Vorlesungsmitschrift WS 2010/2011

Informations- und Kodierungstheorie

von Steve Göring
email: stg7@gmx.de

Inhaltsverzeichnis

Hinweise

Im Skript werden für Zahlenbereiche keine doppelt schrafierten Buchstaben verwendet, d.h.: $\mathbb{N} = N, \mathbb{R} = R, \mathbb{C} = C$
Das SKript entstand aus den Mitschriften von:
Markus Hartwig, Andreas Loth,Steve Göring
Dank an Steffen Hirte für das Korrekturlesen.

1 Kapitel I: Elementare Kombinatorik

Vorlesung 1

1.1 Mengen, Einfache Abzählaussagen

Mengen $A, A_1, ..., B$

- $x \in A$: x ist Element von A
- $\emptyset$: leere Menge
- $A \subseteq B$: A ist Teilmenge von B ($x \in A \Rightarrow x \in B$)
- $A = B$: A ist gleich B ($x \in A \Leftrightarrow x \in B$)
- $|A|$: Mächtigkeit von A (Anzahl der Elemente)
- A ist endliche Menge, falls $|A| \geq 0$ und $|A|$ eine natürliche Zahl ist

Mengenoperationen .

- Vereinigung: $A \cup B := \{x | x \in A \vee x \in B\}$
- Durchschnitt: $A \cap B := \{x | x \in A \wedge x \in B\}$
- Differenz: $A - B := \{x | x \in A \wedge x \notin B\}$
- Kartesisches Produkt:
  $A \times B := \{x = (x_1, x_2) | x_1 \in A \wedge x_2 \in B\}$
  $A_1 \times .. \times A_n := \{x = (x_1, .., x_n) | x_i \in A_i \text{ für } i = 1, ..., n\}$
  $A^n := A \times ... \times A$ n mal $= \{x = (x_1, .., x_n) | x_i \in A_i; \text{ für } i = 1, ..., n\}$
  $x = (x_1, .., x_n)$: Folge der Länge n, n- Tupel, Zeilenvektor mit n Komponenten
- A, B heißen disjunkt, falls $A \cap B = \emptyset$ ist

Abbildungen .

- $f : A \to B$ f ist Abbildung von A in B
- BILD MIT MENGEN DING
- f injektiv (eineindeutig): $a \neq a' \Rightarrow f(a) \neq f(a') \forall a, a' \in A$
- f surjektiv (Abb. auf B): $\forall b \in B \exists a \in A$ mit $f(a) = b$
- f bijektiv: f injektiv und f surjektiv
- $A \cong B$ (A gleichmächtig zu B oder A isomorph zu B),
  falls es eine bijektive Abb. von A auf B gibt

Einfache Regeln .

- $A \cong B \Rightarrow B \cong A$
- $A \cong A$
- $A \cong B \wedge B \cong C \Rightarrow A \cong C$
- $A = B \Rightarrow A \cong B$ (Umkehrung gilt nicht)

1.1.1 Gleichheitsregeln

$|A| = |B| \Leftrightarrow A \cong B$

- $|A| = 0 \Leftrightarrow A = \emptyset$
- $|A| = n \Leftrightarrow \{1, ..., n\} \cong A$, n ist natürliche Zahl

1.1.2 Produktregel

$|A \times B| = |A| \cdot |B|$

- $|A_1 \times .. \times A_n| = |A_1| \cdot .. \cdot |A_n|$
- $|A^n| = |A|^n$
- $|\{0,1\}^n| = 2^n$

1.1.3 Summenregel

A,B disjunkt $\Rightarrow |A \cup B| = |A| + |B|$

- $A_1, ..., A_n$ paarweise disjunkt $\Rightarrow |A_1 \cup .. \cup A_n| = |A_1| + .. + |A_n|$

Beispiel

- 6 lateinische Bücher $L = \{l_1, .., l_6\}$ $|L| = 6$
- 5 griechische Bücher $G = \{g_1, .., g_5\}$ $|G| = 5$
- 8 englische Bücher $E = \{e_1, .., e_8\}$ $|E| = 8$

Auf wieviel verschiedene Arten kann man 2 Bücher verschiedener Sprachen auswählen?
B sei die Menge der Möglichkeiten $\Rightarrow B \cong L \times G \cup L \times E \cup G \times E$ (Mengen paarweise disjunkt)
$\Rightarrow |B| = |L \times G| + |L \times E| + |G \times E| = 30 + 48 + 40 = 118$

1.2 Wortmengen, Multinomialsatz

Alphabet A : endliche, nicht-leere Menge

Buchstaben : Element aus A

Wort der Länge n über A : Folge der Länge n über A $w = (w_1, ..., w_n) \mathrel{\widehat{=}} w_1..w_n$ mit $w_i \in A$ für $i = 1..n$

A^n = Menge aller Wörter der Länge n über A

leeres Wort : Folge der Länge 0, wird mit ε bezeichnet
$A^0 = \{\varepsilon\}$

A^* $:= \bigcup_{n=0}^{\infty} A^n$: Menge aller Wörter über A

1.2.1 Satz

$|A^n| = |A|^n \; \forall n \geq 0$

1.2.2 Definiton

$W\begin{pmatrix} a_1 & .. & a_r \\ k_1 & .. & k_r \end{pmatrix}$ sei die Menge aller Wörter w der Länge $n = k_1 + ... + k_r$, wobei der Buchstabe a_i in w genau k_i mal auftaucht $\forall i = 1..r$

Beispiel

$W\begin{pmatrix} a & b \\ 1 & 2 \end{pmatrix} = \{abb, bab, bba\}$
$W\begin{pmatrix} a & b & c \\ 1 & 1 & 1 \end{pmatrix} = \{abc, bac, cab, acb, bca, cba\}$
$W\begin{pmatrix} a & b & c \\ 1 & 2 & 0 \end{pmatrix} = W\begin{pmatrix} a & b \\ 1 & 2 \end{pmatrix}$

1.2.3 Satz

$\left| W\begin{pmatrix} a_1 & .. & a_r \\ k_1 & .. & k_r \end{pmatrix} \right| = \frac{(k_1+...+k_r)!}{k_1! \cdot ... \cdot k_r!}$ für $k_1, ..k_r \geq 0$

Beweis

(Induktion über $n = k_1 + ... + k_r$)

(IA)

n=0: $k_1 = ... = k_r = 0$
$W\begin{pmatrix} a_1 & .. & a_r \\ 0 & .. & 0 \end{pmatrix} = \{\epsilon\}$, $|W| = \frac{0!}{0!} = 1$

(IS)

$(n-1 \Rightarrow n)$
$n = k_1 + ... + k_r \geq 1$
$W = W\begin{pmatrix} a_1 & .. & a_r \\ k_1 & .. & k_r \end{pmatrix}$

- $W_i = \{w \in W | w \text{ beginnt mit Buchstaben } a_i\}$ für $i = 1..r$
- $W = \bigcup\limits_{i=1}^{r} W_i$
  W_i sind paarweise disjunkt
- $\Rightarrow |W| = |W_1| + .. + |W_r|$
- $W_i = W\begin{pmatrix} a_1 & .. & a_i & .. & a_r \\ k_1 & .. & k_i - 1 & .. & k_r \end{pmatrix}$ (lassen den ersten Buchstaben a_i weg)
- Aus (IV) folgt dann:
  $|W_i| \cong \left| W\begin{pmatrix} a_1 & .. & a_i & .. & a_r \\ k_1 & .. & k_i - 1 & .. & k_r \end{pmatrix} \right|$
  $= \frac{(k_1+...+k_r-1)!}{k_1! \cdot .. (k_i-1)! \cdot .. \cdot k_r!} = k_i \cdot \frac{(k_1+...+k_r-1)!}{k_1! \cdot .. \cdot k_r!}$
- $|W| = |W_1| + .. + |W_r|$
  $= \sum_{i=1..r} k_i \cdot \frac{(k_1+...+k_r-1)!}{k_1! \cdot ... \cdot k_r!}$ (gleichen Term $\frac{(k_1+...+k_r-1)!}{k_1! \cdot ... \cdot k_r!}$ ausklammern) $= (k_1 + ... + k_r) \cdot \frac{(k_1+...+k_r-1)!}{k_1! \cdot ... \cdot k_r!} = \frac{(k_1+...+k_r)!}{k_1! \cdot ... \cdot k_r!}$
  q.e.d.

Spezialfälle

- $\left| W\begin{pmatrix} a & b \\ k & n-k \end{pmatrix} \right| = \frac{n!}{k! \cdot (n-k)!} = \begin{pmatrix} n \\ k \end{pmatrix}$
- $\left| W\begin{pmatrix} a_1 & .. & a_n \\ 1 & .. & 1 \end{pmatrix} \right| = n!$

1.2.4 Multinomialsatz

$a_1, .., a_r \in R, n \geq 1\ n \in N$

$$(a_1 + ... + a_r)^n = \sum_{(k_1,..,k_r) \text{mit} \sum\limits_{i=1}^{r} k_i = n, k_i \geq 0} \frac{(k_1+..+k_r)!}{k_1! \cdot .. \cdot k_r!} a_1^{k_1} \cdot .. \cdot a_r^{k_r}$$

Beweis

umformen

Spezialfall

Binomischer Lehrsatz : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^k \cdot b^{n-k}$

Spezialfall: $2^n = \sum_{k=0}^{n} \binom{n}{k}$

1.2.5 Teilmengen, Permutationen

A sei endliche Menge

$\mathcal{P}(A) := \{X | X \subseteq A\}$ Potenzmenge von A, alle Teilmengen von A

$\mathcal{P}_k(A) := \{X | X \subseteq A \textbf{ , } |X| = k\}$ alle k-elementigen Teilmengen von A

$\mathcal{S}(A) := \{f | f : A \to A \textbf{ bijektiv}\}$ f heißt Permutation über A

Satz

Ist $|A| = n$ so gilt:

1. $|\mathcal{P}(A)| = 2^n$
2. $|\mathcal{P}_k(A)| = \binom{n}{k}$
3. $|\mathcal{S}(A)| = n!$

Beweis

$A = \{a_1, ..., a_n\}$

1. Betrachten Abbildungen $X \in \mathcal{P}(A) \to W_x = (w_1, .., w_n)$ mit

   $$w_i = \begin{cases} 1, & \text{falls } a_i \in X \\ 0, & \text{falls } a_i \notin X \end{cases}$$
   Die Abbildung ist bijektiv,also gilt:
   $|\mathcal{P}(A)| = |\{0,1\}|^n = 2^n$

Vorlesung 2

2. $P_k(A) \cong \{w \in \{0,1\}^n |$w hat genau k Einsen $\}$
$= W \begin{pmatrix} 1 & 0 \\ k & n-k \end{pmatrix} \Rightarrow |P_k(A)| = |W \begin{pmatrix} 1 & 0 \\ k & n-k \end{pmatrix}| = \binom{n}{k}$

3. $f : A \to A$ bijektiv : Wertetabelle: $f \mathrel{\widehat{=}} \begin{pmatrix} a_1 & ... & a_n \\ a_{i1} & ... & a_{in} \end{pmatrix}$ (alle a_{ix} verschieden)
mit $f(a_k) = a_{ik}\ \forall i = 1..n$
$w_f = (a_{i1}, ..., a_{in}) \in W \begin{pmatrix} a_1 & ... & a_n \\ 1 & ... & 1 \end{pmatrix}$
Die Abbildung $f \in S(A) \to w_f \in W \begin{pmatrix} a_1 & ... & a_n \\ 1 & ... & 1 \end{pmatrix}$ ist bijektiv.
$\Rightarrow |S(A)| = |W \begin{pmatrix} a_1 & ... & a_n \\ 1 & ... & 1 \end{pmatrix}| = n!$

1.2.6 Kombinationen und Variationen

Anzahl der Möglichkeiten k Elemente aus n gegebenen Elementen auszuwählen

1. mit Berücksichtigung der Reihenfolge mit Wiederholungen: n^k
2. mit Berücksichtigung der Reihenfolge ohne Wiederholungen: $\frac{n!}{(n-k)!}$
3. ohne Berücksichtigung der Reihenfolge ohne Wiederholungen: $\binom{n}{k}$
4. ohne Berücksichtigung der Reihenfolge mit Wiederholungen: $\binom{n+k-1}{k}$

Beweis

- $A = \{a_1, ..., a_n\}$ Menge der n gegebenen Elemente
- M = Menge aller Möglichenkeiten k Elemente aus A auszuwählen, entsprechend (1)-(4)
- $|M| =?$, Codierung der Elemente aus M in geeigneter Form

1. Jede Auswahl aus M lässt sich als Wort der Länge k über A darstellen, wobei gilt: $M \cong A^k \Rightarrow |M| = |A^k| = |A|^k = n^k$
2. $M \cong \{w \in A^k |$w ist Wort ohne Wdh von Buchstaben $\} = W$
   - **Beh:** $|M| = |W| = \frac{n!}{(n-k)!}$
   - Beweis durch Induktion über die Wortlänge k
   - (IA) $k = 1$: $W = A^1 = A \Rightarrow |W| = |A| = n = \frac{n!}{(n-1)!} = n$
   - (IS) $k - 1 \to k$: $W = \{w \in A^k |$w Wort ohne Wdh $\}$

- $W_i = \{w \in W | \text{w beginnt mit Buchstaben } a_i\}$ mit $i = 1..n$
  $w \in W_i \Leftrightarrow w = (a_i, w')$ mit $w' \in (A - \{a_i\})^{k-1}$ und w' ist Wort ohne Wdh
  $\widehat{W_i} = \{w' | w = (a_i, w') \in W\} = \{w \in (A - \{a_i\})^{k-1} | w' \text{ Wort ohne Wdh}\}$
- Die Abbildung $w = (a_i, w') \in W \mapsto w' \in \widehat{W_i}$ ist bijektiv
  $\Rightarrow |W_i| = |\widehat{W_i}| \Rightarrow_{\text{IV}} \frac{(n-1)!}{((n-1)-(k-1))!} = \frac{(n-1)!}{(n-k)!}$
- $W = W_1 \cup W_2 \cup .. \cup W_n$ und $W_1, ..., W_n$ sind disjunkt
  $\Rightarrow |W| = |W_1| + ... + |W_n| = n \cdot \frac{(n-1)!}{(n-k)!} = \frac{n!}{(n-k)!}$ wzbw

3. $M \cong P_k(A)$ (jede Auswahl entsprechend (3) lässt sich eindeutig durch eine k-elementige Teilmenge von A beschreiben)
   $|M| = |P_k(A)| =_{(2.5)} \binom{n}{k}$
4. $f \in M \Leftrightarrow$ f Auswahl von k Elementen aus $A = \{a_1, ..., a_n\}$ ohne Beachtung der Reihenfolge, aber mit Wiederholungen
   $\Leftrightarrow f : \{a_1, ..., a_n\} \to \{0, 1, .., k\}$ mit $\sum_{i=1}^{n} f(a_i) = k$ (Bem: $f(a_i)$ gibt an wie oft a_i ausgewählt wurde)
   Codiere f als Wort w_f über Alphabet $\{0, 1\}$ mit
   $w_f = (\underbrace{1, .., 1, 0}_{f(a_1)}, \underbrace{1, .., 1, 0}_{f(a_2)}, ..., \underbrace{1, .., 1, 0}_{f(a_n)})$
   dann ist $w_f \in W\begin{pmatrix} 1 & 0 \\ k & n-1 \end{pmatrix}$ und die Abbildung $f \in M \to w_f \in W\begin{pmatrix} 1 & 0 \\ k & n-1 \end{pmatrix}$ ist bijektiv. Daraus folgt:
   $|M| = |W\begin{pmatrix} 1 & 0 \\ k & n-1 \end{pmatrix}| = \binom{n+k-1}{k}$ wzbw.

