Vorlesung am 30.06.06

(10. V)

IC
SS-06

2.3.3 : Der Hammingcode (Fort.)

Das Ziel des Hammingcodes ist alle Einbitfehler korrigieren zu können. Dies bedeutet $d_{min} = 3$. Der Hammingcode ist ein linearer Blockcode. Dies bedeutet

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

Im Hammingcode gilt die Regel:

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

q	1	2	3	4	5	
n	1	3	7	15		
k	0	1	4	11		

Die Codeeffizienz (Coderate) $R_c = \frac{k}{n} = \frac{n-q}{n}$

$$= 1 - \frac{q}{n} = 1 - \frac{q}{2^q - 1}$$

$$R_c = 1 - \frac{q}{e^{q \ln 2} - 1}$$

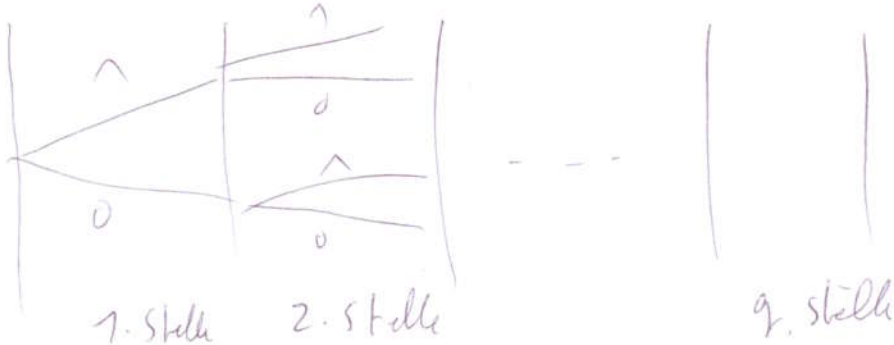
$$\lim_{q \to \infty} R_c = 1 - \frac{1}{\ln 2 \cdot \lim_{q \to \infty} e^{q \ln 2}} = 1$$

Um alle Einbitfehler korrigieren zu können, muß [P] aus alle Zeilen mit mindestens zwei Einsen bestehen.

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

$(k \times q)$

Die gesamte Zahl der Zeilen aus q binäre Stelle ist 2^q



Darunter gibt's die alles-Nullen-Zeile und die Zeilen mit einer Eins. Die Zahl der Zeilen mit einer Eins ist $q \Rightarrow$ gesamte Zahl der Zeilen mit mindestens zwei Einsen $= 2^q - q - 1$

$= n - q = k$

Beispiel 1: $q = 2 \rightarrow n = 3, \; k = 1$

Da das alles-Nullen-Code dabei sein muß $\Rightarrow$

$$\underline{X}_0 = \left[\begin{array}{c|cc} 0 & 0 & 0 \\ \underline{M}_0 & \multicolumn{2}{c}{\underline{C}_0} \end{array}\right] \Rightarrow \underline{C}_0 = [0 \; 0]$$

Für $\underline{X}_1$, kann man das Argument benutzen

$$w_{min} = 3 \Rightarrow \underline{X}_1 = \left[\begin{array}{c|cc} 1 & 1 & 1 \\ \underline{M}_1 & \multicolumn{2}{c}{\underline{C}_1} \end{array}\right] \Rightarrow \underline{C}_1 = [1 \; 1]$$

oder $\underset{k \times q}{[P]} = [P_{11} \; P_{12}] = [1 \; 1]$ (mindestens zwei Einsen)

$$\Rightarrow \underline{C}_1 = \underline{M}_1 [P] = [1] \, [1 \; 1] = [1 \; 1]$$

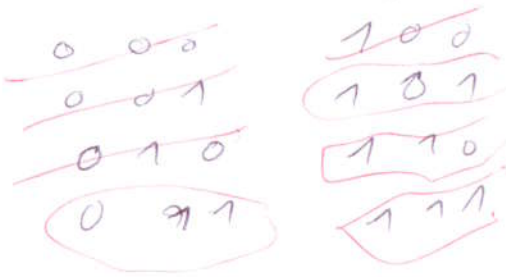
Dies ist in der Tat der Widerholungscode.

