Berechenbarkeit und Komplexität
9. Vorlesung

TECHNISCHE UNIVERSITÄT ILMENAU

Prof. Dr. Dietrich Kuske

welt offenes Thüringen

FG Automaten und Logik, TU Ilmenau

Sommersemester 2024

Universelle Turing-Maschine

Wir wollen jetzt zeigen, daß es eine Turing-Maschine gibt, die jede Turing-Maschine simulieren kann, wenn deren Kodierung gegeben ist.

Problem: Bandalphabete sind beliebig groß, die zu konstruierende universelle TM hat aber ein festes Bandalphabet.

Lösung: Kodiere Buchstaben des Bandalphabets als Wörter über $\{0, 1, 2\}$ mit $\square = 2$. Ab jetzt nehmen wir an, daß wir immer dieses Bandalphabet haben.

Definition

Eine Turing-Maschine U heißt universelle Turing-Maschine, wenn sie die folgende partielle Funktion berechnet:

$$\begin{array}{rcl} \{0,1\}^* & \dashrightarrow & \{0,1\}^* \\ y & \mapsto & \begin{cases} \varphi_w(x) & \text{falls } y = w000x, w \in L_{TM}, x \in \{0,1\}^* \\ \text{undef.} & \text{sonst} \end{cases} \end{array}$$

Bemerkung

Ist U universelle TM, so gilt insbes. für alle $w \in L_{TM}$ und $x \in \{0,1\}^*$:

- U hält bei Eingabe $w\,000\,x$ genau dann, wenn M_w bei Eingabe x hält.
- U akzeptiert $w\,000\,x$ genau dann, wenn M_w das Wort x akzeptiert.

Satz

Es gibt eine universelle Turing-Maschine.

Beweis

zunächst eine Turing-Maschine mit drei Bändern (daraus kann dann eine TM mit einem Band konstruiert werden). Während der Berechnung haben die Bänder die folgende Bedeutung:

- 1. Band: Kode w der zu simulierenden Turing-Maschine M_w
- 2. Band: aktueller Zustand der zu simulierenden Turing-Maschine M_w
- 3. Band: augenblicklicher Bandinhalt der Turing-Maschine M_w

Initialisierung: Auf 1. Band steht $w\,000\,x$ mit $w \in L_{TM}$. Kopiere x auf 3. Band und lösche $000\,x$ auf erstem, schreibe 010 (d.h. Kode von z_0) auf 2. Band.

Simulation eines Schrittes von M_w: stehen auf 2. Band $01^{i+1}0$ (d.h. z_i) und auf 3. an Kopfposition j, so suche auf 1. Band $001^{i+1}01^{j+1}01^{i'+1}01^{j'+1}01^{y}0$ (d.h. Anweisung $(z_{i'}, a_{j'}, y) = \delta(z_i, a_j)$) und

- schreibe $01^{i'+1}0$ auf 2. Band
- ersetze j an Kopfposition auf 3. Band durch j'
- bewege 3. Kopf entsprechend y nach rechts, links oder aber nicht.

„*Aufräumen*“ bei Erreichen einer akzeptierenden Haltekonfiguration auf 3. Band. □

Satz

Das spezielle Halteproblem $K = \{w \in L_{TM} \mid M_w \text{ angesetzt auf } w \text{ hält}\}$ ist semi-entscheidbar.

Beweis:

Berechne die „halbe“ charakteristische Funktion $\chi'_K : \{0,1\}^* \to \{1\}$ mit folgender TM M:

- Gehört die Eingabe nicht zu L_{TM}, so gehe in Endlosschleife.
- Bei Eingabe von $w \in L_{TM}$: schreibe $\#w$ hinter Eingabe (auf dem Band steht jetzt $w\#w$) und starte eine universelle Turing-Maschine U.
- Nach Termination von U ersetze Bandhinhalt durch 1 und halte an.

Für $w \in L_{TM}$:

$$\begin{aligned} M \text{ hält (mit Ausgabe 1)} &\iff U \text{ hält bei Eingabe von } w\#w \\ &\iff M_w \text{ hält bei Eingabe von } w \\ &\iff w \in K. \end{aligned}$$

□

(Analog sind H_0 und H semi-entscheidbar, aber nicht entscheidbar.)