1.3 Das Prinzip der Inklusion und Exklusion

1.3.1 Aufgabe

Gegeben:

- nat Zahlen n,m,k
- Alphabet $A = \{a_1, ..., a_n\}$
- $M = \{w \in A^k | \text{wenigstens einer der Buchstaben } a_1, ..., a_n \text{ kommt nicht in w vor}\}$

Gesucht:
$|M| =?$
Lösungansatz:

- $A_i = \{w \in A^k | \ a_i \text{ kommt nicht in w vor}\}$

- $A_i = (A - \{a_i\})^k \Rightarrow |A_i| = (n-1)^k$
- $M = A_1 \cup A_2 \cup ... \cup A_m$ aber $A_1, ..., A_m$ nicht paarweise disjunkt
  $\rightarrow$ daher $|M| \neq \sum\limits_{i=1}^{m} |A_i|$

1.3.2 Siebformel

Satz: (Prinzip der Inklusion / Exklusion)

Es seien $A_1, ..A_m$ endliche Mengen, dann gilt:
$|\bigcup_{i=1}^{m} A_i| = \sum_{I \subseteq \{1,..,m\}, I \neq \emptyset} (-1)^{|I|+1} \cdot |\bigcap_{i \in I} A_i|$

Spezialfälle

- $|A_1 \cup A_2| = \underbrace{|A_1|}_{I=\{1\}} + \underbrace{|A_2|}_{I=\{2\}} - \underbrace{|A_1 \cap A_2|}_{I=\{1,2\}}$
- $|A_1 \cup A_2 \cup A_3| = \underbrace{|A_1|}_{I=\{1\}} + \underbrace{|A_2|}_{I=\{2\}} + \underbrace{|A_3|}_{I=\{3\}} - \underbrace{|A_1 \cap A_2|}_{I=\{1,2\}} - \underbrace{|A_1 \cap A_3|}_{I=\{1,3\}}$
  $- \underbrace{|A_2 \cap A_3|}_{I=\{2,3\}} + \underbrace{|A_1 \cap A_2 \cap A_3|}_{I=\{1,2,3\}}$

Beweis

siehe Literatur

1.3.3 Lösung der Aufgabe (1.3.1)

- $A = \{a_1, ..., a_n\}$
- $M = \{w \in A^k|$ wenigstens einer der Buchsten $a_1, ..., a_n$ kommt in w nicht vor$\}$
- $|M| =?$
- $A_i = \{w \in A^k| \ a_i$ kommt in w nicht vor$\}$
- $M = A_1 \cup ... \cup A_m \Rightarrow |M| = \sum_{I \subseteq \{1,..,m\}, I \neq \emptyset} (-1)^{|I|+1} \cdot |\bigcap_{i \in I} A_i|$
- $I \subseteq \{1, ..., m\}, |I| = l \geq 1$
- $\bigcap_{i \in I} A_i = \{w \in A^k|$ w enthält nicht a_i mit $i \in I\} = (A - \{a_i | i \in I\})^k \Rightarrow |\bigcap_{i \in I} A_i| = |(A - \{a_i | i \in I\})^k| = (|A| - |I|)^k = (n-l)^k$
- somit ergibt die Siebformel für $M = \bigcup_{i=1}^{m} A_i$
  $|M| = \sum_{I \subseteq \{1,..,m\}, I \neq \emptyset} (-1)^{|I|+1} \cdot |\bigcap_{i \in I} A_i| = \sum_{l=1}^{m} (\sum_{I \subseteq \{1,..,m\}, |I| = l} (-1)^{|I|+1} \cdot |\bigcap_{i \in I} A_i|)$

$$= \sum_{l=1}^{m} (\underbrace{\sum_{I \subseteq \{1,..,m\}, |I|=l}}_{\text{Anzahl der Summanden } = |P_l(\{1,..,m\})| = \binom{m}{l}} (-1)^{l+1} \cdot (n-l)^k)$$

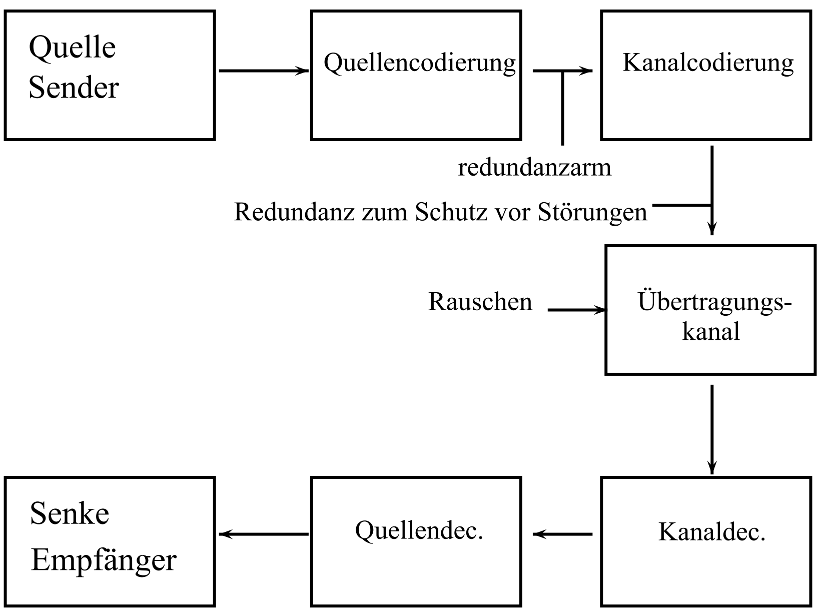
$$= \sum_{l=1}^{m} \binom{m}{l} (-1)^{l+1} \cdot (n-l)^k$$

2 Kapitel II: Quellenkodierung

- R.W.Hamming: Information und Kodierung, VCH, 1987
- H. Klimant ua: Informations und Kodierungstheorie, Teubner, 2006
- C. E. Shannon: A Mathematical Theorie of Communication, The Bell System Technical Journal, Vol. 27, 1948

2.1 Allgemeines Modell der Nachrichtenübertragung

2.1.1 Quellenkodierung und Kanalkodierung



Quelle/ Sender

Betrachten nur diskrete Quellen: senden taktweise Zeichen über einem Alphabet $X = \{x_1, ..., x_n\}$. Man nennt X dann das Klartextalphabet bzw. Quellenalphabet

Quellencodierung / decodierung

Modell zur effizienten Codierung und Decodierung von Nachrichten (Informationen) der Quelle: Datenkompression, Entzifferbarkeit von Codes

Kanalcodierung/ decodierung

Bereits codierte Nachricht wird nochmals codiert: Ziel ist die Entdeckung und Korrektur von Fehlern, die bei der Übertragung auftreten
(verursacht durch das Rauschen im Kanal). Vorlesung 3

2.1.2 Grundbegriffe

(1) Alphabet A: endliche nicht-leere Menge
$a \in A$: Buchstabe / Symbol / Zeichen aus A

(2) Ein Wort w der Länge n über A : ist eine Folge
$w = (a_1, ..., a_n) \widehat{=} a_1 a_2 ... a_n$ mit $a_1, ..., a_n \in A$

leeres Wort: Wort der Länge 0, wird mit ϵ bezeichnet

l(w): Länge des Wortes w

A^n: Menge der Wörter der Länge n über A

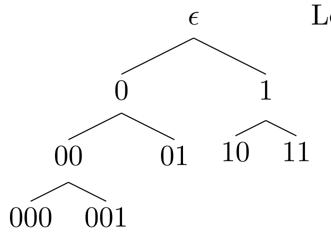
$A^* := \bigcup_{n=0}^{\infty} A^n$: Menge aller Wörter über A

(3) Verknüpfung von Wörtern: Operation der Form:
$u = (a_1, ..., a_n), v = (b_1, ..., b_m) \in A^* \rightarrow u \cdot v = (a_1, ..., a_n, b_1, ..., b_m)$

- $(u \cdot v) \cdot w = u \cdot (v \cdot w)$
- $\epsilon \cdot u = u \cdot \epsilon = u$
- $l(u \cdot v) = l(u) + l(v)$
- $u = (a_1, ..., a_n) \in A^* \Rightarrow u = a_1 \cdot a_2 \cdot ... \cdot a_n, a_i \in A$

(4) Präfix : $u \in A^*$ heißt Präfix von $w \in A^*$, falls es ein Wort $v \in A^*$ gibt mit:
$w = u \cdot v$

Beispiel: $A = \{0, 1\}, A^0 = \epsilon, A^1 = A, A^2 = \{00, 01, 10, 11\}$
$|A^n| = |A|^n = 2^n$



Level n beschreibt A^n

$u = 101$ $v = 110 \Rightarrow u \cdot v = 101110$

2.1.3 Diskrete Quelle

Eine diskrete Quelle ohne Gedächnis ist Paar $Q = (X, p)$ mit

(a) X ist Alphabet (Klartextalphabet)

(b) p ist Wahrscheinlichkeitsverteilung über X, d.h.
$p : X \mapsto [0, 1]$ mit $\sum_{x \in X} p(x) = 1$

Die Funktion
$H_r(Q) := -\sum_{x \in X} p(x) \cdot \log_r(p(x))$
heißt dann Entropie der Quelle Q zur Basis $r \geq 2$
wobei wir $0 \cdot \log_r(0) = 0$ setzen

Bemerkung Ist $X = (x_1, ..., x_n)$ und $p(x_i) = p_i$ so schreibt man statt
$H_r(Q)$ auch $H_r(p_1, ..., p_n)$

2.2 Quellencodierung

Gegeben :

- $Q = (X, p)$ Quelle mit $X = \{x_1, ..., x_n\}$, $n \geq 1$
- A: Codealphabet mit $r = |A| \geq 2$

2.2.1 Eindeutig entzifferbare Codes

Def1: Eine Quellencodierung von X (bzw. Q) über A ist eine Abbildung
$w : X \to A^*$
Man nennt dann $w = w(x)$ das Codewort von x und
$C = \{w(x)|x \in X\}$ heißt dann Quellencode.

Def2: Ein Quellencode $w : X \to A^*$ wird dann wie folgt zur Abbildung
$w^* : X^* \to A^*$ erweitert
$\underbrace{T = x_{i_1}x_{i_2}...x_{i_p} \in X^*}_{\text{Klartext}} \to \underbrace{w^*(T) = w(x_{i_1})...w(x_{i_p})}_{\text{codierter Text}}$
Die Quellencodierung bzw der Quellencode C heißt eindeutig entzifferbar, falls die Abbildung
$T \mapsto w^*(T)$ injektiv ist, d.h. falls für alle
$T_1, T_2 \in X^*$ gilt:
$w^*(T_1) = w^*(T_2) \Rightarrow T_1 = T_2$

Folgerung Für den Quellencode $C = \{w_1 = w(x_1), ..., w_n = w(x_n)\}$ sind folgende Bedingungen äquivalent:

(a) C ist eindeutig entzifferbar

(b) aus $w_{i_1} \cdot w_{i_2} \cdot ... \cdot w_{i_p} = w_{j_1} \cdot w_{j_2} \cdot ... \cdot w_{j_q}$ folgt stets:
$p = q$ und $w_{i_1} = w_{j_1}$, ... ,$w_{i_p} = w_{j_q}$

Beispiel1
- $X = \{a, b, c, d\}$
- $A = \{0, 1\}$
-

x	a	b	c	d
w(x)	0	01	11	101

- $C = \{0, 01, 11, 101\}$
- $T_1 = bb \mapsto w^*(T_1) = 0101$
- $T_1 = ad \mapsto w^*(T_2) = 0101$
- $\Rightarrow$ Code nicht eindeutig entzifferbar

Beispiel2
- $X = \{a, b, c\}$
- $A = \{0, 1\}$
-

x	a	b	c
w(x)	00	01	1

- $C = \{00, 01, 1\}$
- $w^*(T) = 00|01|01|1|1|01| \mapsto T = abbccb$ (von links nach rechts decodieren)
- $\Rightarrow C$ ist eindeutig entzifferbar

2.2.2 Präfixcode

Def $C = \{w(x)|x \in X\} \subseteq A^*$ heißt Präfixcode, falls kein Codewort aus C Präfix eines anderen Codewortes von C ist.

Bemerkung
- $C = \{\epsilon\}$ ist Präfixcode, aber nicht eindeutig entzifferbar
- Ist $C \subseteq A^*$ eindeutig entzifferbar, so ist $\epsilon \notin C$
- Ist $C \subseteq A^*$ ein Präfixcode und $\epsilon \in C$, so ist $C = \{\epsilon\}$
- Ist $C \subseteq A^*$ ein Präfixcode und $C \neq \{\epsilon\}$, so ist C eindeutig entzifferbar
- also jeder Präfixcode $C \subseteq A^* - \{\epsilon\}$ ist eindeutig entzifferbar

Beweis Sei also $C \subseteq A^*$ Präfixcode und $\epsilon \notin C$

Müssen nun zeigen, dass C eindeutig entzifferbar ist.

Benutzen Folgerung aus (2.2.1)

Sei also $C = \{w_1, ...w_n\}$, sei nun :

$w_{i_1} w_{i_2} ... w_{i_p} = w_{j_1} ... w_{j_q}$

Dann ist etwa $l(w_{i_1}) \leq l(w_{j_1})$ und somit w_{i_1} Präfix von w_{j_1}

Da C Präfixcode ist und $\epsilon \notin C$, gilt dann $w_{i_1} = w_{j_1}$

Dann ist aber $w_{i_2}...w_{i_p} = w_{j_2}...w_{j_q}$ und durch vollständige Induktion

zeigen wir dann:
$w_{i_2} = w_{j_2}, ..., w_{i_p} = w_{j_q}$ und $p = q$ q.e.d

2.2.3 Zielstellung der Quellencodierung

Ist $C = \{w(x)|x \in X\} \subseteq A^*$ ein eindeutig entzifferbarer Code der Quelle $Q = (X, p)$ so nennt man:

$L(C) := \sum_{x \in X} p(x) \cdot l(w(x))$
die mittlere Codewortlänge von C bzw. $w : X \to A^*$

und

$K_r(C) = L(C) - H_r(C)$
die absolute Redundanz von C bezüglich der Basis r.

Weiterhin sei:

$L_r^{min}(Q) = \min\{L(C)|C$ ist eindeutig entzifferbar$\}$ die minimale mittlere Codewortlänge von Q.

Ein optimaler Quellencode von $Q = (X, p)$ ist ein eindeutig entzifferbarer Code C mit:

$L(C) = L_r^{min}(Q)$ mit $r = |A|$

Bemerkung Ist $X = \{x_1, ..., x_n\}$ und $p(x_i) = p_i$ so schreibt man statt:

$L_r^{min}(Q)$ auch $L_r^{min}(p_1, ..., p_n)$.

2.2.4 Satz: Kraftsche Ungleichung

Ist $C = \{w(x)|x \in X\} \subseteq A^*$ ein eindeutig entzifferbarer Code über das Alphabet A mit $|A| = r$, so gilt: Vorlesung 4

$\sum_{w \in C} \frac{1}{r^{l(w)}} \leq 1$

Beweis

a) $L := \max\{l(w)|w \in C\}$

b) $C \subseteq A^*$ ist eindeutig entzifferbar, d.h. schreiben wir Codewörter aus C auf unterschiedliche Art hintereinander, so erhalten wir unterschiedliche Wörter (siehe (2.2.1) Folgerung)
$\Rightarrow m_{k_1} \cdot ... \cdot m_{k_p} =$ Anzahl der Wörter aus A^*, die sich als Verknüpfung von p Codewörtern darstellen lassen, wobei das i-te Codewort die Länge k_i hat
(Gesamtlänge ist dann: $\sum_{i=1}^{p} k_i$)

c) $d_{pl} = \sum_{(k_1,...,k_p) \text{mit} \sum k_i = l} m_{k_1} \cdot m_{k_2} ... \cdot m_{k_p}$

$\Rightarrow d_{pl}$ = Anzahl der Wörter der Länge l über A, die sich als Verknüpfung von p Codewörtern darstellen lassen.
Alle diese Wörter sind aus $A^l \Rightarrow$
$d_{pl} \leq |A^l| = |A|^l = r^l$

d) $\sum_{w \in C} \frac{1}{r^{l(w}} = \sum_{k=1}^{L} m_k \cdot \frac{1}{r^k}$

Für ein beliebiges $p \in N$ gilt:

$$(\sum_{w \in C} \frac{1}{r^{l(w}})^p = (\sum_{k=1}^{L} m_k \cdot \frac{1}{r^k})^p$$
$$= (\frac{m_1}{r^1} + \frac{m_2}{r^2} + ... + \frac{m_L}{r^L})^p$$
$$= \underbrace{(\frac{m_1}{r^1} + \frac{m_2}{r^2} + ... + \frac{m_L}{r^L}) \cdot ... \cdot (\frac{m_1}{r^1} + \frac{m_2}{r^2} + ... + \frac{m_L}{r^L})}_{\text{p mal}}$$
$$= \sum_{(k_1,...,k_p) \text{ mit } 1 \leq k_i \leq L} \frac{m_{k_1}}{r^{k_1}} \cdot \frac{m_{k_2}}{r^{k_2}} \cdot ... \cdot \frac{m_{k_p}}{r^{k_p}}$$
$$= \sum_{(k_1,...,k_p) \text{ mit } 1 \leq k_i \leq L} \frac{1}{r^{k_1 + ... + k_p}} \cdot m_{k_1} \cdot ... \cdot m_{k_p}$$
$$= \sum_{l=1}^{p \cdot L} \frac{1}{r^l} \cdot (\sum_{(k_1,...,k_p) \text{ mit } \sum k_i = l} m_{k_1} \cdot ... \cdot m_{k_p})$$
$$=_{(c)} \sum_{l=1}^{p \cdot L} \frac{1}{r^l} \cdot d_{pl}$$
$$\leq \sum_{l=1}^{p \cdot L} \frac{1}{r^l} \cdot r^l \text{ (da : } d_{pl} \leq r^l)$$
$$= \sum_{l=1}^{p \cdot L} 1 = p \cdot L$$
$$\Rightarrow$$
$$(\sum_{w \in C} \frac{1}{r^{l(w)}})^p \leq p \cdot L$$
$$\Rightarrow$$
$$\sum_{w \in C} \frac{1}{r^{l(w)}} \leq \sqrt[p]{p \cdot L} \ (\forall p \in N) \text{ mit: } lim_{p \to \infty} \sqrt[p]{p \cdot L} = 1$$
$$\Rightarrow \sum_{w \in C} \frac{1}{r^{l(w)}} \leq 1 \text{ q.e.d}$$

2.2.5 Hauptsatz der Quellencodierung

Es sei A ein Alphabet mit $|A| = r \geq 2$.
Weiterhin seien $n \geq 1$ natürliche Zahlen $l_1, ..., l_n \geq 1$ gegeben.
Dann sind folgende Bedingungen äquivalent:

(a) Es gibt Präfixcode $C = \{w_1, ..., w_n\} \subseteq A^*$ mit den Codewortlängen $l(w_i) = l_i$ $i = 1..n$

(b) Es gibt einen eindeutig entzifferbaren Code $C = \{w_1, ..., w_n\} \subseteq A^*$ mit den Codewortlängen $l(w_i) = l_i \; i = 1..n$

(c) Es gilt die Kraftsche Ungleichung, d.h.
$\sum_{i=1}^{n} \frac{1}{r^l} \leq 1$

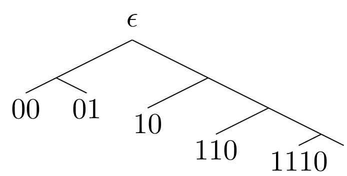
Beweis

- $(a) \Rightarrow (b)$: gilt, da $l_i \geq 1$ ist und somit $\epsilon \notin C$ ist. Dann ist der Präfixcode eindeutig entzifferbar.

