4. Woche
Decodierung; Maximale, Perfekte und Optimale Codes

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 gedächtnislos: Ws unabhängig von vorigen Ereignissen. Insbesondere: für je zwei Wörter $\mathbf{c} = c_1 c_2 \cdots c_n$ und $\mathbf{x} = x_1 x_2 \cdots x_n$ der Länge n gilt
  - für die Vorwärts-Kanalws:

$$\mathcal{W}s(\mathbf{x} \text{ empfangen} \mid \mathbf{c} \text{ gesendet}) = \prod_{i=1}^{n} \mathcal{W}s(x_i \text{ empfangen} \mid c_i \text{ gesendet})$$

  - für die Rückwärts-Kanalws:

$$\mathcal{W}s(\mathbf{x} \text{ gesendet} \mid \mathbf{c} \text{ empfangen}) = \prod_{i=1}^{n} \mathcal{W}s(x_i \text{ gesendet} \mid c_i \text{ empfangen})$$

Idealer Beobachter

Definition

Für eine empfangene Nachricht x, ein *Idealer Beobachter* wählt ein Codewort $c \in C$, derart dass

$$\mathcal{W}s(\mathbf{c} \text{ gesendet } | \mathbf{x} \text{ empfangen})$$

maximal ist. Mit anderen Worten, c ist das Codewort, das *am wahrscheinlichsten* die gesendete Nachricht war, in dem Fall, dass x empfangen wird.

- Am wahrscheinlichsten gesendetes Codewort nicht unbedingt eindeutig.

  Allgemeiner: Mehrere Codeworte können die selbe Wahrscheinchkeit haben, durch Fehler in das selbe empfangene Codewort umgewandelt zu werden.

- Man braucht dann ein Kriterium, um in diesem Fall ein Wort zu wählen z.B.
  - erneut senden
  - zufällig wählen
  - das „minimale” Wort (interpretiert als n-Bit Zahl) wählen
  - usw

Decodieren

Definition Decodier-Kriterium

Sei $C \subseteq \{0,1\}^n$ ein (n, M)-Code. Ein Decodier-Kriterium f ist eine Funktion $f : \{0,1\}^n \to C \cup \{\perp\}$. Sei $\mathbf{x} \in \{0,1\}^n$. Ein Decodier-Kriterium liefert $f(\mathbf{x}) \in C$ oder gibt Decodierfehler $f(\mathbf{x}) = \perp$ aus.

Gesucht: Bestimme f, dass Ws des *korrekten* Decodierens maximiert.

Definition Maximum Likelihood Decodierung

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

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

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

Ist f ein idealer Beobachter? In welchen Fällen?

Warum Maximum Likelihood?

Satz Maximum Likelihood optimal für gleichverteilte Codeworte

Sei C ein (n, M)-Code und $\mathcal{W}s(\mathbf{c} \text{ gesendet}) = \frac{1}{M}$ für alle $\mathbf{c} \in C$.
Dann minimiert die Maximum-Likelihood Decodierung die Ws von Decodierfehlern, i.e. Maximum Likelihood Decoding $=$ Decodierung eines idealen Beobachters.

Beweis. Nach dem Satz von Bayes:

$$\begin{aligned}\mathcal{W}s(\mathbf{x} \text{ empfangen} \mid \mathbf{c} \text{ gesendet}) &= \frac{\mathcal{W}s(\mathbf{x} \text{ empfangen} \cap \mathbf{c} \text{ gesendet})}{\mathcal{W}s(\mathbf{c} \text{ gesendet})} \\ &= \mathcal{W}s(\mathbf{c} \text{ gesendet} \mid \mathbf{x} \text{ empfangen}) \cdot \frac{\mathcal{W}s(\mathbf{x} \text{ empfangen})}{\mathcal{W}s(\mathbf{c} \text{ gesendet})} \\ &= \mathcal{W}s(\mathbf{c} \text{ gesendet} \mid \mathbf{x} \text{ empfangen}) \ .\end{aligned}$$

Also: Maximum Likelihood $\Leftrightarrow$ Idealer Beobachter. □

Decodieren zum Nachbarn minimalen Abstands

Definition Hamming-Abstand

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

Satz

In jedem binären symmetrischen Kanal ist das Decodier-Kriterium, das ein $\mathbf{x}$ zum Codewort minimalen Hamming-Abstands decodiert ein Maximum-Likelihood Kriterium.

