Vorlesung am 07.07.06

11. V NEU

IC SS-06

2.5: Der zyklische Code

in diesem Manuskript soll (2.5.5.) (S.7 → S.11) nach (2.5.4) (S.12 → S.19) behandelt werden. Wegen der Länge der Herleitung sollen nur die Endergebnisse dieser zwei Abschnitte vorgestellt werden.

2.5.1: Das Codepolynom

Für den Codevektor $\underline{X} = [x_{n-1}\ x_{n-2} \cdots x_1\ x_0]$

definiert man das Codepolynom $X(p)$ nach:

$$X(p) = x_0 + x_1 p + x_2 p^2 + \cdots + x_{n-1} p^{n-1}$$

$X(p)$ ist ein Polynom der Ordnung $(n-1)$

$$\underline{X} + \underline{Z} \longleftrightarrow X(p) + Z(p)$$

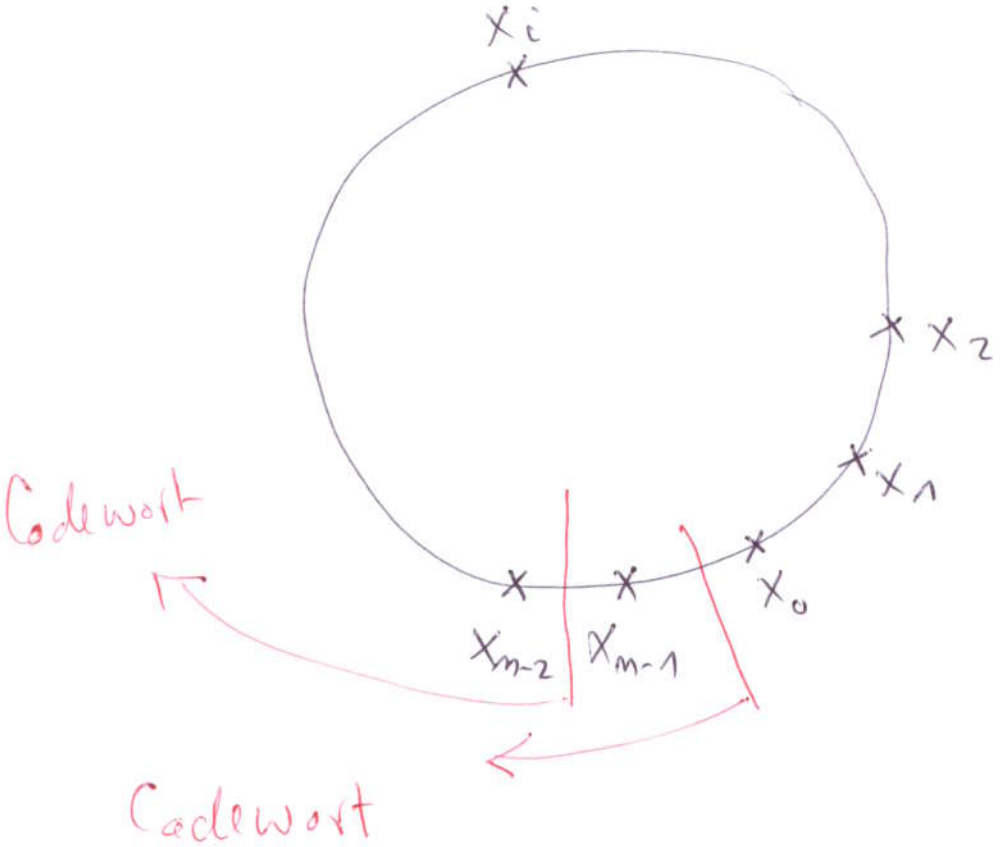
wobei $+$ bezeichnet "Modulo M"; $M = 2$

für binäre Codierung.