- $(b) \Rightarrow (c)$: folgt aus Satz (2.2.4)
- $(c) \Rightarrow (a)$: Beweis: siehe Literatur, Konstruktion von C erfolgt nach Greedy Prinzip

Beispiel

- $A = \{0, 1\}, r = 2, n = 5, l_1 = l_2 = l_3 = 2, l_4 = 3, l_5 = 4$
- $\sum_{i=1}^{5} = 3 \cdot \frac{1}{4} + \frac{1}{8} + \frac{1}{16} = \frac{15}{16} \leq 1$
- Konstruktion von C: (links=0, rechts=1)



- Präfixcode $C = \{\underline{w}_1 = 00, \underline{w}_2 = 01, \underline{w}_3 = 10, \underline{w}_4 = 110, \underline{w}_5 = 1110\}$
- Kraftsche Ungleichung am Bsp:
$\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} < 1$

Folgerung

Für die Quelle $Q = (X, p)$ und $r \geq 2$ gilt:
$L_r^{min}(Q) = \min\{\sum_{x \in X} l(w(x)) \cdot p(x) | w : X \to A^* - \{\epsilon\} \text{ ist Präfixcode}\}$

2.2.6 Satz

Für die Quelle $Q = (X, p)$ und $r \geq 2$ gilt::
$H_r(Q) \leq L_r^{min}(Q) \leq H_r(Q) + 1$

Beweis

- $X = \{x_1, ..., x_n\}$, $n \geq 1$, $p(x_i) = p_i$
  $0 \leq p_i \leq 1$, $\sum\limits_{i=1}^{n} p_i = 1$

- $H_r(Q) = H_r(p_1, ..., p_n) = -\sum\limits_{i=1}^{n} p_i \cdot \log_r(p_i)$
  (dabei setzen wir: $0 \cdot \log_r(0) = 0$)

- Ist $p_i = 1$ für ein i, etwa $p_1 = 1$, so ist $p_j = 0 \; \forall j \neq i$
  und $H_r(Q) = 0$. Wählen Präfixcode:
  $w : X \to A^* - \{\epsilon\}$ mit $w(x_i) = a$ für ein $a \in A$ und $w(x_j)$ für $j \neq i$ irgendwie.
  Für den Präfix-Code $C = \{w(x_i) | i = 1..n\}$ gilt dann :
  $L(C) = 1$
  Also ist: $L_r^{min}(Q) \leq L(C) = 1$ und die Aussage gilt somit.

- Im Folgenden sei also:
  $0 < p_i < 1 \; \forall i = 1..n$ und somit $r \geq 2$

- Betrachten optimalen Präfixcode
  $w : X \to A^* - \{\epsilon\}$ mit $w(x_i) = w_i$ und
  $l(w_i) = l_i$. Dann ist:
  $L_r^{min}(Q) = \sum\limits_{i=1}^{n} p_i \cdot l_i$

- Aus Satz (2.2.4) folgt:
  $\sum\limits_{i=1}^{n} \frac{1}{r}^{l_i} \leq 1$

- Aus Analysis folgt: $\ln(x) \leq x - 1$

- und somit: $\log_r x \leq \frac{1}{\ln r} \cdot (x - 1)$

- Somit gilt:
  $H_r(Q) - L_r^{min}(Q) = -\sum\limits_{i=1}^{n} p_i \cdot \log_r(p_i) - \sum\limits_{i=1}^{n} p_i \cdot l_i$ mit $l_i = \log_r(r^{l_i})$
  $= \sum\limits_{i=1}^{n} p_i \cdot (-\log_r(p_i) - \log_r(r^{l_i}))$
  $= \sum\limits_{i=1}^{n} p_i \cdot \log_r(\frac{1}{p_i \cdot r^{l_i}})$
  $\leq \sum\limits_{i=1}^{n} p_i \cdot \frac{1}{\ln r} \cdot (\frac{1}{p_i \cdot r^{l_i}} - 1)$
  $= \frac{1}{\ln r} \cdot \sum\limits_{i=1}^{n} (\frac{1}{r^{l_i}} - p_i)$
  $= \frac{1}{\ln r} \cdot (\underbrace{\sum_{i=1}^{n} \frac{1}{r^{l_i}}}_{\leq 1} - \underbrace{\sum_{i=1}^{n} p_i}_{=1}) \leq 0$

- woraus folgt: $H_r(Q) \leq L_r^{min}(Q)$
- es sei l_i natürliche Zahlen mit:
  $-\log_r(p_i) \leq l_i \leq -\log_r(p_i) + 1$ für $i = 1..n$
  Dann ist $r^{-l_i} \leq p_i$ und somit:
  $\sum\limits_{i=1}^{n} \frac{1}{r^{l_i}} \leq \sum\limits_{i=1}^{n} p_i = 1$
- Aus Satz (2.2.5) folgt dann: es gibt einen Präfixcode
  $C = \{w_1, ..., w_n\} \subseteq A^*$ mit $l(w_i) = l_i$
  $L_r^{min}(Q) \leq L(C) = \sum\limits_{i=1}^{n} p_i \cdot l_i \leq \sum\limits_{i=1}^{n} p_i(-\log_r(p_i) + 1)$
  $= \underbrace{-\sum\limits_{i=1}^{n} p_i \cdot \log_r(p_i)}_{=H_r(Q)} + \underbrace{\sum\limits_{i=1}^{n} p_i}_{=1}$
  wzbw.

2.2.7 Huffman-Algorithmus

Eingabe

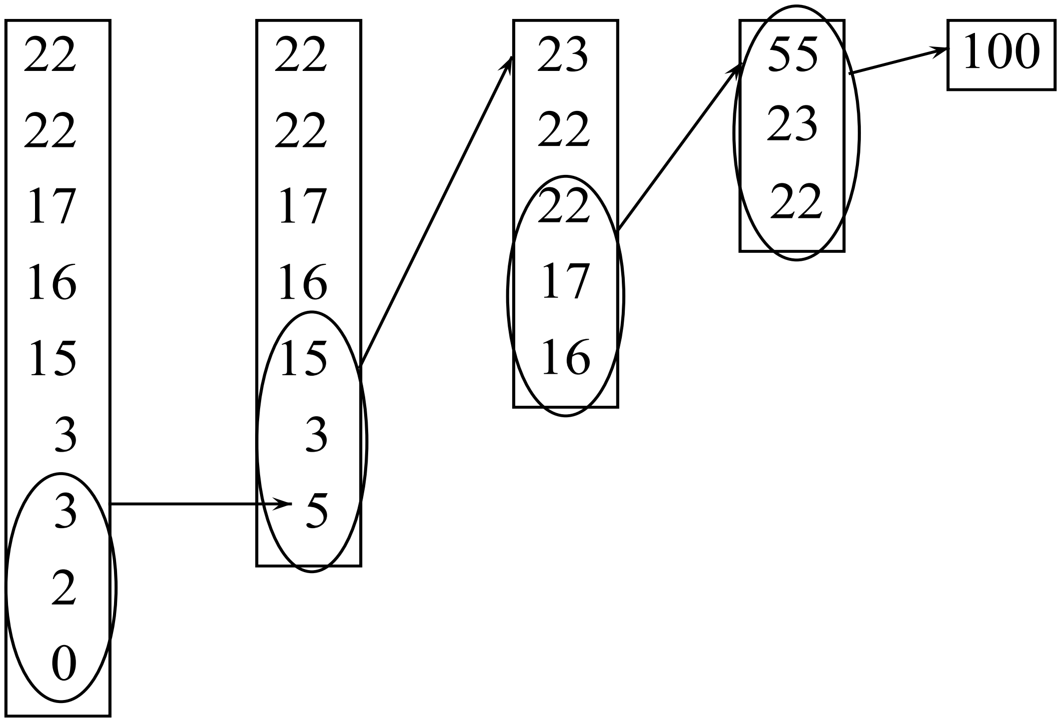
- Quelle $Q = (X, p)$: z.B. $X = \{x_1, ..., x_n\}$, $p(x_i) = p_i$,$n = 8$
  mit $(p_1, ..., p_8) = \frac{1}{100}(22, 22, 17, 16, 15, 3, 3, 2)$
- Alphabet A mit $|A| \geq 2$ z.B. $A = \{0, 1, 2\}$, $r = 3$

Ausgabe

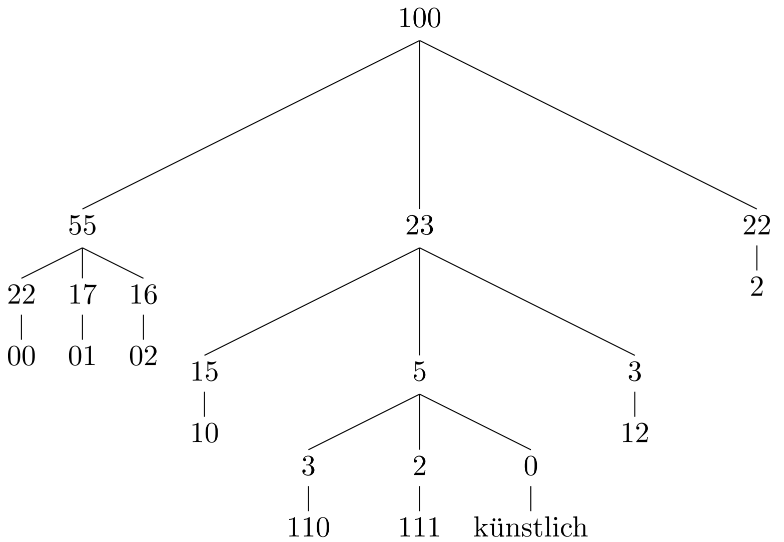
- Optimaler Präfixcode $C = \{w_1, ..., w_8\}$,d.h.
  Präfixcode mit $L_r^{min}(Q) = L(C) = \sum\limits_{i=1}^{8} p_i \cdot l(w_i)$

Methode

- füge $p_9 = 0$ hinzu (damit die Aufteilung klappt)
- Ordne die Wahrscheinlichkeiten p_i der Größe nach ;
  ersetze die kleinsten $r = 3$ Werte durch ihre Summe ;
  wiederhole das Verfahren



- erzeuge rückwärts einen Baum (oder 'hinschauen und direkt ablesen')



wobei (Links=0, Mitte=1 , Rechts=2)

- wir erhalten den optimalen Code:
  $C = \{w_1 = 2, w_2 = 02, w_3 = 01, w_4 = 00, w_5 = 10, w_6 = 12, w_7 = 110, w_8 = 111\}$
  mit $L_3^{min}(Q) = L(C) = \frac{1}{100}(22+(22+17+16+15+3)\cdot 2+3\cdot(3+2)) = \frac{183}{100} = 1.83$

- Entropie:
  $H_r(Q) = H_r(p_1, ..., p_8) = 1.67$
- Redundanz von $C = L(C) - H_r(Q) = 1.83 - 1.67 > 0$

Vorlesung 5

2.2.8 Der erste Hauptssatz von Shannon

(1)Wort-Codierung

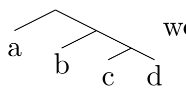
Betrachten Quelle $Q = (X, p)$ mit $X = \{a, b, c, d\}$ und p mit

x	a	b	c	d
p(x)	0.4	0.3	0.2	0.1

Dann ist $H_2(Q) = -\sum_{x \in X} p(x) \cdot \log_2(p(x)) \approx 1.8464$

Die Huffman Codierung mit $A = \{0, 1\}$ und $|A| = r = 2$ ergibt folgenden optimalen Präfixcode:

$$0.4,\ 0.3,\ \underbrace{0.2,\ 0.1}$$
$$0.4,\ \underbrace{0.3,\ 0.3}$$
$$\underbrace{0.4,\ 0.6}_{1}$$

ergibt Baum:  wobei Links = 0 , Rechts = 1

Codierung:
$w(a) = 0$
$w(b) = 10$
$w(c) = 110$
$w(d) = 111$

Somit ist:
$L_2^{min}(Q) = \sum_{x \in X} p(x) \cdot l(w(x)) = 0.4 \cdot 1 + 0.3 \cdot 2 + 0.2 \cdot 3 + 0.1 \cdot 3 = 1.9$

Also ist die Redundanz
$K_2(X) = L_2^{min}(Q) - H_2(Q) = 0.0536 > 0$

Wir betrachten nun Paare aus X^2 also die Quelle:
$Q^2 = (X^2, p)$ mit $p : X^2 \to [0, 1]$ ist Abbildung mit $p(x, y) = p(x) \cdot p(y)$ also :

z	aa	ab	...	dd
p(z)	0.16	...	...	0.01

Dann ergibt die Huffman-Codierung einen optimalen Präfixcode C für Q^2 mit
$L_2^{min}(Q^2) = 3.73$

Dies ist die optimale mittlere Codewortlänge für Paare aus X^2.

Für die Buchstaben aus X ergibt sich also eine mittlere Codewortlänge von:
$\frac{1}{2} \cdot 3.73 = 1.865 < 1.9$

(2) Produkt von Quellen

Es seien $Q_1 = (X_1, p_1)$ und $Q_2 = (X_2, p_2)$ zwei Quellen.
Es sei $X = X_1 \times X_2$ und $p : X \to [0, 1]$ die Abbildung mit
$p(a, b) = p_1(a) \cdot p_2(b)$ für $(a, b) \in X = X_1 \times X_2$.
Mann nennt dann $Q = (X, p)$ das Produkt der Quellen Q_1 und Q_2.

Satz

$H_r(Q_1 \times Q_2) = H_r(Q_1) + H_r(Q_2)$

Beweis

Übungsaufgabe

(3) Wort-Codierungen

Es sei $Q = (X, p)$ eine Quelle und $k \geq 1$ eine natürliche Zahl.

Betrachten die Produktquelle:

$$Q^k := \underbrace{Q \times Q ... \times Q}_{kmal}$$

also $Q^k = (X^k, p^\sim)$ mit $p^\sim(x_1, .., x_k) = p(x_1) \cdot ... \cdot p(x_k)$ mit $(x_1, .., x_k) \in X^k$.

Dann ist
$L_r^{min}(Q^k)$ die optimale mittlere Codewortlänge für Wörter der Länge k.

Dann ist:
$\bar{L}_r^k(Q) = \frac{1}{k} \cdot L_r^{min}(Q^k)$ die mittlere Codewortlänge für die Buchstaben der Quelle Q bei der Huffman-Codierung der Quelle Q^k.

1. Hauptsatz von Shannon

$H_r(Q) \leq \bar{L}_r^k(Q) \leq H_r(Q) + \frac{1}{k}$ also für $k \to \infty$ gilt:
$\bar{L}_r^k(Q) \to H_r(Q)$ (keine Redundanz)

Beweis

- $\bar{L}_r^k = \frac{1}{k} \cdot L_r^{min}(Q^k)$
- aus (2.2.6) folgt :
  $H_r(Q^k) \leq L_r^{min}(Q^k) \leq H_r(Q^k) + 1$
- $H_r(Q^k) =_{(2)} H_r(Q) + H_r(Q) + .. + H_r(Q) = k \cdot H_r(Q)$
- $\leq L_r^{min}(Q^k) \leq k \cdot H_r(Q) + 1$ (Division durch k)
- $H_r(Q) \leq \frac{1}{k} L_r^{min}(Q^k) \leq H_r(Q) + \frac{1}{k}$
- also : $H_r(Q) \leq \bar{L}_r^k \leq H_r(Q) + \frac{1}{k}$ qed

2.3 Suchtheorie

2.3.1 Suchprobleme und Entscheidungsbäume

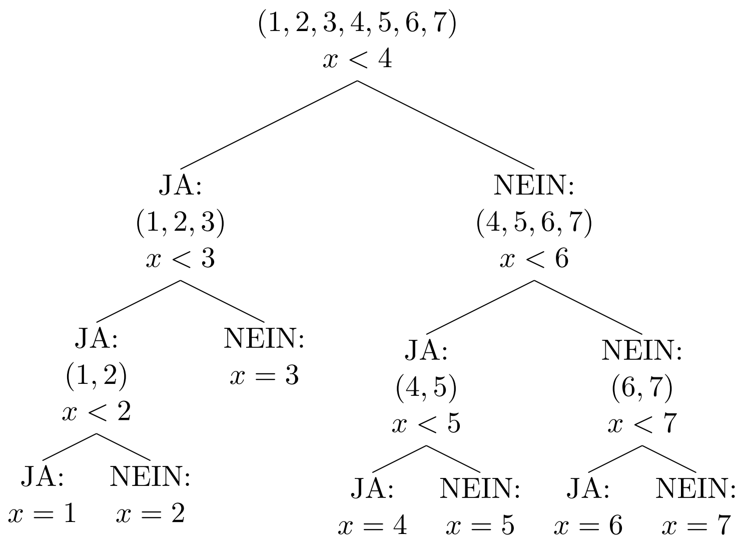
(1) Frage-Algorithmen:

Die Arbeitsweise eines Algorithmus der mit Tests arbeitet lässt sich als Baum darstellen.

Beispiel

- Gesucht ist Zahl $x \in \{1, 2, 3, 4, 5, 6, 7\}$
- zulässige Tests: Fragen der Form 'Ist $x < k$?' mit $k \in N$
- Eine möglicher Algorithmus könnte wie folgt arbeiten:
- $(1, 2, 3, 4, 5, 6, 7)$ $x < 4$
  - JA: $(1, 2, 3)$ $x < 3$:
    - JA: $(1, 2)$ $x < 2$
      - JA: 1
      - NEIN:2
    - NEIN: 3
  - NEIN: $(4, 5, 6, 7)$ $x < 6$
    - JA: $(4, 5)$ $x < 5$
      - JA: 4
      - NEIN:5
    - NEIN: $(6, 7)$ $x < 7$
      - JA: 6
      - NEIN:7

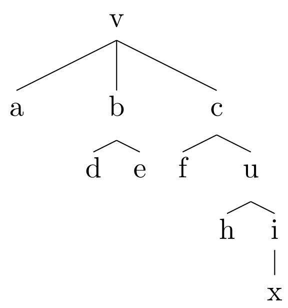
- (als Baum):



- Worst Case : 3 Fragen (ist das optimal?)
- Average Case: $\frac{1}{7} \cdot (1 \cdot 2 + 6 \cdot 3) = \frac{20}{7}$ Fragen (bei Gleichverteilung)

(2) Wurzelbaum, (n,r)-Baum

- T heißt Wurzelbaum mit Wurzel v, falls T ein Baum ist und v eine Ecke von T.
- Baum:



- u = innere Ecke von T mit 2 Nachfolgern
- x Blatt der Länge $l(x) = 4$ hat keine Nachfolger
- $B(T)$ = Menge von Blättern von (T,v)
- $L(T) = \max_{x \in B(T)} l(x)$: Tiefe des Wurzelbaumes
- Hat T genau n Blätter und jede Ecke von T höchstens r Nachfolger, so heißt T bzw. (T,v) ein (n,r)-Baum, kurz: $T \in \mathcal{T}(n, r)$

3 Bemerkung

Modellieren wir einen Suchalgorithmus, der mit Tests arbeitet durch einen Wurzelbaum $T \in \mathcal{T}((N, r)$ so bedeutet

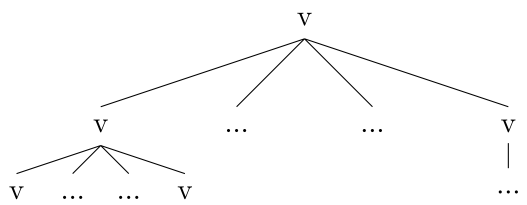
- $r =$ Anzahl möglicher Testausgänge
- $N =$ Größe des Suchbereiches (wir suchen also ein Element aus einer Menge von N Objekten)
- $L(T) =$ maximale Anzahl benötigter Tests (worst case)

2.3.2 Satz: Informationstheoretische Schranke

Sei T ein Wurzelbaum aus $\mathcal{T}(N, r)$ mit $N \geq 1$ und $r \geq 2$. Dann gilt :
$L(T) \geq \lceil \log_r(N) \rceil$
wobei $\lceil x \rceil$ die kleinste ganze Zahl größer oder gleich x ist.

