

# Berechenbarkeit und Komplexität

## 9. Vorlesung

Prof. Dr. Dietrich Kuske

FG Automaten und Logik, TU Ilmenau

Sommersemester 2023

# 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:

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

## Bemerkung

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

- $U$  hält bei Eingabe  $w000x$  genau dann, wenn  $M_w$  bei Eingabe  $x$  hält.
- $U$  akzeptiert  $w000x$  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  $w000x$  mit  $w \in L_{TM}$ . Kopiere  $x$  auf 3. Band und lösche  $000x$  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  $001^{i+1}01^{j+1}01^{i'+1}01^{j'+1}01^y0$  (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. □

## NOTIZ (nach 9.5)

Es gibt kleine universelle Turing-Maschinen:

	Zustände	Bandsymbole
Minsky '62	7	4
Rogozhin	15	2
	9	3
	6	4
	5	5
	4	6
	3	9
	2	18

## 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  $\chi'_K: \{0, 1\}^* \rightarrow \{1\}$  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 Bandinhalt 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  $L(G) = K$ .

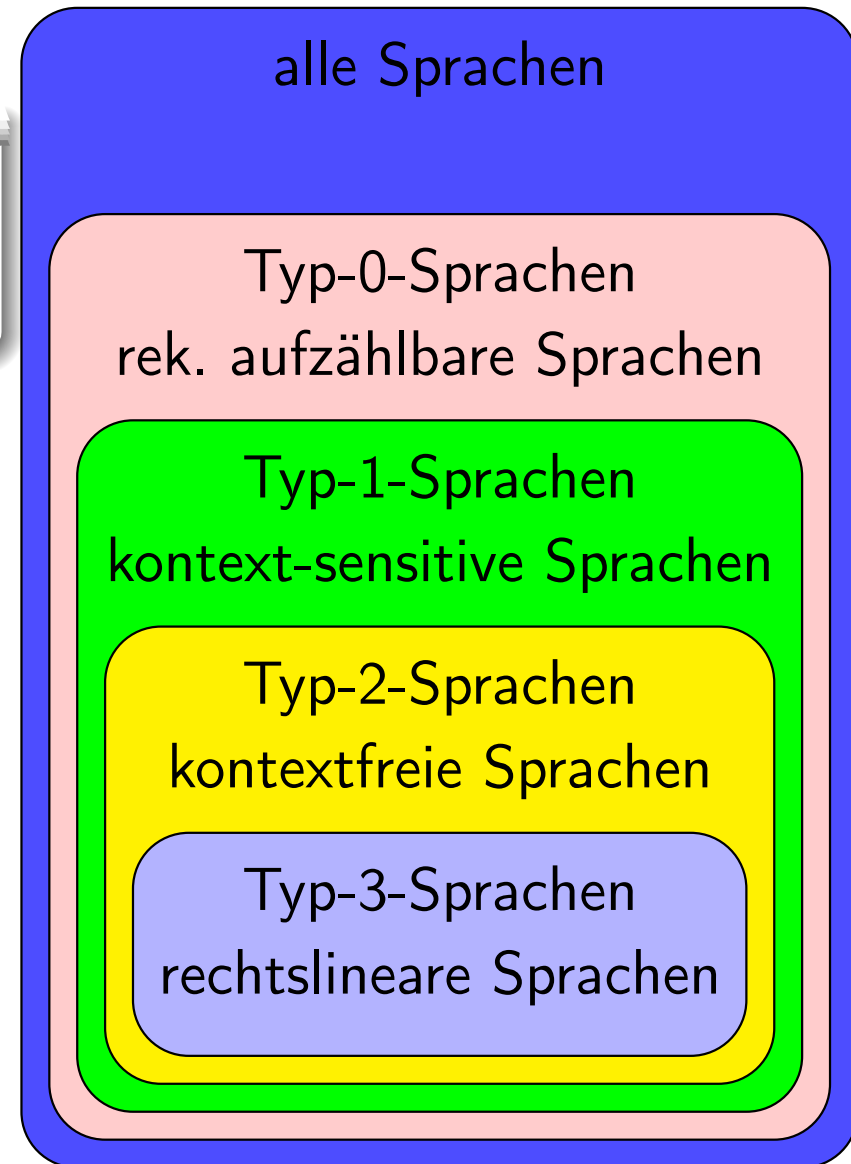
Da  $K$  nach dem Satz auf Folie 7.14 unentscheidbar ist, ist also auch das Wortproblem der Grammatik  $G$  unentscheidbar. □



