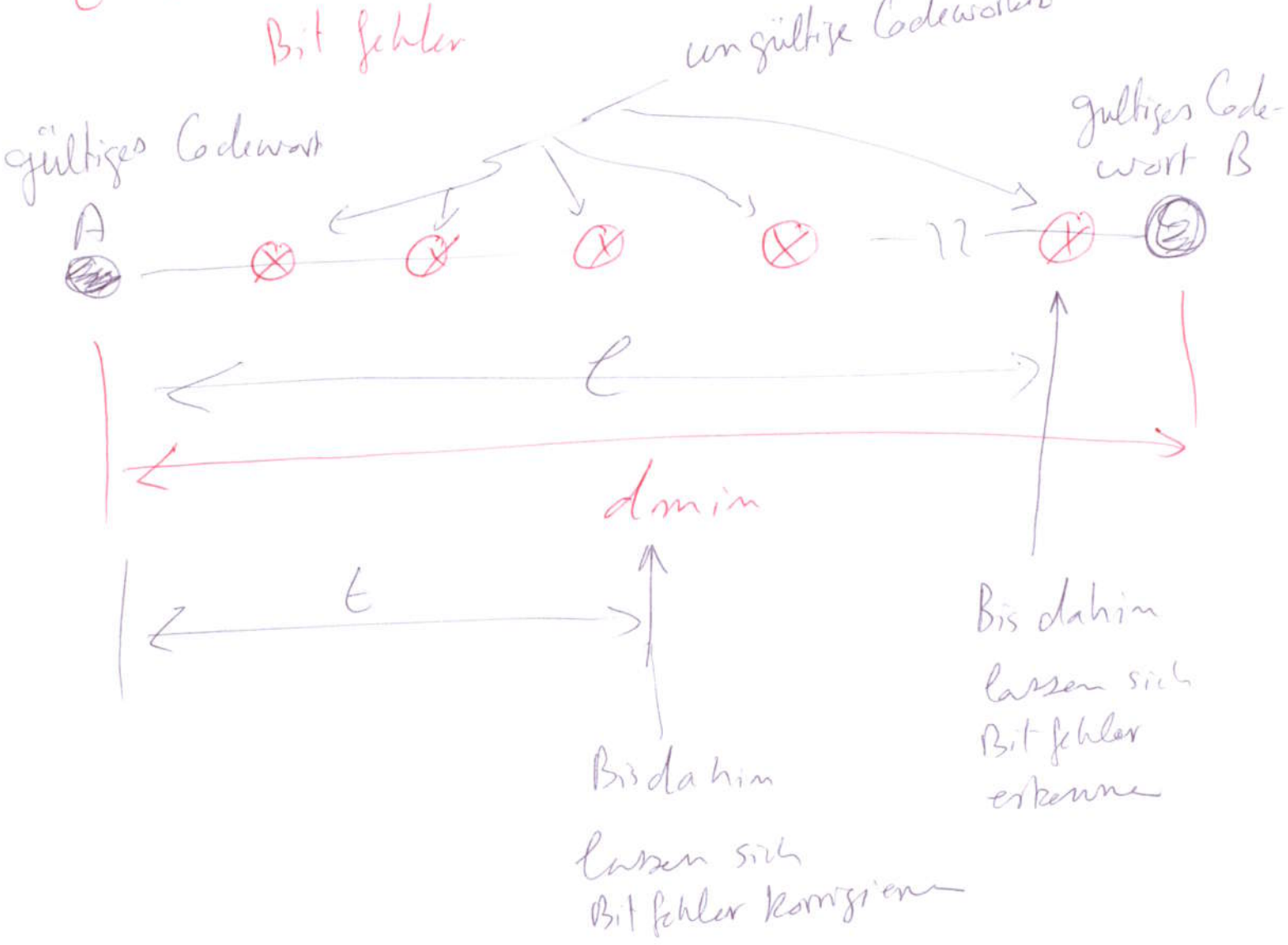
$$d(W_i, W_j) = 2 = d_{min}$$

Einbitfehler ist erkennbar
Es gibt keine Möglichkeit, Fehler zu korrigieren.

Im Allgemeinen definieren wir

ℓ = maximale Zahl der erkennbaren Bit fehler

t = maximale Zahl der korrigierbaren Bit fehler



$\ell = d_{min} - 1$

$t = \frac{d_{min} - 1}{2}$ (falls d_{min} = ungerade).

Erkennung: Falls ein ungültiges Codewort empfangen wurde, das Einbit fehler (Abstand zum korrekten Codewort A = 1) oder Zweibitfehler (Abstand zum A = 2), oder, ..., oder $\ell-1$ - Bitfehler (Abstand zum A = $\ell-1$), aufweist, erkennt man diesen Fehler.

Die Regel der Korrektur ist, das nächste gültige Codewort zum empfangenen Codewort als das korrekte zu nehmen - hier lassen bis $t = \frac{d_{min} - 1}{2}$ Bitfehler korrigieren

2.3.: Der lineare Blockcode

Ein Nachrichtenwort (Block aus k-Bits) lässt sich als einen Zeilenvektor darstellen.

$$\underline{M} = [\underbrace{m_1 \; m_2 \; \cdots \; m_k}_{k \text{ Nachrichtenbits}}]$$

Im einem linearen Code werden die Controlbits (oder Paritätsbits) als lineare Kombinationen der Nachrichtenbits $m_1, m_2, \dots m_k$ konstruiert.

Die Controlbits lassen sich ebenfalls als Zeilenvektor $\underline{C}$ darstellen:

$$\underline{C} = [c_1 \; c_2 \; \dots \; c_q]$$

$$c_i = \sum_{j=1}^{k} p_{ij} \, m_j \quad , \quad i = 1, 2, \dots, q$$

Das gesamte (gültige) Codewort lässt sich konstruieren als Verzahnung von $\underline{M}$ und $\underline{C}$.