2.5.2: Eigenschaften des zyklischen Codes

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

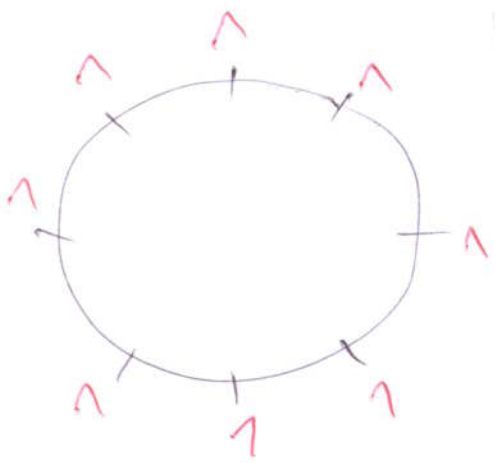
2-) Die Codewörter bilden Zyklen. Innerhalb eines Zyklus bilden die zugehörigen Codewörter einen Ring. Die Verschiebung der Bits um i-Stellen ($1 \leq i < n$) führt zu einem anderen gültigen Codewort:



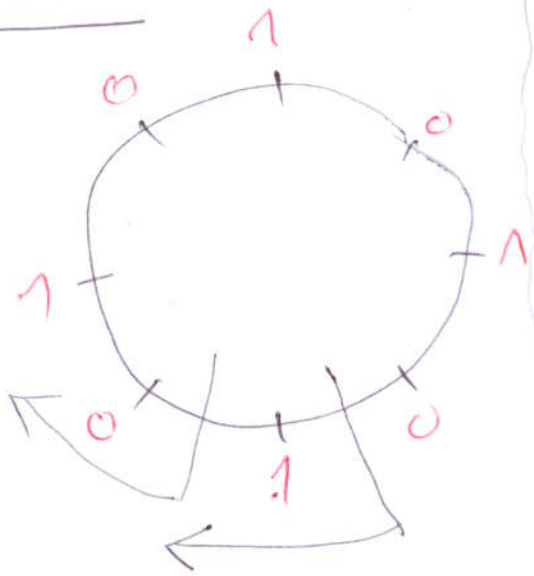
Die Wörter eines Zyklus haben dann das gleiche Gewicht. Die Anzahl der Codewörter (alle sind gültige) innerhalb eines Zyklus ist

maximal n.

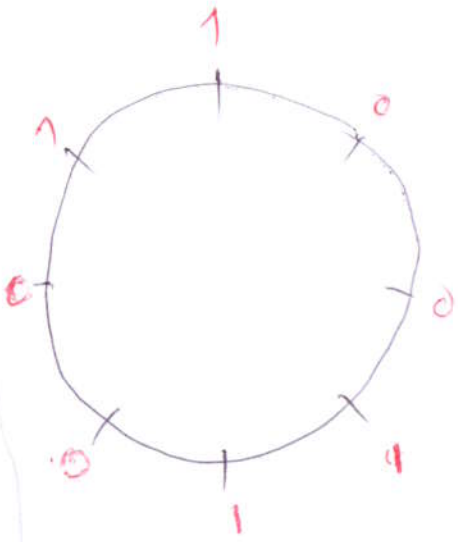
Beispiele mit $n = 8$



Ein Codewort



Zwei Codewörter



Vier Codewörter

2.5.3 : Beschreibung des zyklischen Codes

Für den allgemeinen Fall, betrachten wir eine

M-äre Codierung mit $x_i \in \{0, 1, 2, \ldots, M-1\}$

$$\underline{X}^{(0)} = [x_{n-1} \; x_{n-2} \; \cdots \; x_2 \; x_1 \; x_0]$$

$$\underline{X}^{(1)} = [x_{n-2} \; x_{n-3} \; \cdots \; x_1 \; x_0 \; x_{n-1}]$$

$$\underline{X}^{(2)} = [x_{n-3} \; x_{n-4} \; \cdots \; x_0 \; x_{n-1} \; x_{n-2}]$$

$$\underline{X}^{(i)} = \left[X_{n-i-1} \quad X_{n-i-2} \quad \cdots \quad X_{n-i+1} \quad X_{n-i} \right]$$

$$\underline{X}^{(n-1)} = \left[X_0 \quad X_{n-1} \quad \cdots \quad X_2 \quad X_1 \right]$$

$$\underline{X}^{(n)} = \left[X_{n-1} \quad X_{n-2} \quad \cdots \quad X_1 \quad X_0 \right] = \underline{X}^{(0)}$$

$\underline{X}^{(i)} \; ; \; i = 0, 1, \cdots, n-1$ sind die Codewörter eines Zyklus.

