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.

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: $d(\mathbf{c}, \mathbf{c}') \geq u + 1$. Ein Code ist *genau u-fehlererkennend*, falls er u-fehlererkennend ist, aber nicht $(u+1)$-fehlererkennend.

Bsp:

- 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: Bis zu v können mittels Dekodierung zum eindeutigen Codewort minimaler Hammingdistanz korrigiert werden.
Ein Code ist *genau v-fehlerkorrigierend*, falls er v-fehlerkorrigierend aber nicht $(v+1)$-fehlerkorrigierend ist.

Anmerkung: Existieren zwei verschiedene Codeworte mit minimaler Hammingdistanz, so wird eine Dekodierfehlermeldung $\perp$ ausgegeben.

Bsp:

- $R(3) = \{000, 111\}$ 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.

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.

Bsp:

- $R(n)$ 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 v-fehlerkorrigierend gdw $d(C) \geq 2v + 1$.

Beweis:

$\Leftarrow$:

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

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. Man nennt (n, M, d) die *Parameter des Codes*.

Bsp:

- $R(n)$ ist ein $(n, 2, n)$-Code.
- $C = \{0000, 0011\}$ 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.
   (**Fehlerkorrektur-Schranke)**

Maximale Codes

Definition Maximale Code

Ein (n, M, d)-Code C ist maximal, falls kein $(n, M+1, d)$-Code C' existiert mit $C \subset C'$.

Bsp:

- $C_0 = \{0000, 1111\}$ ist maximal.
- $C_1 = \{0000, 0011, 1111\}$ 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. $\exists \mathbf{x} \cup \{0,1\}^n : C \cup \{\mathbf{x}\}$ 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

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

Beweis:

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

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

Ws für Dekodierfehler bei maximalen Codes

Beweis: Fortsetzung

- Sei $\mathbf{x}$ das bei Übertragung von $\mathbf{c} \in C$ empfangene Wort mit
$$d(\mathbf{x}, \mathbf{c}) \geq d.$$
- Da C maximal ist, existiert ein $\mathbf{c}' \in C$ mit $d(\mathbf{x}, \mathbf{c}') < d \leq d(\mathbf{x}, \mathbf{c})$.
- D.h. $\mathbf{x}$ wird zu $\mathbf{c}'$ dekodiert anstatt zu $\mathbf{c}$.
- Damit erhalten wir bei $\geq d$ Fehlern stets inkorrekte Dekodierung.
- Dies geschieht mit Ws
$$\sum_{k=d}^{n} \binom{n}{k} p^k (1-p)^{n-k}.$$

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

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

Bsp:

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

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

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

Beweis:

- 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 $pr(C) = v$.

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.
- $\{0,1\}^n$ ist ein perfekter $(n, 2^n, 1)$-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.

Beispiele für Codes

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

$$2^{n-h}\left(1 + 2^h - 1\right) = 2^n.$$

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.
Der Golay Code $(23, 2^{12}, 7)$ ist perfekt, denn

$$2^{12} \cdot \sum_{i=0}^{3} \binom{23}{i} = 2^{12} \cdot 2^{11} = 2^{23}.$$

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.

Die einzigen perfekten, binären v-fehlerkorrigierenden Codes mit $v \geq 2$ sind Repetitionscodes und der obige Golay Code $\mathcal{G}_{23}$.

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 $\delta(C) = \frac{\lfloor \frac{d-1}{2} \rfloor}{n}$.

Bsp:

- $C = \{0^n\}$ 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 $A(n,d) \leq M$.
  - Konstruieren (n,M,d)-Code.

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

Singleton-Schranke

Satz Singleton-Schranke

$$A(n,d) \leq 2^{n-d+1}$$

Beweis:

- Sei C ein optimaler (n,M,d)-Code, d.h. $M = A(n,d)$.
- Wir entfernen die letzten $d-1$ Stellen aller M Codeworte.
- Die resultierenden M Worte sind alle verschieden, da sich alle Codeworte in mindestens d Stellen unterscheiden.
- Es gibt M viele unterschiedliche Worte der Länge $n-(d-1)$, d.h.

$$M \leq 2^{n-d+1}.$$

Vereinfachte Plotkin-Schranke

Satz Vereinfachte Plotkin-Schranke

Sei $n < 2d$, dann gilt

$$A(n,d) \leq \frac{2d}{2d-n}.$$

- Sei C ein optimaler $(n,M,d) - Code$ und $S = \sum_{i<j} d(\mathbf{c_i}, \mathbf{c_j})$.
- Je zwei Codeworte besitzen Distanz mindestens d, d.h. $S \geq d\binom{M}{2}$.
- Betrachten erste Stelle in allen Codeworten:
  - Sei k die Anzahl der Nullen und $(M-k)$ die Anzahl der Einsen.
  - Erste Stelle liefert Beitrag von $k(M-k)$ zu S.
  - $k(M-k)$ ist maximal für $k = \frac{M}{2}$, d.h. $k(M-k) \leq \frac{M^2}{4}$.
  - Analog für jede der n Stellen, d.h. $S \leq \frac{nM^2}{4}$.
- Kombination beider Schranken und Auflösen nach M liefert

$$M \leq \frac{2d}{2d-n}.$$

Vergleich der oberen Schranken

n	7	8	9	10	11	12	13
$A(n,7)$	2	2	2	2	4	4	8
Singleton	2	4	8	16	32	64	128
Plotkin	2	2	2	3	4	7	14

Kodierungstheorem von Shannon für fehlerbehaftete Kanäle

Gegeben sei ein binärer symmetrischer Kanal Q mit Fehlerws p. Für alle $R < 1 + p\log_2 p + (1-p)\log_2(1-p) = 1 - H(Q)$ und alle $\epsilon > 0$ gibt es für hinreichend große n einen (n, M)-Code C mit Übertragungsrate $\mathcal{R}(C) \geq R$ und $\mathrm{Ws}(\text{Dekodierfehler}) \leq \epsilon$.

- Beweis komplex, nicht-konstruktiv.
- Resultat gilt nur asymptotisch für genügend große Blocklänge.