## 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. □



## NOTIZ (nach 9.8)

Vor dieser Folie sind „allg. Wortproblem unentscheidbar“, „TOT nicht semi-entscheidbar“ und „es gibt keine Zertifikate für Totalität“ auskommentiert

# Posts Korrespondenzproblem (PCP)

## Definition

- ① Ein **Korrespondenzsystem** ist eine endliche Folge von Paaren  $K = ((x_1, y_1), (x_2, y_2), \dots, (x_k, y_k))$  mit  $x_i, y_i \in \Sigma^+$  für alle  $1 \leq i \leq k$  (dabei ist  $\Sigma$  ein beliebiges Alphabet).
- ② Eine **Lösung von  $K$**  ist eine endliche Folge von Indizes  $i_1, i_2, \dots, i_n \in \{1, 2, \dots, k\}$  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?

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

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

$$\begin{array}{cccc|cccc} 0 & 1 & & & 0 & 1 & 0 & 1 & & & 1 & & 0 & & 1 \\ 0 & 1 & & & 0 & 1 & 0 & 1 & & & 1 & & 0 & & 1 \end{array}$$

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

## Beispiel

Ist das folgende Korrespondenzsystem lösbar?

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

Wir suchen eine Lösung:

$$\begin{array}{ccccccc} \begin{array}{l} 110 \\ 1 \end{array} & \xrightarrow{1} & \begin{array}{l} 110110 \\ 11 \end{array} & \xrightarrow{3} & \begin{array}{l} 1101101 \\ 1101 \end{array} & \xrightarrow{1} & \begin{array}{l} 1101101110 \\ 11011 \end{array} & \xrightarrow{3} & \dots \\ \downarrow 2 & & & & \downarrow 2 & & & & \\ \begin{array}{l} 1100 \\ 11111 \end{array} & & & & \begin{array}{l} 11011010 \\ 11011111 \end{array} & & & & \end{array}$$

Damit folgt, daß es keine Lösung gibt.

## Beispiel

Das folgende Korrespondenzsystem ist lösbar:

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

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:

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

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  $K = ((x_1, y_1), \dots, (x_k, y_k))$  Korrespondenzsystem über  $\Sigma$  mit  $\$ \notin \Sigma$

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

$$\vec{w} = a_1 \$ a_2 \$ \dots a_m \$ \quad \overleftarrow{w} = \$ a_1 \$ a_2 \$ \dots a_m \$ \quad \overleftrightarrow{w} = \$ a_1 \$ a_2 \$ \dots a_m \$$$

setze  $f(K) = ((\vec{x}_1, \overleftarrow{y}_1), (\vec{x}_2, \overleftarrow{y}_2), \dots, (\vec{x}_k, \overleftarrow{y}_k), (\overleftrightarrow{x}_1, \overleftarrow{y}_1), (\$, \$))$

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

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



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

Eine Lösung  $i'_1, i'_2, \dots, i'_n$  von  $K$  erhält man, indem man in der Folge  $i_1, i_2, \dots, i_n$

- 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  $i_2 = k + 2$ .

⋮

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

$M$  hält bei leerer Eingabe  $\iff K(M)$  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:

- $(x_1, y_1) = (\#, \# \triangleright z_0 \square \triangleleft)$  ist erstes Wortpaar
- Kopierpaare  $(a, a)$  für  $a \in \Gamma \cup \{\triangleright, \triangleleft\}$
- Überführungspaare  $(z, z' \in Z, a, b, c \in \Gamma)$ 
  - $(za, z'c)$  für  $(z', c, N) = \delta(z, a)$
  - $(za, cz')$  für  $(z', c, R) = \delta(z, a)$
  - $(bza, z'bc)$  für  $(z', c, L) = \delta(z, a)$
  - $(\triangleright za, \triangleright z' \square c)$  für  $(z', c, L) = \delta(z, a)$
  - $(z \triangleleft, z'c \triangleleft)$  für  $(z', c, N) = \delta(z, \square)$
  - $(z \triangleleft, cz' \triangleleft)$  für  $(z', c, R) = \delta(z, \square)$
  - $(bz \triangleleft, z'bc \triangleleft)$  für  $(z', c, L) = \delta(z, \square)$
- Löschpaare  $(azb, zb)$  und  $(zba, zb)$  für alle  $z \in E, a, b \in \Gamma$  mit  $\delta(z, b) = (z, b, N)$
- Abschlußpaare  $(\triangleright za \triangleleft \#, \#)$  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  $H_0 \leq \text{MPCP}$ .