In Abhängigkeit der entsprechenden Codepolynome hat man folgendes:

$$X^{(0)}(P) = X_0 + X_1 P + \cdots + X_{n-2} P^{n-2} + X_{n-1} P^{n-1}$$

$$P X^{(0)}(P) = X_0 P + X_1 P^2 + \cdots + X_{n-2} P^{n-1} + X_{n-1} P^n$$

$$X^{(1)}(P) = X_{n-1} + X_0 P + X_1 P^2 + \cdots + X_{n-2} P^{n-1}$$

$$\Rightarrow \boxed{P X^{(0)}(P) - X^{(1)}(P) = X_{n-1} (P^n - 1)}$$

$$\Longrightarrow \boxed{X^{(1)}(p) = pX^{(0)}(p) - (p^n - 1)\,[X_{n-1}]}$$

($[X_{n-1}]$: Polynom 0-ter Ordnung)

Ähnlich $X^{(2)}(p) = pX^{(1)}(p) - X_{n-2}(p^n - 1)$

$$= p\left[pX^{(0)}(p) - X_{n-1}(p^n - 1)\right]$$

$$- X_{n-2}(p^n - 1)$$

$$\boxed{X^{(2)}(p) = p^2 X^{(0)}(p) - (p^n - 1)\,\underbrace{\left[X_{n-2} + X_{n-1}\cdot p\right]}_{\text{Polynom 1ster Ordnung}}}$$

$$\vdots$$

$$\boxed{X^{(i)}(p) = p^i X^{(0)}(p) - (p^n - 1)\left[X_{n-i} + X_{n-i+1}\,p + \cdots + X_{n-1}\,p^{i-1}\right]}$$

($[\ldots]$: Polynom $(i-1)$ste Ordnung)

Da die Ordnung von $X^{(i)}(p)$ $(n-1)$ ist, wobei die Ordnung von $(p^n - 1)$ (n) ist, dann

$$\text{Rest}\left\{\frac{p^i X^{(0)}(p)}{(p^n - 1)}\right\} = X^{(i)}(p)$$

Für $i = 0$ ist die Ordnung von $p^i X^{(0)}(p)$ $(n-1)$, während die Ordnung von $(p^n - 1)$ (n) ist $\Longrightarrow$ $\text{Rest}\left\{\dfrac{p^i X^{(0)}(p)}{p^n - 1}\right\} = p^i X^{(0)}_{(p)} = X^{(0)}_{(p)}$

wie es sein muß.

Für $i = 1, 2, \ldots, n-1$, ist die Ordnung von $p^i X^{(0)} \geq n \Longrightarrow$ Die Division führt immer zu einem Polynom der Ordnung $(i + n - 1 - n = i - 1)$ zusammen mit einem Rest der Ordnung $< n$. Für $i = n$, $\dfrac{p^i X^{(0)}(p)}{p^n - 1} =$

$$\frac{(p^n - 1) X^{(0)}(p) + X^{(0)}(p)}{(p^n - 1)} \Longrightarrow \text{Rest}\left\{\frac{(p^n - 1) X^{(0)}(p) + X^{(0)}(p)}{(p^n - 1)}\right\}$$

$= X^{(0)}(p)$ da die Ordnung von $X^{(0)}(p)$ $(n-1)$ ist.

Für $i > n$, $\text{Rest}\left\{\dfrac{p^i X^{(0)}(p)}{p^n - 1}\right\} = \text{Rest}\left\{\dfrac{p^{i-n}\left[p^n X^{(0)} - X^{(0)} + X^{(0)}\right]}{p^n - 1}\right\} = \text{Rest}\left\{p^{i-n} X^{(0)} + \dfrac{p^{i-n} X^{(0)}}{p^n - 1}\right\} = \text{Rest}\left\{\dfrac{p^{i-n} X^{(0)}}{p^n - 1}\right\}$.

Da $X^{(0)}(P)$ beliebig gewählt wurde, folgende Aussage kann gemacht werden:

Die Verschiebung der Symbole (Bits im binären Fall) eines gültigen Codewort $\underline{X}^{(j)}$ um $(i-j)$- stellen führt zu einem gültigen Codewort $\underline{X}^{(i)}$ des gleichen Zyklus, wobei

$$X^{(i)}(P) = \text{Rest}\left\{\frac{P^{(i-j)} X^{(j)}(P)}{P^n - 1}\right\}$$

2.5.4. kommt dagegen, S. 12

$$i \geq j$$

2.5.5: Multiplikation von Polynomen

Wir betrachten die erzeugung des zyklischen Codes durch die nachstehende Gleichung (wird später bewiesen):

$$\underbrace{X(P)}_{\text{Ordnung} = (n-1)} = \underbrace{M'(P)}_{\text{Ordnung} = (k-1)} \cdot \underbrace{g(P)}_{\text{Ordnung} = q} \quad \Big\} \; n = k + q$$

wobei

$$X(p) = x_0 + x_1 p + \dots + x_{n-1} p^{n-1} \longleftrightarrow \underline{X} = [x_{n-1}\ x_{n-2}\ \dots\ x_1\ x_0]$$

$$M'(p) = m'_0 + m'_1 p + \dots + m'_{k-1} p^{k-1} \longleftrightarrow \underline{M'} = [m'_{k-1}\ m'_{k-2}\ \dots\ m'_1\ m'_0]$$

$$g(p) = g_0 + g_1 p + \dots + g_q p^q$$

$$M'(p) \cdot g(p) = (g_0 m'_0) + (g_0 m'_1 + g_1 m'_0)\, p + (g_0 m'_2 + g_1 m'_1 + g_2 m'_0)\, p^2 + \dots + (g_{q-1} m'_{k-1} + g_q m'_{k-2})\, p^{n-2} + (g_q \cdot m'_{k-1})\, p^{n-1}$$

$\Downarrow$

$$x_0 = g_0 m'_0 \qquad (\textstyle\sum \text{Indizes} = 0)$$

$$x_1 = g_0 m'_1 + g_1 m'_0 \qquad (\textstyle\sum \text{Indizes} = 1)$$

$$x_2 = g_0 m'_2 + g_1 m'_1 + g_2 m'_0 \qquad (\textstyle\sum \text{Indizes} = 2)$$

$$\vdots$$

$$x_{n-2} = g_{q-1} m'_{k-1} + g_q m'_{k-2} \qquad (\textstyle\sum \text{Indizes} = n-2)$$

$$x_{n-1} = g_q \cdot m'_{k-1} \qquad (\textstyle\sum \text{Indizes} = n-1)$$

Dies lässt sich in folgende Matrix-Form umschreiben:

$$[x_{m-1}\ x_{m-2} \dots x_2\ x_1\ x_0] = [m'_{k-1}\ m'_{k-2} \dots m'_2\ m'_1\ m'_0] \cdot$$

$$\begin{bmatrix} g_q & g_{q-1} & & & 0 & 0 & 0 \\ 0 & g_q & & & 0 & 0 & 0 \\ 0 & 0 & & & \vdots & \vdots & \vdots \\ 0 & 0 & & & \vdots & \vdots & \vdots \\ \vdots & \vdots & & & g_0 & 0 & 0 \\ g & 0 & & & g_1 & g_0 & 0 \\ 0 & 0 & & & g_2 & g_1 & g_0 \end{bmatrix} \longleftarrow (k \times n)$$

$$\Downarrow$$

$$\underline{X} = \underline{M}' [g]$$

$[g]$ hat k Zeilen der Dimension $(1 \times n)$.

$$\underline{g}_1 = [\underbrace{g_q\ g_{q-1}\ g_{q-2} \dots g_1\ g_0}_{(q+1)\text{ Stellen}}\ \underbrace{0 \dots 0}_{(k-1)\text{ Nullen}}]$$

↑ 1ste Zeile

2te Zeile

$$\underline{g}_2 = [0 \; \underbrace{g_q \; g_{q-1} \; \cdots \; g_1 \; g_0}_{(q+1)\text{ Stellen}} \; \underbrace{0 \; \cdots \; 0}_{(k-2)\text{ Nullen}}]$$

k-te Zeile

$$\underline{g}_k = [\underbrace{0 \; 0 \; \cdots \; 0}_{(k-1)\text{ Nullen}} \; \underbrace{g_q \; g_{q-1} \; \cdots \; g_1 \; g_0}_{(q+1)\text{ Stellen}}]$$

Die Zeilen von $[g]$ erhält man durch Verschiebung der (z.B.) ersten Zeile nach rechts.

