Vorlesung am 14.07.06

(12.V)

IC
SS-06

2.5.6 : Berechnung der Generator-Matrix des zyklischen Codes

In (2.5.5) haben wir gezeigt, daß die systematische Form des Codeworts $\underline{X} = [\underline{M} \mid \underline{C}]$ wie nachstehend ausgedrückt werden kann:

$$\underset{(1\times n)}{\underline{X}} = \underset{(1\times k)}{\underline{M}} \underset{(k\times n)}{[G]} = \underset{(1\times k)}{\underline{M}'} \underset{(k\times n)}{[g]}$$

wobei $[G]$ die systematische Generator-Matrix und $[g]$ eine Matrix, die bei zyklischen Codes (als Untermenge der linearen Block codes) vorhanden ist. $[g]$ wird wie folgt konstruiert:

$$[g] = \begin{bmatrix} g_q & g_{q-1} & \cdots & g_1 & g_0 & 0 & 0 & \cdots & 0 \\ 0 & g_q & & & g_1 & g_0 & 0 & \cdots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & - & - & - & & \cdots & g_1 & g_0 \end{bmatrix} \quad (k\times n)$$

($q+1$ Spalten; $k-1$ Spalten)

Im (2.5-4) haben wir gezeigt, daß die Kontrollbits wie folgt berechnet werden:

$$X(P) = P^q M(P) + C(P) = M'(P)\, g(P)$$

$$\Longrightarrow \quad C(P) = \text{Rest}\left\{\frac{-P^q M(P)}{g(P)}\right\}$$

Die Gleichung $\underline{X} = \underline{M}\,[G]$ bedeutet, daß die Zeilen von $[G]$ (k Zeilen) $\underline{X}_i$; $i = 1, 2, \ldots, k$ sind, wobei $\underline{M}_i = [0\ 0\ \ldots\ 1\ \ldots\ 0]$

↑ i-te Stelle

Dies bedeutet, daß die Generator-Matrix des zyklischen (aller linearen Blockcodes auch!) durch die Berechnung von $\underline{X}_i$; $i = 1, 2, \ldots, k$ vollständig bestimmt wird.

Beispiel: $(n=7,\ k=4,\ q=3)$-Code mit $g(P) = P^3 + P + 1$

$$\underline{X}_1 = [1\ 0\ 0\ 0] \Rightarrow X_1(P) = P^3 = P^{(4-1)}$$

$$\underline{X}_2 = [0\ 1\ 0\ 0] \Rightarrow X_2(P) = P^2 = P^{(4-2)}$$

$$\underline{X}_3 = [0\ 0\ 1\ 0] \Rightarrow X_3(P) = P = P^{(4-3)}$$

$$\underline{X}_4 = [0\ 0\ 0\ 1] \Rightarrow X_4(P) = 1 = P^{(4-4)}$$

$$X_i(P) = P^{(4-i)}$$

$$C_i(P) = \text{Rest}\left\{\frac{P^{7-i}\cdot X_i(P)}{g(P)}\right\} = \text{Rest}\left\{\frac{P^{(7-i)}}{P^3+P+1}\right\}$$

$$\begin{array}{r|l} P^3+P+1 & P^3+P+1 \\ \hline \cancel{P^6} & \\ \cancel{P^6}+P^4+P^3 & \\ \hline \cancel{P^4}+P^3 & \\ \cancel{P^4}+P^2+P & \\ \hline \cancel{P^3}+P^2+\cancel{P} & \\ \cancel{P^3}+P+1 & \\ \hline P^2+1 & \end{array} \Rightarrow C_1(P) = P^2+1 \Rightarrow \underline{C}_1 = [1\ 0\ 1]$$

$$\begin{array}{r|l} P^3+P+1 & P^2+1 \\ \hline \cancel{P^5} & \\ \cancel{P^5}+P^3+P^2 & \\ \hline \cancel{P^3}+P^2 & \\ \cancel{P^3}+P+1 & \\ \hline P^2+P+1 & \end{array} \Rightarrow C_2(P) = P^2+P+1 \Rightarrow \underline{C}_2 = [1\ 1\ 1]$$