Beweis

- Sei $L = L(T)$ maximale Länge eines Blattes x in T
- T hat N Blätter



  Betrachten der Level des Baumes:
  - Level 0: eine Ecke v
  - Level 1: höchstens r Ecken
  - Level 2: höchstens r^2 Ecken
  - ...
  - Level x: höchstens r^x Ecken
- Offenbar hat T höchstens r^L Blätter
- somit ist $N \leq r^l \Rightarrow L \geq \log_r(N)$ und $L \geq \lceil \log_r(N) \rceil$, da L eine natürliche Zahl ist.

Bemerkung

Gegeben sei ein Suchbereich der Größe N. Erlaubte Tests haben r mögliche Ausgänge. Dann besagt (2.3.2), dass jeder Suchalgorithmus im worst case mindestens $\lceil \log_r(N) \rceil$ Tests benötigt.

Beispiel

1 obiges Bsp:
N= 7, r=2 $\to \lceil \log_2(7) \rceil = 3$ Test im worst case benötigt

2 Sortieralgo:

- geg: Zahlenfolge $(a_1, .., a_n)$ $a_i \neq a_j$ für $i \neq j$
- ges: richtige Reihenfolge der Größe nach geordnet
- Permutaion σ so dass $a_{\sigma(1)} \leq ... \leq a_{\sigma(n)}$
- Test sind Vergleiche zweier Zahlen $a \leq b \to r = 2$
- $\to$ im worst case braucht man mindestens $\lceil \log_2(n!) \rceil \leq n \cdot \log_n$ viele Vergleiche

Vorlesung 6

2.3.3 Beispiel

$S(n) \geq \lceil \log n! \rceil \geq c \cdot n \cdot \log n$ für ein $c \in R^+$ (siehe 3.4)

Beispiel 3

Gegeben: n Münzen, von denen eine falsch ist. Alle echten Münzen haben dasselbe Gewicht, die falsche Münze ist entweder leichter oder schwerer.

Größe des Suchbereiches $N = 2n$ (Anzahl Münzen $\cdot 2$ für Falsche leichter oder Falsche schwerer)

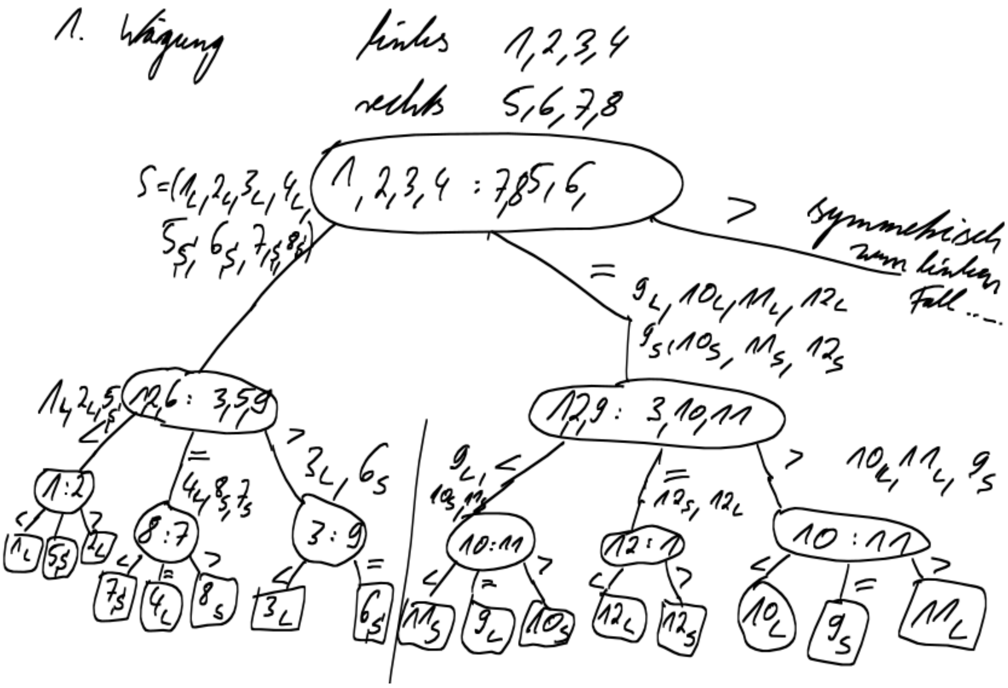
zulässige Tests sind Wägungen mit einer Balkenwaage: also r=3
(gleich, links schwerer als rechts, links leichter als rechts)

Es sei $L(n)$ die kleinste Anzahl von Wägungen mit der man im worst case auskommt, dann besagt Satz (3.2)
$L(n) \geq \lceil \log_3 2n \rceil$

Beh: $L(12) = 3$

Beweis: Informationstheoretische Schranke liefert:
$L(12) \geq \lceil \log_3 24 \rceil$
$L(12) \geq 3$
Wir müssen also nur einen Algorithmus finden, der mit maximal 3 Wägungen auskommt.
Der Suchbereich ist: $S = \{1_L, 1_S, 2_L, 2_S, ..., 12_L, 12_S\}$ mit
m_L bedeutet Münze m ist zu leicht
m_S bedeutet Münze m ist zu schwer

wird später eventuell digitalisiert



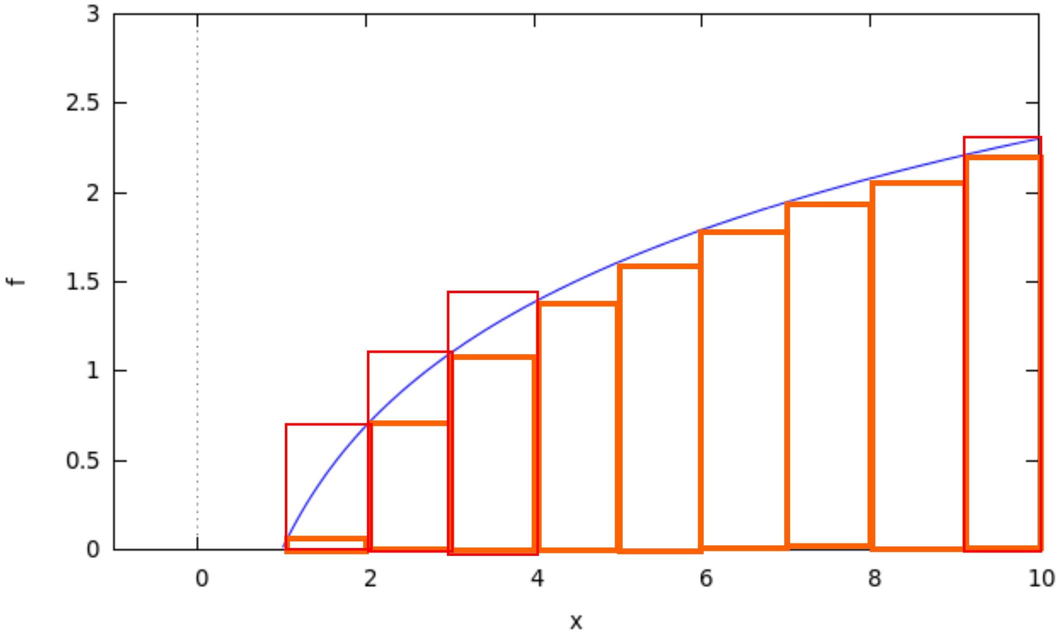
2.3.4 Stirlingsche Formel

Satz 1

Für eine natürliche Zahl n gilt:
$n \cdot \log n - n + 1 \leq \log(n!) \leq (n+1) \cdot \log n - n + 1$

Beweis

$\log(n!) = \sum_{k=1}^{n} \log(k)$ (geht aus Logarithmengesetz hervor)
Betrachten Funktion $\log(k)$:



Rot = Obersumme, Orange = Untersumme
Vergleich der Flächeninhalte ergibt:
$\sum\limits_{k=1}^{n} \log(k) \leq \int\limits_{1}^{n} \log(x)dx \leq \sum\limits_{k=2}^{n} \log(k) = \sum\limits_{k=1}^{n} \log(k)$
also gilt: $\int\limits_{1}^{n} \log(x)dx \leq \log(n!) \leq \int\limits_{1}^{n} \log(x)dx + \log(n)$
weiterhin ist: $\int\limits_{1}^{n} \log(x)dx = n \cdot \log(n) - n + 1$ wzbw.

Stirlingsche Formel

$n! \approx \sqrt{2\pi n}(\frac{n}{e})^n$
$\log n! \approx n \cdot \log(n)$

2.3.5 Satz

Es sei $n \geq 1$ natürliche Zahlen $l_1, ..., l_n$ gegeben und es sei $r \geq 2$. Dann sind folgende Bedingungen äquivalent:

(a) Es gibt einen Wurzelbaum $T \in \mathcal{T}(n, r)$ mit n Blättern $\{x_1, ..., x_n\}$ der Längen $l_1, ..., l_n$ mit $l(x_i) = l_i$

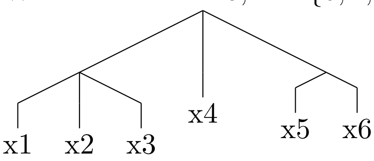
(b) Es gilt die Kraftsche Ungleichung:
$\sum_{i=1}^{n} \frac{1}{r^{l_i}} \leq 1$

Beweis

Betrachten die Bedingung:

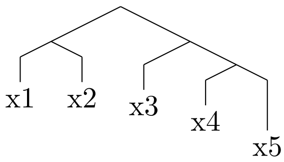
(a') Es gibt Präfixcode $C = \{w_1, ..., w_n\} \subseteq A^*$ mit $|A| = r$ und $l(w_i) = l_i$. Aus Satz (1.2.5) folgt dann: (a') $\Leftrightarrow$ (b). Es ist leicht zu zeigen, dass (a') $\Leftrightarrow$ (a) gilt.

- Wurzelbaum $r = 3$,$A = \{0, 1, 2\}$, Präfixcode $C = \{00, 01, 02, 1, 20, 21\}$



Beispiel

$r = 2$, $l_1 = l_2 = l_3 = 2$, $l_4 = 3$, $l_5 = 4$



2.3.6 Hauptsatz der Suchtheorie

Gegeben:
- natürliche Zahl $N \geq 1$ (Größe des Suchbereiches)
- natürliche Zahl $r \geq 2$ (Anzahl der Testausgänge)
- Wahrscheinlichkeitsverteilung $(p_1, ..., p_N)$ wobei p_i = Wahrscheinlichkeit, dass i-tes Objekt gesucht wird.

Gesucht: Wurzelbaum $T \in \mathcal{T}(N, r)$ mit Blättern $x_1, ..., x_N$ derart, dass $\bar{L}(T) = \sum_{i=1}^{N} p_i \cdot l(x_i)$ ein Minimum ist. Dabei ist $\bar{L}(T)$ die durchschnittliche Tiefe des Suchbaumes. Wir suchen also
$L_r^{min}(p_1, ..., p_N) := min\{\bar{L}(T), T \in \mathcal{T}(N, r)\}$

Dann gilt:

(a) $H_r(p_1, ..., p_N) \leq L_r^{min}(p_1, ..., p_N) \leq H_r(p_1, ..., p_N) + 1$

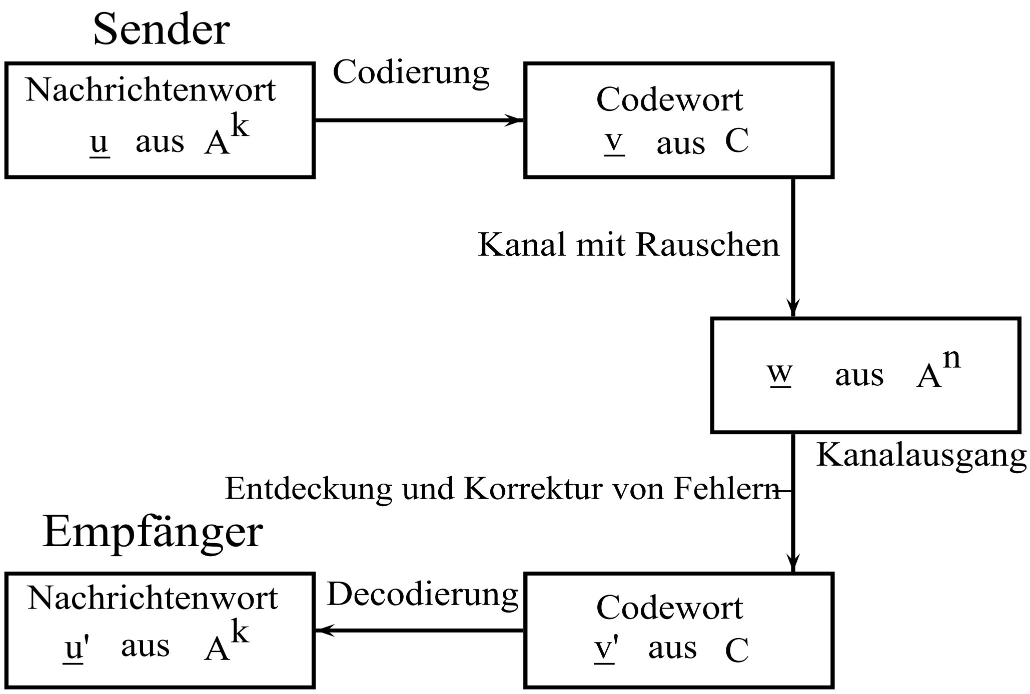
(b) Konstruktion eines optimalen Suchbaumes erfolgt mit dem Huffman Algo.

Beweis (a) folgt aus (2.3.5) und (2.2.6)
(b) folgt aus (2.3.5) und (2.2.7)

3 Kapitel III: Kanalkodierung

3.1 Entdecken und Korrigieren von Fehlern

3.1.1 Aufgabenstellung der Kanalkodierung



1. Der zu sendende bereits kodierte Text $T \in A^*$ wird in Wörter(=Blöcke) der Länge k zerlegt :
   $T = \underline{u}_1, \underline{u}_2, \underline{u}_3, ...$ mit $\underline{u}_i \in A^k$

2. Kanalkodierung ist injektive Abbildung:
   $f : A^k \to A^n$
   $\underline{u} \mapsto \underline{v}$
   Nachritenwort $\mapsto$ Codewort
   $C := \{\underline{v} = f(\underline{u}) | \underline{u} \in A^k\}$ Menge aller Codewörter

3. Codewort $\underline{v} = f(\underline{u}) \in C \subseteq A^n$ wird gesendet, aber $\underline{w} \in A^n$ wird empfangen.

Decodierer wählt Codewort $v' \in C$ mit Abstand $(\underline{w}, v') \to min$
Dann bestimmt er das Nachrichtenwort $u' = f^{-1}(v')$

Ziel möglichst $u' = \underline{u}$, $\underline{v} = v'$

3.1.2 Blockcodes und Hammingabstand

Voraussetzung

A sei ein Alphabet mit $|A| = r \geq 2$
$n \geq 2$ natürliche Zahl

Definition 1

$C \subseteq A$ wird Blockcode (kurz Code) der Länge n über A genannt. Die Wörter aus C heißen Codewörter.

Bemerkung

$\underline{w} \in A^n$ $\underline{w} = (w_1, ..., w_n)$ mit $w_i \in A$

Definiton 2

(a) Für Wörter $\underline{w} = (w_1, ..., w_n)$, $\underline{u} = (u_1, ..., u_n)$ aus A^n sei:
$d(\underline{w}, \underline{u}) = |\{i | w_i \neq u_i\}|$
der Hammingabstand von $\underline{w}$ und $\underline{u}$.

(b) Für einen Code $C \subseteq A^n$ sei:
$d(C) = min_{\underline{u},\underline{v} \in C, \underline{u} \neq \underline{v}} d(\underline{u}, \underline{v})$ der Abstand von C

Vorlesung 7

Satz

Der Hammingabstand ist eine Metrik auf A, d.h. für $\underline{u}, \underline{v}, \underline{w} \in A^n$ gilt:

(M1) $d(\underline{u}, \underline{v}) \geq 0$
$d(\underline{u}, \underline{v}) = 0 \Leftrightarrow \underline{u} = \underline{v}$

(M2) $d(\underline{u}, \underline{v}) = d(\underline{v}, \underline{u})$

(M3) $d(\underline{u}, \underline{v}) \leq d(\underline{u}, \underline{w}) + d(\underline{w}, \underline{v})$

Beweis

- M1, M2 offensichtlich
- (M3) $\underline{u} = (u_1, ..., u_n)$ $\underline{v} = (v_1, ..., v_n) \Rightarrow u_i \neq v_i \Rightarrow u_i \neq w_i$ oder $v_i \neq w_i$

- $d(\underline{u},\underline{v}) = |\{i|u_i \neq v_i\}| = |\{i|u_i \neq w_i\} \cup \{i|v_i \neq w_i\}| \leq |\{i|u_i \neq w_i\}| + |\{i|v_i \neq w_i\}| = d(\underline{u},\underline{w}) + d(\underline{v},\underline{w})$
- qed

Beispiel: 2-facher Wiederholungscode

- $C = \{\underline{v} = \underline{uuu}|\underline{u} \in A^k\} \subseteq A^n, n = 3 \cdot k, k \geq 1$
- Nachrichtenwort $\underline{u} \mapsto$ Codewort $\underline{uuu}$
- Informationsrate $\frac{k}{n} = \frac{1}{3}$
- $\underline{v} = \underline{uuu}$, $v' = \underline{u'}\underline{u'}\underline{u'}$
  $v \neq v' \Rightarrow u \neq u' \rightarrow d(v,v') = 3 \cdot d(u,u') \geq 3$
- $d(C) \geq 3$

3.1.3 Abstandsmethode zur Fehlerkorrektur

Gegeben

$C \subseteq A^n$
senden Codewort $\underline{v} \in C \rightarrow_{Kanal}$ empfangenes Wort $\underline{w} \in A^n \rightarrow$ bestimme Codewort $v' \in C$ mit kleinstem Abstand zu $\underline{w}$ ($v' \in C$ mit $d(v',w) \rightarrow \min$)
Ziel: $v' = v$

Annahme

Bei der Kanalübertragung sind höchstens t Fehler aufgetreten, d.h. $d(\underline{w},\underline{v}) \leq t$
Dann gilt:
Ist $v = v'$, so ist $d(v',w) \leq d(v,w) \leq t$ ansonsten hätten wir nicht v' sondern v gewählt.
Also gilt für die Codewörter $v, v' \in C$:
$d(\underline{v},\underline{v'}) \leq d(\underline{v},\underline{w}) + d(\underline{v'},\underline{w}) \leq t + t = 2t$ und somit $d(C) \leq 2t$
Ist hingegen $d(C) \geq 2t+1$, so wird stets $v = v'$ gewählt, d.h. treten bei der Übertragung höchstens t Fehler auf, so werden diese erkannt und korrigiert.