Da der zyklische Code ein linearer Blockcode ist, wobei

$$\underset{(1\times m)}{\underline{X}} = \underset{(1\times k)}{\underline{M}} \; \underset{(k\times m)}{[G]} \quad , \text{ wobei}$$

$$\underset{k\times m}{[G]} = \left[\underset{k\times k}{[E_k]} \;\middle|\; \underset{k\times q}{[P]} \right]$$

Es gibt dann eine $(n \times n)$ invertierbare Transformationsmatrix $[T]$, wobei

$$\underset{1\times m}{X} = \underset{1\times n}{M}\left(\underset{n\times n}{[T]}^{-1}\underset{n\times n}{[T]}\right)\underset{n\times m}{[G]}$$

$$= \left(\underset{1\times n}{M}\underset{n\times n}{[T]}^{-1}\right)\cdot\left(\underset{n\times n}{[T]}\underset{n\times m}{[G]}\right)$$

$$= \underline{M}' \cdot [g]$$

$$\underline{M}' = \underline{M}\,[T]^{-1}$$

$$[g] = [T][G]$$

$$= [T]\left[[E]_n \,\middle|\, [P]\right]$$

$$= \left[[T] \,\middle|\, \underset{n\times n}{[T]}\underset{n\times q}{[P]}\right]$$

$$\underset{1\times n}{\underline{M}} = \underset{1\times n}{\underline{M}'}\cdot\underset{n\times n}{[T]}, \quad \underset{n\times m}{[g]} = \left[\underset{n\times n}{[T]} \,\middle|\, \underset{n\times q}{[T][P]}\right]$$

2.5.4: Erzeugung des zyklischen Codes

Von hier bis S. 19 muß nicht detailliert vorgestellt werden

Da der zyklische Code ein linearer Blockcode ist,

dann, wenn $X_1(P)$ und $X_2(P)$ gültige Codepolynome sind, dann $a_1 X_1(P) + a_2 X_2(P)$ ebenfalls ein gültiges Codepolynom ist, wobei

$a_1, a_2 \in \{0, 1, \dots, M-1\}$, $+$: Modulo-M-Addition

[für binäre Codierung, a_1, a_2 können nur "0" oder "1" sein] $\Rightarrow \sum_i a_i X_i(P)$ ist ebenfalls ein gültiges Codepolynom ist.

Mit $X_i(P) = X^{(i)}(P) = \text{Rest}\left\{\frac{P^i X^{(\ )}(P)}{P^n - 1}\right\}$

und der Tatsache, daß die Rest $\left\{\frac{\dots}{P^n-1}\right\}$ eine lineare Operation ist [In der Tat ist

$\text{Rest}\left\{\frac{\dots}{P^n-1}\right\} = \text{Modulo}(P^n-1)$]

$$\Rightarrow \text{Rest}\left\{\frac{\overbrace{\left(\sum a_i p^i\right)}^{Y(p)} X^{(0)}(p)}{p^n-1}\right\}$$ ← ebenfalls ein gültiges

Codepolynom ist.

Es ist wichtig zu bemerken, daß $\text{Rest}\left\{\frac{p^i X(p)}{p^n-1}\right\}$ ein Codepolynom im gleichen Zyklus wie $X(p)$ ist, während $X_1(p) + X_2(p)$ zu einem anderen Zyklus (als die von $X_1(p)$ und $X_2(p)$) gehört. Das gleiche gilt für $a\,X(p)$, das zu einem anderen Zyklus (als dem von $X(p)$) gehört (wenn $a \neq 1$)

Beispiel: binäre Codierung mit $X(p) + X(p) = 0$; "0" bildet einen eigenen Zyklus.

Wir definieren nun den Satz $\underline{X}$, der alle gültigen Codepolynome enthält. Wir haben schon gezeigt, daß, wenn $X^{(0)}(p) \in \underline{X}$, dann $\text{Rest}\left\{\frac{Y(p)\,X^{(0)}(p)}{p^n-1}\right\} \in \underline{X}$, wobei $Y(p)$ ein

beliebiges Polynom ist. In der Tat enthält $\bar{X}$ alle möglichen Zyklen des Codes. Eine Multiplikation mit p^i bleibt im gleichen Zyklus (eine einfache Verschiebung um i Stellen), wobei Addition und Multiplikation mit einer Konstanten ($\neq 1$) zum Landen in einem anderen Zyklus führt.

