Literatur

W.I.Löwenstein, Kodierungstheorie. In: *Diskrete Mathematik und mathematische Fragen der Kybernetik*, Herausg.: S.W.Jablonski/O.B.Lupanov, Akademie-Verlag, 1980.

A.Salomaa, *Jewels of Formal Language Theory*. Comp. Sci. Press, 1981.

H.J.Shyr, *Free Monoids and Languages*. Hon Min Book Co., Taichung, Taiwan, 1991.

J. Duske/H.Jürgensen, *Kodierungstheorie*. BI-Taschenb., Mannheim, 1977.

T. Grams, *Codierungsverfahren*. BI-Taschenbuch, Mannheim, 1986.

P. Sweeney, *Codierung zur Fehlererkennung und Fehlerkorrektur*. Hanser-Verlag, 1992.

W.W.Peterson/E.J.Weldon, *Error-Correcting Codes.* MIT Press, Cambridge, 1972.

J.Berstel/D.Perrin, *Theorie of Codes*. Academic Press, 1985.

Einige Mengen

$$
\begin{aligned}
C_0 &= \{a, ba, ab\}, \\
C_1 &= \{a, bb, aab, bab\}, \\
C_2 &= \{aa, bb, aba, baa\}, \\
C_3 &= \{aaa, aba, bab, bbb\}, \\
C_4 &= \{a, ab, bb\}
\end{aligned}
$$

Code – Definition

Definition:

Eine eineindeutige Funktion $\phi : A \rightarrow C$ ist eine Codierung der Menge A durch die nichtleere Sprache C über dem Alphabet X, wenn die homomorphe Erweiterung von ϕ auf A^* eine injektive Funktion von A^* in X^* ist.

Eine nichtleere Sprache C (über X) heißt Code, wenn C Wertevorrat einer Kodierung ist.

Code – Charakterisierung

Satz: Eine nichtleere Sprache C ist genau dann ein Code, wenn für beliebige

$$x_{i_1}, x_{i_2}, \ldots, x_{i_n}, x_{j_1}, x_{j_2}, \ldots, x_{j_m} \in C,\ n \geq 1, m \geq 1$$

aus $x_{i_1}x_{i_2}\ldots x_{i_n} = x_{j_1}x_{j_2}\ldots x_{j_m}$ die Gleichheit $x_{i_1} = x_{j_1}$ folgt.

Satz: Eine Sprache C ist genau dann ein Code, wenn für beliebige

$$x_{i_1}, x_{i_2}, \ldots, x_{i_n}, x_{j_1}, x_{j_2}, \ldots, x_{j_m} \in C,\ n \geq 1, m \geq 1,$$

aus $x_{i_1}x_{i_2}\ldots x_{i_n} = x_{j_1}x_{j_2}\ldots x_{j_m}$ die Gleichheiten

$$n = m \quad \text{und} \quad x_{i_t} = x_{j_t} \text{ für } 1 \leq t \leq n$$

folgen.

Strenger Code

Definition: Eine Code C heißt strenger Code,
wenn für beliebige $x_{i_k} \in C$ und $\overline{x_{j_k} \in C}$, $k \geq 1$, so dass für $n \geq 1$
$x_{i_1}x_{i_2}\ldots x_{i_n}$ ein Präfix von $x_{j_1}x_{j_2}\ldots x_{j_n}$ oder
$x_{j_1}x_{j_2}\ldots x_{j_n}$ ein Präfix von $x_{i_1}x_{i_2}\ldots x_{i_n}$ ist
die Gleichheit $x_{i_1} = x_{j_1}$ gilt.

Bemerkung: Eine Code C ist ein strenger Code,
wenn für beliebige $x_{i_k} \in C$ und $x_{j_k} \in C$, $k \geq 1$, so dass für $n \geq 1$
$x_{i_1}x_{i_2}\ldots x_{i_n}$ ein Präfix von $x_{j_1}x_{j_2}\ldots x_{j_n}$ oder
$x_{j_1}x_{j_2}\ldots x_{j_n}$ ein Präfix von $x_{i_1}x_{i_2}\ldots x_{i_n}$ ist
die Gleichheiten $x_{i_k} = x_{j_k}$ für $k \geq 1$ gelten.

Spezielle Codes

Definition:
Eine nichtleere Sprache C heißt Präfixcode, wenn kein Wort aus C Präfix eines anderen Wortes aus C ist.

