

# FGI 1

Automaten, Formale Sprachen,  
Berechenbarkeit

Christopher Habel & Matthias Jantzen

## Kap 20 (Entscheidbarkeit, Gödelisierung, Halteproblem)

Matthias Jantzen

M. Jantzen, FGI-1, SoSe 2009: 1

Montag, 6. Juli 2009

1

## Hierarchie

Folgende Beziehungen hatten wir bisher gezeigt:

Klasse der **regulären Mengen**

$\subseteq$  Klasse der **kontextfreien Mengen**

$\subseteq$  Klasse der **kontextsensitiven Mengen**

$\not\subseteq$  Klasse der **entscheidbaren Mengen**

$\not\subseteq$  Klasse der **aufzählbaren Mengen**

$\not\subseteq$  Klasse der **abzählbaren Mengen**

$\neq$  Klasse der **überabzählbaren Mengen**

Das  
kommt  
noch:

Existenz überabzählbarer Mengen ist bekannt.  
(z.B. aus *Diagonalbeweis*).

M. Jantzen, FGI-1, SoSe 2009: 2

Montag, 6. Juli 2009

2

# Inklusionen der Chomsky-Hierarchie

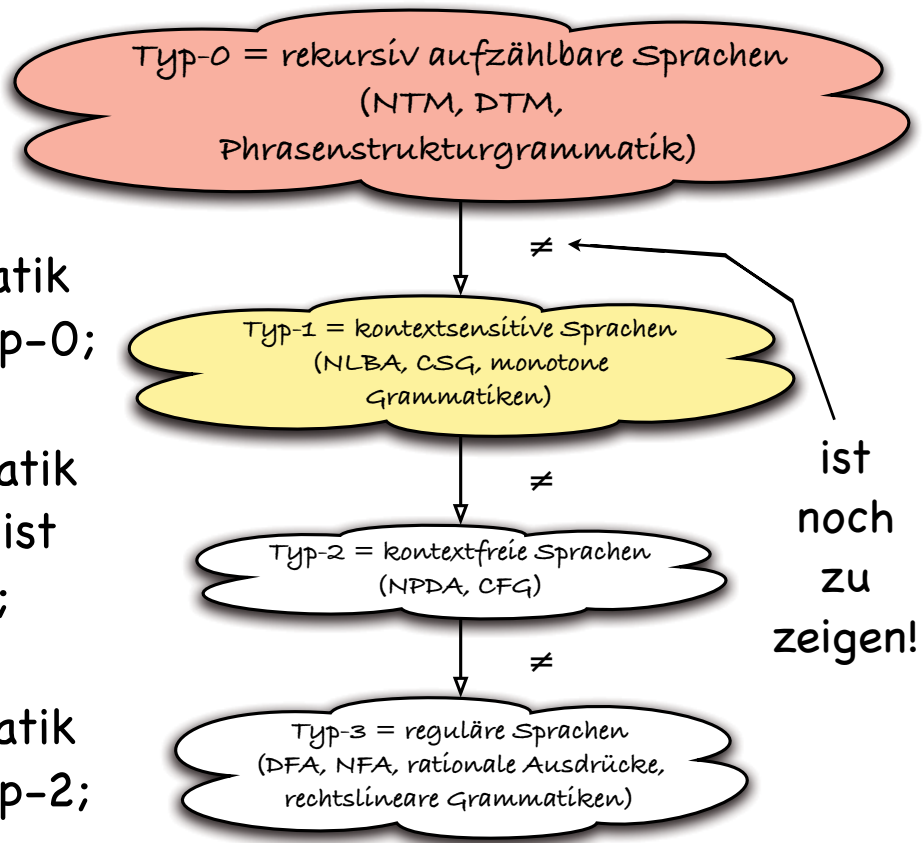
Jede Typ-1 Grammatik ist zugleich vom Typ-0;



Jede Typ-2 Grammatik ohne  $\epsilon$ -Produktion ist zugleich vom Typ-1;