$$\begin{array}{r|l} & P \\ \hline P^3+P+1 & P^4 \\ & P^4+P^2+P \\ \hline & PP^2+P \end{array} \Longrightarrow C_3(P) = P^2+P \Rightarrow \underline{C}_3 = [1\ 1\ 0]$$

$$\begin{array}{r|l} & 1 \\ \hline P^3+P+1 & P^3 \\ & P^3+P+1 \\ \hline & P+1 \end{array} \Longrightarrow C_4(P) = P+1 \Rightarrow \underline{C}_4 = [0\ 1\ 1]$$

$$\Rightarrow \underline{X}_1 = [1\ 0\ 0\ 0 \mid 1\ 0\ 1] \quad (X_1(P) = P^6+P^2+1)$$

$$\underline{X}_2 = [0\ 1\ 0\ 0 \mid 1\ 1\ 1] \quad (X_2(P) = P^5+P^2+P+1)$$

$$\underline{X}_3 = [0\ 0\ 1\ 0 \mid 1\ 1\ 0] \quad (X_3(P) = P^4+P^2+P)$$

$$\underline{X}_4 = [0\ 0\ 0\ 1 \mid 0\ 1\ 1] \quad (X_4(P) = P^3+P+1)$$

$$\Downarrow$$

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

2.5.7: Nichtsystematische Form des zyklischen Codes

Die systematische Form eines Codes ist $\underline{X} = [\underline{M} \mid \underline{C}]$

Die entsprechende systematische Generator-Matrix ist $[\underline{G}] = [[E]_k \mid [P]]$. Diese Form hat den Vorteil, daß während der Sender einen Nachrichtenvektor $\underline{M}$ sendet, wird der Kontrollvektor $\underline{C}$ gerechnet und im Anschluß der Übertragung von $\underline{M}$ gesendet. Eine beim zyklischen Code einfachere Form ist:

$$\tilde{X}_j(P) = M_j(P) \cdot g(P) \qquad j = 1, 2, \dots, M^k$$

Der Empfänger kann $M(P)$ wiederherstellen durch die Operation:

$$M_j(P) = \frac{\tilde{X}_j(P)}{g(P)} \quad \text{(ohne Rest)}$$

Falls $\text{Rest}\left\{\frac{\tilde{X}'(P)}{g(P)}\right\} \neq 0$ deutet dies darauf hin, daß es ein Fehler vorhanden ist und $\tilde{X}'(P) \neq \tilde{X}_j(P)$.

empfangenes Codepolynom — gültiges Codepolynom

Das andere Fehlererkennungsverfahren, daß sowohl

für $X_j(P) = M'_j(P) \cdot g(P)$ als auch für $\tilde{X}_j(P) = M_j(P) \cdot g(P)$

gilt, ist $$\text{Rest}\left\{\frac{X_j(P)\cdot h(P)}{P^n-1}\right\} = 0$$

$$\text{Rest}\left\{\frac{\tilde{X}_j(P)\cdot h(P)}{P^n-1}\right\} = 0$$

wobei $$\boxed{P^n - 1 = g(P)\cdot h(P)}$$

Dies wird begründet mit der Tatsache,

daß gültige Codepolynome (sowohl $X_j(P)$ als auch $\tilde{X}_j(P)$) sind proportional zu $g(P)$

$$\Longrightarrow h(P)\cdot X_j(P) = m'_j(P)\cdot h(P)\cdot g(P) = m'_j(P)(P^n-1)$$

$$h(P)\cdot \tilde{X}_j(P) = m_j(P)\cdot h(P)\cdot g(P) = m_j(P)(P^n-1)$$

2.5.8 : Struktur des Codevektors $\underline{\tilde{X}}$

Aus der Gleichung $\tilde{X}_j(P) = m_j(P)\cdot g(P)$

erhalten wir $\underline{\tilde{X}}_j = \underline{M}_j[g]$

$$= \underline{M}_j[T][G]$$

$$= \underline{\tilde{M}}_j[G] \quad ; \quad \underline{\tilde{M}}_j = \underline{M}_j[T]$$

Dies ist zu vergleichen mit $\underline{M}_j' = \underline{M}_j [T]^{-1}$

Da $[G] = [[E]_k \mid [P]] \Longrightarrow$ $\boxed{\underline{\tilde{X}}_j = [\underline{\tilde{M}}_j \mid \underline{\tilde{C}}_j]}$

Mit $\underline{\tilde{C}}_j = \underline{\tilde{M}}_j [P] = \underline{M}_j [T] [P]$

Wichtig hier ist die Tatsache, daß die ersten k Stellen von $\underline{\tilde{X}}_j$ lineare Kombinationen der Informationsbits, während die letzten q Stellen von $\underline{\tilde{X}}_j$ Kontrollbits (nicht die gleichen wie $\underline{C}_j$) bleiben.