Nun betrachten wir den Fall, wobei $X^{(0)}(p)$ eines der Polynome mit der minimalen Ordnung "q" → mit dem Koeffizienten von p^q gleich 1 (monisches Polynom). Wir nennen dieses Polynom $g(p)$

$$O\{g(p)\} = \text{Minimum} = q$$

Koeffizient von $p^q = 1$

$$\Longrightarrow \quad X^{(0)}(p) = g(p) \in X$$

$$\text{Rest}\left\{\frac{Y(p)\,g(p)}{p^n - 1}\right\} \in \bar{X}$$

Die Eigenschaft des linearen Blockcodes dass wenn $X(p)$ ein gültiges Codepolynom ist, dann $aX(p)$ ebenfalls ein gültiges Codepolynom ist garantiert die Existenz von $X^{(0)}(p) = g(p) =$ monisches Polynom der minimalen Ordnung q.

Wir definieren $\bar{X}_0$ als eine Untermenge von $\bar{X}$ wobei $O\{Y(p)\} \leq n - q - 1$

In diesem Fall ist $\partial\{Y(P) - g(P)\} \leq (n-q-1)+q$
$= (n-1)$

$$\Longrightarrow \text{Rest}\left\{\frac{Y(P)\,g(P)}{P^n-1}\right\} = Y(P) = g(P)$$

Dieses $Y(P)$, mit $\partial\{Y(P)\} \leq n-q-1$ wird ab jetzt $Q_j(P)$ genannt. Dies bedeutet,

$$\vec{X}_0 = \left\{ X_j(P) = g(P) \cdot Q_j(P),\ j = 1, 2, \dots, N \right\},$$

wobei N = Anzahl der möglichen $Q_j(P)$;
$\partial\{Q_j(P)\} \leq n-q-1$. Für eine M-äre Codierung nehmen die Koeffizienten der Polynome nur die Werte $(0, 1, 2, \dots, M-1)$ an. Die Anzahl der Koeffizienten in $Q_j(P)$ mit $\partial\{Q_j\} \leq n-q-1$ (einschließlich der verschwindenen Koeffizienten) ist $n-q$.
Dies bedeutet, daß $M^{(n-q)}$ verschiedene $Q_j(P)$ mit $\partial\{Q_j\} \leq n-q-1$ existieren $\Rightarrow$ $\boxed{N = M^{(n-q)}}$

Nun, $\bar{X}_0 \subset \bar{X}$, da $X^{(0)}(P) = g(P)$ ein gültiges Codepolynom ist, und $X_j(P) = Q_j(P) \cdot g(P)$

$$= \text{Rest}\left\{ \frac{Q_j(P) \cdot g(P)}{P^n - 1} \right\} \quad \left(\text{da } O(g(P) \cdot Q_j(P)) \leq n-1\right)$$

Wir werden jetzt beweisen, daß $\bar{X}_0 = \bar{X}$.

↓ nicht wichtige Details

Angenommen, daß es ein Polynom $X(P)$ gibt das in $\bar{X}$ aber nicht in $\bar{X}_0$ ist $\Longrightarrow$

$O\{X(P)\} < n$, $X(P) \neq g(P) \cdot Q_j(P)$ (mit $O\{Q(P)\} < (n-q)$). Allerdings wird es ein Polynom $r(P)$ geben, mit $Q\{r(P)\} < q$, so daß

$$X(P) = g(P) \cdot Q(P) + r(P)$$

Da $g(P) \cdot Q(P) \in \bar{X}_0 \subset \bar{X}$, $\bar{X}_0 \subset \bar{X} \longrightarrow g(P) \cdot Q(P)$ sowie $X(P)$ sind in $\bar{X}$. Da diese lineare Kombination von zwei Polynomen in $\bar{X}$ ist ebenfalls in $\bar{X} \Longrightarrow r(P) = X(P) - g(P) \cdot Q(P)$ ist in $\bar{X}$. Aber $Q\{r(P)\} < q$, was wiederspricht der

Annahme, daß q die minimale Ordnung aller Polynome in $\bar{X}$ ist $\Rightarrow V(P) = 0 \Longrightarrow \bar{X}_0 = \bar{X}$

Wir haben denn:

Alle gültigen Codepolynome (d.h., alle Polynome in $\bar{X}$) haben die Form $X_j(P) = g(P) \cdot Q_j(P)$;

$j = 1, 2, \dots, N = M^{(n-q)}$. Da [wenn $X(P) \in \bar{X}$, dann Rest $\left\{\frac{Y(P) \cdot X(P)}{P^n - 1}\right\} \in \bar{X}$], alle Rest $\left\{\frac{\tilde{Y}(P) - g(P)}{P^n - 1}\right\} \in X$