Beweis: *Übung. (Prüfungsrelevant.)*

Der Hamming-Abstand definiert eine Metrik.

Satz Metrik Hamming-Abstand

Der Hamming-Abstand 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: $d(\mathbf{x}, \mathbf{z}) \leqslant d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z})$.

Beweis: *Übung. (Prüfungsrelevant.)*

Fehlererkennung

Definition *u*-fehlererkennend

Sei C ein Code und $u \in \mathbb{N}$. C ist *u-fehlerkennend*, falls für alle Codeworte $\mathbf{c}, \mathbf{c}' \in C$ gilt: $d(\mathbf{c}, \mathbf{c}') \geqslant u + 1$. 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.

Fehlerkorrektur

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 Decodierung zum Codewort minimalen Hamming-Abstands korrigiert werden.
- Existieren zwei verschiedene Codeworte mit minimalem Hamming-Abstand, so wird eine Decodierfehlermeldung $\perp$ 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 $\left\lfloor \frac{n-1}{2} \right\rfloor$-fehlerkorrigierend.
- $C = \{0^9, 0^4 1^5, 1^9\}$ ist genau 1-fehlerkorrigierend.

Minimal-Abstand eines Codes

Definition Minimal-Abstand

Sei C ein Code mit $|C| \geqslant 2$. Der *MinimalAbstand* $d(C)$ 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 der minimaler Abstand zweier verschiedener Codeworte.

- $R(n)$ besitzt Minimal- $d(R(n)) = n$.
- $C = \{0001, 0010, 0101\}$ 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 $d(C) \geqslant u + 1$.

Fehlerkorrektur vs Minimal-Abstand

Satz Fehlerkorrektur vs MinimalAbstand

Ein Code C ist v-fehlerkorrigierend gdw $d(C) \geqslant 2v + 1$.

$\Leftarrow$:

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

Beweis der Hinrichtung "$\Rightarrow$"

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

- 1.Fall: $d(\mathbf{c}, \mathbf{c}') \leqslant v$. $\mathbf{c}$ kann durch Ändern von höchstens v Stellen in $\mathbf{x} = \mathbf{c}'$ überführt werden. $\mathbf{x}$ wird fälschlich zu $\mathbf{c}'$ decodiert (Widerspruch: C ist v-fehlerkorrigierend)
- 2. Fall: $v + 1 \leqslant d(\mathbf{c}, \mathbf{c}') \leqslant 2v$.
- 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 $d(\mathbf{c}, \mathbf{x}) = v \geqslant d(C) - v = d(\mathbf{c}', \mathbf{x})$.
- D.h. entweder wird $\mathbf{x}$ fälschlich zu $\mathbf{c}'$ decodiert, oder es entsteht ein Decodierfehler. (Widerspruch: C ist v-fehlerkorrigierend)

(n, M, d)-Code

Definition (n, M, d)-Code

Sei $C \subseteq \{0,1\}^n$ mit $|C| = M$ und Abstand $d(C) = d$. 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 $\left\lfloor \frac{d-1}{2} \right\rfloor$-fehlerkorrigierend.

Maximale Codes

Definition Maximale Code

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

Beispiele von $(4, M, 2)$-Codes:

- $C_1 = \{0000, 0011, 1111\}$ 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 $d(\mathbf{x}, \mathbf{c}) < d$.

"$\Rightarrow$"

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

"$\Leftarrow$"

- Sei $C' \supset C$ ein (n, M', d)-Code mit $M' > M$.
- Wähle $x \in C' \setminus C$, dann gilt $d(\mathbf{x}, \mathbf{c}) \geqslant d$ für alle $\mathbf{c} \in C$.

