Institut für Nachrichtentechnik

Grundlagen der Informationstechnik - Nachrichtentechnik

Vorlesung: Eduard A. Jorswieck
Übung: Dr. Bile Peng

Wintersemester 2023-2024, 7. Dezember 2023

Kanal-Decodierung I

- Im Kanal tritt der Fehlervektor $\boldsymbol{e}$ auf und wir empfangen den Vektor

$$\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}.$$

- Wir berechnen das *Syndrom*

$$\boldsymbol{H} \cdot \boldsymbol{y}^T = \boldsymbol{H} \cdot \boldsymbol{c}^T + \boldsymbol{H} \cdot \boldsymbol{e}^T = \boldsymbol{H} \cdot \boldsymbol{e}^T = \boldsymbol{s}^T.$$

- Das Syndrom enthält nur Informationen zum Fehler und kann deshalb zur Decodierung verwendet werden.
- Bei der **Fehlererkennung:** Wenn der Fehler kein Codewort ist, können wir ihn mit $\boldsymbol{s} \neq \boldsymbol{0}$ erkennen. Wenn kein Fehler auftritt oder der Fehler ein Codewort ist, entscheiden wir falsch.

Kanal-Decodierung II

- Bei der **Fehlerkorrektur:** Der Decodierer trifft eine Entscheidung für das (wahrscheinlichste) Codewort $\hat{\boldsymbol{c}}$.

Satz

Ein Code $\mathcal{C}(n, k, d) \subseteq \mathbb{F}_2^n$ mit der Mindestdistanz d kann beliebige $0 \leqslant t \leqslant d - 1$ Fehler sicher erkennen. Man kann $0 \leqslant t \leqslant \lfloor \frac{d-1}{2} \rfloor$ Fehler eindeutig korrigieren.

Kanal-Decodierung III

Satz: Hamming-Schranke, Sphere packing bound

Für die Parameter eines Codes $\mathcal{C}(n, k, d) \subseteq \mathbb{F}_2^n$ muss gelten

$$2^k \sum_{l=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{l} \leqslant 2^n.$$

Institut für Nachrichtentechnik

Kanal-Decodierung IV

Definition: MAP Decodierung von Codeworten

Die optimale MAP Decodierentscheidung unter der Annahme, dass die bedingten Wahrscheinlichkeiten des Kanals und die Quellenstatistik exakt bekannt sind, ergibt sich als

$$\hat{c} = \arg\max_{c \in \mathcal{C}} f(c|y) = \arg\max_{c \in \mathcal{C}} f(y|c) f(c).$$

Ist das Maximum nicht eindeutig, so wird eins zufällig davon gewählt.

- ML Decodierung ist

$$\hat{c} = \arg\max_{c \in \mathcal{C}} f(y|c).$$

Kanal-Decodierung V

- Man kann die Entscheidung auch symbolweise treffen, berücksichtigt aber trotzdem, dass ein Code benutzt wird.

Definition: Symbolweise MAP Decodierung

Die optimale s-MAP Decodierentscheidung für die Stelle i, unter der Annahme, dass die bedingten Wahrscheinlichkeiten des Kanals exakt bekannt sind, ergibt sich als

$$\hat{c}_i = \arg\max\{ \sum_{c \in \mathcal{C}, c_i = 0} f(y|c) f(0), \sum_{c \in \mathcal{C}, c_i = 1} f(y|c) f(1) \}.$$

Dies wird für alle n Codestellen durchgeführt.

Kanal-Decodierung VI

- Beachte, dass die n Decodiererergebnisse nicht notwendigerweise ein gültiges Codewort ergeben müssen.

