

Spezielle Protokolle des IoT

Redundanz - Fehlerkorrektur



Einleitung

Fehlerdetektion und -korrektur

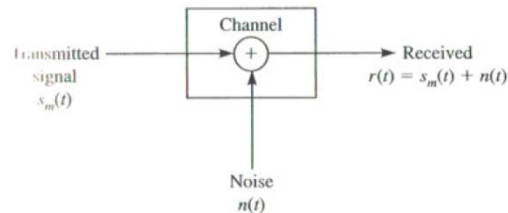
- ▶ Einführung
- ▶ Definitionen
- ▶ Lineare Block Codes
 - ▶ Repetition Codes
 - ▶ Hamming Codes
 - ▶ Verkürzte Codes (Shortening)
 - ▶ Dekodierung (Hard Decision)
- ▶ Weitere Codes



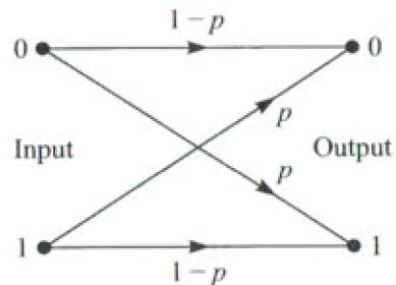
Fehlererkennung und -korrektur

Modellierung eines fehlerbehafteten Übertragungskanals

- Hinzufügen von Weißem Gaußischem Rauschen (AWGN: Additional White Gaussian Noise)



- Kanal mit gleicher Bitfehlerwahrscheinlichkeit (BSC: Binary Symmetric Channel)



- Kanal mit Informationsverlust (BEC: Binary Erasure Channel; Packet Erasure Channel)
- Beispiele?

Definitionen

Definition von Operatoren

- ▶ Die meisten folgenden Operationen finden bitweise statt
- ▶ Die boolsche Operation Exclusive-Or (bzw. Addition mit 1 bit ohne Überlauf) wird mit

„+“ abgekürzt (sonst häufig mit \oplus)

Gewicht eines Codeworts Die Gewichtung eines Wortes ist die Anzahl der Zeichen ungleich Null, die es enthält.

- ▶ Das Gewicht (Weight) eines Codeworts ist die Anzahl von ~~x~~ verschiedener Komponenten ungleich Null (meist Bits)
 $w(001010111)=5$

Hamming-Distanz

- ▶ Die Hamming-Distanz (Hamming Distance) zwischen zwei Codeworten ist die Anzahl sich unterscheidender Komponenten
 $d(01011,01000)=2$

Parität (Parity)

- ▶ Ein Paritätsbit ergänzt eine Folge von Bits so, dass deren binäre Summe gerade (even parity) oder ungerade (odd parity) wird, z.B. muss bei 111 das Paritätsbit für gerade Parität 1 sein



Lineare Block Codes

Lineare Block Codes

- ▶ Hier: Einschränkung auf binäre Codes
- ▶ Idee: Um k Bits Nutzdaten zu übertragen, werden n Bits verwendet
- ▶ Die Rate ist $R=k/n$, man spricht von einem (n,k) -Code, z.B. von einem $(7,4)$ -Code
- ▶ Aufgabe: Entwurf eines Codes, so dass einzelne Übertragungsfehler korrigiert werden können
- ▶ Verfahren: 2^n Codewörter stehen zur Verfügung, aber nur 2^k werden genutzt
- ▶ Fehlerdetektion: Es kann (dann und nur dann) kein Fehler detektiert werden, wenn durch Übertragungsfehler ein Codewort in ein anderes gültiges Codewort umgeformt wird
- ▶ Fehlerkorrektur: Durch Feststellen des nächsten Nachbarn im Coderaum kann einem ungültigen Codewort ein gültiges Codewort zugeordnet werden → Annahme, dass der geringstmögliche Fehler aufgetreten ist



Lineare Block Codes

Matrizenschreibweise

- ▶ Gegeben die Informationssequenz u_m der Länge k
- ▶ Gegeben die sogenannte Generatormatrix G eines (n,k) -Codes
- ▶ Ergibt $c_m = u_m G$ das Codewort c_m der Länge n

Systematische Lineare Block Codes

- ▶ Ein LBC ist dann systematisch, wenn die Generatormatrix aus einer Einheitsmatrix I_k gefolgt von einer sogenannten Parity-Check Matrix besteht, d.h.

$$G = [I_k \mid P]$$

Praktisch bedeutet dies, dass die ersten Bits des Codeworts den Bits der Informationssequenz entsprechen

- ▶ Jeder Lineare Block Code kann in eine systematische Form überführt werden
- ▶ Beispiel (7,4)-Code:

$$G = [I_4 \mid P] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$



Lineare Block-Codes

Dekodierung und Fehlerkontrolle

- Zu jedem (n,k) systematischen Code mit der Generatormatrix

$$G = [I_k \mid P]$$

kann eine sog. Parity-Check Matrix erstellt werden:

$H = [-P^T \mid I_{n-k}]$ (I ist wieder die Einheitsmatrix, P^T ist die transponierte Matrix von oben, für binäre Codes gilt $P^T = -P^T$)

- Beispiel:

$$H = [P^T \mid I_{n-k}] = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$G = [I_4 \mid P] = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

- Anmerkung:

- Zu jedem (n,k) Code existiert ein $(n, n-k)$ Dualer Code
- Die Generatormatrix dieses dualen Codes ist die Parity-Check Matrix



Lineare Block Codes

Typische Block-Codes

- ▶ Wiederholungs-Codes (Repetition Codes): $(n,1)$ Code mit n -facher Wiederholung des Informationsbits, die minimale Hamming-Distanz ist $d_{\min}=n$.
Anmerkung: Der Duale Code ist ein $(n,n-1)$ Code, der ein Paritätsbit (gerade) an die Informationsbits anhängt und eine minimale Hamming-Distanz von 2 aufweist
- ▶ Hamming-Codes
 $(2^i - 1, 2^i - i - 1)$ -Codes mit $i > 2$
Die Spalten der Parity Check Matrix bestehen aus allen binären Vektoren der Länge i (ausschließlich des 0-Vektors).
Beispiel: Parity-Check Matrix eines $(7,4)$ Hamming Codes in systematischer Darstellung
Man findet in den Spalten: 001, 010, 011, ...

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



Standard Array und Syndrom

Nutzung der Paritätsinformation

- ▶ Mit Hilfe der Paritätsinformation können Fehler erkannt werden, wenn das Fehlermuster das gesendete Codewort nicht zu einem existenten Codewort verfälscht hat
- ▶ Um für ein empfangenes (ungültiges) Codewort das nächstgelegene gültige Codewort zu finden, wird das Standard-Array konstruiert:
 - ▶ Die erste Zeile enthält alle Codewörter, startend bei demjenigen, mit dem geringsten Gewicht (gewöhnlich 0000..)
 - ▶ In der zweiten Zeile wird dasjenige Bitmuster geschrieben, das in der ersten Zeile nicht vorkam und das geringste Gewicht hat (zufällige Auswahl falls mehrere vorhanden). Dies ist das erste Fehlermuster und es wird binär auf alle Codewörter aus der ersten Zeile addiert
 - ▶ Dies wird fortgeführt bis zur Zeile 2^{n-k} , der maximalen Anzahl möglicher Fehlermuster eines (n,k) Codes

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

00000	01011	10101	11110
00001	01010	10100	11111
00010	01001	10111	11100
00100	01111	10001	11010
01000	00011	11101	10110
10000	11011	00101	01110
11000	10011	01101	00110
10010	11001	00111	01100



Standard Array und Syndrom

Nutzung der Paritätsinformation

- ▶ Als „Syndrom“ (Syndrome) werden die Bits der Paritätsinformation bezeichnet.
- ▶ Das Bitmuster des Syndroms kann eindeutig einer Zeile aus dem Standard-Array zugeordnet werden und entspricht somit einem binären Fehlermuster
- ▶ Beispiel: Gemäß Standard-Array soll 10000 zu 00000 dekodiert werden. Die Parity-Check Matrix ist

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

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

- ▶ $[1\ 0\ 0\ 0\ 0]\ H^T = [1\ 0\ 1]$ (Syndrom) aber auch:
 $[1\ 1\ 0\ 1\ 1]\ H^T = [1\ 0\ 1]$

- ▶ Anm.: Für systematische linear Block-Codes geben die niederwertigen Syndrome die Position des Bitfehlers an (z.B. 010=2.Bit)

Syndrome	Error Pattern
000	00000
001	00001
010	00010
100	00100
011	01000
101	10000
110	11000
111	10010

00000	01011	10101	11110
00001	01010	10100	11111
00010	01001	10111	11100
00100	01111	10001	11010
01000	00011	11101	10110
10000	11011	00101	01110
11000	10011	01101	00110
10010	11001	00111	01100



Sonstige Operationen bei LBC

Lineare Block Codes können vielfältig verändert werden

- ▶ Kürzung und Verlängerung
- ▶ Punktuierung und Erweiterung
- ▶ ...

▶ Beispiel: Kürzung

Ein Hamming-Code kann nur mit bestimmten Längen konstruiert werden (7,4), (15,11), ... allerdings können Zeilen in der Generatormatrix weggelassen werden, die nicht benötigt werden, so dass aus einem (15,11) Code ein (12,8) Code oder ein (8,4) Code entsteht (8Bit bzw. 4Bit Nutzdaten), die Minimaldistanz bleibt unberührt, so dass für diesen Code $d_{\min}=4$ gilt, im Gegensatz zu $d_{\min}=3$ für einen (7,4) Hamming Code
Beispiel: (8,4) gekürzter Hamming Code

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



Literaturverweis:

- ▶ Proakis, Salehi, „Digital Communications“, 5th edition, McGraw-Hill, ISBN: 978-0076-126378-8



Danke für Ihre Aufmerksamkeit!

