Grundlagen der Kanalcodierung

Seminar “Nachrichtentechnische Systeme”

Dominik Gedon

20. Januar 2017

Inhalt

Motivation

Was ist Kanalcodierung?

- Bei Übertragung und Speicherung von Daten muss mit Störungen gerechnet werden
- Sicherung der Nachricht gegen Fehler

  $\Longrightarrow$ Sendeseitiges Hinzufügen von **Redundanz**
- Empfänger nutzt diese Redundanz, um Fehler zu erkennen/korrigieren

  Aufgabe: Fehlererkennung und ggf. Fehlerkorrektur anhand von Redundanz

Was ist Kanalcodierung?

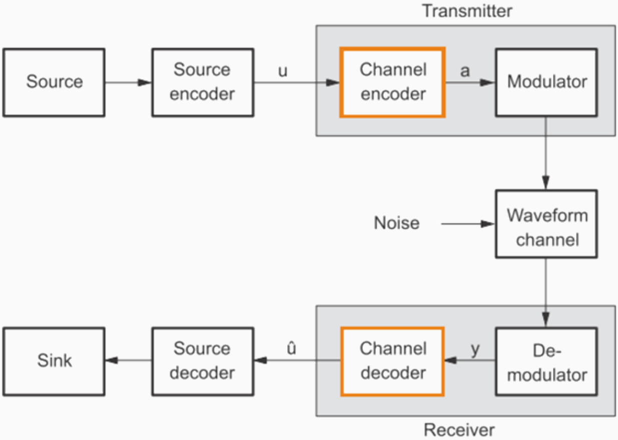


Figure 1: Übersicht Kanalcodierung [2]

Wo wird Kanalcodierung angewendet?

- Mobile Kommunikation (GSM, UMTS, LTE, WLAN)
- Satellitenkommunikation
- Netzwerk (LAN, WAN)
- Speicherung (CD, DVD, Blu-ray Disk, HDDs)
- QR Codes, Barcodes, ISBN, IBAN

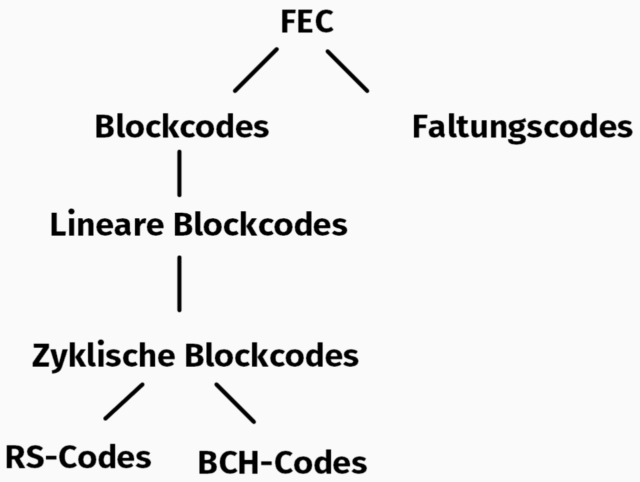
Verfahren der Kanalcodierung

ARQ (Automatic Repeat Request)

- Signal wird durch ausschließlich fehlererkennenden Code geschützt.
- Bei Fehlerdetektion Wiederholung des fehlerhaften Blocks
- Existenz eines Rückkanals erforderlich

FEC (Forward Error Correction)

- Einsatz fehlerkorrigierender Codes
- Höhere Redundanz auch bei guten Übertragungsbed.
- konstanter Datendurchsatz unabhängig vom aktuellen Kanalzustand


FEC
Blockcodes
Faltungscodes
Lineare Blockcodes
Zyklische Blockcodes
RS-Codes
BCH-Codes

Grundbegriffe

3. Grundbegriffe: Hamming-Distanz d

Anzahl der Stellen, in denen sich 2 Codewörter unterscheiden

- **Fehlererkennung**: $t = d_{min} - 1$
- **Fehlerkorrektur**: $t_{corr} = \lfloor \frac{d_{min}-1}{2} \rfloor$
- Wichtiges Maß zur Beurteilung der Leistungsfähigkeit eines Codes