Definition: Sei $n \geq 1$ eine natürliche Zahl. Eine Teilmenge C von X^n heißt Blockcode der Länge n über X.

Satz:
Für einen Code C und eine natürliche Zahl $k \geq 1$ ist auch C^k ein Code.

Decodierung

Definition: Ein Mealy-Automat ist ein 6-Tupel $\mathcal{A} = (X, Y, Z, f, g, z_0)$ mit
– X, Y, Z sind Alphabete (endliche nichtleere Mengen)
– $f : Z \times X \to Z$ und $g : Z \times X \to Y^*$ sind Funktionen, und
– z_0 ist ein Element von Z.

f und g werden auf $Z \times X^*$ fortgesetzt mittels

$$f^*(z, \lambda) = z, \qquad g^*(z, \lambda) = \lambda,$$
$$f^*(z, wa) = f(f^*(z, w), a), \quad g^*(z, wa) = g^*(z, w)g(f^*(z, w), a)$$

für $w \in X^*$, $a \in X$

Satz:
Es gibt einen Algorithmus, der für jede strenge Codierung $\phi : A \to C \subseteq X^+$ und jedes Wort $x \in X^+$ in linearer Zeit $\phi^{-1}(x)$ berechnet bzw. feststellt, dass $\phi^{-1}(x)$ nicht definiert ist.

Produktunabhängige Mengen

Definition:
Eine Sprache L heißt produktunabhängig, falls kein Wort in L als Produkt von mindestens zwei Wörtern aus L dargestellt werden kann.

Satz: Sei C eine produktunabhängige Menge über X. Dann ist C genau dann ein Code, wenn für jedes Wort $w \in X^*$ gilt, dass

$$wC^* \cap C^* \neq \emptyset \text{ und } C^*w \cap C^* \neq \emptyset \quad \text{implizieren} \quad w \in C^*.$$

Entscheidbarkeit der Code-Eigenschaft

Satz: Die Menge $C = \{x, y\}$ bestehe aus zwei nichtleeren Wörtern über X. Dann ist C genau dann ein Code, wenn $xy \neq yx$ gilt.

$$\begin{aligned} K_0(C) &= C, \\ K_{i+1}(C) &= \{w \in X^+ : yw = x \text{ oder } xw = y \text{ für gewisse } x \in C, y \in K_i(C)\}. \end{aligned}$$

Satz: Eine nichtleere Sprache C über X ist genau dann ein Code, wenn $K_i(C) \cap C = \emptyset$ für $i \geq 1$ gilt.

Satz: Eine nichtleere Sprache endliche C über X ist genau dann ein strenger Code, wenn $K_n(C) = \emptyset$ für $n \geq card(C)(\max\{|c| : c \in C\} - 1) + 1$ gilt.

Satz: Es gibt einen Algorithmus, der für jede endliche Sprache C über dem endlichen Alphabet X entscheidet, ob C ein (strenger) Code ist.

Zwei Lemmata

Lemma: Für jeden Code C, jedes $n \geq 0$ und jedes $w \in K_n(C)$ gilt $y \in Suff(C)$.

Lemma: Ein Wort v_n liegt genau dann in $K_n(C)$, $n \geq 1$, wenn für jedes $i < n$ Wörter $v_i \in K_i(C)$ und Codewörter $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$, $x_{j_1}, x_{j_2}, \ldots, x_{j_l} \in C$ mit $k + l = n - i$ derart existieren, dass entweder

$$v_0 x_{i_1} x_{i_2} \ldots x_{i_k} v_n = x_{j_1} x_{j_2} \ldots x_{j_l} \quad \text{mit} \quad |v_n| < |x_{j_l}|$$

oder

$$v_0 x_{i_1} x_{i_2} \ldots x_{i_k} = x_{j_1} x_{j_2} \ldots x_{j_l} v_n \quad \text{mit} \quad |v_n| < |x_{i_k}| \text{ für } k \neq 0$$

gilt.

Codeindikator I

Definition:

Sei X ein Alphabet der Kardinalität $n \geq 2$. Der Codeindikator $ci(w)$ eines Wortes $w \in X^*$ ist durch

$$ci(w) = n^{-|w|}$$

definiert. Für eine Sprache L mit $X = \min(L)$ setzen wir

$$ci(L) = \sum_{w \in L} ci(w).$$

Codeindikator II

Satz:
Seien L_1 und L_2 zwei Sprachen über dem Alphabet X, das aus n Buchstaben besteht. Dann gilt

$$ci(L_1 \cdot L_2) \leq ci(L_1) \cdot ci(L_2),$$

und die Gleichheit tritt genau dann ein, wenn für je vier Wörter $w_1, w_2 \in L_1$ und $w_3, w_4 \in L_4$ aus $w_1 w_3 = w_2 w_4$ folgt, dass $w_1 = w_2$ gilt.