in dem alle Einbitfehler korrigierbar sind

Beispiel 2: $q=3$, $n=7$, $k=4$

alle Zeilen aus q-stellig

$$[P] = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$



Num, $\underline{c} = \underline{M}\,[P]$

Beispiel $\underline{M} = [1\ 0\ 0\ 0] \Rightarrow$

$\underline{c} = \underline{M}\,[P]$ = erste Zeile in $[P]$

$= [0\ 1\ 1] \Rightarrow$

$\underline{X} = [\underline{M}\,|\,\underline{c}] = [1\ 0\ 0\ 0\ |\ 0\ 1\ 1]$

$w(\underline{X}) = 3$

2.4: Fehlererkennung und Fehlerkorrektur bei linearen Blockcodes

2.4.1: Fehlererkennung

Hier definieren wir die Matrix $[H]$:

$$[H] = \left[\, [P]^T \;\middle|\; [E]_q \,\right]$$

$q \times m$ — $q \times k$ — $q \times q$

$$= \left[\begin{array}{cccc|cccc} P_{11} & P_{21} & \cdots & P_{k1} & 1 & 0 & \cdots & 0 \\ P_{12} & P_{22} & \cdots & P_{k2} & 0 & 1 & \cdots & 0 \\ \vdots & & & & \vdots & & & \\ P_{1q} & P_{2q} & \cdots & P_{kq} & 0 & 0 & \cdots & 1 \end{array}\right]$$

Nicht zu verwechseln mit $[G] = [\,[E]_k \,|\, [P]\,]$ ($k \times m$ — $k \times n$ — $k \times q$)

Nun, $[H]^T = \left[\begin{array}{c} [P] \\ \hline [E]_q \end{array}\right]$ ($n \times q$; $k \times q$ über $q \times q$)

Betrachtet man $\underline{X} \cdot [H]^T = \underline{X} \left[\begin{array}{c} [P] \\ \hline [E_q] \end{array}\right]$

$= [\underline{M} \,|\, \underline{C}] \left[\begin{array}{c} [P] \\ \hline [E_q] \end{array}\right] = \underline{M}[P] + \underline{C} = \underline{C} + \underline{C} = 0$

($1 \times k$, $1 \times q$; $k \times q$; $q \times q$; $\underline{C}$)

Falls $\underline{X}$ ein gültiges Codewort ist,

dann $\underline{X} \cdot [H]^T = 0$

Dies ist die Fehlererkennung.

2.4.2: Fehlerkorrektur

Für ein nicht gültiges (fehlerbehaftetes)

Codewort $\underline{Y}$, gilt $\underline{Y} = \underline{X} + \underline{F}$,

wobei $\underline{X}$ ein gültiges Codewort ist und

$\underline{F}$ ein Fehlerwort ist.

$$W(\underline{F}) = W(\underline{Y} - \underline{X})$$

$$= d(\underline{Y} - \underline{X}) = \text{Anzahl der Bitfehler z. } \underline{Y} \text{ u. } \underline{X}$$

Nun $\underline{Y} \cdot [H]^T = (\underline{X} + \underline{F})[H]^T$

$$\underline{Y} \cdot [H]^T = \underline{X}\,[H]^T + \underline{F}\,[H]^T$$

$$= \underline{0} + \underline{F}\,[H]^T = \underline{S}$$

Der Vektor $\underline{S}$ " Syndromvektor genannt " wird definiert als:

$$\underset{7\times q}{\underline{S}} = \underset{7\times m}{\underline{F}}\,\underset{n\times q}{[H]^T} = \underline{Y}\,[H]^T$$

Die Bestimmung von $\underline{F}$ durch die Benutzung der o.g. Gleichung ist nicht eindeutig, da diese Matrixgleichung q Gleichungen in n-Unbekannten liefert. Jede Lösung $\underline{F}_i$ stellt den Fehler zwischen $\underline{Y}$ und einem gültigen Codewort

Wort $\underline{X}_i$. Die Lösung eines linearen Gleichungssystems aus q Gleichungen in n Unbekannten hat n-q Freiheitsgrade. Das Heißt, n-q Unbekannten können frei bestimmt werden. Da für jede Unbekannte zwei mögliche Werte gibt, nämlich "0" oder "1". Die Anzahl der Lösungen, die einem bestimmten $\underline{S} = \underline{Y}\,[H]^T$ entsprechen ist $2^{n-q} = 2^k$ = Anzahl der gültigen Codewörter $\underline{X}_i$, $i = 1, 2, \ldots 2^k$

* Bestimmung von $\underline{X}_i$, die zu $\underline{Y}$ einen Einbitfehler aufweist

Angenommen, es gäbe ein (oder mehrere) gültige Codewörter $\underline{X}_i$, die einen Einbitfehler zu $\underline{Y}$ aufweisen.