Beispiel: Bestimmen Sie $[T]$ u. $[T]^{-1}$ für einen zyklischen Code ($n=7, q=3$) mit $g(P) = P^3 + P + 1$

Lösung

$$\underset{1\times k}{\underline{\tilde{M}}_j} = \underset{1\times k}{\underline{M}_j} \; \underset{k\times k}{[T]} \qquad \underline{M}_j' = \underline{M}_j [T]^{-1}$$

Die Zeilen von $[T]$ und $[T]^{-1}$ sind $\underline{\tilde{M}}_i$ bzw. $\underline{M}_i'$, die $\underline{M}_i = [0 \; 0 \; \overset{\text{q-te Stelle}}{\downarrow} \; 1 \; \;]$ entsprechen.

Aus $\tilde{X}_i(P) = M_i(P)\, g(P)$ erhalten wir für

$$\underline{M}_i = [\underset{\uparrow}{0}\ 0\ \cdots\ \underset{i=1}{i}\ \cdots\ \underset{\uparrow}{0}] \longleftrightarrow M_i(P) = P^{(k-i)} \quad ;$$

$i = 1, 2, \ldots, k \quad (k=4)$

$$\tilde{X}_i(P) = P^{(4-i)} \cdot g(P) = P^{(4-i)} \left(P^3 + P + 1\right)$$

$$= \left(P^{(7-i)} + P^{(5-i)} + P^{(4-i)}\right)$$

= Polynom der Ordnung $(n-1) = 6$

$$\tilde{X}_1(P) = P^6 + P^4 + P^3 \longrightarrow \underline{\tilde{X}}_1 = [\underbrace{1\ 0\ 1\ 1}_{\underline{\tilde{M}}_1}\ |\ 0\ 0\ 0]$$

$$\underline{\tilde{X}}_2(P) = P^5 + P^3 + P^2 \longrightarrow \underline{\tilde{X}}_2 = [\underbrace{0\ 1\ 0\ 1}_{\underline{\tilde{M}}_2}\ |\ 1\ 0\ 0]$$

$$\underline{\tilde{X}}_3(P) = P^4 + P^2 + P \longrightarrow \underline{\tilde{X}}_3 = [\underbrace{0\ 0\ 1\ 0}_{\underline{\tilde{M}}_3}\ |\ 1\ 1\ 0]$$

$$\underline{\tilde{X}}_4(P) = P^3 + P + 1 \longrightarrow \underline{\tilde{X}}_4 = [\underbrace{0\ 0\ 0\ 1}_{\underline{\tilde{M}}_4}\ |\ 0\ 1\ 1]$$

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

Nun, aus $\dfrac{p^{q_i} M_i(p)}{g(p)} = M_i'(p) - \dfrac{C_i(p)}{g(p)}$

Sind die Vier $M_j'(p)$ das Ergebnis der

Division in S. 3, S. 4, nämlich

$M_1'(p) = p^3 + p + 1 \longrightarrow \underline{M}_1' = [\overset{3}{1}\ \overset{2}{0}\ \overset{1}{1}\ \overset{0}{1}]$

$M_2'(p) = p^2 + 1 \longrightarrow \underline{M}_2' = [\overset{3}{0}\ \overset{2}{1}\ \overset{1}{0}\ \overset{0}{1}]$

$M_3'(p) = p \longrightarrow \underline{M}_3' = [\overset{3}{0}\ \overset{2}{0}\ \overset{1}{1}\ \overset{0}{0}]$

$M_4'(p) = 1 \longrightarrow \underline{M}_4' = [\overset{3}{0}\ \overset{2}{0}\ \overset{1}{0}\ \overset{0}{1}]$

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

Es ist einfach zu zeigen, daß $[T][T]^{-1} = [E]_k$