Kanalcodierung

Allgemeine Bemerkungen zur Kanalcodierung

Die Kanalcodierung gestattet die Erkennung oder sogar die Korrektur von Fehlern, die bei der Übertragung binärer Datenwörter auftreten. Die Codierungstheorie bedient sich der Methoden der Arithmetik endlicher Algebren. Der Einfachheit halber beschäftigen wir uns daher hier mit Verfahren der bitweisen Codierung, die über der binären Algebra GF(2) arbeitet. Mit der

Addition

+	0	1
0	0	1
1	1	0

und der Multiplikation

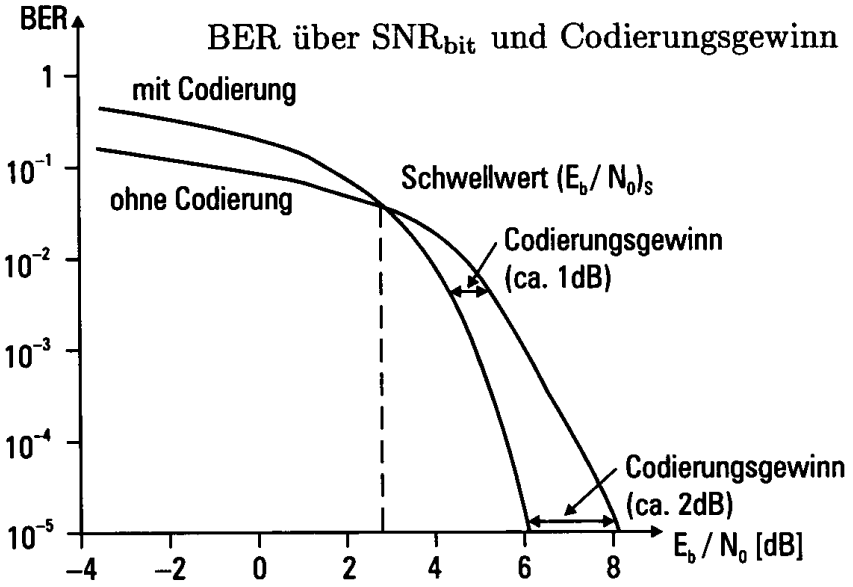
·	0	1
0	0	0
1	0	1

ist über der Menge (0, 1) der ***Körper GF(2)*** erklärt. Körper sind Systeme in denen die arithmetischen Grundoperationen (+, –,·, /) unbeschränkt ausgeführt werden können. Senderseitig wird zur Codierung ein Encoder eingesetzt, dessen Gegenstück im Empfänger als Decoder bezeichnet wird.

Verfahren der Kanalcodierung werden eingesetzt, um bei gegebenem ***Signal-Rausch-Verhältnis (SNR, Signal to Noise Ratio)*** die ***Bitfehlerrate (BER, Bit Error Rate)*** zu senken. Als SNR_{bit} bezeichnet man das dimensionslose Verhältnis der Bitenergie zur Rauschleistungsdichte .

$$SNR_{bit} / dB = 10 \cdot \lg\left\{\frac{E_{bit}}{N_0}\right\}$$

Die Wirksamkeit eines Kanalcodierungsverfahrens zeigt sich im Verhalten der BER über dem SNR_{bit} (Bild).



Gegenüber der nicht codierten Übertragung ergibt sich ein ***Codierungsgewinn***.

