

Szenario für fehlerkorrigierende Codes

Definition (n, M) -Code

Sei $C \subseteq \{0, 1\}^n$ ein binärer Blockcode der Länge n mit $|C| = M$ Codeworten. Dann bezeichnen wir C als (n, M) -Code.

Erinnerung: Binärer symmetrischer Kanal

- Bits 0,1 kippen mit Ws $p, p < \frac{1}{2}$ zu 1,0.
- Korrekte Übertragung $0 \mapsto 0, 1 \mapsto 1$ mit Ws $1 - p$.
- Kanal ist erinnerungslos, d.h. die Ws sind unabhängig von vorigen Ereignissen.
- Vorwärts-Kanalws: $W_s(\mathbf{x} \text{ empfangen} \mid \mathbf{c} \text{ gesendet})$.
- Rückwärts-Kanalws: $W_s(\mathbf{c} \text{ gesendet} \mid \mathbf{x} \text{ empfangen})$.

Dekodieren

Definition Dekodier-Kriterium

Sei $C \subseteq \{0, 1\}^n$ ein (n, M) -Code. Ein Dekodier-Kriterium f ist eine Funktion $f : \{0, 1\}^n \rightarrow C \cup \{\perp\}$. Sei $\mathbf{x} \in \{0, 1\}^n$. Ein Dekodier-Kriterium dekodiert $\mathbf{x}$ zu $f(\mathbf{x}) \in C$ oder gibt Dekodierfehler $f(\mathbf{x}) = \perp$ aus.

- **Ziel:** Konstruktion eines Dekodier-Kriteriums f , dass die Ws des korrekten Dekodierens maximiert.

$Ws(\text{korr. Dekodierung} \mid \mathbf{x} \text{ empfangen}) = Ws(f(\mathbf{x}) \text{ gesendet} \mid \mathbf{x} \text{ empfangen})$

- Summieren über alle möglichen empfangenen $\mathbf{x}$ liefert

$$\begin{aligned} & Ws(\text{korrekte Dekodierung}) \\ &= \sum_{\mathbf{x} \in \{0,1\}^n} Ws(f(\mathbf{x}) \text{ gesendet} \mid \mathbf{x} \text{ empfangen}) \cdot Ws(\mathbf{x} \text{ empfangen}) \end{aligned}$$

- Benötigen Maximierung der Rückwärts-Kanalws

$Ws(f(\mathbf{x}) \text{ gesendet} \mid \mathbf{x} \text{ empfangen})$, d.h. dekodieren zu demjenigen Codewort $\mathbf{c} = f(\mathbf{x})$, das mit höchster Ws gesendet wurde.

Maximum Likelihood Dekodierung

Definition Maximum Likelihood Dekodierung

Ein Dekodierkriterium $f(\mathbf{x})$, dass die Vorwärts- W_s für alle Codeworte maximiert, d.h.

$$W_s(\mathbf{x} \text{ empfangen} | f(\mathbf{x}) \text{ gesendet}) = \max_{c \in C} W_s(\mathbf{x} \text{ empfangen} | c \text{ gesendet}),$$

heißt Maximum-Likelihood Kriterium. Eine Anwendung des Kriteriums bezeichnet man als Maximum-Likelihood Dekodierung.

Warum Maximum Likelihood?

Satz Maximum Likelihood optimal für gleichverteilte Codeworte

Sei C ein (n, M) -Code und $W_s(\mathbf{c} \text{ gesendet}) = \frac{1}{M}$ für alle $\mathbf{c} \in C$. Dann minimiert die Maximum-Likelihood Dekodierung die W_s von Dekodierfehlern.

$W_s(\mathbf{c} \text{ gesendet} | \mathbf{x} \text{ empfangen})$

$$\begin{aligned} &= \frac{W_s(\mathbf{x} \text{ empfangen} | \mathbf{c} \text{ gesendet}) W_s(\mathbf{c} \text{ gesendet})}{\sum_{i=1}^M W_s(\mathbf{x} \text{ empfangen} | \mathbf{c}_i \text{ gesendet}) W_s(\mathbf{c}_i \text{ gesendet})} \\ &= \frac{W_s(\mathbf{x} \text{ empfangen} | \mathbf{c} \text{ gesendet})}{\sum_{i=1}^M W_s(\mathbf{x} \text{ empfangen} | \mathbf{c}_i \text{ gesendet})} \end{aligned}$$

- Nenner ist konstant für jeden Kanal.
- Maximierung des Zählers maximiert den Term.