Satz

Es gibt eine Grammatik G, deren Wortproblem $L(G)$ unentscheidbar ist.

Beweis:

Das spezielle Halteproblem K ist semi-entscheidbar.

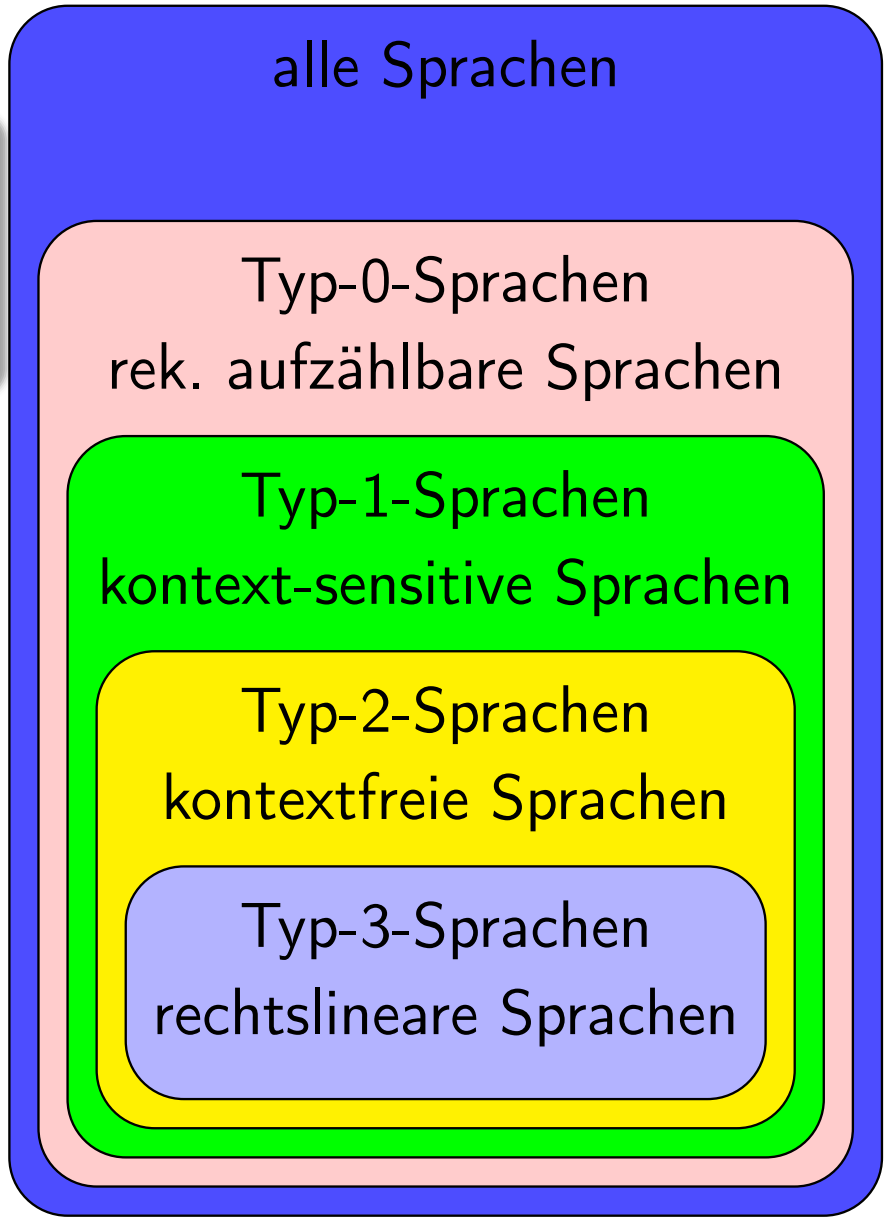
Nach dem Satz auf Folie 8.16 ist K vom Typ 0, d.h. es gibt eine Grammatik G mit $L(G) = K$.

Da K nach dem Satz auf Folie 7.14 unentscheidbar ist, ist also auch das Wortproblem der Grammatik G unentscheidbar. □

Folgerung

Es gibt eine Typ-0-Sprache, die nicht vom Typ 1 ist.

