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)

0^n ist ein Codewort

Lemma Äquivalenter Code mit 0^n

Sei C ein (n, M, d)-Code. Dann gibt es einen (n, M, d)-Code C' mit $0^n \in C'$.

- Sei $c \in C$ mit k Nullen und $n - k$ Einsen.
- Permutiere Positionen in c so, dass c mit den k Nullen beginnt.
- Wende dieselbe Permutation auf die anderen Codeworte in C an.
  - Beachte: Die Distanz ändert sich nicht durch eine Permutation der Stellen.
- Flippe in jedem Codewort die letzten $n - k$ Stellen.
  - Beachte: Die Distanz ändert sich nicht durch ein Flippen der Bits.
- Der resultierende Code C' enthält 0^n und ist ein (n, M, d)-Code.

Bsp: $C = \{0101, 1010\}$ wird zu $C' = \{0000, 1111\}$.

Erstes nicht-triviales Resultat

Satz

$A(4,3) = 2$.

- Sei C ein optimaler $(4, M, 3)$-Code. OBdA $0000 \in C$.
- Worte mit Distanz mindestens 3 von 0000:

$$0111, 1011, 1101, 1110, 1111.$$

- Je zwei Worte besitzen Distanz höchstens 2, d.h. $A(4,3) \leq 2$.
- Für $C = \{0000, 0111\}$ gilt $d(C) = 3$ und damit $A(4,3) = 2$.

Verkürzen eines Codes

Definition Verkürzter Code

Sei C ein (n, M, d)-Code und $j \in [n]$, $b \in \{0, 1\}$. Der *bezüglich b-Bit an j-ter Position verkürzte Code* C'

1. besteht aus denjenigen Codeworten aus C, deren j-tes Bit b ist,
2. besitzt Länge $n - 1$ durch Herausstreichen der j-ten Stelle.

- **Bsp:** Kürzen von $C = \{001, 010, 101\}$ bezüglich 0-Bit an 1. Position liefert $C' = \{01, 10\}$.
- Beachte C besitzt Distanz 1, aber $d(C') = 2$.

Satz Verkürzter Code

Sei C ein (n, M, d)-Code und C' ein verkürzter Code. Dann gilt $d(C') \geq d$.

- Betrachten nur die bezüglich einer Stelle j konstanten Codeworte.
- Stelle j kann nicht zur Distanz beitragen.

Rekursive Schranke für $A(n, d)$

Lemma Rekursive Schranke

Für $n \geq 2$ gilt: $A(n, d) \leq 2 \cdot A(n-1, d)$.

- Sei C ein optimaler (n, M, d)-Code.
- Sei C_b der bezügl. b-Bit, $b \in \{0, 1\}$ an 1. Position verkürzte Code.
- Aus $d(C_b) \geq d$ folgt

$$\begin{aligned} A(n, d) = M = |C_0| + |C_1| &\leq A(n-1, d(C_0)) + A(n-1, d(C_1)) \\ &\leq A(n-1, d) + A(n-1, d). \end{aligned}$$

Korollar

$A(5, 3) = 4$.

- $A(5, 3) \leq 2 \cdot A(4, 3) = 4$.
- $C = \{00000, 11100, 00111, 11011\}$ besitzt $d(C) = 3$.

Schnitt von Strings

Definition Gewicht, Schnitt

Seien $\mathbf{x}, \mathbf{y} \subseteq \{0,1\}^n$. Das Gewicht von $\mathbf{x}$ ist definiert als die Anzahl von Einsen in $\mathbf{x}$.
Seien $\mathbf{x} = x_1 \dots y_n$, $\mathbf{y} = y_1 \dots y_n$. Dann ist der Schnitt definiert als

$$\mathbf{x} \cap \mathbf{y} = x_1 \cdot y_1 \dots x_n \cdot y_n$$

Lemma Distanz via Gewicht

Seien $\mathbf{x}, \mathbf{y} \subseteq \{0,1\}^n$. Dann gilt

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} \cap \mathbf{y})$$

- Sei $a_{b_0 b_1}$: Anzahl Position mit b_0 in $\mathbf{x}$ und b_1 in $\mathbf{y}$, $b_i \in \{0,1\}$.
- Es gilt

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}) = a_{10} + a_{01} &= (a_{10} + a_{11}) + (a_{01} + a_{11}) - 2a_{11} \\ &= w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} \cap \mathbf{y}) \end{aligned}$$

Ungerade d genügen

Satz

Sei $d \geq 1$ ungerade. Dann existiert ein (n, M, d)-Code C gdw ein $(n+1, M, d+1)$-Code C' existiert.