Dekodieren zum Nachbarn minimaler Distanz

Definition Hamming-Distanz

Seien $\mathbf{x}, \mathbf{y} \in \{0, 1\}^n$. Die Hamming-Distanz $d(\mathbf{x}, \mathbf{y})$ ist die Anzahl der Stellen, an denen sich $\mathbf{x}$ und $\mathbf{y}$ unterscheiden.

Satz

In jedem binären symmetrischen Kanal ist das Dekodier-Kriterium, das ein $\mathbf{x}$ zum Codewort minimaler Hamming-Distanz dekodiert ein Maximum-Likelihood Kriterium.

Beweis:

- Ws von genau k Fehlern an festen Stellen beim Senden von $\mathbf{c}$

$$\text{Ws}(\mathbf{x} \text{ empfangen} | \mathbf{c} \text{ gesendet}) = p^k (1 - p)^{n-k}.$$

- Wegen $p < \frac{1}{2}$ gilt $p < 1 - p$. Müssen Term maximieren.
- Wählen k minimal, d.h. Codewort $\mathbf{c}$ mit minimalem $d(\mathbf{x}, \mathbf{c})$.

Die Hamming-Distanz definiert eine Metrik.

Satz Metrik Hamming-Distanz

Die Hamming-Distanz ist eine Metrik auf $\{0, 1\}^n$, d.h. für alle $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \{0, 1\}^n$ gilt:

- 1 Positivität: $d(\mathbf{x}, \mathbf{y}) \geq 0$, Gleichheit gdw $\mathbf{x} = \mathbf{y}$.
- 2 Symmetrie: $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$.
- 3 Dreiecksungleichung: $d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

Beweis für 3:

Ann.: $d(\mathbf{x}, \mathbf{z}) > d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$

- Verändern erst $\mathbf{x}$ zu $\mathbf{y}$, dann $\mathbf{y}$ zu $\mathbf{z}$.
- Müssen dazu $d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) < d(\mathbf{x}, \mathbf{z})$ stellen ändern.
Widerspruch: $\mathbf{x}$ und $\mathbf{z}$ unterscheiden sich an $d(\mathbf{x}, \mathbf{z})$ Stellen.

Definition u -fehlererkennend

Sei C ein Code und $u \in \mathbb{N}$. C ist u -fehlererkennend, falls für alle Codeworte $\mathbf{c}, \mathbf{c}' \in C$ gilt: $d(\mathbf{c}, \mathbf{c}') \geq u + 1$. Ein Code ist *genau* u -fehlererkennend, falls er u -fehlererkennend ist, aber nicht $(u + 1)$ -fehlererkennend.

- Repetitionscode $R(3) = \{000, 111\}$ ist genau 2-fehlererkennend.
- $R(n) = \{0^n, 1^n\}$ ist genau $(n - 1)$ -fehlererkennend.
- $C = \{000000, 000111, 111111\}$ ist genau 2-fehlererkennend.

Definition v -fehlerkorrigierend

Sei C ein Code und $v \in \mathbb{N}$. C ist v -fehlerkorrigierend, falls für alle $\mathbf{c} \in C$ gilt:

- Treten bis zu v bei der Übertragung von $\mathbf{c}$ auf, so können diese mittels Dekodierung zum Codewort minimaler Hammingdistanz korrigiert werden.
- Existieren zwei verschiedene Codeworte mit minimaler Hammingdistanz, so wird eine Dekodierfehlermeldung $\perp$ ausgegeben.

Ein Code ist *genau* v -fehlerkorrigierend, falls er v -fehlerkorrigierend aber nicht $(v + 1)$ -fehlerkorrigierend ist.

- $R(3) = \{000, 111\}$ ist genau 1-fehlerkorrigierend.
- $R(4)$ ist genau 1-fehlerkorrigierend.
- $R(n)$ ist genau $\lfloor \frac{n-1}{2} \rfloor$ -fehlerkorrigierend.
- $C = \{0^9, 0^4 1^5, 1^9\}$ ist genau 1-fehlerkorrigierend.

Minimaldistanz eines Codes

Definition Minimaldistanz

Sei C ein Code mit $|C| \geq 2$. Die *Minimaldistanz* $d(C)$ eines Codes ist definiert als

$$d(C) = \min_{\mathbf{c} \neq \mathbf{c}' \in C} \{d(\mathbf{c}, \mathbf{c}')\}$$

D.h. $d(C)$ ist die minimale Distanz zweier verschiedener Codeworte.