$\tilde{Y}(P) = Y(P) \cdot Q(P) =$ beliebiges Polynom

$Y(P)$: beliebiges Polynom

$Q(P)$: einer der $Q_j(P)$

Zunächst werden wir beweisen, daß $g(P)$ ein Faktorpolynom von $(P^n - 1)$ sein muß

Angenommen, daß dies nicht der Fall ist. In diesem Fall wird es die Polynome $h(P)$ and $s(P)$ geben, mit $\partial\{h(P)\} = (n-q)$ und $\partial\{s(P)\} \leq q$, so daß

$$P^n - 1 = h(P) \cdot g(P) + s(P)$$

Wegen der Linearität der Rest $\left\{ \frac{\cdot\cdot\cdot}{p^n-1} \right\}$-Operation haben wir:

$$\text{Rest}\left\{\frac{p^n-1}{p^n-1}\right\} = \text{Rest}\left\{\frac{h(p)\cdot g(p)}{p^n-1}\right\} + \text{Rest}\left\{\frac{s(p)}{p^n-1}\right\}$$

($\text{Rest}\left\{\frac{p^n-1}{p^n-1}\right\} = 0$; $\text{Rest}\left\{\frac{s(p)}{p^n-1}\right\} = s(p)$)

$$\Rightarrow s(p) = -\text{Rest}\left\{\frac{h(p)\cdot g(p)}{p^n-1}\right\} = \text{Rest}\left\{\frac{-h(p)\cdot g(p)}{p^n-1}\right\}$$

Aber alle $\text{Rest}\left\{\frac{\tilde{Y}(p)\cdot g(p)}{p^n-1}\right\} \in \underline{X}$, wobei $\tilde{Y}(p)$ beliebig ist $\Rightarrow s(p) \in \underline{X}$. Dies widerspricht die Annahme, daß q die minimale Ordnung aller Polynome in $\underline{X}$ ist

$\Rightarrow s(p) = 0$ und

$$(p^n-1) = h(p)\cdot g(p)$$

* Die Rolle von $\circ\{h(p)\} = n-q$ $h(p)$

Für ein gültiges Codepolynom $X_j(p) \in \underline{X}$ gilt

$$X_j(P) = g(P) \cdot Q_j(P) \Longrightarrow h(P) \cdot X_j(P) = h(P) \cdot g(P) \cdot Q_j(P)$$
$$= (P^n - 1) \cdot Q_j(P)$$

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

$$\Downarrow$$

Für alle gültigen Codepolynome $X_j(P)$ gilt:

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

ab S. 12 bis hier muß nicht detailiert vorgestellt werden

Nun, mit $\underline{X}_j = [\underline{M}_j \mid \underline{C}_j]$, $j = 1, 2, \ldots, M^k$

($n = 2$ für binäre Codierung), haben wir

$$\underline{X}_j = [x_{n-1}^{(j)} \; x_{n-2}^{(j)} \; \ldots \; x_1^{(j)} \; x_0^{(j)}] \qquad (1 \times n)$$

$$\underline{M}_j = [m_{k-1}^{(j)} \; m_{k-2}^{(j)} \; \ldots \; m_1^{(j)} \; m_0^{(j)}] \qquad (1 \times k)$$

$$\underline{C}_j = [C_{q-1}^{(j)} \; C_{q-2}^{(j)} \; \ldots \; C_1^{(j)} \; C_0^{(j)}] \qquad (1 \times q$$

$$\Downarrow$$

$$x_i^{(j)} = C_i^{(j)} \; ; \quad i = 0, 1, \ldots, (q-1)$$

$$x_i^{(j)} = m_{i-q}^{(j)} \; ; \quad i = q, q+1, \ldots, (n-1)$$

$$X_j(P) = m_{k-1}^{(j)} P^{(n-1)} + m_{k-2}^{(j)} P^{(n-2)} + \dots + m_1^{(j)} P^{(q+1)} +$$

$$m_0^{(j)} P^q + C_{q-1}^{(j)} P^{q-1} + \dots + C_1^{(j)} q + C_0^{(j)}$$

$M_j(P)$

$$= P^q \left[m_{k-1}^{(j)} P^{(k-1)} + m_{k-2}^{(j)} P^{(n-2)} + \dots + m_0^{(j)} \right]$$

$$+ \left[C_{q-1}^{(j)} P^{(q-1)} + C_{q-2}^{(j)} P^{(q-2)} + \dots + C_0^{(j)} \right]$$