Satz: Blockfehlerwahrscheinlichkeit bei der Decodierung

Die Blockfehlerwahrscheinlichkeit P_B von ML, MAP, und BMD-Decodierern für einen Code $\mathcal{C}(n, k, d)$ kann abgeschätzt werden durch:

$$P_B \leqslant \sum_{i=e+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} = 1 - \sum_{i=0}^{e} \binom{n}{i} p^i (1-p)^{n-i}.$$

Kanal-Decodierung VII

Fehlerwahrscheinlichkeit bei Fehlererkennung

Die Fehlerwahrscheinlichkeit bei Fehlererkennung für einen Code $\mathcal{C}(n, k, d)$ mit Gewichtsverteilung $A = [A_0, A - 1, ..., A_n]$ ist

$$P_F = \sum_{i=d}^{n} A_i p^i (1 - p)^{n-i}.$$

Kanalcodierungstheorem I

- Das Kanalcodierungstheorem von Shannon besagt, dass Codes mit Coderate R existieren, bei denen die Blockfehlerwahrscheinlichkeit P_B gegen 0 geht, falls R kleiner als die Kanalkapazität C ist. Die Codelänge n geht dabei gegen unendlich.
- Falls $R \geqslant C$ ist, ist die Blockfehlerwahrscheinlichkeit P_B gleich 1.
- Shannons Beweis ist leider nicht-konstruktiv und beschreibt somit weder Codekonstruktionen noch Decodierverfahren, die praktisch einsetzbar sind.
- Trotzdem handelt es sich um ein bahnbrechendes Ergebnis.
- Es hat Generationen von Codiertheoretikern motiviert, Codeklassen und Decoderverfahren zu finden, die immer näher an die Kanalkapazität herankamen.

Kanalcodierungstheorem II

- Heute kann die Kapazität praktisch erreicht werden.

Erinnere 4. Vorlesung letzte Folie

Für einen diskreten gedächtnislosen Kanal (DMC) ist die Kanalkapazität die maximal erreichbare wechselseitige Information

$$C = \max_{f_X(x)} I(X;Y) = \max_{f_X(x)} \{H(X) - H(X|Y)\} = \max_{f_X(x)} \{H(Y) - H(Y|X)\}.$$

Kanalcodierungstheorem III

Shannons Kanalcodierungstheorem und Rückrichtung

C sei die Kanalkapazität eines Kanals und $\mathcal{C}(n, k, d)$ ein Blockcode.

a) Ist $R < C$, so existieren Blockcodes der Rate R und Länge n für die gilt $\lim_{n\to\infty} P_B^n \to 0$.

b) Ist $R \geqslant C$, so gilt für alle Codes $\lim_{n\to\infty} P_B^n = 1$.

- Kapazität für BSC mit Bitflip-Wahrscheinlichkeit ϵ gilt

$$C_{BSC} = 1 - H_b(\epsilon).$$

- Für den BEC ist die Kapazität

$$C_{BEC} = 1 - \epsilon.$$

Kanalcodierungstheorem IV

- Für den AWGN mit Sendeleistung P und Rauschleistung N ist die Kapazität
$$C_{AWGN} = \log_2(1 + P/N).$$
- Wir werden später weitere komplexere Kanäle und deren Kapazität besprechen.

Faltungscodes I

- Faltungscodes sind eine große Klasse von Codes, die auf diskreten linearen zeitinvarianten Systemen basieren.
- Analytische Aussagen bei Faltungscodes sind schwierig, deshalb wird Faltungscodierung an einem Beispiel eingeführt.

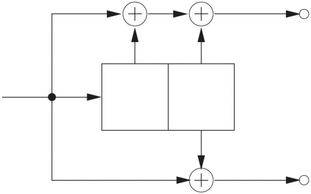

Abbildung 1: Faltungscodierer

Faltungscodes II

- Ein Faltungscodierer besteht aus Schieberegistern und linearen Verknüpfungen der Register.
- In dem Beispiel werden aus einem Informationsbit zwei Codebits.
- Codiere die Bitfolge $1011|00$
- Zur Decodierung verwendet man die Darstellung eines Faltungscodes durch ein so genanntes Trellis.
- Die Codefolge am Ausgang hängt nur vom Eingang und dem Speicherinhalt ab.
- Im Beispiel gibt es nur vier mögliche Zustände: 00, 01, 10, 11.
- Je nachdem in welchem der vier Zustände man ist, kann man in zwei nachfolgende Zustände übergehen (für 0 und 1 am Eingang).