- $R(n)$ besitzt Minimaldistanz $d(R(n)) = n$.
- $C = \{0001, 0010, 0101\}$ besitzt $d(C) = 1$.
- $C = \{0^9, 0^4 1^5, 1^9\}$ besitzt $d(C) = 4$.

Korollar Fehlererkennung

Ein Code C ist u -fehlererkennend gdw $d(C) \geq u + 1$.

Fehlerkorrektur vs Minimaldistanz

Satz Fehlerkorrektur vs Minimaldistanz

Ein Code C ist ν -fehlerkorrigierend gdw $d(C) \geq 2\nu + 1$.

$\Leftarrow$:

- **Ann.:** C ist nicht ν -fehlerkorrigierend.
- D.h. bei Übertragung von $\mathbf{c}$ entsteht $\mathbf{x}$ mit $d(\mathbf{x}, \mathbf{c}) \leq \nu$ und $\exists \mathbf{c}' \neq \mathbf{c} : d(\mathbf{c}', \mathbf{x}) \leq \nu$
- Dreiecksungleichung: $d(\mathbf{c}, \mathbf{c}') \leq d(\mathbf{c}, \mathbf{x}) + d(\mathbf{x}, \mathbf{c}') \leq 2\nu$
(Widerspruch: $d(C) \geq 2\nu + 1$)

Beweis der Hinrichtung “ $\Rightarrow$ ”

Ann.: Es gibt $\mathbf{c} \neq \mathbf{c}' \in C$ mit $d(\mathbf{c}, \mathbf{c}') = d(C) \leq 2v$.

- 1. Fall: $d(\mathbf{c}, \mathbf{c}') \leq v$. $\mathbf{c}$ kann durch Ändern von höchstens v Stellen in $\mathbf{x} = \mathbf{c}'$ überführt werden. $\mathbf{x}$ wird fälschlich zu $\mathbf{c}'$ dekodiert (Widerspruch: C ist v -fehlerkorrigierend)
- 2. Fall: $v + 1 \leq d(\mathbf{c}, \mathbf{c}') \leq 2v$.
- OBdA unterscheiden sich in $\mathbf{c}, \mathbf{c}'$ in den ersten $d(C)$ Positionen. (Anderfalls sortiere die Koordinaten um.)
- Betrachten $\mathbf{x}$, das durch v Fehler in den ersten Koordinaten von $\mathbf{c}$ entsteht, so dass
 - ▶ $\mathbf{x}$ stimmt mit $\mathbf{c}'$ auf den ersten v Koordinaten überein.
 - ▶ $\mathbf{x}$ stimmt mit $\mathbf{c}$ auf den folgenden $d(C)$ Koordinaten überein.
 - ▶ $\mathbf{x}$ stimmt mit $\mathbf{c}, \mathbf{c}'$ auf den restlichen Koordinaten überein.
- Es gilt $d(\mathbf{c}, \mathbf{x}) = v \geq d(C) - v = d(\mathbf{c}', \mathbf{x})$.
- D.h. entweder wird $\mathbf{x}$ fälschlich zu $\mathbf{c}'$ dekodiert, oder es entsteht ein Dekodierfehler. (Widerspruch: C ist v -fehlerkorrigierend)

(n, M, d) -Code

Definition (n, M, d) -Code

Sei $C \subseteq \{0, 1\}^n$ mit $|C| = M$ und Distanz $d(C) = d$. Dann bezeichnet man C als (n, M, d) -Code, wobei man (n, M, d) die *Parameter des Codes* nennt.

- $R(n)$ ist ein $(n, 2, n)$ -Code.
- $C = \{000, 0011\}$ ist ein $(4, 2, 2)$ -Code.
- $C = \{00, 01, 10, 11\}$ ist ein $(2, 4, 1)$ -Code.

Korollar

Sei C ein (n, M, d) -Code.

- 1 C ist genau v -fehlerkorrigierend gdw $d = 2v + 1$ oder $d = 2v + 2$.
- 2 C ist genau $\lfloor \frac{d-1}{2} \rfloor$ -fehlerkorrigierend.

Definition Maximale Code

Ein (n, M, d) -Code ist maximal, falls er nicht in einem $(n, M + 1, d)$ -Code enthalten ist.

- $C_1 = \{0000, 0011, 1111\}$ ist nicht maximal.
- $C_2 = \{0000, 0011, 1111, 1100\}$ ist nicht maximal.
- $C_3 = \{0000, 0011, 1111, 1100, 1001, 0110, 1010, 0101\}$ ist maximal.