3.1.4 Definition

Sei $C \subseteq A^n$

(a) C heißt t-fehlerkorrigierend, falls $d(C) \geq 2t + 1$

(b) C heißt t-fehlererkennend, falls $d(C) \geq t + 1$

3.1.5 Zielstellung der Kanalkodierung

Suchen $C \subseteq A^n$ mit $d(C)$ groß (gute Fehlerkorrektur) und $|C|$ groß (viele Nachrichtenwörter kodierbar). Dabei ist A und n gegeben.
$M(r,n,t) := \max\{|C||C \subseteq A^n, |A| = r, d(C) \geq 2t+1\}$
sei die maximale Mächtigkeit eines t-fehlerkorrigierenden Codes über einem Alphabet A mit r Buchstaben.

3.1.6 Hammingschranke, perfekte Codes

Definition 1

$\underline{a} \in A^n$, $k, t > 0$ natürliche Zahlen

(a) $S_k(\underline{a}) = \{\underline{x} \in A^n | d(\underline{a}, \underline{x}) = k\}$ Sphäre

(b) $B_t(\underline{a}) = \{\underline{x} \in A^n | d(\underline{a}, \underline{x}) \leq t\}$ Kugel, Ball

Lemma

Ist $|A| = r \geq 2$ und $k, t \geq 0$, so gilt:

(1) $B_t(\underline{a}) = \bigcup\limits_{k=0}^{t} S_t(\underline{a})$

(2) $|S_k(\underline{a})| = \binom{n}{k}(r-1)^k$

(3) $|B_t(\underline{a})| = \sum\limits_{k=0}^{t} \binom{n}{k}(r-1)^k$

Beweis

(a) $d(\underline{a}, \underline{x})$ ist ganzzahlig und ≥ 0

(b) $d(\underbrace{\underline{a}}_{fest}, \underbrace{\underline{x}}_{variabel}) = k$

- für k Stellen ist $a_i \neq x_i$ sonst $x_i = a_i$
- $x_i \neq a_i$ ergibt r-1 Möglichkeiten, also insgesamt $(r-1)^k$
- $\binom{n}{k}$ = Anzahl der Möglichkeiten die k Fehlerstellen zu wählen
- $|\{\underline{x} \in A^n | d(\underline{x}, \underline{a}) = k\}| = \binom{n}{k}(r-1)^k$

(1) folgt aus (a) und (b) und der Tatsache dass die Sphären $S_k(\underline{a})$ für $k = 0, ..., t$ paarweise disjunkt sind. $|A \cup B| = |A| + |B|$ falls $A \cap B = \emptyset$

Satz1

Für $C \subseteq A^n$ sind folgende Aussagen äquivalent:

(a) C ist t-fehlerkorrigierend, d.h. $d(C) \geq 2t+1$

(b) Die Kugeln $B_t(\underline{a})$ mit $\underline{a} \in C$ sind paarweise disjunkt

Beweis

(a)⇒(b)

Indirekt: Annahme: es gibt $\underline{a}, \underline{b} \in C$ mit $B_t(\underline{a}) \cap B_t(\underline{b}) \neq \emptyset$, also es gibt ein $\underline{v} \in A^n$ mit $\underline{v} \in B_t(\underline{a}) \cap B_t(\underline{b})$
Dann ist $d(\underline{a}, \underline{b}) \leq d(\underline{a}, \underline{v}) + d(\underline{v}, \underline{b}) \leq t + t = 2 \cdot t$
Widerspruch zu (a)

(b)⇒(a)

Indirekt: Angenommen $d(C) < 2t+1 \Rightarrow d(C) \leq 2t$. Dann gibt es 2 Codewörter $\underline{a}$ und $\underline{b} \in C$ mit $k := d(\underline{a}, \underline{b}) \leq 2t$ und $\underline{a} \neq \underline{b}$
Es gibt also k Stellen $i \in \{1, .., n\}$ mit $a_i \neq b_i$.
O.B.d.A: seien dies die Stellen $1, ..., k$
Es gilt also $a_1 \neq b_1, ..., a_k \neq b_k$ und $a_{k+1} = b_{k+1}, ..., a_n = b_n$. Beachte $k \leq 2 \cdot t$.

$$\begin{array}{ccccccccc} \underline{a} & = (& a_1, & a_2, & ..., & a_k, & a_{k+1}, & ..., & a_n &) \\ & & \neq & \neq & \neq & \neq & =_{2t} & = & = & \\ \underline{b} & = (& b_1, & b_2, & ..., & b_k, & b_{k+1}, & ..., & b_n &) \end{array}$$

⇒ also gilt: $a_i = b_i$ für $i \geq 2t+1$.
Dann sei v das Wort mit:

$$v_i = \begin{cases} a_i & i \leq t \\ b_i & i > t \end{cases}$$

ergibt somit:

$$\begin{array}{llll} \underline{a} = & (a_1, ..., a_t, & a_{t+1}, ..., a_{2t}, & a_{2t+1}, ..., a_n) \\ \underline{b} = & (b_1, ..., b_t, & b_{t+1}, ..., b_{2t}, & b_{2t+1}, ..., b_n) \\ \underline{v} = & (a_1, ..., a_t, & b_{t+1}, ..., b_{2t}, & b_{2t+1}, ..., b_n) \end{array}$$

Somit gilt $d(\underline{v}, \underline{a}) \leq t$ (höchstens die Stellen t+1 bis 2t verschieden) und $d(\underline{v}, \underline{a}) \leq t$ (höchstens die ersten t Stellen verschieden) also $\underline{v} \in B_t(\underline{a}) \cap B_t(\underline{b})$ Widerspruch zu (b), qed.

Satz 2: Hammingschranke

Sei $|A| = r \geq 2$, $n, t \geq 1$. Ist $C \subseteq A^n$ ein t-fehlerkorrigierender Code, d.h. $d(C) \geq 2t+1$ so gilt:

$$|C| \leq H(r, n, t) = \frac{r^n}{\sum\limits_{k=0}^{t} \binom{n}{k} (r-1)^k}$$

Beweis:

Aus Satz1 folgt: Die Kugeln $B_t(\underline{a})$ mit $\underline{a} \in C$ sind paarweise disjunkt. Somit gilt:
$r^n = |A^n| \geq |\bigcup\limits_{\underline{a}\in C} B_t(\underline{a})|$ (da $\bigcup\limits_{\underline{a}\in C} B_t(\underline{a}) \subseteq A^n$)
$= \sum\limits_{\underline{a}\in C} |B_t(\underline{a})|$ (wegen Disjunktheit)
$= \sum\limits_{\underline{a}\in C} \sum\limits_{k=0}^{t} \binom{n}{k} \cdot (r-1)^k$ (wegen Lemma)
$= |C| \sum\limits_{k=0}^{t} \binom{n}{k} \cdot (r-1)^k$
Daraus folgt:
$|C| \leq \frac{r^n}{\sum_{k=0}^{t} \binom{n}{k} (r-1)^k}$ qed.

Folgerung

Es gilt also $M(r,n,t) \leq H(r,n,t) = \frac{r^n}{\sum_{k=0}^{t} \binom{n}{k} (r-1)^k}$

Definition 2

Ein Code $C \subseteq A^n$ mit $|A| = r \geq 2$ heißt t-perfekt, falls gilt:
C ist t-fehlerkorrigierend und $|C| = H(r,n,t)$

Satz 3

Für $C \subseteq A^n$ und $t \geq 0$ sind äquivalent:

(a) C ist t-perfekt

(b) Die Kugeln $B_t(\underline{a})$ mit $\underline{a} \in C$ bilden eine Zerlegung von A^n (d.h. A^n disjunkte Vereinigung der $B_t(\underline{a})$)

Beweis

$(a) \Rightarrow (b)$

C sei t-perfekt. Dann ist C t-fehlerkorrigierend und aus Satz 1 folgt, dass $B_t(\underline{a})$ paarweise disjunkt sind. Aus $t \geq 0$ folgt $B_t(\underline{a}) \neq \emptyset$. Somit genügt zu zeigen:
$A^n = \bigcup\limits_{\underline{a}\in C} B_t(\underline{a})$
Angenommen das gilt nicht, dann gilt:
$\bigcup\limits_{\underline{a}\in C} B_t(\underline{a}) \subset A^n$
also :
$|\bigcup\limits_{\underline{a}\in C} B_t(\underline{a})| < |A^n| = r^n$

$\Rightarrow$(siehe Beweis von Satz 2)
$|C| < \frac{r^n}{\sum_{k=0}^{t} \binom{n}{k} (r-1)^k} = H(r,n,t)$
Widerspruch zu (a)

$(b) \Rightarrow (a)$

Aus (b) folgt wegen Satz 1, dass C t-fehlerkorrigierend ist. Weiterhin gilt $r = |A|$
$r^n = |A^n| =_{(b)} | \bigcup_{\underline{a} \in C} B_t(\underline{a})|$.
Weiter wie im Beweis von Satz 2, folgt:
$|C| = \frac{r^n}{\sum_{k=0}^{t} \binom{n}{k} (r-1)^k}$ qed.

3.2 Der 2. Hauptsatz von Shannon

Wir betrachten nun binäre Codes, d.h. $C \subseteq A^n$ mit $|A| = r = 2$. Dann setzen wir $A = Z_2$, also Z_2 ist Körper und Z_2^n Vektorraum über Z_2. Weiterhin sei $\log x = \log_2 x$

3.2.1 Informationsrate

Für einen Code $C \subseteq Z_2^n$ sei :
$I(C) = \frac{\log |C|}{n}$
die Informationsrate von C.

Bemerkung 1

Bei der Kanalkodierung betrachten wir die injektive Abbildung f mit:
$f : Z_2^k \to Z_2^n$
$\underbrace{\underline{u}}_{Nachrichtenwort} \mapsto \underbrace{\underline{v} = f(\underline{u})}_{Codewort}$
Dann ist $C = \{\underline{v} = f(\underline{u}) | \underline{u} \in Z_2^k\} \subseteq Z_2^n$ ein Code der Länge n über Z_2. Da f injektiv ist, gilt dann:
$|C| = |Z_2|^k = 2^k$. Dann ist:
$I(C) = \frac{\log 2^k}{n} = \frac{k}{n}$

Bemerkung 2

Ist $C \subseteq Z_2^n$, so ist $|C| \leq |Z_2^k| = 2^k$ und somit gilt:
$I(C) = \frac{\log |C|}{n} \leq \frac{\log 2^n}{n} = \frac{n}{n} = 1$

Ziel:

Suche Code $C \subseteq Z_2^n$ mit $I(C) \to 1$(groß oder nahe 1)

3.2.2 Fehlerwahrscheinlichkeiten

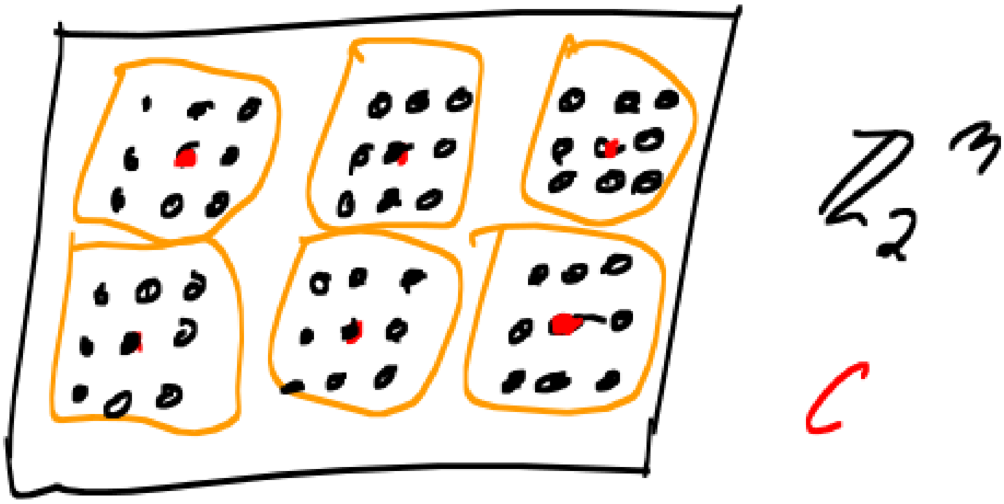
Es sei $F = (\underline{w}_1, ..., \underline{w}_m)$ eine Folge von Wörtern $\underline{w}_1, ..., \underline{w}_m \in Z_2^n$. Wir betrachten die Abbildung:
$m_F : Z_2^n \to \{\underline{w}_1, ..., \underline{w}_n, (?)\}$ mit:
$m_F(\underline{v}) = \begin{cases} \underline{w}_i & \text{falls } d(\underline{v}, \underline{w_i}) < d(\underline{v}, \underline{w_j}) \forall j \in \{1.., m\} - \{i\} \\ (?) & sonst \end{cases}$
Weiterhin sei $X = (X_1, ..., X_n)$ ein Zufallsvektor von n unabhängigen Bernoulli- verteilten Zufallsvariablen, d.h.
$P(X_i = 1) = p$ und $P(X_i = 0) = 1 - p$ mit $p \in [0, 1]$.
Die Zahl:
$p_F := \frac{1}{m} \sum_{i=1}^{m} P(m_F(\underline{w_i} + X) \neq \underline{w_i})$ ist dann Fehlerwahrscheinlichkeit der Folge F unter der Störung X bei Maximum-Likelihood-Decodierung m_F

Bemerkung 1

- $X = (X_1, ..., X_n)$ entspricht einem zufälligem Wert aus Z_2^n und beschreibt die 'Störung' im Kanal. Senden Wort $\underline{w}$ und empfangen Wort $\underline{w} + X$ (+: Addition modulo 2 in Z_2)
  Also $X_i = 1$ besagt, dass in der i-ten Komponente ein Fehler auftritt.
- p_F ist unabhängig von der Reihenfolge der Wörter in F
- Ist $C \subseteq Z_2$ in Code mit $C = \{\underline{w_1}, ..., \underline{w_m}\}$ also mit m Codewörtern, so heißt $p_C = p_F$ mit $F = \{\underline{w}_1, ..., \underline{w}_m\}$ die Fehlerwahrscheinlichkeit von C unter der Störung X bei M-L-Decodierung m_C.
- Ziel: p_c soll klein sein

Beispiel

Es sei $C \subseteq Z_2^n$ ein t-perfekter Code. Dann bilden die Kugeln $B_t(\underline{w})$ mit $\underline{w} \in C$ eine Zerlegung von Z_2^n. Somit gibt es zu jedem Wort $\underline{v} \in Z_2^n$ genau ein Codewort $\underline{w} \in C$ mit $d(\underline{v}, \underline{w}) \leq t$.



Sei nun $\underline{w} \in C$ ein Codewort und $\underline{x} \in Z_2^n$ ein beliebiges Wort (Störung).

Behauptung: $m_C(\underline{w} + \underline{x}) = \underline{w} \Leftrightarrow d(\underline{x}, 0) \leq t$

Beweis: Übungsaufgabe

Sei nun $X = (X_1, ..., X_n) \in Z_2^n$ ein zufälliges Wort, also ein Zufallsvektor von n unabhängigen Bernoulli-verteilten Zufallsgrößen zur Wahrscheinlichkeit p. Dann gilt:
$p_C = \frac{1}{|C|} \sum\limits_{\underline{w} \in C} P(m_C(\underline{w} + X) \neq \underline{w}) =_{sieheBeh} \frac{1}{|C|} \sum\limits_{\underline{w} \in C} P(d(X, 0) \geq t+1) = P(d(X, 0) \geq t+1)$
(da $P(d(X, 0) \geq t+1)$ nicht von $\underline{w}$ abhängt, $X = (X_1, ..X_n)$, $X_i = 0$ oder $X_i = 1$, $d(X, 0) =$ Anzahl Einsen in $X = \sum X_i$)
$= P(\sum X_i \geq t+1)$ ($Y = \sum X_i$ ist dann binomialverteilt)
$= P(Y \geq t+1) = \sum\limits_{k=t+1}^{n} P(Y = k)$
$= \sum\limits_{k=t+1}^{n} \binom{n}{k} p^k \cdot (1-p)^{n-k}$

3.2.3 Satz (2. Hauptsatz von Shannon 1948)

Es sei $p \in (0, \frac{1}{2})$, $0 < r < 1 + p \cdot \log p + (1-p) \cdot \log(1-p)$ und $\epsilon > 0$. Dann gibt es zu genügend großem n ein Code $C \subseteq Z_2^n$ mit:
$I(C) = \frac{\lfloor n \cdot r \rfloor}{n}$ und $p_C < \epsilon$

Beweis: siehe Literatur

Bemerkung

- p ist die Wahrscheinlichkeit dafür, dass bei der Übertragung an einer der n Stellen ein Fehler auftritt

- Fehler wird dann durch den Zufallsvektor $X = (X_1, ..., X_n)$ modelliert mit $P(X_i = 1) = p$ und $P(X_i = 0) = 1 - p$. Also statt Codewort $\underline{w}$ wird Wort $\underline{w} + X$ empfangen und mit $m_c(\underline{w} + X)$ korrigiert

- $f(p) = 1 + p \log p + (1 - p) \log(1 - p)$: obere Schranke
  für r z.B.:
  $f(\frac{1}{10}) \approx 0.53$
  $f(\frac{1}{100}) \approx 0.92$

- Ist also $p = \frac{1}{10}$, so können wir $r = 0.53$ wählen und $\epsilon > 0$ beliebig wählen. Dann gibt es zu hinreichend großem n einen Code $C \subseteq Z_2^n$ mit $I(C) = \frac{\lfloor n \cdot r \rfloor}{n}$ und $p_C < \epsilon$

n	10	100	1000
$\frac{\lfloor n \cdot r \rfloor}{n}$	0.5	$\frac{53}{100}$	$\frac{53}{100}$

- Der Beweis des Satzes ist nicht konstruktiv, d.h. er liefert kein Verfahren zur Konstruktion eines solchen Codes $C \subseteq Z_2^n$; er liefert aber eine Aussage über die Größenordnung von n.