Faltungscodes III

- Es bietet sich ein Zustandsdiagramm an:

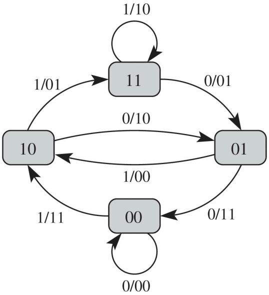

Abbildung 2: Zustandsdiagramm des Faltungscodierers.

Faltungscodes IV

- Ein *Trellis* ist ein sogenannter Graph, in dem die vier Zustände als Knoten und die Zustandsübergänge als Zweige bezeichnet werden.
- An die Zweige schreiben wir die Codefolge.
- Gestrichelte Zweige bedeuten, dass eine 0 am Eingang liegt, durchgezogene Zweige sind eine 1.

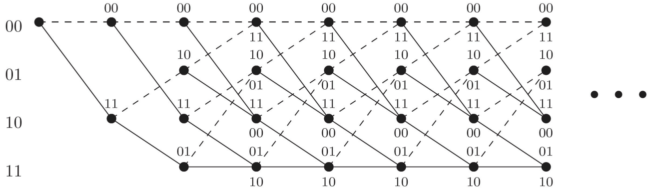

Abbildung 3: Trellis des Faltungscodierers.

Institut für Nachrichtentechnik

Faltungscodes V

- Jede mögliche Codefolge ist ein Pfad durch das Trellis.
- Durch das Anhängen der beiden Nullen an die Informationssequenz erzwingen wir, dass jedes gültige Codewort im Zustand 00 enden muss.

Faltungscodes VI

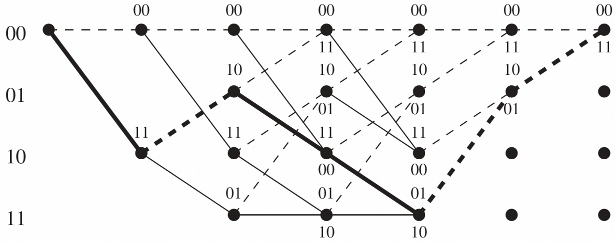

Abbildung 4: Codeworte der Länge 12 des Faltungscodierers.

Faltungscodes VII

- In GSM wird ein Faltungscode der Rate $1/2$ verwendet.
- Bei $k = 185$ Informationsbits existieren $2^{185} = 4.9 \cdot 10^{55}$ Codewörter.
- Der Codierer hat vier Schieberegister und der Trellis damit 16 Zustände.
- Das Trellis besitzt eine Länge von 185, also müssen $16 \cdot 185 = 2960$ Zustände gespeichert werden.
- Dazu müssen noch doppelt so viele Zweige gespeichert werden.
- In diesem aus ca. 3000 Zuständen und 6000 Zweigen bestehenden Trellis sind dann alle $4.9 \cdot 10^{55}$ Codeworte enthalten.

Faltungscodes VIII

- Wir wollen nun den Viterbi-Algorithmus zur Fehlerkorrektur an dem Beispiel beschreiben:

$$\text{gesendet } 111000010111, \rightarrow \text{ empfangen } 1\mathbf{0}10000\mathbf{0}0111.$$

- Ziel der Decodierung ist es, aus der empfangenen Folge ein gültiges Codewort zu berechnen.
- Für die Erklärung des Viterbi-Decodierers benötigen wir folgende Notation:
- Teile die empfangenen Bits in Symbole aus zwei Bits auf:

$$y_1 = 10, y_2 = 10, y_3 = 00, y_4 = 00, y_5 = 01, y_6 = 11.$$

- Wir benötigen ein Maß, mit dem wir die Abweichung der empfangenen Folge von einer gültige Codefolge messen.