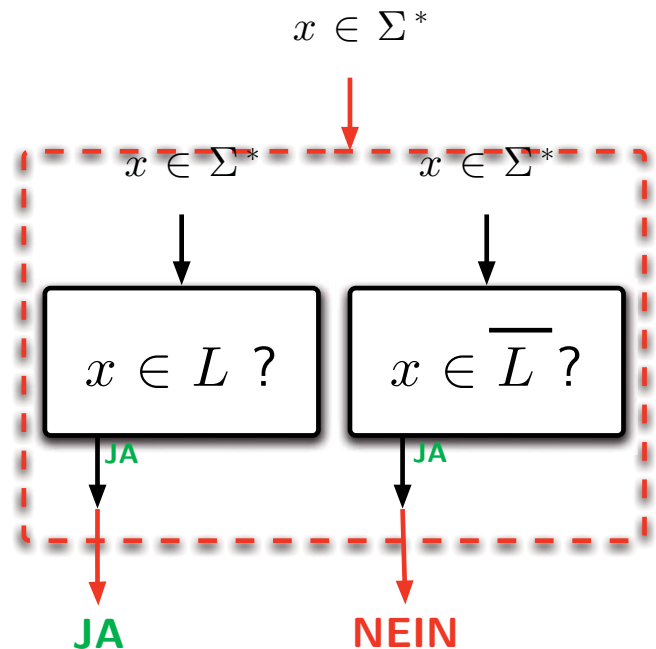
Jede Typ-3 Grammatik ist zugleich vom Typ-2;



## ein wichtiger Zusammenhang:

### Satz 35:

Eine Menge  $L$  ist genau dann rekursiv (entscheidbar) wenn  $L$  selbst, und auch ihr Komplement  $\bar{L}$  rekursiv aufzählbar sind.



Entscheidbare Mengen sind stets aufzählbar! (Wie?)

Die andere Richtung folgt aus Erklärung zu obigem Bild!

# nichtaufzählbare Sprachen

Wenn es also eine aufzählbare, nicht entscheidbare Menge gibt, so wissen wir, dass deren Komplement nicht aufzählbar sein kann!

1. **Frage:** Gibt es formale Sprachen, die von **keiner DTM** akzeptiert werden können?
2. Wir zeigen, dass es eine Sprache  $L \subseteq \{0, 1\}^*$  gibt, die von keiner DTM akzeptiert werden kann!
3. Wir benötigen: **Codierung von Automaten als Wörter über einem endlichen Alphabet**, d.h. eine *injektive* Funktion

$$\text{code} : \text{Menge aller DTM} \rightarrow \{0, 1\}^*$$

4. ... wir können die lexikalische Ordnung wählen, aber es gibt seit Gödel's Beweisen auch andere!

M. Jantzen, FGI-1, SoSe 2009: 5

Montag, 6. Juli 2009

5

## Was sind Gödelnummern?

### Definition 61:

Eine Funktion  $\nu_\Sigma : \Sigma^* \rightarrow \mathbb{N}$  ( $\Sigma$  ein endliches Alphabet) heißt **Gödelisierung**, wenn gilt:

1.  $\forall u, v \in \Sigma^* : u \neq v$  impliziert  $\nu_\Sigma(u) \neq \nu_\Sigma(v)$ ,  $\nu_\Sigma$  ist also injektiv.
2. Aus jedem Argument  $w \in \Sigma^*$  kann  $\nu_\Sigma(w)$  in endlich vielen Schritten effektiv bestimmt werden.
3. Für jedes  $n \in \mathbb{N}$  kann in endlich vielen Schritten effektiv bestimmt werden, ob es ein  $w \in \Sigma^*$  gibt, für das  $\nu_\Sigma(w) = n$  gilt.
4. Wenn es ein  $w \in \Sigma^*$  mit  $\nu_\Sigma(w) = n$  gibt, dann kann  $w$  in endlich vielen Schritten effektiv aus  $n$  konstruiert werden.

