Diskrete Mathematik

Arne Dür Kurt Girstmair Simon Legner
Georg Moser Harald Zankl

Fakultät für Mathematik, Informatik und Physik @ UIBK
Sommersemester 2011

Zusammenfassung der letzten LV

Definition

eine TM U heißt universell, wenn bei Eingabe

- des Codes $\ulcorner M \urcorner$ einer TM M
- und des Codes $\ulcorner x \urcorner$ einer Eingabe x für M

die TM U, die TM M auf x simuliert

1. U kontrolliert Korrektheit der Codes; wenn inkorrekt, verwirft U
2. U simuliert M mit 3 Bändern auf der Eingabe x
   - Band 1 enthält die Beschreibung von M
   - Band 2 enthält das (dekodierte) Eingabewort x
   - Band 3 enthält (simulierten) Bandinhalt des Bandes von M
3. wenn M jemals auf der Eingabe x hält, hält U ebenfalls und akzeptiert; beziehungsweise verwirft entsprechend

Übersicht

Endliche Automaten

Automaten, reguläre Sprachen und Grammatiken, (nicht)-deterministische endliche Automaten, Teilmengenkonstruktion, ϵ-NEAs, Umwandlung endlicher Automaten in reguläre Ausdrücke, Pumpinglemma, Minimierung

Berechenbarkeitstheorie

Einführung in die Berechenbarkeitstheorie, Turingmaschinen, Entscheidungsprobleme, Universelle Maschinen und Diagonalisierung

Komplexitätstheorie

Einführung in die Komplexitätstheorie, die Klassen P und NP, logarithmisch platzbeschränkte Reduktionen, Speicherplatzkomplexität

Übersicht

Endliche Automaten

Automaten, reguläre Sprachen und Grammatiken, (nicht)-deterministische endliche Automaten, Teilmengenkonstruktion, ϵ-NEAs, Umwandlung endlicher Automaten in reguläre Ausdrücke, Pumpinglemma, Minimierung

Berechenbarkeitstheorie

Einführung in die Berechenbarkeitstheorie, Turingmaschinen, Entscheidungsprobleme, Universelle Maschinen und Diagonalisierung

Komplexitätstheorie

Einführung in die Komplexitätstheorie, die Klassen P und NP, logarithmisch platzbeschränkte Reduktionen, Speicherplatzkomplexität

Unentscheidbarkeit des Halteproblems

Definition

definiere Halteproblem und Zugehörigkeitsproblem von TMs

$$\mathrm{HP} := \{M\sharp x \mid M \text{ hält bei Eingabe } x\}$$
$$\mathrm{MP} := \{M\sharp x \mid x \in \mathrm{L}(M)\}$$

Unentscheidbarkeit des Halteproblems

Definition

definiere Halteproblem und Zugehörigkeitsproblem von TMs

$$\mathrm{HP} := \{M\sharp x \mid M \text{ hält bei Eingabe } x\}$$
$$\mathrm{MP} := \{M\sharp x \mid x \in \mathrm{L}(M)\}$$

Definition

1. M_x ist TM (mit Eingabealphabet $\{0,1\}$) deren Code (mit Kodierungsalphabet $\{0,1\}$) gleich x
2. wenn x kein Code, definiere M_x beliebig

Unentscheidbarkeit des Halteproblems

Definition

definiere Halteproblem und Zugehörigkeitsproblem von TMs

$$\mathrm{HP} := \{M\sharp x \mid M \text{ hält bei Eingabe } x\}$$
$$\mathrm{MP} := \{M\sharp x \mid x \in \mathrm{L}(M)\}$$

Definition

1. M_x ist TM (mit Eingabealphabet $\{0,1\}$) deren Code (mit Kodierungsalphabet $\{0,1\}$) gleich x
2. wenn x kein Code, definiere M_x beliebig

Unentscheidbarkeit des Halteproblems

Definition

definiere Halteproblem und Zugehörigkeitsproblem von TMs

$$\text{HP} := \{M\sharp x \mid M \text{ hält bei Eingabe } x\}$$
$$\text{MP} := \{M\sharp x \mid x \in \mathsf{L}(M)\}$$

Definition

1. M_x ist TM (mit Eingabealphabet $\{0,1\}$) deren Code (mit Kodierungsalphabet $\{0,1\}$) gleich x
2. wenn x kein Code, definiere M_x beliebig

Aufzählung aller Turingmaschinen

$$M_\epsilon, M_0, M_1, M_{00}, M_{01}, M_{10}, M_{11}, M_{000}, \ldots$$

	ϵ	0	1	00	01	10	11	000	001	010	$\dots$
M_ϵ	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	
M_0	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_1	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_{00}	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_{01}	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\dots$
M_{10}	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	
M_{11}	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	
M_{000}	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	
M_{001}	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	
$\vdots$						$\vdots$					$\ddots$