Ws für Decodierfehler bei maximalen Codes

Satz Decodierfehler bei maximalen Codes

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

$$\sum_{k=d}^{n} \binom{n}{k} p^k (1-p)^{n-k} \leqslant \mathcal{W}s(\text{Decodierfehler}) \leqslant 1 - \sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{k} p^k (1-p)^{n-k}$$

- Korrekte Decodierung bei $\leqslant \lfloor \frac{d-1}{2} \rfloor$ Fehlern, d.h. mit Ws mindestens

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

- Inkorrekte Decodierung 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 $(2^m, 2^{1+\binom{m}{1}+\ldots+\binom{m}{r}}, 2^{m-r})$-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

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

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 Abstand 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 $pr(C) = v$.

Perfekte Codes

Definition Perfekter Code

Sei $C \subseteq \{0,1\}^n$ ein (n, M, d)-Code. C heißt *perfekt*, falls

$$M \cdot V^n\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right) = 2^n.$$

D.h. die maximalen disjunkten Hammingkugeln um die Codeworte partitionieren $\{0,1\}^n$.

- Nicht für alle (n, M, d), die obige Bedingung erfüllen, gibt es auch einen Code.

Perfekte Codes

- $\{0,1\}^n$ ist ein $(n, 2^n, 1)$-Code
  - Packradius ist 0, Hammingkugeln bestehen nur aus Codewort selbst.
  - Perfekter Code, aber nutzlos für Fehlerkorrektur.
- $R(n)$ ist für ungerade n ein perfekter $(n, 2, n)$-Code.
  - $2 \cdot \sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i} = 2 \cdot \frac{2^n}{2} = 2^n$
  - Code ist nutzlos, da er nur zwei Codeworte enthält.
- Der Golay Code $(23, 2^{12}, 7)$ ist perfekt.
  - $2^{12} \cdot \sum_{i=0}^{3} \binom{23}{i} = 2^{11} \cdot 2^{12} = 2^{23}$
- Der Hamming Code $\mathcal{H}(h) = (n, M, d) = (2^h - 1, 2^{n-h}, 3)$ ist perfekt.
  - $2^{n-h}\left(1 + 2^h - 1\right) = 2^n$
- Die einzigen perfekten, binären v-fehlerkorrigierenden Codes mit $v \geq 2$ sind Repetitionscodes und der obige Golay Code.

Die Rate eines Codes

Definition Rate eines Codes

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

1. Die *Übertragungsrate* ist definiert als $\mathcal{R}(C) = \frac{\log_2(M)}{n}$.
2. Die *Fehlerrate* ist definiert als $\delta(C) = \frac{\lfloor \frac{d-1}{2} \rfloor}{n}$.

Beispiele:

- $C = \{0^n\}$ hat Übertragungrate 0, aber perfekte Fehlerkorrektur.
- $C = \{0, 1\}^n$ hat Übertragungrate 1, aber keine Fehlerkorrektur.
- $\mathcal{R}(R(n)) = \frac{1}{n}$ und $\delta(R(n)) = \frac{\lfloor \frac{n-1}{2} \rfloor}{n}$.
  - Übertragungsrate konvergiert gegen 0, Fehlerrate gegen $\frac{1}{2}$.
- $\mathcal{R}(\mathcal{H}(h)) = \frac{n-h}{n} = 1 - \frac{h}{n}$ und $\delta(\mathcal{H}(h)) = \frac{1}{n}$.
  - Übertragungsrate konvergiert gegen 1, Fehlerrate gegen 0.

Die Größe $A(n, d)$ und optimale Codes

Definition Optimaler Code

Wir definieren

$$A(n, d) = \max\{M \mid \exists \text{ binärer } (n, M, d) - \text{Code}\}$$

Ein (n, M, d)-Code heißt optimal, falls $M = A(n, d)$.

- Bestimmung von $A(n, d)$ ist offenes Problem.
- Zeigen hier obere und untere Schranken für $A(n, d)$.
- Für kleine Werte von n, d bestimmen wir $A(n, d)$ wie folgt:
  - Zeigen $A(n, d) \leqslant M$.
  - Konstruieren (n, M, d)-Code.

- $A(n, d) \leqslant 2^n$ für $d \in [n]$: höchstens 2^n Codeworte der Länge n.
- $A(n, 1) = 2^n$: $C = \{0, 1\}^n$.
- $A(n, n) = 2$: $R(n)$.
- $A(n, d) \leqslant A(n, d')$ für $d, d' \in [n]$ mit $d' \leqslant d$ (Übung)