Beispiel:
15 Bits werden übertragen und durch vertikale und horizontale gerade *Paritätskontrolle* gesichert:

$l =$		1	2	3	4	5	P_R
$m=$	1	1	1	0	1	0	1
	2	1	0	1	0	0	1
	3	0	1	1	0	0	0
	P_C	0	0	1	1	0	0

Im Empfänger wird festgestellt, dass die Paritätsbits für $m = 2$ und $l = 3$ falsch sind. Damit ist erkannt, dass die unterstrichene 1 falsch ist und in eine 0 verwandelt werden muß.
Für einen Code der bis zu t Fehler erkennen oder korrigieren kann, kann die Restfehlerwahrscheinlichkeit abgeschätzt werden durch

$$P_F \le \sum_{i=t+1}^{n} \binom{n}{i} \cdot p^i \cdot (1-p)^{n-1}$$

Darin ist mit n die Länge der Codewörter bezeichnet. Blockcodes sind dadurch gekennzeichnet, dass sie ein *k-bit-Datenwort* in ein *n-bit-Codewort* transformieren. Sie werden auch als (n, k)-Codes bezeichnet. Ihre ***Coderate*** ist

$$r = \frac{n}{k}$$

Für das o.g. Beispiel ergibt sich $r=15/24=0{,}625$.
Die Vorteile der Kanalcodierung werden erkauft durch

- erhöhten schaltungstechnischen Aufwand in Sender und Empfänger,
- zusätzliche Verzögerungen durch En- und Decoder-Durchlaufzeiten,
- eine um r verkleinerte (Netto-) Datenrate bei der Übertragung.

Blockcodes

Systematische Blockcodes

Im folgenden werden lineare Blockcodes betrachtet, d.h. die $(n - k)$ Paritycheckbits sind Linearkombinationen der k Datenbits. Ein Blockcode ist systematisch, wenn seine n-bit-Codewörter so aufgebaut sind, dass an das k-bit-Datenwort das (n – k)-bit-Paritycheckwort angehängt wird.
Der Encoder berechnet aus dem Datenwort d das Codewort c (Datenworte als Spaltenvektoren)

$$c^T = d^T \cdot G$$

worin G die ***Codegeneratormatrix*** ist. G hat die Form

$$G = \left[I_k P \right]$$

I_k ist die $k \times k$ Einheitsmatrix, P ist die $(n-k) \times k$ Prüfmatrix und G spiegelt die Verknüpfungen zwischen, Daten- und Paritycheckwörtern wider.

Beispiel:

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

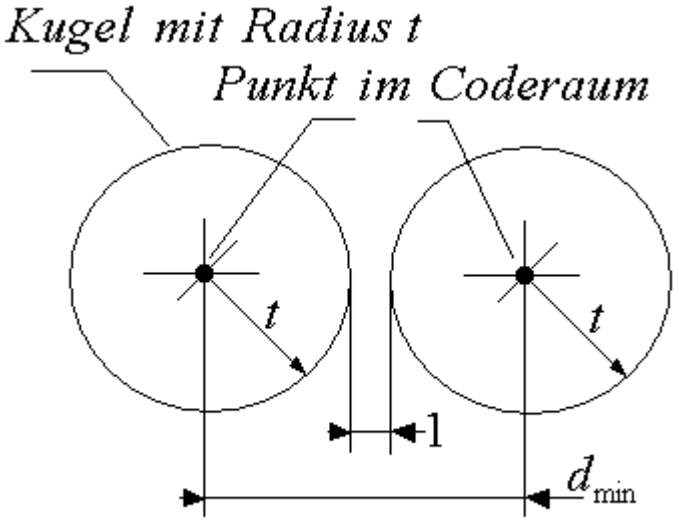
definiert einen (7, 3)-Code. Der Code ist systematisch und die Codewörter sind:

d^T	$c^T \times G$
000	*0000000*
001	*0011111*
010	*0100110*
011	*0111001*
100	*1001100*
101	*1010011*
110	*1101010*
111	*1110101*

Alle Codewörter unterscheiden sich in mindestens 3 Bitpositionen.
Allgemein heißt die Anzahl der Komponenten, an denen sich zwei Codewörter unterscheiden, ***Hammingabstand***.
Für einen Code, mit dem *t* Bitfehler korrigiert werden können, muß notwendigerweise gelten, dass der minimale Hammingabstand d_{min} zweier Codewörter die Ungleichung

$$d_{\min} \geq 2 \cdot t + 1$$

erfüllt.