	ϵ	0	1	00	01	10	11	000	001	010	$\dots$
M_ϵ	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	
M_0	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_1	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_{00}	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_{01}	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\dots$
M_{10}	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	
M_{11}	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	
M_{000}	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	
M_{001}	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	
$\vdots$						$\vdots$					$\ddots$

	ϵ	0	1	00	01	10	11	000	001	010	…
M_ϵ	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	
M_0	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_1	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_{00}	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_{01}	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	…
M_{10}	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	
M_{11}	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	
M_{000}	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	
M_{001}	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	
$\vdots$						$\vdots$					$\ddots$

	ϵ	0	1	00	01	10	11	000	001	010	…
M_ϵ	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	
M_0	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_1	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_{00}	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	
M_{01}	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	…
M_{10}	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	
M_{11}	$\checkmark$	$\checkmark$	$\circlearrowright$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	
M_{000}	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\circlearrowright$	
M_{001}	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	$\circlearrowright$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$	
$\vdots$						$\vdots$					$\ddots$

Behauptung

die dem Komplement der Diagonale entsprechende Sprache wird von keiner der TMs:

$$M_\epsilon, M_0, M_1, M_{00}, M_{01}, M_{10}, M_{11}, M_{000}, \dots$$

akzeptiert

Behauptung

die dem Komplement der Diagonale entsprechende Sprache wird von keiner TM in der Aufzählung akzeptiert

Behauptung

die dem Komplement der Diagonale entsprechende Sprache wird von keiner TM in der Aufzählung akzeptiert

Beweis.

sei $\Sigma \supseteq \{\checkmark, \circlearrowright\}$ ein Alphabet

$s_0, s_1, s_2, \ldots$ eine Folge unendlicher Wörter über $\{\checkmark, \circlearrowright\}$

$$\begin{aligned}
s_0 &= s_{00} s_{01} s_{02} s_{03} s_{04} \ldots \\
s_1 &= s_{10} s_{11} s_{12} s_{13} s_{14} \ldots \\
s_1 &= s_{20} s_{21} s_{22} s_{23} s_{24} \ldots \\
&\vdots
\end{aligned}$$

dann ist die Folge

$$d_n = \begin{cases} \circlearrowright & \text{wenn } s_{nn} = \checkmark \\ \checkmark & \text{wenn } s_{nn} = \circlearrowright \end{cases}$$

eine neue Folge

Behauptung

die dem Komplement der Diagonale entsprechende Sprache wird von keiner TM in der Aufzählung akzeptiert

Beweis.

sei $\Sigma \supseteq \{\checkmark, \circlearrowright\}$ ein Alphabet

$s_0, s_1, s_2, \ldots$ eine Folge unendlicher Wörter über $\{\checkmark, \circlearrowright\}$

$$\begin{aligned} s_0 &= s_{00}s_{01}s_{02}s_{03}s_{04}\ldots \\ s_1 &= s_{10}s_{11}s_{12}s_{13}s_{14}\ldots \\ s_1 &= s_{20}s_{21}s_{22}s_{23}s_{24}\ldots \\ &\vdots \end{aligned}$$

dann ist die Folge

$$d_n = \begin{cases} \circlearrowright & \text{wenn } s_{nn} = \checkmark \\ \checkmark & \text{wenn } s_{nn} = \circlearrowright \end{cases}$$

eine neue Folge ∎

Satz

HP *ist nicht rekursiv, aber rekursiv aufzählbar*

Satz

HP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweis.

wir zeigen Nicht-Rekursivität

1. angenommen $\exists$ totale TM K, sodass $\mathrm{HP} = \mathrm{L}(K)$

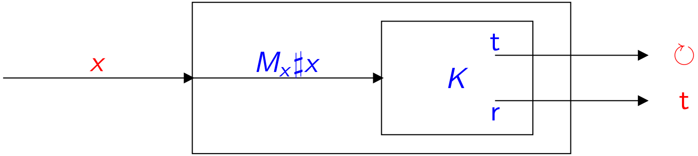
Satz

HP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweis.

wir zeigen Nicht-Rekursivität

1. angenommen $\exists$ totale TM K, sodass HP $= \mathrm{L}(K)$
2. Definition von TM D



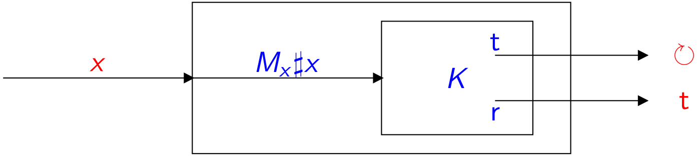
Satz

HP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweis.