Am einfachsten:

Paritätsmatrix $(k \times q)$

$$\underline{X} = [\underline{M} \mid \underline{C}] \quad , \quad \underline{C} = \underline{M}\,[P]$$

$$\underline{X} = \underbrace{[m_1 \; m_2 \; \dots \; m_k \mid c_1 \; c_2 \; \dots \; c_q]}_{n = k+q}$$

2.3.1: Mathematische Behandlung des linearen Block-Codes

– Addition von Codewörter

$$\underline{X} + \underline{Z} = \left[x_1 \oplus z_1 \quad x_2 \oplus z_2 \quad \cdots \quad (x_n \oplus z_n) \right]$$

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

$\oplus$ Modulo 2 - Addition.

Falls man M-är codiert, entspricht $\oplus$ Modulo M-Addition.

$\underline{X} + \underline{Z} = 0$ nur wenn $\underline{X} = \underline{Z} \Longrightarrow$

$\underline{X} - \underline{Z} = 0 \Longrightarrow \underline{X} + \underline{Z} = \underline{X} - \underline{Z}$ (nur für binär)

Addieren $\triangleq$ Subtrahieren

– Gewicht des Codeworts

Das Gewicht eines Codeworts $\underline{X}$ wird als die

Anzahl der Einsen im Codewort definiert

$W(\underline{X})$ = Anzahl der Einsen in $\underline{X}$

- Die Hammingdistanz zwischen zwei Codewörtern

Die Hammingdistanz zwischen den Codeworten $\underline{X}$ und $\underline{Z}$ ist die Anzahl der unterschiedlichen Bits

$d(\underline{X}, \underline{Z})$ = Anzahl der unterschiedlichen Bits in $\underline{X}$ und $\underline{Z}$

Da $1 \oplus 1 = 0$ und $0 \oplus 0 = 0$

während $1 \oplus 0 = 1$ und $0 \oplus 1 = 1$

Dann $(\underline{X} + \underline{Z})$ ist ein Wort mit Einsen an den Stellen, wo die Zweiwörter

$\underline{X}$ und $\underline{Z}$ unterschiedliche Bits haben

$$\Rightarrow W(\underline{X}+\underline{Z}) = d(\underline{X}, \underline{Z})$$

2.3.2: Eigenschaften des linearen Blockcodes

1-) $\underline{X} = 0$ ist ein gültiges Codewort

2-) Die Summe von zwei gültigen Codewörtern ist ein gültiges Codewort

3-) Die minimale Hamming distanz d_{min} stimmt mit dem minimalen Gewicht der gültigen Codewörter überein

Beweis

Ein linearer Blockcode kann durch eine Generatormatrix $[G]$ eindeutig beschrieben werden,

Beweis

wobei: $\underset{(1\times m)}{\underline{X}} = \underset{(1\times k)}{\underline{M}} \; \underset{(k\times m)}{[G]}$. Dies wird wie

folgt gezeigt: Einheitsmatrix

$$[G] = \underset{(k\times k)}{[E]} \mid \underset{(k\times q)}{[P]}$$

$$\underline{X} = \underset{(k\times m)}{[\underline{M}]} \mid \underline{C}]$$

Einheitsmatrix

Paritätsmatrix

$$\Rightarrow \underline{X} = [\underline{M}[E] \mid \underline{M}[P]]$$

$$= \underline{M}[[E] \mid [P]] = \underline{M}[G] \quad n = k+q$$

$(1 \times k)$ $(k \times n)$

wobei $[G] = [[E] \mid [P]]$

$k \times n$ $k \times k$ $k \times q$

1-) Da $\underline{M}_0 = [0\ 0\ \cdots\ 0]$ eins der $(1 \times k)$

Nachrichten Wörter ist, Dann

$$\underline{X}_0 = \underline{M}_0[G] = [0\ 0\ \cdots\ 0]$$

$(1 \times n)$

ist ein gultiges Codewort.

2-) Für zwei gultige Codewörter

$\underline{X}_1$ und $\underline{X}_2$ gilt:

$\underline{X}_1 = \underline{M}_1 [G]$; $\underline{X}_2 = \underline{M}_2 [G]$

$\Rightarrow \underline{X}_1 + \underline{X}_2 = (\underline{M}_1 + \underline{M}_2)\,[G]$

Da $\underline{M}_1 + \underline{M}_2$ ein Nachrichtenwort ist

(Alle Knaben im k-dimensionalen Raum Nachrichtenwörter darstellen)

$\Rightarrow$ $\underline{X}_1 + \underline{X}_2$ ist ein gültiges Codewort

3-) Da $d(\underline{X}_1, \underline{X}_2) = W(\underline{X}_1 + \underline{X}_2)$

gültiges CW

$= W(\underline{X}_3)$

$\Rightarrow d_{min} = W_{min}$

(ausgeschlossen $W(\underline{X}_0) = 0$)

Da $\underline{X}_1 + \underline{X}_2 = \underline{X}_0$ nur wenn $\underline{X}_1 = \underline{X}_2$

Der Entwurf eines linearen Blockcodes reduziert sich auf die Bestimmung der Paritätsmatrix [P]

$$[P]_{k \times q} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1q} \\ p_{21} & p_{22} & \cdots & p_{2q} \\ \vdots & & & \\ p_{k1} & p_{k2} & \cdots & p_{kq} \end{bmatrix}$$

2.3.3 : Der Hammingcode

Im Hammingcode gilt:

$$n = 2^q - 1 \quad ; \quad k = n - q$$

Das Ziel ist all Einbitfehler zu korrigieren

Dies bedeutet: $d_{min} = 3$ und

$$W_{min} = 3$$