Satz:
Für jeden Code C gilt $ci(C) \leq 1$.

Codeindikator III

Satz:
Seien $n \geq 2$ und $l_1, l_2, \ldots, l_m$ natürliche positive Zahlen, die der Bedingung

$$\sum_{i=1}^{m} n^{-l_i} \leq 1$$

genügen. Dann gibt es einen Code (Präfixcode)

$$C = \{c_0, c_1, \ldots, c_{m-1}\}$$

über dem n-elementigen Alphabet X mit

$$|c_{i-1}| = l_i \quad \text{für} \quad 1 \leq i \leq m.$$

Maximale Codes

Definition:
Ein Code C heißt maximal, wenn für jedes Wort $w \notin C$ die Menge $C \cup \{w\}$ kein Code ist.

Satz:
Ein Code C mit $ci(C) = 1$ ist ein maximaler Code.

Satz:
Ein endlicher Code C ist genau dann maximal, wenn $ci(C) = 1$ gilt.

Kosten und Optimalität von Codes

Definition: i) Für einen Code $C = \{c_1, c_2, \ldots, c_m\}$ und eine Wahrscheinlichkeitsverteilung $P = \{p_1, p_2, \ldots, p_m\}$, $p_i \geq 0$ für $1 \leq i \leq m$, $\sum_{i=1}^{m} p_i = 1$, definieren wir die Kosten von C unter P durch

$$\mathcal{L}(C, P) = \sum_{i=1}^{m} p_i |c_i|.$$

ii) Für eine Wahrscheinlichkeitsverteilung $P = \{p_1, p_2, \ldots, p_m\}$, $p_i \geq 0$ für $1 \leq i \leq m$, $\sum_{i=1}^{m} p_i = 1$, und ein Alphabet X setzen wir

$$\mathcal{L}_X(P) = \inf \mathcal{L}(C, P),$$

wobei das Infimum über alle m-elementigen Codes über X zu nehmen ist. Ein Code C' über X heißt optimal für P, wenn $\mathcal{L}(C', P) = \mathcal{L}_X(P)$ gilt.

Optimale Codes I

Satz: Für jede Verteilung P, deren Wahrscheinlichkeiten alle positiv sind, und jedes Alphabet X existiert ein (Präfix)-Code über X, der optimal für P ist.

Satz: Für jede Verteilung $P = \{p_0, p_1, \ldots, p_m\}$ und jedes Alphabet X mit $card(X) = n$ gilt

$$\sum_{i=1}^{m} p_i \log_n \left(\frac{1}{p_i}\right) \leq \mathcal{L}_X(P) \leq 1 + \sum_{i=1}^{m} p_i \log_n \left(\frac{1}{p_i}\right),$$

wobei die Gleichheit $\mathcal{L}_X(P) = \sum_{i=1}^{m} p_i \log_n \left(\frac{1}{p_i}\right)$ genau dann gilt, wenn $\log_n(p_i)$ für $1 \leq i \leq m$ ganze Zahlen sind.

Optimale Codes II

Satz: Es sei $C = \{c_1, c_2, \ldots, c_m\} \subseteq \{0,1\}^+$ ein optimaler Präfixcode für die Verteilung $P = \{p_1, p_2, \ldots p_m\}$. Ferner gelte

$$p_j = q_0 + q_1$$

und

$$p_1 \geq p_2 \geq \ldots \geq p_{j-1} \geq p_j \geq p_{j+1} \geq \ldots \geq p_m \geq q_0 \geq q_1.$$

Dann ist

$$C' = \{c_1, c_2, \ldots, c_{j-1}, c_{j+1}, \ldots, c_m, c_j 0, c_j 1\}$$

ein optimaler Präfixcode für die Verteilung

$$P' = \{p_1, p_2, \ldots, p_{j-1}, p_{j+1}, \ldots, p_m, q_0, q_1\}.$$

Fehlertypen I

Definition:
Unter einem Austauschfehler verstehen wir die Übertragung einer 0 anstelle einer 1 bzw. die Übertragung einer 1 anstelle einer 0.
Unter einem Ausfallfehler verstehen wir den Ausfall eines Symbols während der Übertragung, d.h. an einer Stelle wird das übertragene Wort durch Löschen eines Buchstaben gekürzt.
Unter einem Einschubfehler verstehen wir die Übertragung eines zusätzlichen Symbols, d.h. das empfangene Wort wird durch den Einschub eines Symbols an einer Stelle im übertragenen Wort verlängert.