M. Jantzen, FGI-1, SoSe 2009: 6

Montag, 6. Juli 2009

6

# Die Paarfunktion ist Gödelisierung;

zur Erinnerung:

## Definition 51:

paar :  $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$  sei definiert durch

$$\text{paar}(i, j) := i + \frac{(i + j)(i + j + 1)}{2} = i + \binom{i + j + 1}{2}$$

...aber wie berechnen wir zu einer Zahl

$$k \in \mathbb{N}$$

das zugehörige Tupel

$$(i, j)?$$

## Formel für $\text{paar}^{-1}(k)$

Dieses hier ohne Beweis...

(in die Berechnungsformel einsetzen würde ausreichen!):

### Satz 36:

Für

$$\pi_1(k) := k - \frac{1}{2} \cdot \left[ \sqrt{2 \cdot k + \frac{1}{4}} - \frac{1}{2} \right] \cdot \left[ \sqrt{2 \cdot k + \frac{1}{4}} + \frac{1}{2} \right],$$

$$\pi_2(k) := \left[ \sqrt{2 \cdot k + \frac{1}{4}} - \frac{1}{2} \right] - \pi_1(k)$$

gilt:

$$k = \text{paar}(\pi_1(k), \pi_2(k)).$$

**Warum  
reicht das  
aus?**

# Gödelisierung *i. A. nicht bijektiv!*

Es ist bei Gödelisierungen keine Bijektion zwischen  $\Sigma^*$  und  $\mathbb{N}$  gefordert!

Es gibt verschiedene Möglichkeiten spezielle Gödelisierungen anzugeben, von denen wir z.B. die Cantorsche Paarfunktion kennengelernt haben.

Die Paarfunktionen paar, und Ihre Erweiterung auf beliebige Zahlentupel sind Gödelisierungen nur für Zahlentupel über  $\mathbb{N}$  mit fester Dimension.

Wenn wir allerdings endliche Zahlenfolgen oder Zeichenketten variabler Länge kodieren möchten, so taugen diese Abbildungen herzlich wenig.

Von Gödel stammt die bijektive Abbildung von Zahlenfolgen/Wörtern auf Zahlen über Primzahlprodukte:

$$\nu_{\mathbb{N}\text{-seq}}(\alpha_1, \alpha_2, \dots, \alpha_m) := \prod_{i=1}^m p_i^{\alpha_i + [i = m]} - 1$$

M. Jantzen, FGI 1, SoSe 2009: 9

Montag, 6. Juli 2009

9

## allgemeine Notation für Gödelnummerncodierungen

### Definition/Vereinbarung 62:

Gödelisierungen werden von nun an immer als bijektive Abbildungen angesehen und – sofern das Alphabet  $G$  (oder ein anderes) festgelegt ist – durch  $\langle \rangle : G^* \rightarrow \mathbb{N}$  notiert.

### Beispiel:

Mit  $\langle abbab \rangle$  wird diejenige natürliche Zahl dargestellt, die gemäß der beliebig gewählten, aber eindeutig festgesetzten Gödelisierung, die Gödelnummer von  $abbab$  ist.

Wir können **immer** auch die lexikalische Anordnung der Wörter benutzen, und benutzen dann  $i$  als Gödelnummer des  $i$ -ten Wortes in dieser Abzählung!

M. Jantzen, FGI-1, SoSe 2009: 10

Montag, 6. Juli 2009

10

## Satz 37:

Sei  $G$  ein Alphabet zur Kodierung von Turingmaschinen bzw. Wörtern, sowie

$w_i$  das  $i$ -te Wort und

$A_j$  die  $j$ -te DTM in der (lexikalischen) Aufzählung der Wörter  $w_i \in G^*$  und  $A_j \in G^*$ .

Dann gilt:

Die Menge  $L_d := \{\langle w_i \rangle \mid w_i \notin L(A_i)\} \subseteq \mathbb{N}$  ist nicht aufzählbar!