Zwei Kugeln mit dem Radius t dürfen keinen gemeinsamen Punkt (Codewort) enthalten

Der Decoder arbeitet mit der durch

$$H = \left[P^T I_{n-k} \right]$$

definierten ***Kontrollmatrix H***.

Beispiel:
Für G aus dem Beispiel ergibt sich

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Der Decoder berechnet für das empfangene Wort *r* das ***Syndrom*** *s*

$$s^T = r^T \cdot H^T$$

Ist r^T ein Codewort c^T , folgt mit dem Parityprüfwort ${c_p}^T$:

$$s^T = c^T \cdot \begin{bmatrix} P \\ I_{n-k} \end{bmatrix} = \left[d^T c_p^T \right] \cdot \begin{bmatrix} P \\ I_{n-k} \end{bmatrix}$$

$$= d^T \cdot [P] + c_p^T \cdot [I_{n-k}] = c_p^T + c_p^T = [0]^T \bmod 2 \quad .$$

Ist r^T kein Codewort, existiert ein vom Nullwort verschiedenes Fehlermuster *e* und ein Codewort *c*, mit dem $r = c+e$ gilt.

Das Zeichen ***s*** heißt ***Syndrom***. Wenn $s \neq [0]^T$ gilt, liegt ein Übertragungsfehler vor.

Beispiel:
G und *H* seien die Matrizen der vorigen Beispiele gegeben.

Wir senden das Codewort $c^T = [1\ 1\ 0\ 1\ 0\ 1\ 0]$.

Es tritt das Fehlermuster e auf $e^T = [0\ 0\ 1\ 0\ 0\ 0\ 0]$.

Wir empfangen $r^T = [1\ 1\ 1\ 1\ 0\ 1\ 0]$.

Im Decoder wird das Syndrom s berechnet

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

Der Vergleich mit H^T zeigt die Übereinstimmung mit der dritten Zeile, d.h. es ist e^T = (0010000). Es muß also das dritte Bit fehlerhaft sein.

Für die Korrekturfähigkeit eines Blockcodes gilt die ***Hammingungleichung*** :
Um *t* Fehler korrigieren zu können, muß die Anzahl der möglichen Parityprüfwörter mindestens der Anzahl der Möglichkeiten entsprechen, unter denen bis zu *t* Fehler auftreten können:

$$2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i}$$

Die ***Hammingungleichung*** ist eine ***notwendige (keine hinreichende)*** Bedingung!

Zyklische Blockcodes

Ein linearer (n, k)-Blockcode heißt zyklisch, wenn jede zyklische Verschiebung eines Codewortes wieder ein Codewort ist. Mit

$\boldsymbol{c = [c_1, c_2, \ldots, c_n]^T}$ sind dann auch

$\boldsymbol{c = [c_2, c_3, \ldots, c_n, c_1]^T}$, $\boldsymbol{c = [c_3, c_4, \ldots, c_n, c_1, c_2]^T}$ usw. Codewörter.

Solche zyklischen Codes stehen in einem engen Zusammenhang zu bestimmten boolschen Polynomen, die man als Generatorpolynomen bezeichnet. Wir wollen die Zusammenhänge an einem einführenden Beispiel studieren.

Beispiel:

$g(x) = x^4 + x^3 + x^2 + 1$ mit $x \in \{0, \quad 1\}$ sei unser Generatorpolynom.

Damit ist es möglich die Generatormatrix eines zyklischen (7,3)-Codes zu konstruieren. Mit g(x) erhält man die erste Zeile der Generatormatrix, wobei man die Koeffizienten des Polynoms an die entsprechenden Positionen der Zeile schreibt. Die Spalten der Matrix sind dabei so geordnet, das sie den Potenzen von x, beginnend mit x^6 bis x^0, entsprechen. Bei den nicht vorhandenen Potenzen steht eine Null, bei den vorhandenen eine Eins. Jede weitere Zeile erzeugt man nun, indem man das zugehörige Polynom mit x multipliziert und das Ergebnis mod (x^7+1) berechnet. Diese Operation entspricht einer zyklischen Linksverschiebung der Koeffizienten.