Beweis: Jede Typ-1-Sprache ist entscheidbar (Automaten und Formale Sprachen, Folie 2.24), es gibt aber eine unentscheidbare Typ-0-Sprache. □



Posts Korrespondenzproblem (PCP)

Definition

(1) Ein Korrespondenzsystem ist eine endliche Folge von Paaren $K = \big((x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)\big)$ mit $x_i, y_i \in \Sigma^+$ für alle $1 \leq i \leq k$ (dabei ist Σ ein beliebiges Alphabet).

(2) Eine Lösung von K ist eine endliche Folge von Indizes $i_1, i_2, \ldots, i_n \in \{1, 2, \ldots, k\}$ mit $n \geq 1$ und $x_{i_1} x_{i_2} \cdots x_{i_n} = y_{i_1} y_{i_2} \cdots y_{i_n}$.

(3) MPCP („modifiziertes PCP“) ist die Menge der Korrespondenzsysteme, die eine Lösung mit $i_1 = 1$ besitzen.

(4) PCP ist die Menge der Korrespondenzsysteme, die eine Lösung besitzen.

Ziel: die Menge PCP ist unentscheidbar, dazu: $H_0 \leq \text{MPCP} \leq \text{PCP}$

Beispiel

Ist das folgende Korrespondenzsystem lösbar?

$$\begin{array}{llllll} x_1 & = & 0 & x_2 & = & 1 & x_3 & = & 0101 \\ y_1 & = & 010 & y_2 & = & 101 & y_3 & = & 01 \end{array}$$

Eine mögliche Lösung ist $(3, 3, 1, 2)$:

$$\begin{array}{llllllll} 01 & 01 & 010 & 1 & 0 & 1 \\ 01 & 01 & 010 & 1 & 0 & 1 \end{array}$$

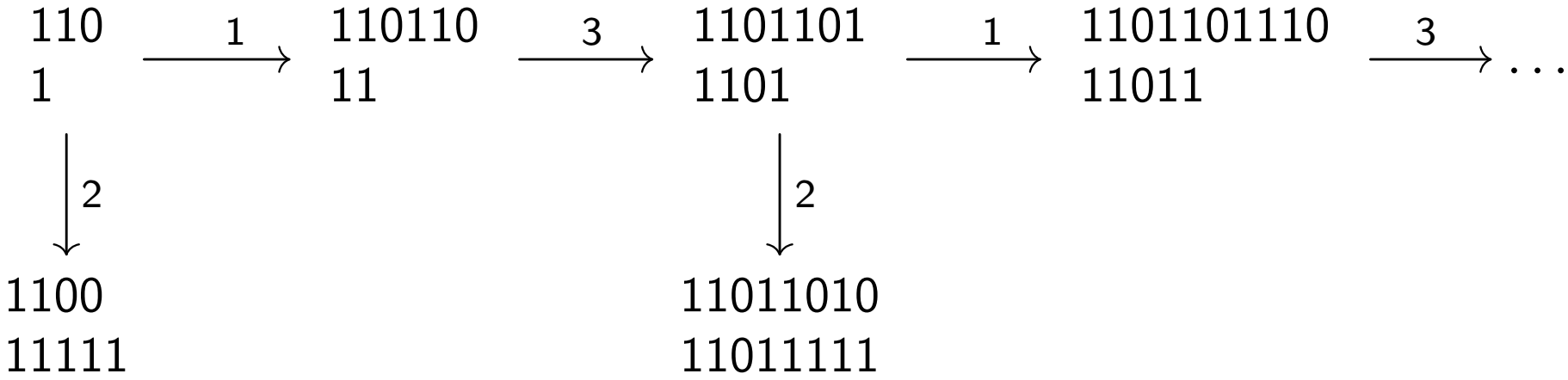
Eine weitere (kürzere) Lösung ist: $(3, 1)$

Beispiel

Ist das folgende Korrespondenzsystem lösbar?

$$\begin{array}{llllll} x_1 = 110 & x_2 = 0 & x_3 = 1 \\ y_1 = 1 & y_2 = 1111 & y_3 = 01 \end{array}$$

Wir suchen eine Lösung:



Damit folgt, daß es keine Lösung gibt.