Das Tupel  $T := (Q, \Sigma, \Gamma, \delta, q_0, \#, F)$ , welches eine DTM spezifiziert, kann als Zeichenkette über dem Alphabet  $G := Q \uplus \Sigma \uplus \Gamma \uplus \{), (, \}, \{, ,\}$  aufgefasst werden, sofern die Übergangsfunktion  $\delta \subseteq Q \times (\Gamma \cup \Sigma) \times (\Gamma \cup \Sigma) \times \{l, r, -\} \times Q$  als Relation notiert wird.

M. Jantzen, FGI-1, SoSe 2009: 11

Montag, 6. Juli 2009

11

## Beweis durch Diagonalisierung:

### Beweis:

$G^*$  ist in der lexikalischen Ordnung aufzählbar. (klar)

Die Teilmenge von  $G^*$  aller derjenigen Wörter, die Kodierung einer Turingmaschine sind, ist auch aufzählbar.

(Es gibt TM, die für  $w \in G^*$  entscheiden kann, ob dieses die zulässige Kodierung einer TM ist.)

Betrachtet man die unendliche Matrix mit den Spalten  $w_1, w_2, w_3, \dots$ , den Zeilen  $A_1, A_2, A_3, \dots$  und den Einträgen: 1, falls  $w_i \in L(A_i)$  bzw. 0, falls  $w_i \notin L(A_i)$ , so entspricht  $L_d$  gerade der Diagonalen, von der nur die Einträge 0 Berücksichtigung fanden.

M. Jantzen, FGI-1, SoSe 2009: 12

Montag, 6. Juli 2009

12

# Die Matrix der charakteristischen Funktion

$L_d \notin \mathcal{R}_e$ :

Charakteristische Funktion für  $L(M_i)$  und  $L_d$ :

	$w_0$	$w_1$	$w_2$	$\dots$	$w_n$	$\dots$
$M_0$	<b>0</b>	1	1	$\dots$	0	$\dots$
$M_1$	1	<b>1</b>	0	$\dots$	1	$\dots$
$M_2$	1	0	<b>0</b>	$\dots$	1	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
$M_n$	1	1	0	$\dots$	<b>1</b>	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
$L_d$	1	0	1	$\dots$	0	$\dots$

Also:  $\forall i \in \mathbb{N} : w_i \in L(M_i) \iff w_i \notin L_d$

Somit  $\forall i \in \mathbb{N} : L(M_i) \neq L_d$

und  $L_d := \{\langle w_i \rangle \mid w_i \notin L(A_i)\}$  ist nicht aufzählbar.

M. Jantzen, FGI-1, SoSe 2009: 13

Montag, 6. Juli 2009

13

## Beendigung des Beweises

Angenommen, es sei  $L_d$  doch aufzählbar, d.h. es gibt eine TM  $A_j$  in der Aufzählung aller (Kodierungen von) Turingmaschinen die  $L_d$  akzeptiert:  $L_d = L(A_j)$ . Nun gilt für das Wort  $w_j$  entweder  $w_j \in L_d$  oder  $w_j \notin L_d$ . In beiden Fällen ergibt sich ein Widerspruch wie folgt:

$$w_j \in L_d \xrightarrow{\text{(Def. von } L_d)}} w_j \notin L(A_j) \xrightarrow{\text{(Annahme)}} w_j \notin L_d.$$

Andererseits auch:

$$w_j \notin L_d \xrightarrow{\text{(Annahme)}} w_j \notin L(A_j) \xrightarrow{\text{(Def. von } L_d)}} w_j \in L_d.$$

Wegen Satz 35 sind weder  $L_d$  noch  $G^* \setminus L_d$  rekursiv (entscheidbar).

$G^* \setminus L_d = \{w_i \mid w_i \in L(A_i)\}$  ist jedoch eine aufzählbare Menge.