$d_{min} \Leftrightarrow$ Fähigkeit Fehler zu erkennen und zu korrigieren

3. Grundbegriffe: Blockcodierung: (n,k)-Blockcodes

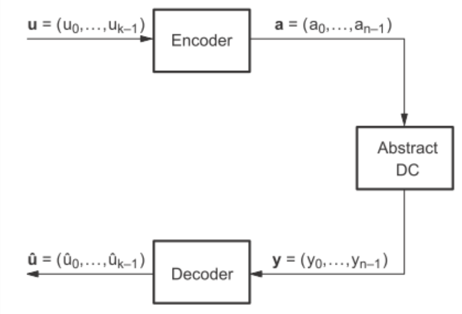


Figure 2: Prinzip des (n,k)-Blockcodes [2]

- Block **u** aus **k** Infobits $\Rightarrow$ Codewort **a** aus **n** Symbolen
- Von 2^n möglichen Wörtern nur 2^k als Codewörter
- Hard-Decision vs. Soft-Decision

- Maximum-Likelihood-Decodierung (MLD)
- Bounded Distance Decodierung (BDD)
- Bounded Minimum-Distance Decodierung (BMD)

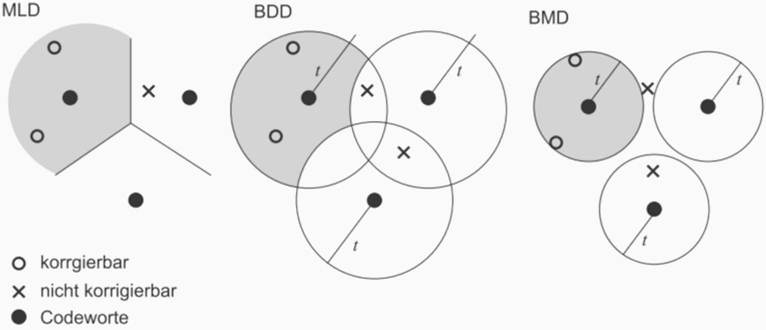


Figure 3: Veranschaulichung von MLD, BDD und BMD [3]

Blockcodes

- Gruppeneigenschaft für Codewörter gefordert
- Einfache Codierbarkeit/Decodierbarkeit

- Binärcodes $a_i \epsilon \{0, 1\}$
- Systematische Encodierung

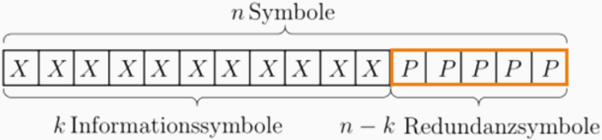


Figure 4: Systematische Encodierung [6]

Generatormatrix

$$\underbrace{(a_0,\ldots,a_{n-1})}_{\text{Codewortvektor } \bar{a}} = \underbrace{(u_0,\ldots,u_{n-1})}_{\text{Informationsvektor } \bar{u}} \cdot \underbrace{\begin{bmatrix} g_{0,0} & \cdots & g_{0,n-1} \\ \vdots & & \vdots \\ g_{k-1,0} & \cdots & g_{k-1,n-1} \end{bmatrix}}_{\text{Generatormatrix } G}$$

Systematische Encodierung

$$G = \left[\begin{array}{ccc|ccc} 1 & \ldots & 0 & P_{0,0} & \ldots & P_{0,n-1} \\ 0 & \ddots & 0 & \vdots & & \vdots \\ 0 & \ldots & 1 & P_{k-1,0} & \ldots & P_{k-1,n-1} \end{array}\right] = [I_{n-k}|P]$$

1. Berechnung des Syndroms s

$$\mathbf{s} = \underbrace{y}_{\text{Empfangswort}} \cdot H^T = (\underbrace{a}_{\text{Codewort}} + \underbrace{e}_{\text{Fehlerwort}}) \cdot H^T = e \cdot H^T$$