Erweiterung nicht-maximaler Codes

Satz Erweiterung von Codes

Sei $C \subseteq \{0, 1\}^n$ ein (n, M, d) -Code. C ist maximal gdw für alle $\mathbf{x} \in \{0, 1\}^n$ gilt: Es gibt ein $\mathbf{c} \in C$ mit $d(\mathbf{x}, \mathbf{c}) < d$.

“ $\Rightarrow$ ”

- **Ann.:** Sei $\mathbf{x} \in \{0, 1\}^n$, so dass für alle $\mathbf{c} \in C : d(\mathbf{x}, \mathbf{c}) \geq d$
- Dann ist $C \cup \{\mathbf{x}\}$ ein $(n, M + 1, d)$ -Code. (Widerspruch: C ist maximal.)

“ $\Leftarrow$ ”

- **Ann.:** Sei C nicht maximal.
- D.h. $\exists \mathbf{x} \in \{0, 1\}^n : C \cup \{\mathbf{x}\}$ ist ein $(n, M + 1, d)$ -Code
- Dann gilt $d(\mathbf{x}, \mathbf{c}) \geq d$ für alle $\mathbf{c} \in C$.

Ws für Dekodierfehler bei maximalen Codes

Satz Dekodierfehler bei maximalen Codes

Sei C ein maximaler (n, M, d) -Code für einen binären symmetrischen Kanal. Für die Fehlerws beim Dekodieren zum Codewort mit minimalem Hammingabstand gilt

$$\sum_{k=d}^n \binom{n}{k} p^k (1-p)^{n-k} \leq \text{Ws}(\text{Dekodierfehler}) \leq 1 - \sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k} p^k (1-p)^{n-k}$$

- Korrekte Dekodierung bei $\leq \lfloor \frac{d-1}{2} \rfloor$ Fehlern, d.h. mit Ws mind.

$$\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k} p^k (1-p)^{n-k}.$$

- Inkorrekte Dekodierung bei $\geq d$ Fehlern, d.h. mit Ws mindestens

$$\sum_{k=d}^n \binom{n}{k} p^k (1-p)^{n-k}.$$

Beispiele für Codes

Repetitionscode: $R(n)$ ist $(n, 2, n)$ -Code.

Hamming Code: $\mathcal{H}(h)$ ist ein $(2^h - 1, 2^{n-h}, 3)$ -Code.

Golay Codes: $\mathcal{G}_{23}$ ist ein $(23, 2^{12}, 7)$ -Code.

$\mathcal{G}_{24}$ ist ein $(24, 2^{12}, 8)$ -Code.

Einsatz: Voyager für Bilder von Jupiter und Saturn.

Reed-Muller Code: $RM(r, m)$ ist ein $(2^m, 2^{1+\binom{m}{1}+\dots+\binom{m}{r}}, 2^{m-r})$ -Code.

$RM(1, m) = (2^m, 2^{m+1}, 2^{m-1})$.

Einsatz: Mariner 9 für Bilder vom Mars.

Hammingkugel

Definition Hammingkugel

Sei $\mathbf{x} \in \{0, 1\}^n$ und $r \geq 0$. Wir definieren die n -dimensionale Hammingkugel mit Mittelpunkt $\mathbf{x}$ und Radius r als

$$B^n(\mathbf{x}, r) = \{\mathbf{y} \in \{0, 1\}^n \mid d(\mathbf{x}, \mathbf{y}) \leq r\}.$$

Beispiel: $B^3(001, 1) = \{001, 101, 011, 000\}$.

Satz Volumen von $B^n(\mathbf{x}, r)$

Das Volumen der Hammingkugel $B^n(\mathbf{x}, r)$ ist $V^n(r) = \sum_{i=0}^r \binom{n}{i}$.

- Es gibt $\binom{n}{i}$ String mit Distanz i von x .

Packradius eines Codes

Definition Packradius eines Codes

Sei C ein (n, M, d) -Code. Der Packradius $pr(C) \in \mathbb{N}$ von C ist die größte Zahl, so dass die Hammingkugeln $B^n(\mathbf{c}, pr(C))$ für alle $\mathbf{c} \in C$ disjunkt sind.

Korollar

Sei C ein (n, M, d) -Code.

- 1 Der Packradius von C ist $pr(C) = \lfloor \frac{d-1}{2} \rfloor$.
- 2 C ist genau v -fehlerkorrigierend gdw $pr(C) = v$.