Faltungscodes IX

- Wir verwenden die Zahl der Übereinstimmungen einer gültigen Codefolge c mit der empfangenen Folge y.
- Immer Teilfolgen mit 2 Bits: $\lambda_i = 2 - \mathrm{dist}(c_i, y_i)$.
- Das Maß für einen Pfad aus m Teilfolgen ist

$$\Lambda_m = \sum_{i=1}^{m} \lambda_i.$$

- Der Codepfad startet im Zustand 00.

Faltungscodes X

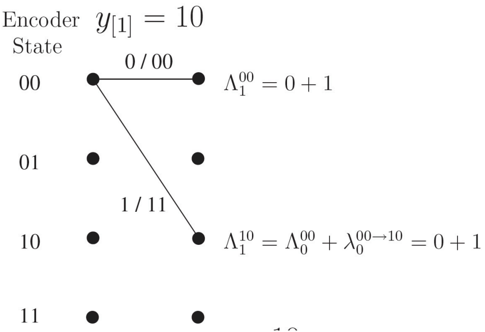

Abbildung 5: Viterbi-Decodierung erster Schritt.

Faltungscodes XI

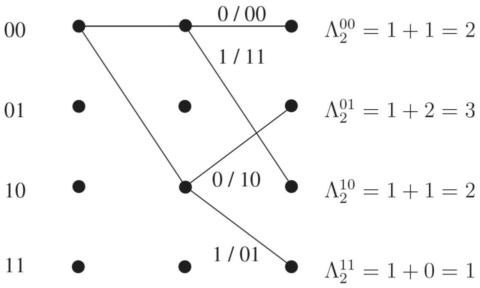

Abbildung 6: Viterbi-Decodierung zweiter Schritt.

Faltungscodes XII

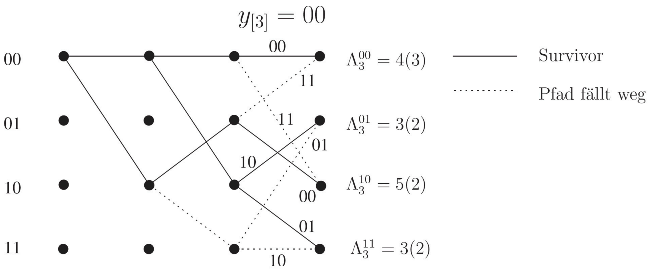

Abbildung 7: Viterbi-Decodierung dritter Schritt.

- Bei der dritten Teilfolge entsteht zum ersten Mal das Problem, dass in jedem Zustand zwei Pfade enden.

Institut für Nachrichtentechnik

Faltungscodes XIII

- Die beiden Pfadmaße sind als Zahl und Zahl in Klammern angegeben.
- Wir wollen den besten Pfad finden, d.h., wir entscheiden uns in jedem Zustand nur für einen, den wahrscheinlicheren Pfad, den *Survivor*.

Faltungscodes XIV

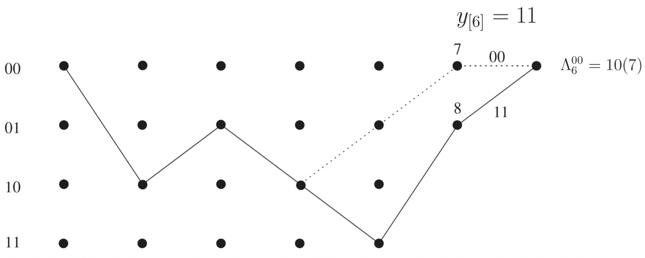

Abbildung 8: Viterbi-Decodierung letzter Schritt.

- Die letzte Teilfolge $y_6 = 11$ muss wegen der zwei angehängten Nullen im Zustand 00 enden.

Faltungscodes XV

- Es konnten beide Fehler decodiert werden und die Informationsfolge wird korrekt abgelesen: 111000010111 $\rightarrow$ 1011.
- Der Algorithmus wird auch in Ihrem Handy verwendet (allerdings mit Soft-Informationen).