   Prüfmatrix H $= [P^T | I_{n-k}]$

   - Es gilt $a \cdot H^T = 0$
   - Übertragung fehlerfrei: **s = 0**

2. Das Syndrom markiert die Fehlerpositionen $i_0, \ldots, i_n$
3. Korrektur des empfangenen Binärwortes an den Stellen $i_0, \ldots, i_n$

- 1-Fehler korrigierend und 2-Fehler erkennend
- Verwendung mehrerer Paritätsbits
- $d_{min} = 3$
- 2^4 = 16 Codewörter

Informationswort u $= (u_1 \quad u_2 \quad u_3 \quad u_4)$,
Codewort a $= (a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad a_7)$

$$\underbrace{\begin{pmatrix}1 & 0 & 0 & 1 & 0 & 1 & 1\end{pmatrix}}_{\text{Codewort a}} = \underbrace{\begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix}}_{\text{Infowort u}} \cdot \underbrace{\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 0 & 1 & 1 & 1\\ 0 & 0 & 0 & 1 & 1 & 0 & 1\end{bmatrix}}_{\text{Generatormatrix G}}$$

4. Lineare Blockcodes: Beispiel (7,4)-Hamming-Code

$$\underbrace{\mathbf{a} = \begin{pmatrix}1 & 0 & 0 & 1 & 0 & 1 & 1\end{pmatrix}}_{\text{gesendet}}, \underbrace{\mathbf{y} = \begin{pmatrix}1 & 0 & 0 & 1 & 0 & 0 & 1\end{pmatrix}}_{\text{empfangen}}$$

$$H = [P^T | I_3] = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$s = y \cdot H^T = \begin{pmatrix}1 & 0 & 0 & 1 & 0 & 0 & 1\end{pmatrix} \cdot \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{pmatrix}0 & 1 & 0\end{pmatrix}$$

Zyklische Blockcodes

5. Zyklische Blockcodes

- Zyklische Verschiebung eines Codewortes ist wiederum ein Codewort
  $(a_0, \ldots, a_{n-2}, a_{n-1}) \Rightarrow (a_{n-1}, a_0, \ldots, a_{n-2})$

- Beschreibung durch Polynome
- Zeichen des Codeworts sind Koeffizienten des Polynoms

- Sehr einfach Encodierung/Decodierung durch Filteroperationen in Schieberegistern

Systematische Encodierung

$$a(x) = (\underbrace{p_0, \ldots, p_{n-k-1})}_{\text{n-k Prüfbits}}, \underbrace{u_0, \ldots, u_{k-1}}_{\text{k Infosymbole}})$$

$$\underbrace{a(x)}_{\text{Codewortpol.}} = \underbrace{u(x)}_{\text{Infowortpolynom}} \cdot \underbrace{g(x)}_{\text{Generatorpol.}} = \underbrace{p(x)}_{\text{Prüfpolynom}} + \underbrace{x^{n-k} \cdot u(x)}_{\text{System. Teil}}$$

- **p(x)** so bestimmen, dass **a(x)** ohne Rest durch **g(x)** teilbar

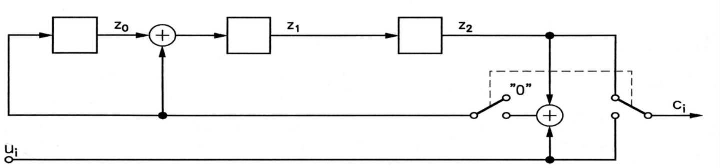
$$\Rightarrow \mathit{Rest} : \mathbf{p(x)} = R_{g(x)}\{x^{n-k}u(x)\} = x^{n-k}u(x) \bmod g(x)$$

g(x) $= 1 \oplus x \oplus x^3$

Infowort u = $(0 \quad 0 \quad 0 \quad 1) \leftrightarrow u(x) = x^3$

$$\begin{aligned} p(x) &= R_{1 \oplus x \oplus x^3}\{x^3 x^3\} \\ &= R_{1 \oplus x \oplus x^3}\{(1 \oplus x)(1 \oplus x)\} \\ &= R_{1 \oplus x \oplus x^3}\{1 \oplus x^2\} \\ &= 1 \oplus x^2 \end{aligned}$$