4 Kapitel IV: lineare Codes

4.1 Einführung

Voraussetzung In diesem Abschnitt sei $K = GF(q)$ ein Körper mit q Elementen. Dann ist q eine Primzahlpotenz und K^n ein Vektorraum über K. Ist q eine Primzahl, so ist $K = Z_q$ (Restklassenring modulo q)

Beispiel $K = GF(5) = Z_5 = \{0, 1, 2, 3, 4\}$
Addition: + d.h. modulo 5
Multiplikation: $\cdot$ d.h. modulo 5
z.B.: $4 + 2 = 1$, $2 \cdot 4 = 3$
$-3 = x \Leftrightarrow x + 3 = 0 \Leftrightarrow x = 2$
$\frac{1}{4} = x \Leftrightarrow 4 \cdot x = 1 \Leftrightarrow x = 4$

Gauß-Jordan-Verfahren Lineares Gleichungssystem:
$\left\{\begin{matrix} x + 3y = 1 \\ x - 3y = 2 \end{matrix}\right\} \begin{pmatrix} 1 & 3 \\ 1 & -3 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$
$A\vec{x} = \vec{b}$
ergibt Lösung:$\vec{x} = \begin{pmatrix} 4 \\ 4 \end{pmatrix}$ (normaler Gauß aber mit mod 5)

Bemerkung 1 K^n ist ein Vektorraum(Zeilenvektoren). Sind dann $\underline{b}_1, ..., \underline{b}_d \in K^n$ Vektoren
und $\alpha_1, ..., \alpha_d \in K$ Skalare, so heißt:
$\underline{v} = \alpha_1 \cdot \underline{b}_1 + ... + \alpha_d \cdot \underline{b}_d$ Linearkombination der Vektoren $\underline{b}_1, ..., \underline{b}_d$, dann gilt:
$\underline{v} = (\alpha_1, ..., \alpha_1) \cdot \begin{pmatrix} \underline{b}_1 \\ ... \\ \underline{b}_d \end{pmatrix}$

Bemerkung 2 Für eine Vektormenge $B = \{\underline{b}_1, ..., \underline{b}_d\}$ sind folgende Bedingungen äquivalent:

(a) B ist linear unabhängig

(b) Kein Vektor $\underline{b} \in B$ ist Linearkombination der Vektoren aus $B - \{\underline{b}\}$

(c) Die Gleichung:
$\alpha_1 \cdot \underline{b}_1 + ... + \alpha_d \cdot \underline{b}_d = \underline{0}$ mit $\alpha_i \in K$ hat nur die triviale Lösung: $\forall i : \alpha_i = 0$

4.1.1 Definition

C heißt linearer Code der Länge n über K, falls $C \subseteq K^n$ ein linearer Unterraum ist,d.h. falls gilt:

U1 $\underline{0} \in C$

U2 $\underline{a}, \underline{b} \in C \Rightarrow \underline{a} + \underline{b} \in C$

U3 $\underline{a} \in C, \alpha \in K \Rightarrow \alpha \cdot \underline{a} \in C$

4.1.2 Definition

Für $\underline{x} = (x_1, ..., x_n) \in K^n$ sei:
$g(\underline{x}) = d(\underline{x}, \underline{0}) = |\{i \mid x_i \neq 0\}|$
das Gewicht von $\underline{x}$

4.1.3 Satz

Ist $C \subseteq K^n$ ein linearer Code, so gilt $d(C) = \min_{\underline{x} \in C, \underline{x} \neq 0} g(\underline{x})$

Beweis

$d(\underline{u}, \underline{v}) = d(\underline{u} - \underline{v}, \underline{0})$
Es sei $d = d(C) = \min_{\underline{a}, \underline{b} \in C, \underline{a} \neq \underline{b}} d(\underline{a}, \underline{b})$
$g := min_{\underline{x} \in C, \underline{x} \neq 0} g(\underline{x})$
zu zeigen: $d = g$

(1) Es gibt $\underline{a}, \underline{b} \in C$ mit $\underline{a} \neq \underline{b}$ und $d(\underline{a}, \underline{b}) = d$
$\Rightarrow \underline{x} = \underline{a} - \underline{b} \in C$ (da linearer Code) ,$\underline{x} \neq 0$
$\Rightarrow g \leq g(\underline{x}) = g(\underline{a} - \underline{b}) = d(\underline{a}, \underline{b}) = d$

(2) Es gibt ein $\underline{x} \in C$ mit $\underline{x} \neq 0$ und $g(\underline{x}) = g$
$\Rightarrow \underline{x} \in C, \underline{0} \in C$ (da linearer Code ,$\underline{x} \neq 0$)
$\Rightarrow d \leq d(\underline{x}, \underline{0}) = g(\underline{x}) = g$

(3) aus (1) und (2) folgt $g = d$ qed.

4.1.4 Generatormatrix

Es sei $C \subseteq K^n$ ein linearer Code. Dann besitzt C eine Basis $B = \{\underline{b}_1, ..., \underline{b}_d\}$ bestehend aus d Vektoren aus K^n, d.h. es gibt:

(B1) $\underline{v} \in C \Leftrightarrow \underline{v} = \alpha_1 \cdot \underline{b}_1 + ... + \alpha_d \cdot \underline{b}_d$ mit $\alpha_i \in K$

(B2) B ist linear unabhängig.
Dann ist $d = \dim(B)$. Bilden die Matrix $G = (\underline{b}_1, ..., \underline{b}_d)^T \in K^{d,n}$
Die Matrix G heißt Generatormatirx von C und es gelten die folgenden Aussagen:

(G1) $C = \{\underline{v} \in K^n \mid \underline{v} = \underline{x} \cdot G, \underline{x} \in K^d\}$

(G2) $\mathrm{rg}(G) = d$

(G3) $\underline{0} = \underline{x} \cdot G \Leftrightarrow \underline{x} = \underline{0}$

(G4) die Abbildung $\underline{x} \in K^d \mapsto \underline{v} = \underline{x} \cdot G \in C$ ist bijektive Abbildung von K^d in C

(G5) $|C| = |K^d| = q^d$ $(K = GF(q), |K| = q)$

(G6) $d(C) = \min_{\underline{v} \in C, \underline{v} \neq \underline{0}} g(\underline{v}) = \min_{\underline{x} \in K^d, \underline{x} \neq 0} g(\underline{x} \cdot G)$

Beweis Aus Vorlesung Mathe1+2 folgt: C besitzt Basis B, für die dann (B1),(B2) gilt.
Ist nun $\underline{x} = (\alpha_1, ..., \alpha_d) \in K^d$ so gilt: $\underline{v} = \underline{x} \cdot G = \alpha_1 \cdot \underline{b}_1 + ... + \alpha_d \cdot \underline{b}_d$
Somit folgt (G1) direkt aus (B1), aus (B2) folgt (G2) und (G3) folgt aus (B2).

Beweis von G4 (bijektiv=surjektiv+ injektiv)
Aus (G1) folgt: C ist Bild der Abbildung, also ist die Abbildung surjektiv. Zum Beweis der Injektivität müssen wir zeigen:
$\underline{x} \neq \underline{x}' \Rightarrow \underline{x} \cdot G \neq \underline{x}' \cdot G$ bzw: $\underline{x} \cdot G = \underline{x}' \cdot G \Rightarrow \underline{x} = \underline{x}'$

$\underline{x} \cdot G = \underline{x}' \cdot G \Rightarrow \underline{x} \cdot G - \underline{x}' \cdot G = 0$
$\Rightarrow (\underline{x} - \underline{x}') \cdot G = 0$
$\Rightarrow_{(G3)} \underline{x} - \underline{x}' = 0$
$\Rightarrow \underline{x} = \underline{x}'$
(G5) folgt aus (G4) und (G6) folgt aus (4.1.3) sowie (G1)+(G3)
qed.

Folgerung

Ist $C \subseteq K^n$ ein linearer Code über $K = GF(q)$, so gilt:
$|C| = q^{\dim(C)}$

Beispiel

$K = GF(2) = Z_2 = \{0, 1\}, n = 5, d = k = 3$

$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$ Zeilen sind linear unabhängig, $rg(G) = 3 = d$

$C = \{\underline{v} = \underline{x} \cdot G \mid \underline{x} \in K^3\}$: linearer Code, $C \subseteq K^5$, mit Generatormatrix G

Codewörter

$\underline{v} = \underline{x} \cdot G = x_1 \cdot (1,0,0,0,1) + x_2 \cdot (0,1,0,1,0) + x_3 \cdot (0,0,1,1,1)$ mit $\underline{x} = (x_1, x_2, x_3)$
$\Rightarrow \underline{v} = (\underline{x}, \underline{y})$ mit $\underline{y} = x_1 \cdot (0,1) + x_2 \cdot (1,0) + x_3 \cdot (1,1) = (x_2 + x_3, x_1 + x_3)$
$\underline{v} = (x_1, x_2, x_3, x_2 + x_3, x_1 + x_3)$

Abstand

$d(C) = \min_{\underline{v} \in C - \{\underline{0}\}} g(\underline{v})$
$\underline{v} = (\underline{x}, \underline{y}) : g(\underline{v}) = g(\underline{x}) + g(\underline{y}) \geq 2$ (falls $\underline{x} \neq \underline{0}$)
$d(C) \geq 2$ (es gilt sogar $d(C) = 2$)
Also C ist 1-fehlererkennend, Korrekturrate ist 0

Fehlerkorrektur

$$\underbrace{\underline{x} \in K^3}_{Nachrichtenwort} \quad \mapsto \underbrace{\underline{v} = \underline{x} \cdot G}_{Codewort} = (\underline{x}, \underline{y}) \in C \subseteq K^5$$

Empfangen: $\underline{w} = 10111 \in K^5 (\underline{x} = 101, \underline{y} = 10, \underline{w}$ ist also kein Codewort)
suchen: Codewort $\underline{v} \in C$ mit $d(\underline{w}, \underline{v}) \to \min$
$d(\underline{w}, \underline{v}) = g(\underline{w} - \underline{v}) = g(\underline{w} - \underline{x} \cdot G)$
Lösung(en):
$\underline{x} = 101 : \underline{v} = 10110 \to d(\underline{v}, \underline{w}) = 1$
$\underline{x} = 001 : \underline{v} = 00111 \to d(\underline{v}, \underline{w}) = 1$

4.1.5 Kontrollmatrix

Es sei $H \in K^{(n,m)}$ und es sei :
$C = \{\underline{v} \in K^n \mid \underline{v} \cdot H = \underline{0}\}$
Dann gilt:

(K1) $C \subseteq K^n$ ist linearer Code

(K2) $\dim(C) = n - \mathrm{rg}(H)$

(K3) $|C| = q^{n - rg(H)}$ $(K = GF(q))$

Beweis von (K1) müssen (U0)-(U2) zeigen:

zu (U0): $\underline{0} \cdot H = \underline{0} \Rightarrow \underline{0} \in C$

zu (U1): $\underline{a}, \underline{b} \in C \Rightarrow \underline{a} \cdot H = \underline{0}, \underline{b} \cdot H = \underline{0}$
$\Rightarrow (\underline{a} + \underline{b}) \cdot H = \underline{a}H + \underline{b}H = \underline{0}$
$\Rightarrow \underline{a} + \underline{b} \in C$

zu (U2): $\underline{a} \in C, \alpha \in K \Rightarrow \underline{a}H = \underline{0} \to (\alpha \cdot \underline{a})H = \alpha \cdot (\underline{a} \cdot H) = \alpha \cdot \underline{0} = \underline{0}$

Beweis von (K2): siehe lineare Algebra

Beweis von (K3): folgt aus (K2) und (4.1.5)

Bemerkung 1 Die Matrix H heißt Kontrollmatrix von C

Bemerkung 2 Jeder lineare Code $C \subseteq K^m$ besitzt eine Kontrollmatrix.

4.2 Hamming Codes

4.2.1 Kontrollmatrix und Abstand

Es sei $K = GF(q)$. Für einen linearen Code:
$C = \{\underline{v} \in K^n \mid \underline{v} \cdot H = \underline{0}\}$
mit $H \in K^{(n,m)}$ und $d \geq 2$ sind folgende Bedingungen äquivalent:

(a) $d(C) \geq d$

(b) je $d-1$ Zeilen von H sind linear unabhängig

Beweis

- $H = \begin{pmatrix} \underline{a}_1 \\ ... \\ \underline{a}_n \end{pmatrix}$ mit $\underline{a}_i \in K^m$
- $\underline{v} \cdot H = v_1 \cdot \underline{a_1} + ... + v_n \cdot \underline{a_n}$ mit $\underline{v} = (v_1, ..., v_n)$
- $C \subseteq K^n$ ist linearer Code und aus Satz (4.1.3) folgt:
  $d(C) = \min_{\underline{v} \in C - \{\underline{0}\}} g(\underline{v})$

Beweis (a) $\Rightarrow$(b)

Sei $d(C) \geq d$. Dann ist $g(\underline{v}) \geq d$ für alle $\underline{v} \in C, \underline{v} \neq \underline{0}$
Angenommen (b) gilt nicht. Dann besitzt H $d-1$ linear abhängige Zeilen, etwa $\underline{a_1}, ..., \underline{a_{d-1}}$.
Dann gibt es Skalare mit $v_1, ..., v_{d-1} \in K$ mit:
$v_1 \cdot \underline{a}_1 + ... + v_{d-1} \cdot \underline{a}_{d-1} = \underline{0}$ und v_i nicht alle 0. Dann ist $\underline{v} = (v_1, ..., v_{d-1}, 0, .., 0) \in K^n$ ein Wort mit $\underline{v} \neq \underline{0}$ und $\underline{v} \cdot H = \underline{0}$.
Also ist $\underline{v} \in C, \underline{v} \neq \underline{0}$ und $g(\underline{v}) \leq d-1$, Widerspruch zu (a).

Beweis (b) $\Rightarrow$(a) (indirekt)

Seien je $d-1$ Zeilen von H linear unabhängig. Angenommen $d(C) \leq d-1$. Dann gibt es ein Codewort $\underline{v} \in C, \underline{v} \neq \underline{0}$ mit $g(\underline{v}) = k \leq d-1$, also etwa
$\underline{v} = (v_1, ..., v_n)$ mit $v_1 \neq 0, ..., v_k \neq 0, v_{k+1} = 0, ..., v_n = 0$. Beachte $k \geq 1$, da $\underline{v} \neq 0$. Da $\underline{v} \in C$ ist, gilt dann :

$\underline{0} = \underline{v} \cdot H = v_1 \cdot \underline{a}_1 + ... + v_n \cdot \underline{a}_n =$
$v_1 \cdot \underline{a}_1 + ... + v_k \cdot \underline{a}_k$.
Woraus folgt: die k Zeilen $\underline{a}_1, ..., \underline{a}_k$ sind linear abhängig, ein Widerspruch zu (b), da $k \leq d - 1$

4.2.2 Satz (Hemming 1950)

Sei $K = GF(q)$ und $r \leq 2$. Weiterhin sei $n = \frac{q^r-1}{q-1}$ und $k = n - r$
Dann gibt es einen linearen Code mit folgenden Eigenschaften:

(a) $\dim(C) = k$

(b) C ist 1-perfekt, d.h. $d(C) \geq 3$ und $|C| = H(q, n, 1)$

Beweis

Beschreiben C durch Kontrollmatrix H , d.h. $C = \{\underline{v} \mid \underline{v} \cdot H = \underline{0}\}$ mit $H \in K^{(n,r)}$

K^r besteht aus q^r vielen Wörtern (da $q = |K|$ ist), also gilt für $M = K^r - \{\underline{0}\}$:
$|M| = q^r - 1$

Für $\underline{a}, \underline{b} \in M$ definieren wir eine Relation $\sim$ mit:
$\underline{a} \sim \underline{b} \Leftrightarrow \underline{a}, \underline{b}$ sind linear abhängig
$\Leftrightarrow \underline{a}$ ist Vielfaches von $\underline{b}$
$\Leftrightarrow \underline{b}$ ist Vielfaches von $\underline{a}$

Dann ist $\sim$ eine Äquivalenzrelation auf M, d.h. es gilt:

(1) $\underline{a} \sim \underline{a}$ (reflexiv)

(2) $\underline{a} \sim \underline{b} \Rightarrow \underline{b} \sim \underline{a}$ (symetrisch)

(3) $\underline{a} \sim \underline{b}, \underline{b} \sim \underline{c} \Rightarrow \underline{a} \sim \underline{c}$ (transitiv)

Für die zu $\underline{a}$ gehörenden Äquivalenzklassen gilt dann:
$[\underline{a}] :=_{def} \{\underline{b} \mid \underline{a} \sim \underline{b}\}$

Dann gilt:

(4) $[\underline{a}] \cap [\underline{b}] \neq \emptyset$ oder $[a] = [b]$

(5) $[\underline{a}] = [\underline{b}] \Leftrightarrow \underline{a} \sim \underline{b}$

offenbar gilt dann auch:
$[\underline{a}] = \{\underline{b} \in K^r \mid \underline{b} = \alpha \cdot \underline{a}, \alpha \in K - \{0\}\}$
und somit ist $|[\underline{a}]| = |K - \{0\}| = q - 1$

Die Äquivalenzklassen haben alle die Mächtigkeit $q-1$ und bilden eine Zerlegung von $M = K^r - \{\underline{0}\}$
Da $|M| = q^r - 1$ ist, gibt es somit:
$n = \frac{q^r-1}{q-1}$
viele Äquivalenzklassen. Wählen aus jeder der n Äquivalenzklassen einen Vektor und erhalten dann n Wörter (Zeilenvektoren)
$\underline{a}_1, .., \underline{a}_n \in K^r$, wobei keine zwei dieser Zeilen linear abhängig sind.