Beispiel

Das folgende Korrespondenzsystem ist lösbar:

$$\begin{array}{llllllllll} x_1 & = & 001 & x_2 & = & 01 & x_3 & = & 01 & x_4 & = & 10 \\ y_1 & = & 0 & y_2 & = & 011 & y_3 & = & 101 & y_4 & = & 001 \end{array}$$

Eine kürzeste Lösung besteht aus 66 Indizes:
$(2,4,3,4,4,2,1,2,4,3,4,3,4,4,3,4,4,2,1,4,4,2,1,3,4,1,1,3,$
$4,4,4,2,1,2,1,1,1,3,4,3,4,1,2,1,4,4,2,1,4,1,1,3,4,1,1,3,$
$1,1,3,1,2,1,4,1,1,3)$.

Beispiel

Das folgende Korrespondenzsystem ist lösbar:

$$\begin{array}{llllllllll} x_1 & = & 0 & x_2 & = & 0000 & x_3 & = & 0001 & x_4 & = & 101 \\ y_1 & = & 00 & y_2 & = & 0101 & y_3 & = & 10 & y_4 & = & 1 \end{array}$$

Angeblich besteht eine kürzeste Lösung aus 781 Indizes.

An der Komplexität dieser Lösung kann man bereits die Schwierigkeit des Problems ablesen.

Lemma

MPCP $\leq$ PCP

Beweis:

sei $K = \big((x_1, y_1), \ldots, (x_k, y_k)\big)$ Korrespondenzsystem über Σ mit $\$ \notin \Sigma$

für $w = a_1 a_2 \ldots a_m \in \Sigma^*$:

$$\overrightarrow{w} = a_1\$a_2\$\cdots a_m\$ \qquad \overleftarrow{w} = \$a_1\$a_2\$\cdots a_m \qquad \overleftrightarrow{w} = \$a_1\$a_2\$\cdots a_m\$$$

setze $f(K) = \big((\overrightarrow{x_1}, \overleftarrow{y_1}), (\overrightarrow{x_2}, \overleftarrow{y_2}), \cdots (\overrightarrow{x_k}, \overleftarrow{y_k}), (\overleftrightarrow{x_1}, \overleftarrow{y_1}), (\$, \$\$)\big)$

da f berechenbar ist, ist noch $K \in$ MPCP $\iff f(K) \in$ PCP zu zeigen:

„$\Rightarrow$“ Sei $K \in$ MPCP. Dann existiert Lösung $1, i_2, \ldots, i_n$ von K. Also ist $k+1, i_2, i_3, \ldots, i_n, k+2$ Lösung von $f(K)$, d.h. $f(K) \in$ PCP.

„$\Leftarrow$“ Sei nun $f(K) \in \text{PCP}$. Dann existiert Lösung $i_1, i_2, \ldots, i_n$ von $f(K)$.

Eine Lösung $i'_1, i'_2, \ldots, i'_{n'}$ von K erhält man, indem man in der Folge $i_1, i_2, \ldots, i_n$

- alle Vorkommen von $k+1$ durch 1 ersetzt und
- alle Vorkommen von $k+2$ streicht.

Vergleich der ersten Buchstaben liefert $i_1 \in \{k+1, k+2\}$.

Angenommen, $i_1 = k+2$. Der Vergleich der zweiten Buchstaben liefert $i_2 \in \{k+1, k+2\}$.
Der Vergleich der dritten Buchstaben sichert $i_2 = k+2$.
$\vdots$
Dann ist aber $x_{i_1} \cdots x_{i_n} = \$^n$ kürzer als $y_{i_1} \cdots y_{i_n} = \$^{2n}$, im Widerspruch zu deren Gleichheit.

Also erhalten wir $i_1 = k+1$, und damit $i'_1 = 1$, d.h. $K \in \text{MPCP}$. □

Wir werden nun $H_0 \leq \text{MPCP}$ zeigen, d.h. aus (dem Kode) einer Turing-Maschine $M = (Z, \Sigma, \Gamma, \delta, z_0, \square, E)$ werden wir ein Korrespondenzsystem $K(M)$ berechnen mit

$$M \text{ hält bei leerer Eingabe} \iff K(M) \text{ hat eine Lösung mit } i_1 = 1\,.$$

Wir können annehmen, daß die TM M nur anhält, wenn sie sich in Endzustand aus E und der Kopf sich am Anfang des beschrifteten Bandes befindet.