"$\Leftarrow$": Sei C' ein $(n+1, M, d+1)$ Code.

- Seien $\mathbf{c}, \mathbf{c}' \in C'$ mit $d(\mathbf{c}, \mathbf{c}') = d+1$ und i eine Position mit $\mathbf{c_i} \neq \mathbf{c'_i}$.
- Lösche i-te Position aus C'. Resultierender Code C besitzt $d(C) = d$ und Länge n.

"$\Rightarrow$": Sei C ein (n, M, d) Code.

- C: Erweitere C um Paritätsbit, so dass $w(\mathbf{c})$ gerade für alle $\mathbf{c} \in C'$.
- Mittels Lemma

$$d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x}) + w(\mathbf{y}) - 2w(\mathbf{x} \cap \mathbf{y}) = 0 \mod 2 \text{ für alle } \mathbf{x}, \mathbf{y} \in C'.$$

- Wegen $d = d(C)$ ungerade und $d \leq d(C') \leq d+1$ folgt $d(C') = d+1$.

Einige Werte von $A(n, d)$ (Quelle: Sloane 1982)

Korollar

$A(n, d) = A(n+1, d+1)$ für $d \geq 1$ ungerade.

n	5	6	7	8	9	10	11	16
$d = 3$	4	8	16	20	40	72-79	144-158	2560-3276
$d = 5$	2	2	2	4	6	12	24	256-340
$d = 7$	-	-	2	2	2	2	4	36-37

Sphere-Covering und Sphere-Packing

Satz Schranken Sphere-Covering und Sphere-Packing

$$\frac{2^n}{V^n(d-1)} \leq A(n,d) \leq \frac{2^n}{V\left(\lfloor \frac{d-1}{2} \rfloor\right)}.$$

Untere Schranke:

- Sei C ein optimaler (n, M, d)-Code, d.h. $M = A(n, d)$.
- Für alle $\mathbf{x} \in \{0,1\}^n \exists\, \mathbf{c} \in C$: $d(\mathbf{x}, \mathbf{c}) < d$ (Warum?)

$$\{0,1\}^n \subseteq \bigcup_{i=1}^{M} B^n(c_i, d-1) \quad \Rightarrow \quad 2^n \leq V^n(d-1) \cdot M.$$

Obere Schranke:

- C korrigiert $\lfloor \frac{d-1}{2} \rfloor$ Fehler, d.h. Hammingkugeln mit diesem Radius sind disjunkt

$$\bigcup_{i=1}^{M} B^n\left(c_i, \left\lfloor \frac{d-1}{2} \right\rfloor\right) \subseteq \{0,1\}^n \quad \Rightarrow \quad V^n\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right) \cdot M \leq 2^n$$

Bsp $A(n, 3)$ für Sphere-Covering und Sphere-Packing

n	5	6	7	8	9	10	11	16
untere	2	3	5	7	12	19	31	479
$A(n, 3)$	4	8	16	20	40	72-79	144-158	2560-3276
obere	5	9	16	28	51	93	170	3855

Singleton-Schranke

Satz Singleton-Schranke

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

- Sei C ein optimaler (n, M, d)-Code. Entferne letzte $d-1$ Stellen.
- Resultierende Codeworte sind alle verschieden, da sich $\mathbf{c} \in C$ in mindestens d Stellen unterscheiden.
- Es gibt M viele verkürzte unterschiedliche Codeworte der Länge $n-(d-1)$:

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

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 ein binärer symmetrischer Kanal mit Fehlerws p. Für alle $R < 1 + p\log_2 p + (1-p)\log_2(1-p)$ 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.

Erinnerung: Der Vektorraum $\mathbb{F}_2^n$

Schreiben $\{0,1\}^n$ als $\mathbb{F}_2^n$.

Definition Vektorraum $\mathbb{F}_2^n$

$(\mathbb{F}_2^n, +, \cdot)$ mit Addition modulo 2, $+ : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ und skalarer Multiplikation $\cdot : \mathbb{F}_2 \times \mathbb{F}_2^n \to \mathbb{F}_2^n$ definiert einen Vektorraum, d.h.

1. Assoziativität: $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$
2. Kommutativität: $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$
3. $\exists$ neutrales Element $\mathbf{0^n} : \mathbf{0^n} + \mathbf{x} = \mathbf{x} + \mathbf{0^n} = \mathbf{x}$
4. Selbstinverse: $\forall \mathbf{x} : \mathbf{x} = -\mathbf{x}$, d.h. $x + x = \mathbf{0^n}$.
5. Skalare Multiplikation: $\alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}$.