Da die Einheitsvektoren $\underline{e}_1, ..., \underline{e}_n \in K^r$ zu verschiedenen Äquivalenzklassen gehören, können wir o.B.d.A wählen: $\underline{a}_i = \underline{e}_i$

Dann setzen wir $H = \begin{pmatrix} \underline{a}_1 \\ ... \\ \underline{a}_n \end{pmatrix} \in K^{(n,r)}$

Dann ist $\text{rg}(H) = r$ und je 2 Zeilen von H sind linear unabhängig.

Setzen $C = \{\underline{v} \in K^n \mid \underline{v} \cdot H = \underline{0}\}$. Damit ist $C \subseteq K^n$ ein linearer Code mit $\dim(C) = n - \text{rg}(H) = n - r = k$ (siehe 1.6) und $d(C) \geq 3$ (siehe 2.1)

Aus (1.6) folgt:
$|C| = q^{\dim(C)} = q^k = q^{n-r} = \frac{q^n}{q^r} = \frac{q^n}{1+n\cdot(q-1)} = H(q,n,1)$

Damit ist (4.2.2) bewiesen.

4.2.3 Bemerkungen

Die in Satz (4.2.2) konstruierten 1-perfekten Codes $C \subseteq K^n$ heißen Hamming Codes, kurz:
$C = \text{Ham}_q(n,k)$ wobei $q = |K|, K = GF(q)$, $k = \dim(C)$, $C \subseteq K^n$
Diese Codes existieren nur für $n = \frac{q^r-1}{q-1}$ und $k = n - r$ mit $r \geq 2$ beliebig.

Beispiel

- $K = GF(q) = Z_2$, $q = 2$, $r = 3$, $n = \frac{q^r-1}{q-1} = 7$, $k = n - r = 4$
- $C = \text{Ham}_2(7,4) = \{\underline{v} \in K^7 \mid \underline{v} \cdot H = \underline{0}\}$
- Kontrollmatrix $H \in K^{(n,r)} = K^{(7,3)}$, besteht aus $n = 7$ Zeilen aus $K^r = K^3$ etwa:
- $H = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$

- $d(C) \geq 3$, $|C| = q^k = 2^4 = 16$, C ist 1-perfekt

4.2.4 Satz

Es sei $C \subseteq A^n$ ein t-perfekter Code der Länge n über dem Alphabeth A mit $|A| = q$, wobei q ein Primzahlpotenz ist. Ist $|C| \geq 3$ so gilt:

(1) $n = \frac{q^r-1}{q-1}$ für ein $r \geq 2$ und $t = 1$ oder

(2) $n = 23, t = 3$ und $q = 2$ oder

(3) $n = 11, t = 2$ und $q = 3$

Beweis: siehe Literatur

Bemerkung

Es wird in dem Satz nicht vorausgesetzt das A ein Körper ist. Beispiel für (1) sind die Hamming Codes, für (2) und (3) die Golay Codes.

4.2.5 Reed-Solomon-Codes

Bemerkung werden bei der Fehlerkorrektur von Compact Discs verwendet

Voraussetzungen $K = GF(q) = \{0, 1, a_1, ..., a_{q-2}\}$ mit $q \geq 2$ Primzahlpotenz

Vandermonde- Matrix Sind $x_1, ..., x_n \in K$ so heißt die Matrix

$$V = \begin{pmatrix} 1 & x_1 & x_1^2 & ... & x_1^{n-1} \\ ... & ... & ... & ... & ... \\ 1 & x_n & x_n^2 & ... & x_n^{n-1} \end{pmatrix} \in K^{n,n}$$

Vandermonde Matrix $V = V(x_1, ..., x_n)$. Dann gilt: $\det(V) = \prod\limits_{1 \leq i < j < n} (x_i - x_j)$.

Sind also $x_1, ..., x_n$ paarweise verschieden, so ist $\det(V) \neq 0$ und die Zeilen (bzw. Spalten) von V linear unabhängig

Reed-Solomon-Codes $C = C_d$ mit $d \geq 3$

Betrachten die Matrix:

$$H = \begin{pmatrix} 0 & 0 & 0 & ... & 0 & 1 \\ 1 & 0 & 0 & ... & 0 & 0 \\ 1 & 1 & 1 & ... & 1 & 1 \\ 1 & a_1 & a_1^2 & ... & a_{q-2}^{d-3} & a_{q-2}^{d-2} \\ ... & ... & ... & ... & ... & ... \\ 1 & a_1 & a_1^2 & ... & a_{q-2}^{d-3} & a_{q-2}^{d-2} \end{pmatrix}$$

setzen: $C = \{\underline{v} \in K^n \mid \underline{v} \cdot H = \underline{0}\}$ $n = q + 1$

Dann gilt:

- $H \in K^{(q+1,d-1)}$
- $\mathrm{rg}(H) = d - 1$
- Je $d - 1$ Zeilen sind linear unabhängig

daraus folgt:

- $C \subseteq K^n$ ist linearer Code mit
- $\dim(C) = n - \mathrm{rg}(H) = n - d + 1 = q + 2 - d$
- $|C| = q^{\dim(C)} = q^{q+2-d}$
- Informationsrate:
  $I(C) := \frac{\log_q |C|}{n} = \frac{q+2-d}{q+1} = 1 + \frac{1-d}{q+1}$

Also $I(C)$ nahe 1 für große q

Beispiel $q = 2^8$, $d = 11$, $C = C_d$
$n = q + 1 = 257$, $C \subseteq K^{257}$
$\dim(C) = n - d + 1 = 257 - 10 = 247$

- $d(C) \geq 11$ (C ist 5 fehlerkorrigierend)
- $I(C) = \frac{258-11}{257} = 1 - \frac{10}{257}$
- $GF(2^8)$ ist Vektorraum der Dimentsion 8 über $GF(2)$
  also $GF(2^8) \cong GF(2)^8$
  Wir können also jedes Wort der Länge 8 (Zeilenvektor mit 8 Komponenten) über diesen Körper $GF(2) = Z_2$ darstellen
- dann ist jedes Codewort $\underline{v} \in C \subseteq K^{257}$ darstellbar als 0,1 Wort der Länge $8 \cdot 257 = 2056$, etwa:
  $\underline{v} = (v_1^{(1)}, ...v_1^{(8)}, ..., v_{257}^{(1)}, ..., v_{257}^{(8)})$
- somit entspricht C also einem Code $C' \subseteq GF(2)^{2056}$

Beh: C' kann bis zu 33 aufeinanderfolgende Fehler korrigieren (burst error)

Bew: Die 33 aufeinaderfolgende Fehler in $\underline{v} \in C'$ treten in höchstens 5 aufeinanderfolgender 8er Blöcken auf. Da der ursprüngliche Code aber 5-fehlerkorrigierend ist, kann C' diese 33 aufeinanderfolgenden Fehler korrigieren. q.e.d

Bem: wollte man einen 33-fehlerkorrigierenden Code konstruieren, würde die Informationsrate wesentlich schlechter sein.

4.3 Football Pools

4.3.1 Problemstellung

Gegeben

- n natürliche Zahl: (= Anzahl der Fußballspiele)

- $Z_3 = \{0,1,2\}$: (= Menge der Spielergebnisse)
- Z_3^n: (= Menge aller möglichen Tipps= Spielergebnisse der n Spiele)
- $\underline{s} \subseteq Z_3^n$: (=Siegertipp = tatsächlicher Spielausgang der n Spiele)

Definition

Ein Tipp $\underline{w} \in Z_3^n$ gewinnt den $(r+1)$-ten Preis, falls gilt: $d(\underline{w}, \underline{s}) = r$

Gesucht

- Eine Menge $C \subseteq Z_3^n$ von Tipps, die uns immer wenigstens den $(r+1)$-ten Preis garantieren,d.h. für die gilt:
  $\forall \underline{s} \in Z_3^n, \exists \underline{w} \in C :$ mit $d(\underline{s}, \underline{w}) \leq r$
  Man sagt dann, dass C den covering radius r hat.
- $K_3(n,r) := \min\{|C| \;\; | \; C \subseteq Z_3^n \text{ hat covering radius } r\}$

Beispiel:

- $(n = 4, r = 1)$ $C \subseteq Z_3^4$ besteht aus 9 Wörtern:
  $0000, 1101, 0112, 1210, 0221, 2011, 1022, 2120, 2202$
  Dann hat C den covering radius $r = 1$. Also gilt:
  $K_3(4,1) \leq |C| = 9$
- $\underline{s} = 1111$, $\underline{w} = 1101$, $d(\underline{s}, \underline{w}) \leq 1 = r$
- $\forall \underline{s} \in Z_3^n \exists \underline{w} \in C$ mit $d(\underline{w}, \underline{s}) \leq 1 = r$

Bemerkung

$C \subseteq Z_3^n$ hat covering radius $r = 0 \Leftrightarrow C = Z_3^n$
Also gilt: $K_3(n,0) = 3^n$

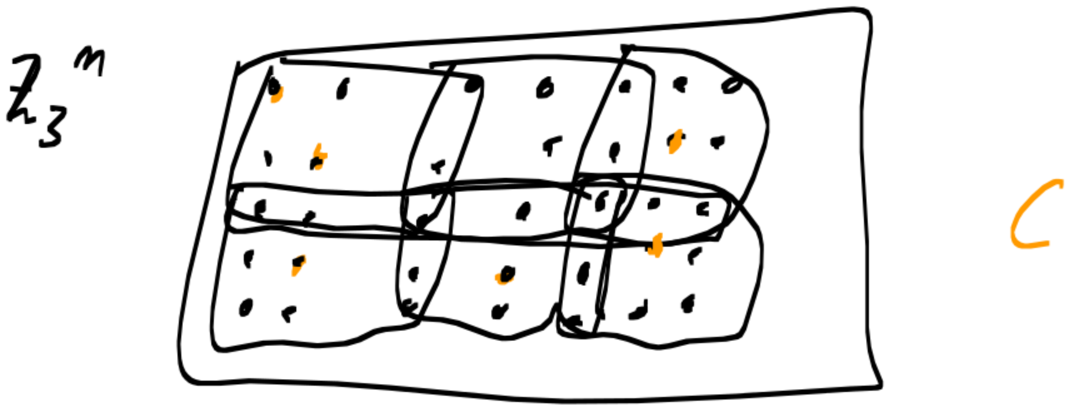
4.3.2 Lemma

Für eine Menge $C \subseteq Z_3^n$ sind folgende Bedingungen äquivalent:

(a) C hat covering radius r

(b) Die Kugeln $B_r(\underline{a}) = \{\underline{w} \in Z_3^n | d(\underline{w}, \underline{a}) \leq r\}$ mit $\underline{a} \in C$ Bilden eine Überdeckung von Z_3^n, d.h. $Z_3^n \subseteq \bigcup\limits_{\underline{a} \in C} B_r(\underline{a})$

Beweis



$C \subseteq Z_3^n$ hat covering radius r $\Leftrightarrow_{def} \forall \underline{s} \in Z_3^n \exists \underline{a} \in C$ mit $d(\underline{a}, \underline{s}) \leq r \Leftrightarrow \forall \underline{s} \in Z_3^n \exists \underline{a} \in C$ mit $\underline{s} \in B_r(\underline{a}) \Leftrightarrow Z_3^n \subseteq \bigcup\limits_{\underline{a} \in C} B_r(\underline{a})$

4.3.3 Satz

Es sei $C \subseteq Z_3^n$ eine Menge mit covering radius $r \geq 1$
Dann ist:
$|C| \geq \frac{3^n}{\sum\limits_{k=0}^{r} \cdot \binom{n}{k} \cdot 2^k} =: H(q = 3, n, t = r)$
Somit gilt:
$K_3(n, r) \geq H(3, n, r)$

Beweis

Es sei $C \subseteq Z_3^n$ Menge mit covering radius $r \geq 1$. Aus (4.3.2) folgt:
$Z_3^n \subseteq \bigcup\limits_{\underline{a} \in C} B_r(\underline{a})$. Mit Hilfe von Lemma (1.6) aus Kapitel IV schließen wir dann:

$3^n = |Z_3|^n \leq |\bigcup\limits_{\underline{a} \in C} B_r(\underline{a})| \leq \sum\limits_{\underline{a} \in C} |B_r(\underline{a})| \leq_{(1.6)} \sum\limits_{\underline{a} \in C} \sum\limits_{k=0}^{r} \binom{n}{k} \cdot 2^k = |C| \cdot \sum\limits_{k=0}^{r} \binom{n}{k} \cdot 2^k$
$\Rightarrow |C| \geq \frac{3^n}{\sum\limits_{k=0}^{r} \binom{n}{k} \cdot 2^k}$
q.e.d

4.3.4 Folgerung

Es sei $1 \leq r \leq n$. Ist $C \subseteq Z_3^n$ ein r-perfekter Code, so hat C den covering radius r und es gilt dann:
$|C| = K_3(n, r) = H(3, n, r)$

Beweis

Es sei $C \subseteq Z_3^n$ ein r-perfekter Code. Dann ist $|C| = H(3,n,r)$. Aus Satz 3 in (1.6) aus Kapitel III folgt:
Die Kugeln $B_r(\underline{a})$ mit $\underline{a} \in C$ bilden eine Zerlegung von Z_3^n also auch eine Überdeckung von Z_3^n. Aus Lemma (4.3.2) folgt dann: C hat covering radius r. Also gilt: $K_3(n,r) \leq |C| = H(3,n,r)$. Aus Satz (4.3.3) folgt: $K_3(n,r) \geq H(3,n,r)$. Also gilt $K_3(n,r) = H(3,n,r)$ q.e.d

4.3.5 Beispiele

(1) Fall r=1

1-perfekte Codes $C \subseteq Z_3^n$ existieren, falls gilt:
$n = \frac{3^k-1}{2}$ mit $k \geq 1$, etwa die Hamming Codes aus (4.2.2),(4.2.3). Dann ist:
$K_3(n,1) = H(3,n,1) = \frac{3^n}{2n+1}$.
Dies ergibt folgende exakte Werte für:

$k=$	$n=$	$K_3(n,1)$
1	1	1
2	4	9
3	13	3^{10}

(2) Fall $r \geq 2$

Für $1 < r < n$ existiert genau ein r-perfekter Code, nämlich für $r = 2$ und $n = 11$
Beispiel für einen 2-perfekten Code ist der sogenannte Golay-Code (wurde 1947 in finnischer Fußballzeitschrift veröffentlicht) besteht aus allen Wörtern $\underline{v} = (v_1, ..., v_{11})$ mit:

$$\begin{pmatrix} v_7 \\ v_8 \\ v_9 \\ v_{10} \\ v_{11} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \\ v_6 \end{pmatrix}$$

und $(v_1, .., v_6) \in Z_3^6$. Somit gilt: $K_3(11,2) = H(3,11,2) = 3^6 - 9^3 = 729$

4.3.6 Tabelle der bekannten Werte für $K_3(n, r)$

n	$r = 1$	$r = 2$	$r = 3$
3	5	3	1
4	9	3	3
5	27	8	3
6	73	12-17	3
...			
11	7767-9477	729	115-243
...			
13	59049	5062-6561	609-1215

Tippsystem 1 für $n = 13$ Spiele, $r = 4$

- $C_1 \subseteq Z_3^4$ sei 1-perfekter Code, $|C| = 9$
- $C = \{\underline{w} = (w_1, w_2, w_3, 1) \mid \underline{w}_1, \underline{w}_2, \underline{w}_3 \in C_1\} \subseteq Z_3^{13}$
- $|C| = 9^3 = 729$
- C_1 hat covering radius $r = 1$, also hat C covering radius $r = 4$
- $\underline{s} = (\underline{s}_1, \underline{s}_2, \underline{s}_3, \_)$
- also gilt: $K_3(13, 4) \leq 729$
- weiterhin $K_3(13, 4) \geq H(3, 13, 4) \approx 113$
- also $K_3(13, 4) \geq 114$

Tippsystem 2 für $n = 13$ Spiele, $r = 4$

- $C_2 \subseteq Z_3^n$ sei 2-perfekter Code, $|C| = 729$
- $C = \{\underline{w}, = (\underline{u}, 1, 1) \mid \underline{u} \in C_2\} \subseteq Z_3^{13}$
- $|C| = 729$
- C_2 hat covering radius $r = 2$, also hat C covering radius $r = 4$

5 Kapitel V: Prüfziffersysteme

5.1 Einführung

5.1.1 Häufigkeit der Eingabefehler (Verhoff 1969)

Fehlertyp	Symbol	Häufigkeit
Einzelfehler: Verwechselung eines Buchstaben	$a \to b$	79.0%
Nachbartransposition	$ab \to ba$	10.2%
Sprungtransposition	$abc \to cba$	0.8%
Zwillingsfehler	$aa \to bb$	...
phonetischer Fehler: z.b. $30 \to 13$	$a0 \to 1a$	0.5%
Sprungzwillingsfehler	$aca \to bcb$	0.3%
übrige Fehler	_	8.6%

5.1.2 Prüfziffersysteme

Gegeben

Alphabet A mit $|A| = r \geq 2$, natürliche Zahl $n \geq 2$

Definition

Ein Code $C \subseteq A^n$ heißt Prüfziffersystem der Länge n über A, falls gilt:
$C = \{\underline{w} \in A^n \mid \underline{w} = (\underline{u}, f(\underline{u})), \underline{u} \in A^{n-1}\}$
wobei $f : A^{n-1} \to A$ eine Abbildung ist.

Bemerkung

Zu C gehört die Abbildung:
$\underbrace{\underline{u} \in A^{n-1}}_{\text{Nachrichtenwort}} \mapsto \underbrace{\underline{w} = (\underline{u}, f(\underline{u})) \in A^n}_{\text{Codewort}}$
Das Codewort $\underline{w} = (\underline{u}, f(\underline{u}))$ besteht also aus dem Nachrichtenwort $\underline{u} \in A^{n-1}$ und dem Kontrollwort $f(\underline{u}) \in A$, man nennt $f(\underline{u})$ auch Prüfziffer.
Es gilt $|C| = |A^{n-1}| = r^{n-1}$, woraus für die Informationsrate von C folgt: $I(C) = \frac{log_r|C|}{n} = \frac{n-1}{n} = 1 - \frac{1}{n}$

Ziel

Wollen erreichen dass $d(C) \geq 2$ ist und C somit alle Einzelfehler erkennt. Außerdem soll C noch möglichst alle Nachbartranspositionen erkennen.