$$G = \begin{matrix} x^6 & x^5 & x^4 & x^3 & x^2 & x^1 & x^0 \\ \end{matrix}$$
$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{matrix} \leftarrow x^2 \cdot g(x) = x^6 + x^5 + x^4 + x^2 \\ \leftarrow x \cdot g(x) = x^5 + x^4 + x^3 + x^1 \\ \leftarrow g(x) = x^4 + x^3 + x^2 + x^0 \end{matrix}$$

Diese Generatormatrix hat noch den Nachteil das zwar eine zyklischen, aber keinen systematischen Code erzeugt. Das lässt sich leicht erreichen, da man die erste (3,3)-Teilmatrix durch Linearkombination der Zeilen von G zu einer 3-Einheitsmatrix umformen kann. Es entsteht dabei ein äquivalenter aber systematischer zyklischer Code.
Formt man wie folgt um:

Z1neu = Z1alt + Z2alt, Z2neu = Z2alt + Z3alt und Z3neu = Z3alt erhält man

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix} \begin{matrix} \leftarrow & x^6 \cdot g(x) & \mod(x^7+1) \\ \leftarrow & x^5 \cdot g(x) & \mod(x^7+1) \\ \leftarrow & g(x) & \mod(x^7+1) \end{matrix}$$

Man kann zeigen, dass das Element der k-ten Zeile und n-ten Spalte der Generatormatrix G eines zyklischen Codes eine 1 sein muß, G also die Form

Jeder zyklische (n, k)-Blockcode besitzt ein Generatorpolynom der Gestalt

$$g(x) = x^{n-k} + \ldots\ldots + x^0$$

das den Grad $n - k$ und immer den Koeffizienten 1 bei x^0 hat.

Es gilt folgender Satz:

- Das Generatorpolynom g(x) erzeugt genau dann einen zyklischen (n, k)- Code, wenn es Teiler von $x^n + 1$ ist.

Beispiel:
Wir suchen (7, k)-Codes, benötigen also Teiler von $x^7 + 1$. Man kann nachrechnen, dass

$$x^7 + 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1)$$

gilt und die Faktoren der rechten Seite irreduzibel sind. Durch

$$g(x) = (x+1)(x^3 + x+1) = x^4 + x^3 + x^2 + 1$$

wird also, wie wir aus den Beispielen wissen, ein zyklischer (7, 3)- Code defniert.

Die Konstruktion zyklischer Codes verläuft wie folgt:

1. Durch Auswertung der ***Hamming-Ungleichung*** findet man eine geeignete (n, k)-Kombination für eine vorgegebene Fehlerkorrekturfähigkeit *t*.
2. Ein Teiler von $x^n + 1$ mit dem Grad $n - k$ wird als Generatorpolynom g(x) benutzt.
3. Aus $g(x)$ wird die Generatormatrix G berechnet.
4. Der so gefundene Code muß, da die ***Hamming-Ungleichung*** nur eine notwendige Bedingung liefert, noch dahingehend untersucht werden, ob er die gewünschte Korrekturfähigkeit auch wirklich besitzt.

Zur Generierung eines zyklischen Codes werden ***linear rückgekoppelte Schieberegister*** eingesetzt. Dazu werden Datenwort d und Codewort c zunächst als Polynome geschrieben:

$$d(x) = d_1 x^{k-1} + d_2 x^{k-2} + d_3 x^{k-3} + \ldots\ldots + d_{k-1} x + d_k$$

$$c(x) = c_1 x^{n-1} + c_2 x^{n-2} + c_3 x^{n-3} + \ldots\ldots + c_{n-1} x + c_n$$