$K(M)$ hat folgende Wortpaare:

- $(x_1, y_1) = (\#, \# \rhd z_0 \square \lhd)$ ist erstes Wortpaar
- Kopierpaare (a, a) für $a \in \Gamma \cup \{\rhd, \lhd\}$
- Überführungspaare $(z, z' \in Z, a, b, c \in \Gamma)$

$$
\begin{array}{rll}
(za, z'c) & \text{für} & (z', c, N) = \delta(z, a) \\
(za, cz') & \text{für} & (z', c, R) = \delta(z, a) \\
(bza, z'bc) & \text{für} & (z', c, L) = \delta(z, a) \\
(\rhd za, \rhd z' \square c) & \text{für} & (z', c, L) = \delta(z, a) \\
(z\lhd, z'c\lhd) & \text{für} & (z', c, N) = \delta(z, \square) \\
(z\lhd, cz'\lhd) & \text{für} & (z', c, R) = \delta(z, \square) \\
(bz\lhd, z'bc\lhd) & \text{für} & (z', c, L) = \delta(z, \square)
\end{array}
$$

- Löschpaare (azb, zb) und (zba, zb) für alle $z \in E$, $a, b \in \Gamma$ mit $\delta(z, b) = (z, b, N)$
- Abschlußpaare $(\rhd za \lhd \#, \#)$ für alle $z \in E$, $a \in \Gamma$ mit $\delta(z, a) = (z, a, N)$

Lemma

Die Abbildung K, die der Turing-Maschine M das Korrespondenzsystem $K(M)$ zuordnet, ist eine Reduktion von H_0 auf MPCP, es gilt also $H_0 \leq$ MPCP.

Beweis

Beobachtung (a)

Sind uzv und $u'z'v'$ Konfigurationen von M mit $uzv \vdash u'z'v'$, so existieren $i_1, i_2, \ldots, i_n \in \{1, 2, \ldots, k\}$ mit

$$\begin{aligned} x_{i_1} x_{i_2} \cdots x_{i_n} &= \quad \triangleright uzv \triangleleft \\ y_{i_1} y_{i_2} \cdots y_{i_n} &= \quad \triangleright u'z'v' \triangleleft \end{aligned}$$

Begründung: sei $v = aw$ und sei $(z', c, y) = \delta(z, a)$, so daß $u'z'v'$ aus $uzaw$ durch Ausführung dieser Regel entsteht, z.B. $y = N$. Dann gilt $u' = u$ und $v' = cw$.
Also: zunächst durch Kopierpaare, dann durch $(x_i, y_i) = (za, z'c)$ und dann durch Kopierpaare:

$$\begin{aligned} x_{i_1} x_{i_2} \cdots x_{i_n} &= \quad \triangleright uzaw \triangleleft \\ y_{i_1} y_{i_2} \cdots y_{i_n} &= \quad \triangleright u'z'cw \triangleleft \end{aligned}$$

Beobachtung (b)

Sind $u, v \in \Gamma^*$, $z \in E$ und $a, b \in \Gamma$ mit $\delta(z, b) = (z, b, N)$, so existieren $i_1, \ldots, i_n \in \{1, 2, \ldots, k\}$ mit $x_{i_1} x_{i_2} \cdots x_{i_n} = \rhd uazbv \lhd$

$y_{i_1} y_{i_2} \cdots y_{i_n} = \rhd uzbv \lhd$

Begründung: wie oben durch Kopierpaare und Löschpaar (azb, zb), da $\delta(z, b) = (z, b, N)$

Beobachtung (c)

Sind $u, v \in \Gamma^*$, $z \in E$ und $a, b \in \Gamma$ mit $\delta(z, b) = (z, b, N)$, so existieren $i_1, \ldots, i_n \in \{1, 2, \ldots, k\}$ mit $x_{i_1} x_{i_2} \cdots x_{i_n} = \rhd uzbav \lhd$