Bezeichnung: $1 \to 0,\ 0 \to 1,\ 0 \to \lambda,\ 1 \to \lambda,\ \lambda \to 0,\ \lambda \to 1$

Fehlertypen II

$G = \{1 \to 0,\ 0 \to 1,\ 0 \to \lambda,\ 1 \to \lambda,\ \lambda \to 0,\ \lambda \to 1\}$

Definition:
Eine Teilmenge von G bezeichnen wir als Fehlertyp.
Ein Fehlertyp F heißt symmetrisch, falls F durch Vereinigung aus den Mengen $\{0 \to 1, 1 \to 0\}$, $\{\lambda \to 0, 0 \to \lambda\}$ und $\{\lambda \to 1, 1 \to \lambda\}$ gewonnen werden kann.

Für einen Fehlertyp F und Wörter w und v über $\{0, 1\}$ setzen wir

$$w \overset{F,t}{\Longrightarrow} v,$$

falls bei der Übertragung durch das simultane Auftreten von t Fehlern aus F aus dem Wort w das Wort v entsteht.

Fehlerkorrektur I

Definition:
Sei F ein Fehlertyp und C ein Blockcode über $\{0,1\}$. C heißt Code mit Korrektur von s Fehlern aus F, falls für jedes Wort $v \in \{0,1\}^*$ höchstens ein Wort $w \in C$ mit $w \stackrel{F,t}{\Longrightarrow} v$ und $t \leq s$ existiert.

Für einen Fehlertyp F und Wörter $w, v \in \{0,1\}^*$ definieren wir

$$d_F(w,v) = \begin{cases} \min\{t : w \stackrel{F,t}{\Longrightarrow} v\} & \text{falls dies existiert} \\ \infty & \text{sonst} \end{cases} .$$

Satz:
Für einen symmetrischen Fehlertyp F ist durch d_F eine Abstandsfunktion in $\{0,1\}^*$ definiert.

Fehlerkorrektur II

Definition:
Für einen symmetrischen Fehlertyp F und einen endlichen Code C definieren wir den Codeabstand $d_F(C)$ als

$$d_F(C) = \min\{d_F(x, y) : x, y \in C, x \neq y\}.$$

Satz:
Sei F ein symmetrischer Fehlertyp. Dann ist ein endlicher Code C genau dann ein Code mit Korrektur von s Fehlern aus F, wenn

$$d_F(C) \geq 2s + 1$$

gilt.

Abschätzungen I

Für natürliche Zahlen $n \geq 1$ und $d \geq 1$ setzen wir

$$m(n,d) = \max\{\#(C) \mid C \subseteq \{0,1\}^n, d(C) \geq d\}\,.$$

Satz:
Für $n \geq 3$ und $s \geq 1$ gilt

$$\frac{2^n}{\sum_{k=0}^{2s} \binom{n}{k}} \leq m(n,2s+1) \leq \frac{2^n}{\sum_{k=0}^{s} \binom{n}{k}}\,.$$

Abschätzungen II

Satz: Für zwei beliebige positive natürliche Zahlen $n$und d (mit $n \geq d$) gilt

$$m(n,d) \leq 2 \cdot m(n-1,d)\,.$$

Satz: Seien n und d zwei beliebige positive natürliche Zahlen (mit $n \geq d$).
i) Dann gilt $m(n,d) \geq m(n+1,d+1)$.
ii) Ist d ungerade, so gilt sogar $m(n,d) = m(n+1,d+1)$.

Satz: Für zwei beliebige positive natürliche Zahlen $n$und d (mit $n \geq d$) gilt

$$m(2n,2d) \geq m(n,d) \cdot m(n,2d)\,.$$

Abschätzungen III

Satz: Seien n und d zwei beliebige positive natürliche Zahlen $n$und d (mit $n \geq d$).

i) Für gerades d gilt
$m(n,d) \leq 2 \cdot \lfloor \frac{d}{2d-n} \rfloor$ für $2d > n$,
$m(n,d) \leq 2n$ für $2d = n$.

ii) Für ungerades d gilt
$m(n,d) \leq 2 \cdot \lfloor \frac{d+1}{2d+1-n} \rfloor$ für $2d+1 > n$,
$m(n,d) \leq 2n$ für $2d+1 = n$.

iii) Für $n \geq 2d$ gilt
$m(n,d) \leq d \cdot 2^{n-2d+2}$ für gerades d,
$m(n,d) \leq (d+1) \cdot 2^{n-2d+1}$ für ungerades d.