$C_j(P)$

$$= P^q M_j(P) + C_j(P)$$

$$\Downarrow$$

$$\boxed{X_j(P) = P^q M_j(P) + C_j(P)}$$

Ordnung $< q$

Da für $\underline{M}_j \neq 0$, $\underline{M}_j$ mindestens ein nicht verschwindendes Element haben muß $\Longrightarrow$

$$O\{M_j(P)\} > 0 \Rightarrow O(X_j(P)) \geq q$$

Für $\underline{M}_1 = [0 \; 0 \; \dots \; 0 \; a]$; $a \in \{0, 1, 2, \dots, M-1\}$

gilt $O\{M_1(P)\} = 0 \Rightarrow O\{X_1(P)\} = q =$ minimale Ordnung in $\underline{X}$.

Ein zyklischer Code muß dann ein Generator-Polynom $g(P)$ der Ordnung q haben. Für so einen Code gilt:

$$X_j(P) = g(P) \cdot M_j'(P)$$

wobei $M_j'(P)$ eins der Polynome $\{Q_i(P);$ $i = 1, 2, \dots, M^{(k-1)}$ mit $O\{Q_i(P)\} \leq k-1\}$

$$\Rightarrow \underbrace{P^q M_j(P)}_{\text{Ordnung} \leq (n-1)} + \underbrace{C_j(P)}_{\text{Ordnung} \leq (q-1)} = \underbrace{g(P)}_{\text{Ordnung} = q} \cdot \underbrace{M_j'(P)}_{\text{Ordnung} \leq k-1}$$

$$\Rightarrow P^q M_j(P) = \underbrace{g(P)}_{\text{Ordnung} = q} \cdot M_j'(P) - \underbrace{C_j(P)}_{\text{Ordnung} < q}$$

$$\Rightarrow \frac{P^q M_j(P)}{g(P)} = \underbrace{M_j'(P)}_{\text{Polynom}} - \frac{C_j(P) \leftarrow \text{Ordnung} < q}{g(P) \leftarrow \text{Ordnung} = q}$$

$$\Rightarrow C_j(P) = \text{Rest}\left\{\frac{-P^q M_j(P)}{g(P)}\right\}$$

Beispiel: Zyklischer $(n=7,\ k=4,\ q=3)$-Code (binär)

Wichtig: Jeder zyklische Code ist ein linearer Blockcode, der eine Matrix-Beschreibung (neben der Polynom-Beschreibung) hat.

Wir suchen ein Generator-Polynom $g(p)$ dessen Ordnung q ist so daß $\frac{p^n-1}{g(p)} = h(p) =$ Polynom der Ordnung $k = n-q$. Da wir binär arbeiten, dann gibt's keinen Unterschied zwischen (+) und (-) $\Longrightarrow p^n-1 \Rightarrow p^n \oplus 1$

$$p^n \oplus 1 = (p \oplus 1)(p^3 \oplus p^2 \oplus 1)(p^3 \oplus p \oplus 1) \cdot \text{Eins}$$

der zwei Polynome p^3+p^2+1 u. p^3+p+1 kann als $g(p)$ gewählt werden.

Nehmen wir $g(p) = p^3+p^2+1 \Longrightarrow$

$h(p) = p^4+p^3+p^2+1$

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

$\Longrightarrow M(p) = p^3+p \Rightarrow \text{Rest}\left\{\frac{p^q M(p)}{g(p)}\right\} = 1 = C(p)$

$$\begin{array}{r|l} p^3+p^2+1 & p^3+p^2+1 \\ \hline & p^6+p^4 \\ & p^6+p^5+p^3 \\ \hline & p^5+p^4+p^3 \\ & p^5+p^4+p^2 \\ \hline & p^3+p^2 \\ & p^3+p^2+1 \\ \hline \end{array}$$

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

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

$X(p) = p^6+p^4+1$; $h(p)\cdot X(p) = (p^6+p^4+1)$

$(p^4+p^3+p^2+1) = (p^3+1)(p^3+p^2+1) \Rightarrow \text{Rest}\left\{\frac{h(p)\cdot X(p)}{p^3+p^2+1}\right\} = 0$