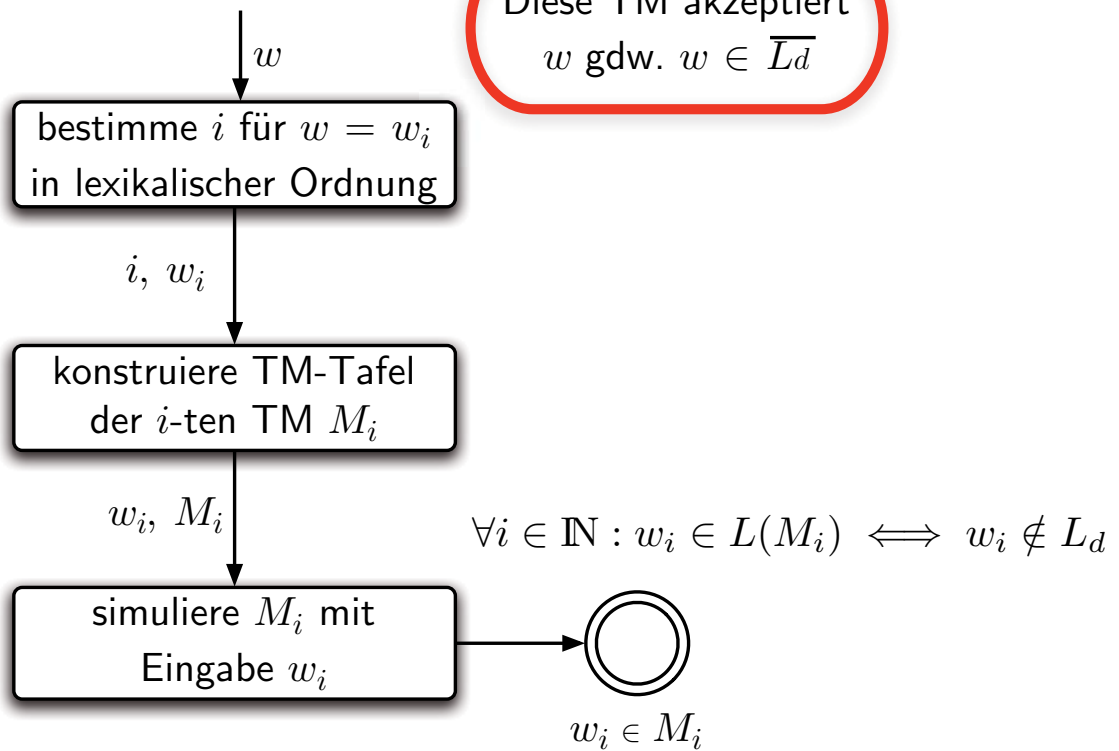
M. Jantzen, FGI-1, SoSe 2009: 14

Montag, 6. Juli 2009

14

# das Komplement von $L_d$

... ist aufzählbar:



M. Jantzen, FGI-1, SoSe 2009: 15

Montag, 6. Juli 2009

15

# Das Halteproblem

Def. hier nur wiederholt!

**Definition 60:**

Sei  $H := \left\{ \langle A \rangle \langle w \rangle \in \{0, 1\}^* \mid \right.$   
die TM  $A$  hält bei Eingabe von  $w \in \Sigma^*$  an  $\left. \right\}$ .

Wichtig zur Erkennung von Endlosschleifen in Programmen!

Programm  $P =$  Turingmaschine  $A$

Programmeingabe  $x =$  Eingabewort  $w$  der TM  $A$

aber:

**Satz 37:**

Die Menge  $H$  aus Def. 60 ist nicht entscheidbar.