Da $d(x)$ maximal den Grad $k - 1$ hat, besitzt $x^{n-k} d(x)$ maximal den Grad $n - 1$. Wir berechnen

$$\frac{x^{n-k} \cdot d(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}$$

Die Division liefert ein Polynom $q(x)$ maximal $(k - 1)$-ten Grades und einen Rest $r(x)$. Wegen $r(x) + r(x) = 0 \pmod 2$ ist $x^{n-k} d(x) + r(x)$ durch $g(x)$teilbar.
Da die Zeilen der Generatormatrix in Polynomform, sukzessive unter Beachtung der Regeln der linearen Algebra aus der letzten Zeile, die $g(x)$ enthält, konstruiert werden (siehe Beispiel), stellt jede dieser Zeilen ein mit $g(x)$ multipliziertes Polynom dar. Daher gilt für das Codewortpolynom

$$c(x) = a(x) \cdot g(x)$$

Das Polynom $a(x)$ hat maximal den Grad $(k - 1)$, es gibt also genau $\boldsymbol{2^k}$ verschiedene Polynome $a(x)$.
Da $x^{n-k} d(x) + r(x)$ durch $g(x)$ teilbar ist, gibt es also ein Codewort

$$c(x) = a(x) \cdot g(x) = x^{n-k} \cdot d(x) + r(x)$$

$x^{n-k}\ d(x)$ ist aber nichts weiter als eine Linksverschiebung der Datenbits um $(n-k)$ Stellen. Da der Code systematisch ist, muß also

$$r(x) = rest\left[\frac{x^{n-k} \cdot d(x)}{g(x)}\right]$$

das Paritätsprüfwort sein.

Beispiel:

$$g(x) = x^4 + x^3 + x^2 + 1$$

erzeugt einen zyklischen (7, 3)-Code. Mit $d = [0, 0, 1]^T$ und $n - k = 4$ folgt

$$d(x) = 1, x^{n-k} \cdot d(x) = x^4$$

und daraus

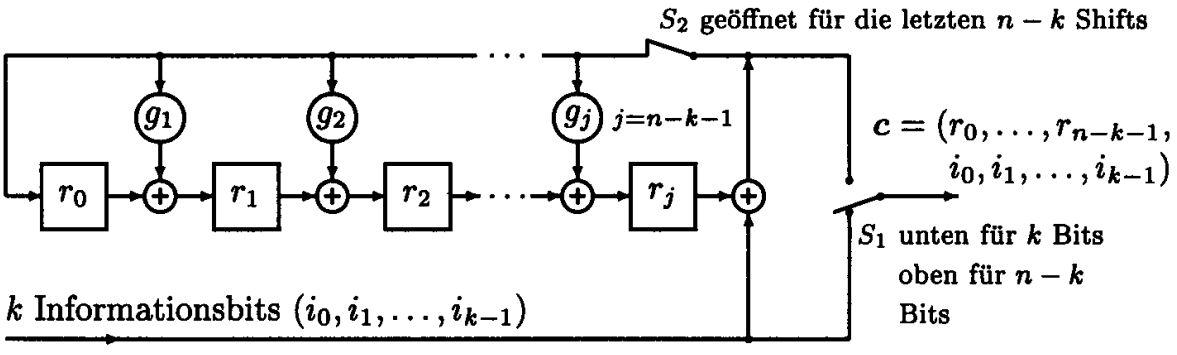
$$r(x) = rest\left[\frac{x^4}{x^4 + x^3 + x^2 + 1}\right] = x^3 + x^2 + 1$$

d wird also codiert in $c = [0\ 0\ 1\ 1\ 1\ 0\ 1]^T$.

Die Berechnung des Rests einer Polynomdivision, kann als linear rückgekoppeltes Schieberegister mit $n - k$ Speicherzellen implementiert werden. Die Codierung des systematischen Datenworts d (bzw. $d(x)$) geschieht dann wie im folgenden Abschnitt beschrieben.

Codierung von zyklischen Codes

In der Abbildung ist eine Schieberegisterschaltung dargestellt, die die drei notwendigen arithmetischen Operationen der systematischen Codierung eines zyklischen (n,k)-Codes durchführt.