In diesem Fall gilt $W(\underline{Y}-\underline{X}_i) = W(\underline{F}_i) = 1$

$\Longrightarrow$ $\underline{F}_i$ enthält eine einzige "1"

Da $\text{Dim}\{\underline{F}_i\} = (1 \times n)$ $\Longrightarrow$ $\underline{F}_i$ ist eine der folgenden Möglichkeiten:

$$\left.\begin{array}{l} \underline{F}_1 = [1\ 0\ 0\ 0\ \cdots\ 0] \\ \underline{F}_2 = [0\ 1\ 0\ 0\ \cdots\ 0] \\ \vdots \\ \underline{F}_n = [0\ 0\ \cdots\ \cdots\ 1] \end{array}\right\} (1 \times n)$$

$(n \times q)$ $(1 \times m)$ $(m \times q)$

Nun $\underline{S} = \underline{Y}\,[H]^T = \underline{F}_i\,[H]^T$

Vorgegeben — gesucht

Da $\underline{F}_i\,[H]^T = [0\ 0 \cdots \underset{\text{i-te Stelle}}{1} \cdots 0] \cdot [H]^T$ $(m \times q)$

$= i$-te Zeile von $[H]^T$

$\Rightarrow \underline{S} = i$-te Zeile von $[H]^T$

Nun gibt's folgende Möglichkeiten

1-) Vorgegebenes $\underline{S} = \underline{Y}\,[H]^T$ stimmt mit keiner der Zeilen von $[H]^T$ überein $\Rightarrow$ Es gibt kein gültiges Codewort $\underline{X}_i$, das ein Einbitfehler zu $\underline{Y}$ aufweist.

2-) Vorgegebenes $\underline{S} = \underline{Y}\,[H]^T$ stimmt mit mehr als einer Zeile von $[H]^T$ überein $\Rightarrow$ Es gibt mehr als ein gültiges Codewort $\underline{X}_i$, das ein Einbit-Fehler zu $\underline{Y}$ aufweist.

3-) Vorgegebenes $\underline{S} = \underline{Y}\,[H]^T$ stimmt mit einem einzigen Zeile von $[H]^T$ überein $\Rightarrow$ Es gibt ein einziges gültiges Codewort $\underline{X}_i$, das ein Einbit-Fehler zu $\underline{Y}$ aufweist.

2.4.3 : Fehlerkorrektur beim Hammingcode

Die Möglichkeit, dass ~~jeine vorgegebenes~~

$\underset{1\times q}{\underline{S}} = \underline{Y}\,[H]^T$ somit einer einzigen Zeile

von $\underset{n\times q}{[H]^T}$ übereinstimmt ist nur möglich,

wenn die Zeilen von $[H]^T$ alle Möglich-

keiten von $\underline{S}$ darstellen. Die Anzahl der

Zeilen von $[H]^T$ ist n. Die Anzahl

der Möglichen $\underline{S}$ ($\underline{S} = [00\ldots0]$ ist

ausgeschlossen) ist $2^q - 1$. Die

eindeutige Korrektur der Einbitfehler

ist nur möglich, wenn $n = 2^q - 1$

Dies bedeutet, daß für ein beliebiges

"nicht gültiges" Codewort $\underline{Y}$ gibt es

immer ein einziges gültiges Codewort $\underline{X}$

das ein Einbitfehler zu $\underline{Y}$ aufweist.

Da $[H]^T = \begin{bmatrix} [P] \\ \hline [E_q] \end{bmatrix}$, und $[E_q]$ besteht

$(n \times q)$

aus allen Zeilen mit einer einzigen Eins

$\Longrightarrow$ $[P]$ besteht aus allen Zeilen

mit mindestens zwei "Einsen".

* Wie wird korrigiert ?

Aus $\underline{S} = \underline{F_i}\,[H]^T$ = i-te Zeile von $[H]^T$

$\underline{F_i}$ hat eine einzige Eins an der i-ten Stelle

und $\underline{F_i} = \underline{Y} - \underline{X_i} \Longrightarrow$ die i-te Stelle von

$\underline{Y}$ ist fehlerhaft.

Beispiel : Hamming (7,4) - Code

hier $q = 3$, $n = 7$, $k = 4$

$$[P] = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \Longrightarrow$$

$$[H]^T = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Nehmen wir $\underline{M} = [1\ 0\ 1\ 1]$

$$\Rightarrow \underline{C} = \underbrace{[1\ 0\ 1\ 1]}_{\underline{M}} \underbrace{\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}}_{[P]}$$

$$= [0\ 0\ 1]$$

$$\Longrightarrow \underline{X} = [1\ 0\ 1\ 1\ 0\ 0\ 1]$$

Fehlerhaft

Angenommen $\underline{Y} = [1\ 0\ 1\ 0\ 0\ 0\ 1]$

4-te Stelle

$$\underline{S} = \underline{Y}\,[H]^T = [1\ 0\ 1\ 0\ 0\ 0\ 1] \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$= [0\ 1\ 1]$$

$\underline{S}$ stimmt mit der 4-ten Zeile von $[H]^T$ überein $\Longrightarrow \underline{X} = [1\ 0\ 1\ \textcircled{1}\ 0\ 0\ 1]$

Korrektur