## Beweis

### Beobachtung (a)

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

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

**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**:

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

## Beobachtung (b)

Sind  $u, v \in \Gamma^*$ ,  $z \in E$  und  $a, b \in \Gamma$  mit  $\delta(z, b) = (z, b, N)$ , so existieren  $i_1, \dots, i_n \in \{1, 2, \dots, k\}$  mit

$$x_{i_1} x_{i_2} \cdots x_{i_n} = \triangleright u a z b v \triangleleft$$

$$y_{i_1} y_{i_2} \cdots y_{i_n} = \triangleright u z b v \triangleleft$$

**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  $i_1, \dots, i_n \in \{1, 2, \dots, k\}$  mit

$$x_{i_1} x_{i_2} \cdots x_{i_n} = \triangleright u z b a v \triangleleft$$

$$y_{i_1} y_{i_2} \cdots y_{i_n} = \triangleright u z b v \triangleleft$$

**Begründung analog**

angenommen, die TM  $M$  hält bei leerer Eingabe. Dann existieren also Konfigurationen  $k_i = u_i z_i v_i$  mit  $z_0 \square = k_0 \vdash k_1 \vdash \dots k_n$ , so daß  $k_n$  akzeptierende Haltekonfiguration ist.

nach Beobachtungen (a,b,c) existieren  $i_1, \dots, i_m \in \{1, 2, \dots, k\}$ , so daß  $x_{i_1} \dots x_{i_m}$  bzw.  $y_{i_1} \dots y_{i_m}$  wie folgt aussehen:

$$\begin{aligned} \triangleright u_0 z_0 v_0 \triangleleft \triangleright u_1 z_1 v_1 \triangleleft \dots \triangleright u_n z_n v_n \triangleleft \dots \triangleright z_n v_n \triangleleft \dots \triangleright z_n b a \triangleleft \\ \triangleright u_1 z_1 v_1 \triangleleft \dots \triangleright u_n z_n v_n \triangleleft \dots \triangleright z_n v_n \triangleleft \dots \triangleright z_n b a \triangleleft \triangleright z_n b \triangleleft \end{aligned}$$

also (mit Anfangspaar  $1$  und einer Schlußregel  $j$ ):

$$\begin{aligned} x_1 x_{i_1} \dots x_{i_m} x_j = \# \triangleright u_0 z_0 v_0 \triangleleft \triangleright u_1 z_1 v_1 \triangleleft \dots \triangleright z_n b a \triangleleft \triangleright z_n b \triangleleft \# \\ y_1 y_{i_1} \dots y_{i_m} y_j = \# \triangleright z_0 \square \triangleleft \triangleright u_1 z_1 v_1 \triangleleft \dots \triangleright z_n b a \triangleleft \triangleright z_n b \triangleleft \# . \end{aligned}$$

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

Damit gezeigt:  $M$  hält bei leerer Eingabe  $\implies K(M) \in \text{MPCP}$ .

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.

$\implies H_0 \leq \text{MPCP}$ .



## 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.  $\square$





Emil Post (1897-1954)

## NOTIZ (nach 9.22)

Emil Leon Post:

- geb. in Rußland (heute Polen), US-Emigration 1904, gest. New York
- Studium Astronomie City College New York, während Bachelor-Studium zwei mathematische Artikel (die erst später erschienen)
- Logik-Promotion Columbia State University, Erfindung der Wahrheitstabellen, der mehrwertigen Logik und der Beweissysteme ( $\Rightarrow$  Menge der wahren Aussagen ist rekursiv aufzählbar)
- bekannt für Arbeiten zu polyadischen Gruppen, rekursiv aufzählbaren Mengen und Graden der Unentscheidbarkeit
- Posts Problem: Gibt es unentscheidbare Menge  $U$  mit  $\neg(H \leq U)$ ?
- lebenslang manisch-depressiv, starb an Herzinfarkt wohl aufgrund einer Elektroschock-Therapie

## 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.  $\square$

## Korollar

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

### Beweis:

PCP unentscheidbar und semi-entscheidbar

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

## 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!