wir zeigen Nicht-Rekursivität

1. angenommen $\exists$ totale TM K, sodass HP $= \mathrm{L}(K)$
2. Definition von TM D



3. D akzeptiert genau die dem Komplement der Diagonale entsprechende Sprache

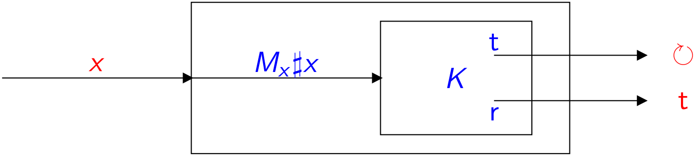
Satz

HP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweis.

wir zeigen Nicht-Rekursivität

1. angenommen $\exists$ totale TM K, sodass $\mathrm{HP} = \mathrm{L}(K)$
2. Definition von TM D



3. D akzeptiert genau die dem Komplement der Diagonale entsprechende Sprache
4. Verhalten von D verschieden von jeder TM M_x in der Aufzählung; Widerspruch

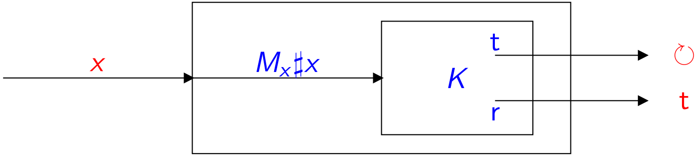
Satz

HP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweis.

wir zeigen Nicht-Rekursivität

1. angenommen $\exists$ totale TM K, sodass HP $= \mathrm{L}(K)$
2. Definition von TM D



3. D akzeptiert genau die dem Komplement der Diagonale entsprechende Sprache
4. Verhalten von D verschieden von jeder TM M_x in der Aufzählung; Widerspruch

Satz

MP *ist nicht rekursiv, aber rekursiv aufzählbar*

Satz

MP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweisskizze

Satz

MP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweisskizze

1. um zu zeigen, dass MP rekursiv aufzählbar, definiere UTM U, die bei Eingabe $M\sharp x$, TM M auf x simuliert

Satz

MP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweisskizze

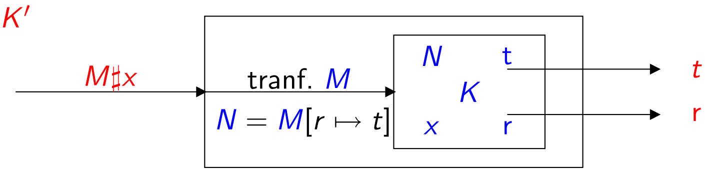
1. um zu zeigen, dass MP rekursiv aufzählbar, definiere UTM U, die bei Eingabe $M\sharp x$, TM M auf x simuliert
2. um zu zeigen, dass MP nicht rekursiv ist, verwende Reduktion vom Halteproblem

Satz

MP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweisskizze

1. um zu zeigen, dass MP rekursiv aufzählbar, definiere UTM U, die bei Eingabe $M\sharp x$, TM M auf x simuliert
2. um zu zeigen, dass MP nicht rekursiv ist, verwende Reduktion vom Halteproblem
   sei K eine totale TM, sodass $\text{MP} = \text{L}(K)$; definiere K' (totale) TM, sodass $\text{HP} = \text{L}(K')$:

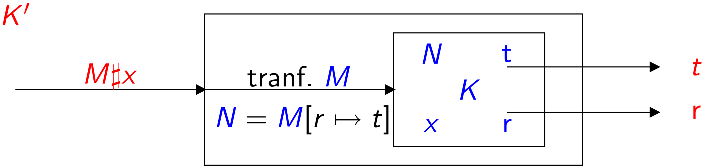


Satz

MP *ist nicht rekursiv, aber rekursiv aufzählbar*

Beweisskizze

1. um zu zeigen, dass MP rekursiv aufzählbar, definiere UTM U, die bei Eingabe $M\sharp x$, TM M auf x simuliert
2. um zu zeigen, dass MP nicht rekursiv ist, verwende Reduktion vom Halteproblem
   sei K eine totale TM, sodass MP $= \mathrm{L}(K)$; definiere K' (totale) TM, sodass HP $= \mathrm{L}(K')$:



Reduktionen

Definition

1. $\exists$ totale DTM T mit Eingabealphabet Σ

Reduktionen

Definition

1. $\exists$ totale DTM T mit Eingabealphabet Σ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf das (erste) Band