Lineare Codes

Definition: Ein Blockcode $C \subseteq \{0,1\}^*$ heißt linearer Code, wenn die Elemente aus C einen linearen Vektorraum über dem Körper $\{0,1\}$ bilden.

linearer Code $C \subseteq \{0,1\}^n$ hat als Vektorraum eine Dimension $dim(C)$
C ist dann ein $[n, dim(C)]$-Code

Definition: Sei C ein $[n,k]$-Code.
i) Eine Matrix G vom Typ (k,n) heißt Erzeugendenmatrix für C, falls die k Zeilen von G ein Erzeugendensystem für C (als Vektorraum) bilden.
ii) Eine Matrix H vom Typ $(n-k,n)$ heißt Kontrollmatrix für C, falls

$$C = \{c \mid c \in \{0,1\}^n, Hc^T = (0^n)^T\}$$

gilt.

Gewicht eines Codes

Definition: i) Unter dem Gewicht $w(c)$ eines Wortes $c \in \{0,1\}^+ *$ verstehen wir die Anzahl der in c vorkommenden Einsen.
ii) Das Gewicht $w(C)$ eines Blockcodes $C \subseteq \{0,1\}^n$ wird definiert durch

$$w(C) = \min\{w(c) \mid w \in C \setminus \{0^n\}.$$

Satz: Es sei C ein linearer $[n,k]$-Code und H eine Kontrollmatrix für C. Dann gilt

$$\begin{aligned} w(C) &= \min\{r \mid \text{es gibt } r \text{ linear abhängige Spalten von } H\} \\ &= \max\{r \mid \text{je } r-1 \text{ Spalten von } H \text{ sind linear unabhängig}\} \end{aligned}$$

Satz: Für einen linearen Code C gilt $d(C) = w(C)$.

Einige Abschätzungen I

$$k(n,d) = \max\{dim(C) \mid C \subseteq \{0,1\}^n \text{ ist linearer Code mit } d(C) \geq d\}$$

$$\begin{aligned}
k(n,d) &\leq k(n-1,d)+1\,, \\
k(n,d) &= k(n+1,d-1) \text{ für ungerades } d\,, \\
k(2n,2d) &\geq k(n,d)+k(n,2d)\,, \\
n(k+1,d) &> n(k,d) \quad \text{und} \quad n(k,d+1) > n(k,d)\,.
\end{aligned}$$

Einige Abschätzungen II

Satz: Für $k > 1$ ist $n(k,d) \geq n\big(k-1, \lceil \frac{d}{2} \rceil\big) + d\,.$

Folgerung: Für $k \geq 1$ gilt

$$n(k,d) \geq \sum_{i=1}^{k-1} \lceil \frac{d}{2^i} \rceil\,.$$

Folgerung: Es gilt

$$k(n,d) \leq \max\{k \mid \sum_{i=1}^{k-1} \lceil \frac{d}{2^i} \rceil \leq n\}\,.$$

Eine Methode zur Konstruktion linearer Codes

Lemma: Seien die linearen Codes C_1 und C_2 mit den Dimensionen k_1 bzw. k_2 und den Codeabständen d_1 und d_2 gegeben. Dann ist

$$C = C_1 \alpha C_2 = \{(c_1, c_1 \oplus c_2) \mid c_1 \in C_1, c_2 \in C_2\}$$

ein linearer Code mit

$$C \subseteq \{0,1\}^{2n}, \quad dim(C) = k_1 + k_2 \quad \text{und} \quad d(C) = \min\{2d_1, d_2\}\,.$$

Existenz linearer Codes mit gewissen Parametern

Satz: Wenn die natürlichen Zahlen n, k und d die Bedingungen

$$k \leq n \quad \text{und} \quad 2^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i}$$

erfüllen, so gibt es einen linearen Code C mit

$$C \subseteq \{0,1\}^n, \quad dim(C) = k \quad \text{und} \quad d(C) \geq d$$

(es gilt also $k(n,d) \geq k$).