Codewortpol. a(x) = $p(x) \oplus x^3 u(x) = 1 \oplus x^2 \oplus x^3 x^3 = 1 \oplus x^2 \oplus x^6$



Step i	u_{k-i}	$u_{k-i} \oplus z_2^{(i)}$	$z_0^{(i+1)}$	$z_1^{(i+1)}$	$z_2^{(i+1)}$	c_j	j
Init			0	0	0		
1	1	1	1	1	0	1	6
2	0	0	0	1	1	0	5
3	0	1	1	1	1	0	4
4	0	1	1	0	1	0	3
5		$\underbrace{\qquad}_{q(x)}$	0	1	0	1	2
6		with $x^{n-k}u(x) =$	0	0	1	0	1
7		$q(x)g(x) \oplus p(x)$	0	0	0	1	0

Figure 5: Schieberegisterschaltung Encodierung [1]

Berechnung des Syndroms $s = R_{g(x)}\{y(x)\}$

$$y(x) = a(x) + e(x) = u(x) \cdot g(x) + e(x)$$

$$s(x) = \underbrace{R_{g(x)}\{u(x) \cdot g(x)\}}_{=0} + R_{g(x)}\{e(x)\} = R_{g(x)}\{e(x)\}$$

$\Rightarrow$ Syndrom hängt nur vom Fehlerpolynom e(x) ab

Fehlererkennung:

- Berechnung des Syndroms
- $\Rightarrow$ Übertragung fehlerfrei, falls $s(x) = 0$

Fehlerkorrektur:

1. Berechnung des Syndroms
2. Fehlermuster des Syndroms bestimmen
   Decoder enthält wahrscheinlichste Fehlermuster in Syndromtabelle
3. Korrektur des empfangenen Polynoms

Korrektur des empfangenen Polynoms mit Hilfe von Schieberegister

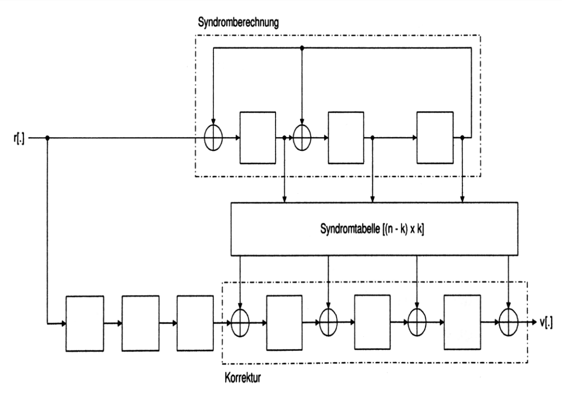


Figure 6: Schieberegisterschaltung Decodierung [4]

Ausblick

Ausblick

BCH-Codes

- Gut zur Korrektur von Einzelfehlern

RS-Codes

- Spezielle BCH-Codes
- Keine Binären Symbole
- Codewörter besitzen spezielle spektrale Eigenschaften
- Hervorragend zur Korrektur von Bündelfehlern

Faltungscodes

- blockfreie Codes
- Redundanz durch Faltung der Information in Kanalcodefolge
- Encoder besitzt Gedächtnis

Zusammenfassung

Zusammenfassung

- Sicherung der Nachricht gegen Fehler
  $\Rightarrow$ **Redundanz**

- Fehlererkennung und ggf. Fehlerkorrektur

- Konstruktion geeigneter Codes

  Anforderung: Gute Fehlererkennungs- und Fehlerkorrektureigenschaften mit möglichst geringer Redundanz

Quellen i

[1] Huber, Fischer, Stierstorfer - Fundamentals of Channel Coding
[2] Bernd Friedrichs - Kanalcodierung
[3] Volker Kühn - Vorlesungsskript Kanalcodierung I SoSe 2016
[4] Markus Hufschmid - Information und Kommunikation
[5] Martin Bossert - Kanalcodierung
[6] Johannes Huber - Vorlesungsskript Nachrichtentechnische Systeme WS 2016/17