Definition Unterraum des $\mathbb{F}_2^n$

$S \subseteq \mathbb{F}_2^n$ ist ein Unterraum des $\mathbb{F}_2^n$ gdw

$$\mathbf{0^n} \in S \text{ und } \forall \mathbf{x}, \mathbf{y} \in S : \mathbf{x} + \mathbf{y} \in S.$$

Erzeugendensystem und Basis

Definition Erzeugendensystem und Basis eines Unterraums

Sei $S \subseteq \mathbb{F}_2^n$ ein Unterraum. Eine Menge $G = \{\mathbf{g_1}, \ldots, \mathbf{g_k}\} \subseteq S$ heißt *Erzeugendensystem* von S, falls jedes $\mathbf{x} \in S$ als Linearkombination

$$\mathbf{x} = \alpha_1 \mathbf{g_1} + \ldots \alpha_k \mathbf{g_k} \quad \text{mit } \alpha_i \in \mathbb{F}_2$$

geschrieben werden kann. Notation: $S = \langle \mathbf{g_1}, \ldots, \mathbf{g_k} \rangle$.
Eine *Basis* B ist ein minimales Erzeugendensystem, d.h. keine Teilmenge von B erzeugt S.

- $C = \{000, 100, 010, 110\}$ wird von $G = \{000, 100, 010\}$ erzeugt.
- $B = \{100, 010\}$ ist eine Basis von C.
- $B' = \{100, 110\}$ ist ebenfalls eine Basis.

Basisergänzung

Erinnerung Eigenschaften einer Basis

Sei $S \subseteq \mathbb{F}_2^n$ ein Unterraum.

1. Jede Basis von S hat dieselbe Kardinalität, genannt die Dimension $dim(S)$.
2. Jedes Erzeugendensystem G von S enthält eine Untermenge, die eine Basis von S ist.
3. Jede linear unabhängige Teilmenge von S kann zu einer Basis ergänzt werden.

Lineare Codes

Definition Linearer Code

Sei $C \subseteq \mathbb{F}_2^n$ ein Code. Falls C ein Unterraum ist, bezeichnen wir C als *linearen Code*. Sei k die Dimension und d die Distanz von C, dann bezeichnen wir C als $[n, k, d]$-Code.

- $C = \{000, 100, 010, 110\}$ ist ein $[3, 2, 1]$-Code.
- $C = \langle 1011, 1110, 0101 \rangle$ ist ein $[4, 2, 2]$-Code.
- Jeder $[n, k, d]$-Code ist ein $(n, 2^k, d)$-Code.
- D.h. wir können $M = 2^k$ Codeworte mittels einer Basis der Dimension k kompakt darstellen.
- Beispiele für lineare Codes:
  Hamming Codes, Golay Codes und Reed-Muller Codes.

Generatormatrix eines linearen Codes

Definition Generatormatrix

Sei C ein linearer $[n, k, d]$-Code mit Basis $B = \{\mathbf{b_1}, \ldots, \mathbf{b_k}\}$. Die $(k \times n)$-Matrix

$$G = \begin{pmatrix} \mathbf{b_1} \\ \vdots \\ \mathbf{b_k} \end{pmatrix}$$

heißt Generatormatrix des Codes C.

Distanz von linearen Codes

Satz Distanz eines linearen Codes

Sei C ein linearer Code. Dann gilt

$$d(C) = \min_{\mathbf{c} \in C, \mathbf{c} \neq 0} \{w(\mathbf{c})\}.$$

"$\leq$":

- Sei $\mathbf{c_m} = \min_{\mathbf{c} \in C, \mathbf{c} \neq 0} \{w(\mathbf{c})\}$. Dann gilt

$$d(C) \leq d(\mathbf{c_m}, \mathbf{0^n}) = w(\mathbf{c_m})$$

"$\geq$":

- Seien $\mathbf{c_i}, \mathbf{c_j}$ Codeworte mit $d(C) = d(\mathbf{c_i}, \mathbf{c_j})$.
- Linearität von C: $\mathbf{c_i} + \mathbf{c_j} = \mathbf{c'} \in C$. Daher gilt

$$d(C) = d(\mathbf{c_i}, \mathbf{c_j}) = w(\mathbf{c_i} + \mathbf{c_j}) = w(\mathbf{c'}) \geq \min_{\mathbf{c} \in C, \mathbf{c} \neq 0} \{w(\mathbf{c})\}.$$

Bsp: $G = \langle 110, 111 \rangle$ besitzt $d(G) = w(001) = 1$.