5.1.3 Gruppen

Ein Paar $G = (A, \circ)$ bestehend aus einer Menge A mit $A \neq \emptyset$ und einer Operation $\circ$ auf A (d.h. Abbildung $a, b \in A \mapsto a \circ b \in A$) heißt Gruppe, falls folgendes gilt:

(G1) $\forall a, b \in A : a \circ b \in A$ (Abgeschlossenheit von $\circ$)

(G2) $\forall a, b, c \in A : a \circ (b \circ c) = (a \circ b) \circ c$ (Assoziativität)

(G3) $\exists e \in A : \forall a \in A : a \circ e = e \circ a = a$ (Existenz eines neutralen Elements)

Bemerkung

Man nennt e das <u>neutrale Element</u> der Gruppe G, es gibt dann genau ein neutrales Element.

(G4) $\forall a \in A : \exists i \in A : a \circ i = i \circ a = e$ (Existenz eines inversen Elements)

Bemerkung

Gilt $a \circ i = i \circ a = e$, so heißt i inverses Element von a, es ist eindeutig bestimmt und wir schreiben: $i = a^{-1}$

Bemerkung

- $(Z, +)$ ist Gruppe: $e = 0$, $a^{-1} = -a$
- $(N, +)$ ist keine Gruppe: (G4) gilt nicht
- $(Z_p, +)$ ist Gruppe: $e = 0$, $a^{-1} = -a$
- $(R, \cdot)$ ist keine Gruppe: 0 besitzt kein Inverses$\rightarrow$ (G4) nicht erfüllt
- $(R \setminus \{0\}, \cdot)$ ist Gruppe: $e = 1$, $a^{-1} = \frac{1}{a}$

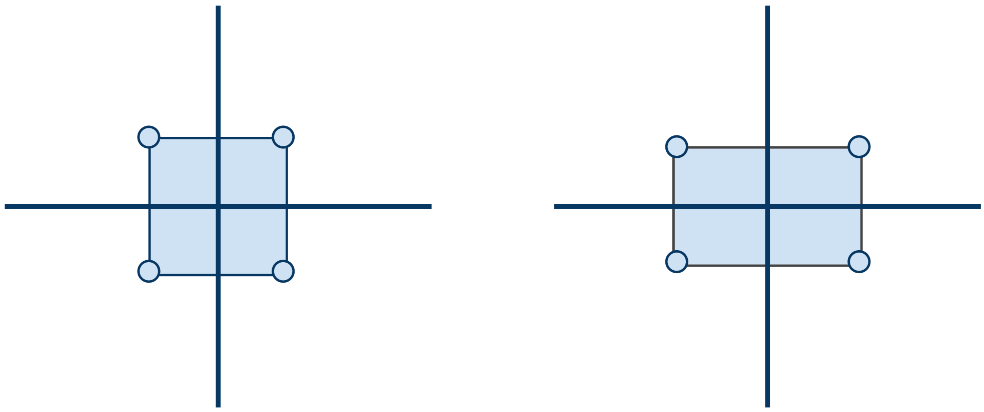
Bemerkung

Gruppe $(A, \circ)$ heißt kommutativ (abelsch), falls gilt: $\forall a, b \in A : a \circ b = b \circ a$

5.1.4 Symetrie Gruppen

Gegeben

Menge A, mit $A \neq \emptyset$ (Ecken= Gruppenelemente, Symetrie durch Spiegelachsen dargestellt)



Bezeichnung

$S(A) := \{\pi \mid \pi : A \to A \text{ bijektive Abbildung}\}$ Man nennt die Abbildung $\pi \in S(A)$ Permutation von A

Bemerkung

Ist A eine endliche Menge, etwa $A = \{1, 2, 3\}$, so lässt sich jede bijektive Abbildung $\pi : A \to A$ als Wertetabelle darstellen: $\pi = (\pi(1), \pi(2), \pi(3))$. Wir erhalten die folgenden 6 Abbildungen: $\pi = (1, 2, 3)(1, 3, 2)(3, 2, 1)(2, 1, 3)(3, 1, 2)(2, 3, 1)$ (das Tupel (a, b, c) immer als Tabelle zu interpretieren : $(f(1), f(2), f(3))$)

Bezeichnung

Für zwei Abbildungen $\pi_1, \pi_2 \in S(A)$ sei $\pi = \pi_1 \circ \pi_2$ die Komposition von π_1 un π_2, d.h. $\pi : A \to A$ ist Abbildung mit:
$\pi(a) = \pi_1(\pi_2(a)), \forall a \in A$. Dann ist auch $\pi \in S(A)$.
Für eine Abbildung $\pi \in S(A)$ sei π^{-1} die Umkehrabbildung von π, d.h. $\pi^{-1} : A \mapsto A$ ist Abbildung mit: $\pi^{-1}(a) = b \Leftrightarrow \pi(b) = a$ für $a, b \in A$. Dann gilt $\pi^{-1} \in S(A)$. Weiterhin sei $id : A \to A$ die identische Abbildung, d.h. $id(a) = a \ \forall a \in A$. Dann ist id $\in S(A)$ und es gelten folgende Aussagen:

1. $id \circ \pi = \pi \circ id = \pi \ \forall \pi \in S(A)$
2. $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = id \ \forall \pi \in S(A)$

Somit gilt

$G = (S(A), \circ)$ ist eine Gruppe, sie wird symmetrische Gruppe der Menge A genannt.

Bemerkung

Für G gilt: $e = id$ (neutrales Element) und π^{-1} (inverses Element)

Beispiel

- $A = \{1, 2, 3, \}$ $|S(A)| = 3! = 6$
- $e = (1, 2, 3)$, $\pi_1 = (1, 3, 2)$, $\pi_2 = (2, 1, 3)$, $\pi_3 = (2, 3, 1)$, $\pi_4 = (3, 1, 2)$, $\pi_5 = (3, 2, 1)$
- ${\pi_2}^{-1} = \pi_2$
- $\pi_4 \circ \pi_3 = \mathrm{id} = e$

5.2 Prüfzeichen-Codierung über Gruppen

5.2.1 Grundmodelle

Gegeben

- A Alphabet mit $|A| = m \geq 2$
- $G = (A, \circ)$ eine Gruppe
- $n \geq 2$ eine natürliche Zahl
- $\pi_1, ..., \pi_n \in S(A)$, $c \in A$

Definition

Eine Menge $C \subseteq A^n$ heißt Prüfzeichen-Codierung über Gruppe G bezüglich $\pi_1, ..., \pi_n$ und c, falls für ein Wort $\underline{w} = (w_1, ..., w_n) \in A^n$ gilt:
$\underline{w} \in C \Leftrightarrow \pi_1(w_1) \circ ... \circ \pi_n(w_n) = c$ (Kontrollgleichung (KG) von C)

Lemma

Für die Prüfzeichen-Codierung $C \subseteq A^n$ mit obiger Kontrollgleichung gilt dann $d(C) \geq 2$, d.h. C kann jeden Einzelfehler erkennen.

Beweis

Ist $i \in \{1, ..., n\}$, so lässt sich die Kontrollgleichung für $\underline{w} = (w_1, ..., w_n) \in C$ nach w_i auflösen (und zwar eindeutig)

$$\underline{w} = (w_1, ..., w_n) \in C$$

$$\downarrow \pi$$

$$\pi_1(w_1) * ... * \pi_i(w_i) * ... * \pi_n(w_n) = c$$

$$i_a * a = a * i_a = e$$

$$a * e = e * a = a$$

$$a * x = y \Leftrightarrow x = i_a * y$$

$$\pi_i(w_i) = \underbrace{{}^{i}(\pi_{i-1}(w_{i-1})) * ... * {}^{i}(\pi_1(w_1)) * c * {}^{i}(\pi_n(w_n)) * ... * {}^{i}(\pi_{i+1}(w_{i+1}))}_{d}$$

$$\pi(a) = b \Leftrightarrow b = \pi^{-1}(a), \pi \in S(A)$$

$$w_i = \pi^{-1}(d)$$

Die i-te Stelle w_i des Codewortes $\underline{w}$ ist eindeutig bestimmt durch die restlichen $n-1$ Stellen von $\underline{w}$. Stimmen also zwei Codewörter $\underline{u}, \underline{v} \in C$ auf den Stellen $j \neq i$ überein ($u_i = v_j$), so gilt $u_i = v_i$ als $\underline{u} = \underline{v}$. Ist also $\underline{u} \neq \underline{v}$, so ist $d(\underline{u}, \underline{v}) \neq 1$ und somit ≥ 2. Also ist $d(C) \geq 2$. w.z.b.w.

5.2.2 Prüfziffer-Codierung modulo m

Gegeben

- $A = Z_m = \{0, 1, 2, ..., m-1\}$. Beachte $(Z_m, +, \cdot)$ ist Restklassenring modulo $m \geq 2$; m muss keine Primzahl sein
- $G = (Z_m, +)$
- $n \geq 2$ natürliche Zahl
- $a_1, ..., a_n \in Z_m$ mit $\text{ggt}(a_i, m) = 1$ (ggt = größter gemeinsamer Teiler)
- $\pi_i : Z_m \to Z_m$ sei Abbildung mit $\pi_i(x) = a_i \cdot x$ für $x \in Z_m$ (Multiplikation in Z_m also modulo m)

Behauptung

$\pi_i \in S(Z_m)$ ist bijektive Abbildung.

Beweis

Übungsaufgabe

Beispiel

- $Z_6 = \{0, 1, 2, 3, 4, 5\}$ $a = 5$, $\mathrm{ggt}(5, 6) = 1$
- $\pi : Z_6 \to Z_6$ mit $\pi(x) = 5 \cdot x \bmod 6$
- Dann gilt:
  - $\pi(0) = 0$
  - $\pi(1) = 5$
  - $\pi(2) = 4$
  - $\pi(3) = 3$
  - $\pi(4) = 2$
  - $\pi(5) = 1$
- also gilt: $\pi = (0, 5, 4, 3, 2, 1), \pi^{-1} = (0, 5, 4, 3, 2, 1) = \pi$

Betrachten

$C \subseteq A^n = Z_m^n$ sei Prüfzeichen-Codierung über G bezüglich $\pi_1, ..., \pi_n$ und $c = 0$. Dann erhalten wir für $\underline{w} = (w_1, ..., w_n)$ die Kontrollgleichung:
$\pi_1(w_1) \circ ... \circ \pi_n(w_n) = c$ also
$a_1 \cdot w_1 + ... + a_n \cdot w_n = 0$

Also gilt

$C = \{\underline{w} = (w_1, ..., w_n) \in Z_m^n \mid \sum\limits_{i=1}^{n} a_i \cdot w_i = 0 \bmod m\}$ ist Prüfzeichen-Codierung.

Beispiel 1: ISBN-Nummer

- $m = 11$,$n = 10$,$a_i = 11 - i$,$\mathrm{ggt}(a_i, 11) = 1$
- Kontrollgleichung $\sum\limits_{i=1}^{n}(11 - i) \cdot w_i = 0 \bmod 11$
- Also :
  $C = \{\underline{w} = (w_1, ..., w_10) \in Z_{11}^{10} \mid \sum\limits_{i=1}^{n}(11 - i) \cdot w_i = 0 \bmod 11\}$
- Da $m = 11$ Primzahl ist, ist $(Z_m, +, \cdot)$ ein Körper und C somit ein linearer Code

Beispiel 2: EAN (europäische Artikel-Nummer)

- $m = 10$, $n = 13$
- $a_i = 1$ falls i ungerade
- $a_i = 3$ falls i gerade
- $\mathrm{ggt}(a_i, 10) = 1$
- Kontrollgleichung für $\underline{w} = (w_1, ..., w_{13}) \in Z_{10}^{13}$:
  $w_1 + 3w_2 + w_3 + ... + 3_{12} + w_1 3 = 0 \bmod 10$
- also:
  $C = \{\underline{w} = (w_1, ..., w_{13}) \in Z_{10}^{13} \mid w_1 + 3w_2 + w_3 + ... + 3_{12} + w_{13} = 0 \bmod 10\}$

5.2.3 Satz

Es sei $C \subseteq A^n$ eine Prüfziffer-Codierung über der Gruppe $G = (A, \circ)$ bezüglich der Permutationen $\pi_1, ..., \pi_n \in S(A)$ und $c \in A$,d.h. mit der Kontrollgleichung:
$\pi_1(w_1) \circ ... \circ \pi_n(w_n) = c$
für $\underline{w} = (w_1, ..., w_n) \in A^n$. Dann sind folgende Bedingungen äquivalent:

(a) C erkennt alle Nachbartranspositionen

(b) $\forall x, y \in A$ mit $x \neq y, \forall i \in \{1, ..., n-1\}$ gilt die Ungleichung:
$x \circ \pi_{i+1}(\pi_i^{-1}(y)) \neq y \circ \pi_{i+1}(\pi_i^{-1}(x))$

Beweis: Übungsaufgabe

5.2.4 Prüfziffersystem für deutsche Banknoten

100 DM Note : AA6186305Z2

Die Diedergruppe D_n

Definition

Die Diedergruppe D_n ist die Symmetriegruppe eines regelmäßigen n-Ecks in der Ebene.

Matrizendarstellung von D_5

bild(5-eck)

- $D = \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix}$: Drehmatrix, Drehung um ϕ
  $D^0 = E, D^1 = D, D^2 = D \cdot D, D^3 = D \cdot D^2, D^4, D^5 = E, D^{-1} = D^4$

- $S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$: Spiegelung an der y-Achse $S \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -x \\ y \end{pmatrix}$
  $S^2 = E$ also $S^{-1} = S$

Dann gilt:

(a) $SDS = SDS^{-1} = D^{-1} = D^4, D^5 = E$

(b) $SD = D^4S = D^{-1}S$

(c) D_5 besteht aus:
$D^0 = E, D^1, D^2, D^3, D^4, D^0S = S, D^1S, D^2S, D^3S, D^4S$
die Gruppenoperation ist die Matrizenmultiplikation

Darstellung von $D_5 = (A, +)$ als additive Gruppe

- $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$
- Kodieren die Matrizen durch Zahlen:

Matrix	D^0	D^1	D^2	D^3	D^4	D^0S	D^1S	D^2S	D^3S	D^4S
Zahl	0	1	2	3	4	5	6	7	8	9

- erhalten dann folgende Operationstafel für $D_5 = (A, +)$

+	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Beispiel: (erst Zeilenwert und dann Spaltenwert (5+2= Zeile mit der 5 links , Spalte mit der 2))
$5 + 2 \to D^0SD^2 = SDD = D^{-1}SD = D^{-1}D^4S = D^3S \to 8$
$3 + 4 \to D^3D^4 = D^7 = D^5D^2 = ED^2 = D^2 \to 2$

Prüfzeichen-Codierung deutscher Banknoten

Bemerkung

Bei den deutschen Banknoten wurden ab 1990 die Zeichen $0, 1, ..., 9, A, D, K, L, N, S, U, Y, Z$ benutzt.
Die Buchstaben wurden wieder in Ziffern übersetzt: $A = 0, D = 1, ...Y = 8, Z = 9$.

Gegeben

- Didergruppe $D_5 = (A, +)$ mit $A = \{0, 1, ..., 9\}$
- $n = 11$
- Permutation $\tau \in S(A)$ mit $\tau = (1, 5, 7, 6, 2, 8, 3, 0, 9, 4) = (\tau(0), ..., \tau(9))$

Bemerkung

- Zyklen von τ: $2 \to 7 \to 0 \to 1 \to 5 \to 8 \to 9 \to 4 \to 2$ und $3 \to 6 \to 3$ (Kreise)
- $\tau^k = \underbrace{\tau \circ ... \circ \tau}_{\text{k-mal}}$: $\tau^2 = (5, 8, 0, 3, 7, 9, 6, 1, 4, 2)$
- Die Permutationen $\tau^1 = \tau, \tau^2, ..., \tau^8$ sind verschieden und $\tau^8 = \text{id}$. Dann ist $\tau^9 = \tau^8 \circ \tau = id \circ \tau = \tau$, $\tau^{-1} = \tau^7$
- Für $x, y \in A$ mit $x \neq y$ gilt: $x + \tau(y) \neq y + \tau(x)$ mit $+$ Addition in $D_5 = (A, +)$

Prüfzeichen-Codierung

$C \subseteq A^{11}$ mit Kontrollgleichung für $\underline{w} = (w_1, ..., w_{11})$:
$\sum\limits_{i=1}^{10} \tau^i(w_i) + w_{11} = 0$
Dabei ist $+$ die Addition in der Diedergruppe $D_5 = (A, +)$.

Bemerkung 1

$C \subseteq A^{11}$ ist Prüfziffer-Codierung über Gruppe $D_5 = (A, +)$ bezüglich der Permutationen $\pi_1 = \tau, ..., \pi_{10} = \tau^{10}, \pi_{11} = \text{id}$ und $c = 0$. Somit kann C alle Einzelfehler erkennen.

Bemerkung 2

C erkennt alle Nachbartranspositionen, bis auf die letzen beiden Ziffern.

Bsp:

$\underline{w} = (w_1, .., w_{11}) \in C \Rightarrow \underline{u} = (w_2, w_1, w_3, ..., w_{11}) \notin C$, sonst hätten wir:
$\tau(w_1) + \tau^2(w_2) + \underbrace{\tau^3(w_3) + ... + \tau^{10}(w_{10}) + w_{11}}_{x} = 0$ und
$\tau(w_2) + \tau^2(w_1) + \underbrace{\tau^3(w_3) + ... + \tau^{10}(w_{10}) + w_{11}}_{x} = 0$
$\Rightarrow \tau(w_1) + \tau^2(w_2) = \tau(w_2) + \tau^2(w_1)$
$\Rightarrow x + \tau(y) = y + \tau(x)$ mit $x = \tau(w_1), y = \tau(w_2)$
im Widerspruch zur Eigenschaft von τ q.e.d.

Beispiel

	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}	w_{11}
Banknote	A	A	6	1	8	6	3	0	5	Z	2
$A = 0, Z = 9$	0	0	6	1	8	6	3	0	5	9	2
$\pi_i(w_i)$	1	5	3	4	0	6	6	0	8	2	2
Aufaddieren in D_5	0										

$\rightarrow$ Erfolg