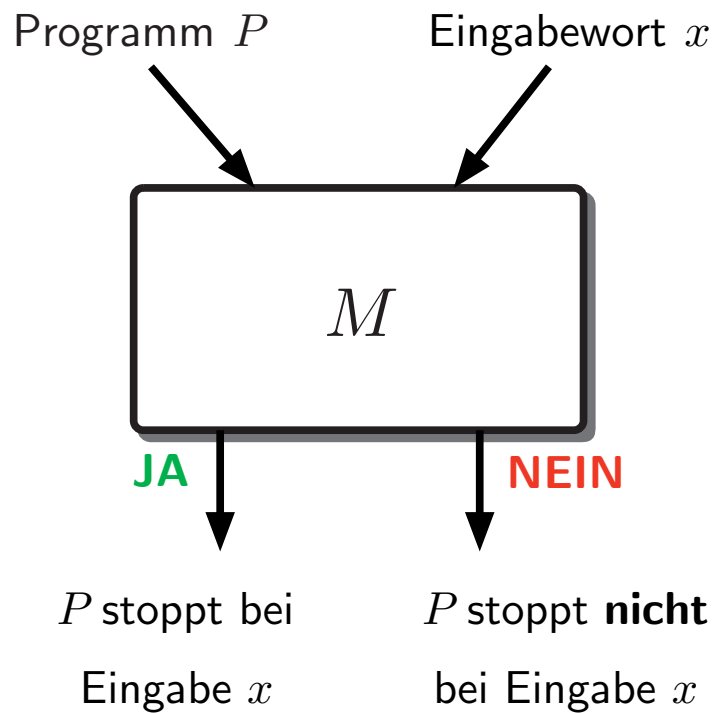
M. Jantzen, FGI-1, SoSe 2009: 16

Montag, 6. Juli 2009

16

# indirekter Beweis durch Selbstanwendung

Angenommen  $M$  löst das Halteproblem  $H$  :



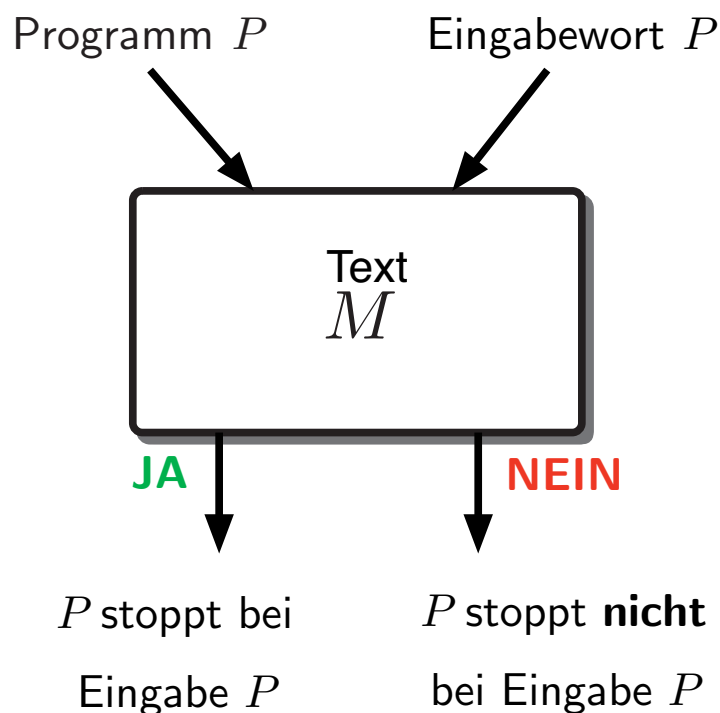
M. Jantzen, FGI-1, SoSe 2009: 17

Montag, 6. Juli 2009

17

## Halteproblem (2)

Eingabewort  $x$  ersetzt durch das Programm  $P$  :