Reduktionen

Definition

1. $\exists$ totale DTM T mit Eingabealphabet Σ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf das (erste) Band

dann heißt $f : \Sigma^* \to \Sigma^*$ berechenbar

Reduktionen

Definition

1. $\exists$ totale DTM T mit Eingabealphabet Σ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf das (erste) Band

dann heißt $f : \Sigma^* \to \Sigma^*$ berechenbar

Definition

Reduktionen

Definition

1. $\exists$ totale DTM T mit Eingabealphabet Σ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf das (erste) Band

dann heißt $f : \Sigma^* \to \Sigma^*$ berechenbar

Definition

1. $\exists$ $R : \Sigma^* \to \Sigma^*$

Reduktionen

Definition

1. $\exists$ totale DTM T mit Eingabealphabet Σ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf das (erste) Band

dann heißt $f\colon \Sigma^* \longrightarrow \Sigma^*$ berechenbar

Definition

1. $\exists$ $R\colon \Sigma^* \longrightarrow \Sigma^*$
2. R berechenbar

Reduktionen

Definition

1. $\exists$ totale DTM T mit Eingabealphabet Σ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf das (erste) Band

dann heißt $f\colon \Sigma^* \to \Sigma^*$ berechenbar

Definition

1. $\exists$ $R\colon \Sigma^* \to \Sigma^*$
2. R berechenbar
3. für $L \subseteq \Sigma^*$, $M \subseteq \Sigma^*$ gilt $x \in L \iff R(x) \in M$

Reduktionen

Definition

1. $\exists$ totale DTM T mit Eingabealphabet Σ
2. bei Eingabe $x \in \Sigma^*$, schreibt T $f(x)$ auf das (erste) Band

dann heißt $f\colon \Sigma^* \to \Sigma^*$ berechenbar

Definition

1. $\exists$ $R\colon \Sigma^* \to \Sigma^*$
2. R berechenbar
3. für $L \subseteq \Sigma^*$, $M \subseteq \Sigma^*$ gilt $x \in L \iff R(x) \in M$

dann ist L auf M reduzierbar; kurz: $L \leqslant_m M$

Reduktionen im Bild

angenommen

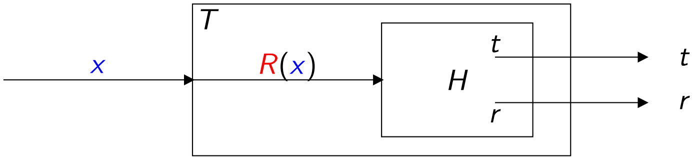
- L, M Sprachen über Σ
- $L \leqslant_m M$ mit $R\colon \Sigma^* \to \Sigma^*$
- die Reduktion R wird von TM T berechnet

Reduktionen im Bild

angenommen

- L, M Sprachen über Σ
- $L \leqslant_m M$ mit $R\colon \Sigma^* \to \Sigma^*$
- die Reduktion R wird von TM T berechnet

$$x \in L \iff R(x) \in M$$

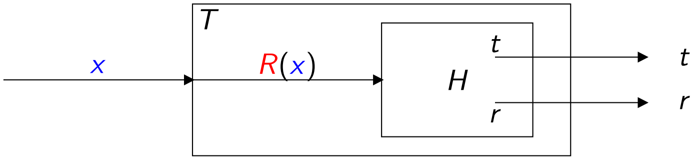


Reduktionen im Bild

angenommen

- L, M Sprachen über Σ
- $L \leqslant_m M$ mit $R\colon \Sigma^* \to \Sigma^*$
- die Reduktion R wird von TM T berechnet

$$x \in L \iff R(x) \in M$$



Lemma

wenn $L \leqslant_m M$ und M rekursiv, dann ist L rekursiv

Satz

jede rekursive Menge ist rekursiv aufzählbar, aber nicht jede rekursiv aufzählbare Menge ist rekursiv

Satz

jede rekursive Menge ist rekursiv aufzählbar, aber nicht jede rekursiv aufzählbare Menge ist rekursiv

Satz

es kann kein Testprogramm für "hello, world" Programme geben

Beweis.

$$\text{HP} \leqslant_m \text{“hello, world” Programme}$$

Satz

jede rekursive Menge ist rekursiv aufzählbar, aber nicht jede rekursiv aufzählbare Menge ist rekursiv

Satz

es kann kein Testprogramm für "hello, world" Programme geben

Beweis.

$$\text{HP} \leqslant_m \text{"hello, world" Programme}$$

■

Satz

die folgenden Probleme sind unentscheidbar:

1. *das Postsche Korrespondenzproblem*
2. *ist eine beliebige Sprache regulär?*