$y_{i_1} y_{i_2} \cdots y_{i_n} = \rhd uzbv \lhd$

Begründung analog

angenommen, die TM M hält bei leerer Eingabe. Dann existieren also Konfigurationen $k_i = u_i z_i v_i$ mit $z_0\Box = k_0 \vdash k_1 \vdash \cdots k_n$, so daß k_n akzeptierende Haltekonfiguration ist.
nach Beobachtungen (a,b,c) existieren $i_1, \ldots, i_m \in \{1, 2, \ldots, k\}$, so daß $x_{i_1} \cdots x_{i_m}$ bzw. $y_{i_1} \cdots y_{i_m}$ wie folgt aussehen:

$$\triangleright u_0 z_0 v_0 \triangleleft \; \triangleright u_1 z_1 v_1 \triangleleft \cdots \triangleright u_n z_n v_n \triangleleft \cdots \triangleright z_n v_n \triangleleft \cdots \triangleright z_n ba \triangleleft$$
$$\triangleright u_1 z_1 v_1 \triangleleft \cdots \triangleright u_n z_n v_n \triangleleft \cdots \triangleright z_n v_n \triangleleft \cdots \triangleright z_n ba \triangleleft \; \triangleright z_n b \triangleleft$$

also (mit Anfangspaar 1 und einer Schlußregel j):

$$x_1 x_{i_1} \cdots x_{i_m} x_j = \# \triangleright u_0 z_0 v_0 \triangleleft \; \triangleright u_1 z_1 v_1 \triangleleft \cdots \triangleright z_n ba \triangleleft \; \triangleright z_n b \triangleleft \#$$
$$y_1 y_{i_1} \cdots y_{i_m} y_j = \# \triangleright \; z_0 \Box \triangleleft \triangleright u_1 z_1 v_1 \triangleleft \cdots \triangleright z_n ba \triangleleft \; \triangleright z_n b \triangleleft \# .$$

Wegen $u_0 = \varepsilon$ hat das Korrespondenzsystem $K(M)$ also eine Lösung mit erstem Index 1, d.h. $K(M) \in$ MPCP.

Damit gezeigt: M hält bei leerer Eingabe $\Longrightarrow K(M) \in$ MPCP.

umgekehrte Implikation wird ähnlich gezeigt (aber wir tun dies hier nicht).

damit: Die Abbildung K, die jeder Turing-Maschine ein Korrespondenzsystem zuordnet, ist eine Reduktion von H_0 auf MPCP.

$\Longrightarrow H_0 \leq$ MPCP. □

Satz (Emil Post, 1947)

PCP ist unentscheidbar.
(T. Neary 2015: 5 Paare reichen hierfür.)

Beweis $H_0 \leq \text{MPCP} \leq \text{PCP}$ nach Lemmata auf Folien 9.18 und 9.14

Nach dem Satz auf Folie 7.27 ist H_0 unentscheidbar, nach dem Lemma auf Folie 7.21 sind also MPCP und PCP unentscheidbar. □

Satz

PCP ist semi-entscheidbar.

Beweis:

Probiere erst alle Indexfolgen der Länge 1 aus, dann alle Indexfolgen der Länge 2, ...

Falls irgendwann eine passende Indexfolge gefunden wird, so gib 1 aus. □

Korollar

Das Komplement $\overline{\text{PCP}}$ von PCP ist nicht semi-entscheidbar.

Beweis:

PCP unentscheidbar und semi-entscheidbar

$\Longrightarrow$ $\overline{\text{PCP}}$ nicht semi-entscheidbar nach Satz auf Folie 8.13 □

Zusammenfassung 9. Vorlesung

in dieser Vorlesung neu

- es gibt universelle Turingmaschinen
- spezielles Halteproblem ist semi-entscheidbar
- es gibt Typ-0-Sprache, die nicht Typ 1 ist
- PCP, Unentscheidbarkeit

kommende Vorlesung

- Menge der allgemeingültigen Aussagen der Prädikatenlogik ist unentscheidbar
- Menge der in $(\mathbb{N}, +, \cdot)$ gültigen Aussagen ist unentscheidbar
- 1. Gödelscher Unvollständigkeitssatz

Syntax und Semantik der Prädikatenlogik wiederholen!