Systematische Codierung eines zyklischen (n,k) Codes

Die Funktionsweise der Schaltung kann in drei Schritten beschrieben werden:

Schritt A

- Zunächst werden die k Informationsbits $i_0, i_1,.....,i_{k-1}$ (oder in Polynomform: $i(x) = i_0+i_1x+.....+i_{k-1}x^{k-1}$) in das Schieberegister eingelesen: i_{k-1} ist hierbei das erste Bit. Der Schalter S_2 ist zunächst geschlossen – das Schieberegister somit rückgekoppelt.
- Durch das Einlesen von "Rechts" wird $i(x)$ automatisch mit x^{n-k} vormultipliziert.
- Sobald die k Informationsbits vollständig in das Schieberegister eingelesen sind, befindet sich der Rest r(x) der Division in den $(n – k)$ Registern.

Schritt B

- Im zweiten Schritt muß nun der Rückkoppelungspfad durch das Gatter S_2 unterbrochen werden. S_1 wird nach oben umgelegt.

Schritt C

- Die $n – k$ Prüfbits $r_0, r_1 ,....,r_{n-k-1}$ können jetzt ausgelesen werden und stellen zusammen mit den Informationsbits das vollständige Codewort $c = [i_0, i_1,.....,i_{k-1} , r_0, r_1 ,....,r_{n-k-1}]$ dar.

Beispiel:

In der nachstehenden Abbildung ist die Schieberegisterschaltung für die Codierung des zyklischen (7,4)-Codes dargestellt. Die Codierung erfolgt systematisch mit $g(x) = x^3 + x + 1$. Die zu codierende Information sei $i = (i_0, i_1, i_2, i_3)^T = (1,1,0,1)^T$. Das Schieberegister durchläuft nun folgende Zustände:

Information	r_0	r_1	r_2	j-ter Shift
	0	0	0	Grundzustand
$i_3 = 1$	1	1	0	1. Shift
$i_2 = 0$	0	1	1	2. Shift
$i_1 = 1$	0	0	1	3. Shift
$i_0 = 1$	0	0	0	4. Shift

Das Codewort lautet also $c = [0\ 0\ 0\ 1\ 1\ 0\ 1]^T$

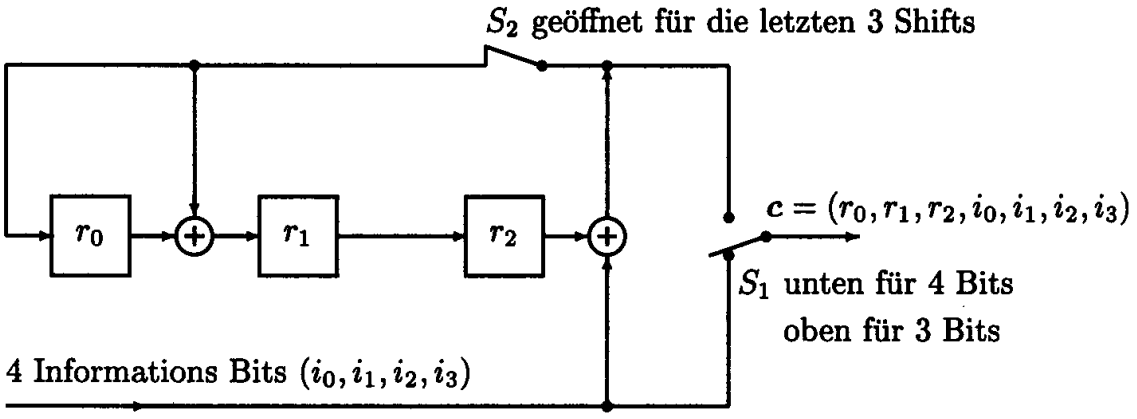


Abbildung 5.6: Systematische Codierung eines zyklischen (7,4) Codes

Syndromberechnung bei zyklischen Codes

In den vorausgegangenen Abschnitten wurde bereits eine Möglichkeit angegeben, den Einfluß des Fehlers, der Syndrom genannt wird, zu bestimmen. Durch Multiplikation des Empfangsvektors mit der Prüfmatrix $s^T = Hr^T$ kann das Syndrom berechnet werden. Gilt $s = 0$, so ist r ein Codewort, im anderen Fall ist r fehlerbehaftet. Für den fehlerbehafteten Empfangsvektor $r = [r_0, r_1, ...,r_{n-1}]^T$ gilt:

$$r = c + e \Leftrightarrow r(x) = c(x) + e(x)$$

wobei $r(x)$ ein Polynom vom Grade $n-1$ ist.
Für zyklisch Codes kann die Berechnung des Syndroms auch durch die Division von r(x) durch g(x) erfolgen:

$$\frac{r(x)}{g(x)} = q(x) + \frac{s(x)}{g(x)} \Leftrightarrow r(x) = q(x) \cdot g(x) + s(x)$$

denn gemäß der Codiervorschrift ergibt sich s(x) = 0 nur dann, wenn r(x) ein Codewort und somit ein Vielfaches von g(x) ist.
Allgemein ist $s(x)$ ein Polynom vom Grad kleiner gleich $n - k - 1$. Die $n - k$ Koeffizienten von $s(x) = s_0+s_1x+....+s_{n-k-1}x^{n-k-1}$ bilden das Syndrom $s=[s_0\ s_1\ ....\ s_{n-k-1}]^T$. Die Berechnung des Syndroms kann wieder mit Hilfe eines linearen rückgekoppelten Schieberegisters gemäß der Abbildung erfolgen.

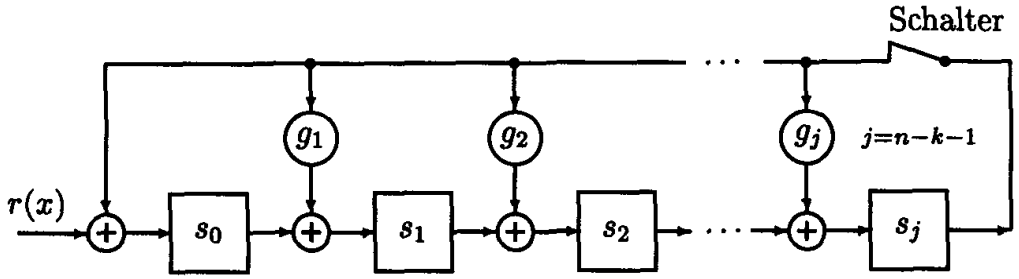


Abbildung : Syndromberechnung bei zyklischen (n,k) Codes

Beispiel:
In der nachstehenden Abbildung ist die Schieberegisterschaltung für die Syndromberechnung des zyklischen (7,4)- Codes mit $g(x) = x^3 + x + 1$ dargestellt.

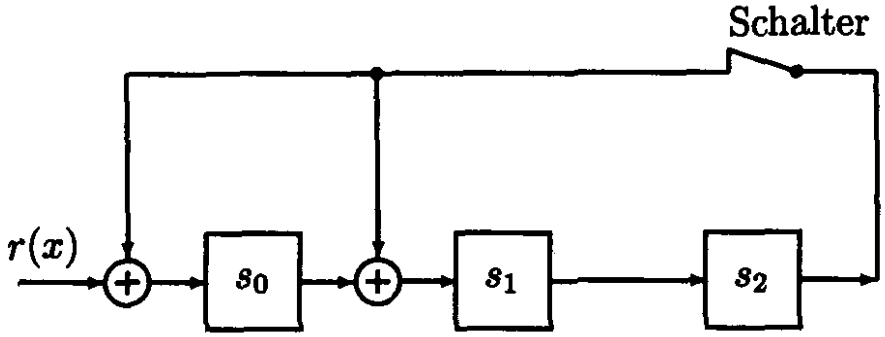


Abbildung: Syndromberechnung eines zyklischen (7,4) Codes