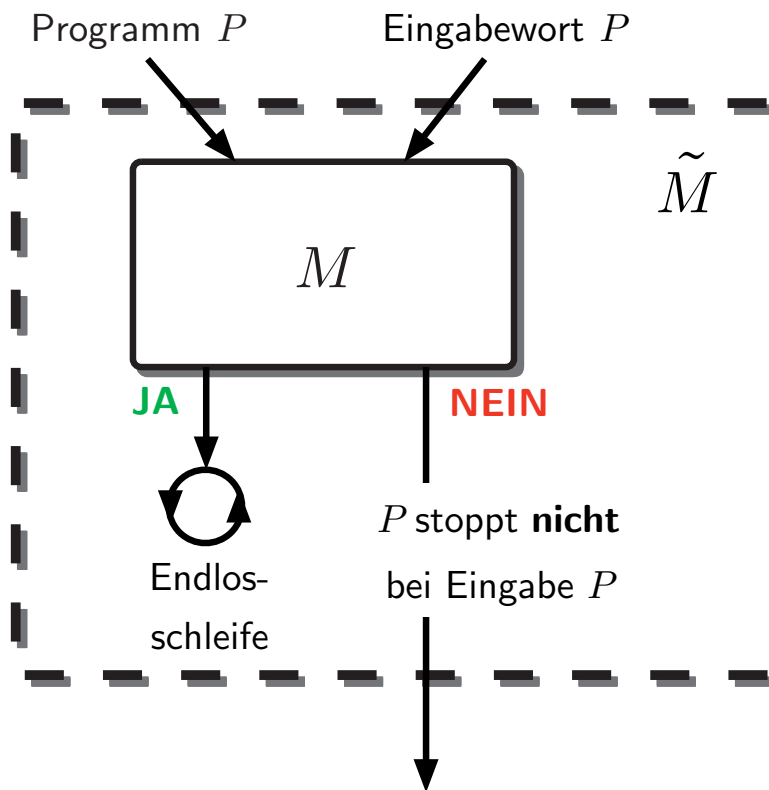
M. Jantzen, FGI-1, SoSe 2009: 18

Montag, 6. Juli 2009

18

# Halteproblem (3)

Neue Maschine  $\tilde{M}$  mit Endlosschleife bei JA :



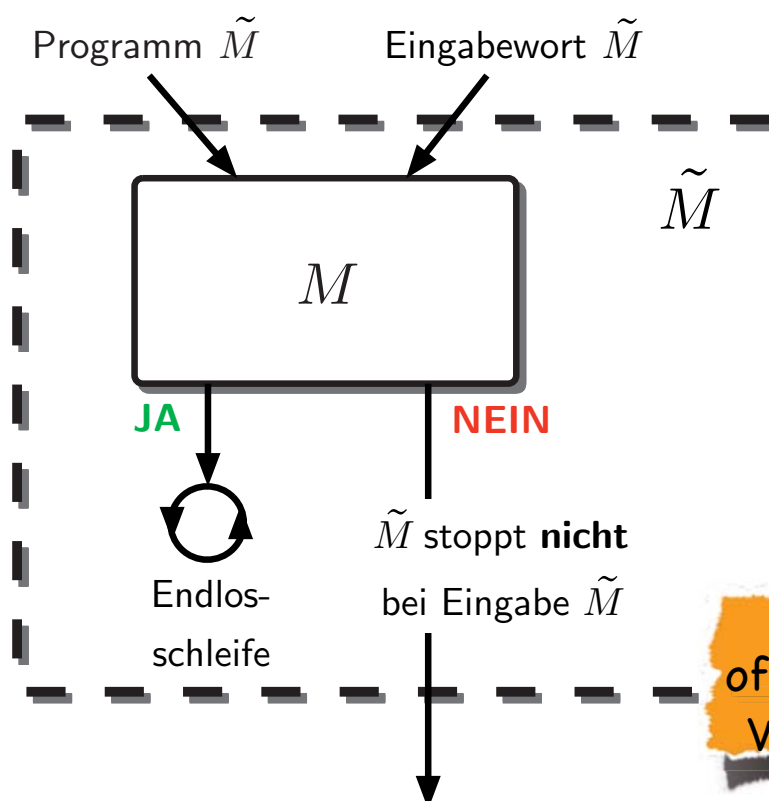
M. Jantzen, FGI-1, SoSe 2009: 19

Montag, 6. Juli 2009

19

# Halteproblem (3): die Selbstanwendung

Als Programm  $P$  verwenden wir nun  $\tilde{M}$ :



dies ist ein offensichtlicher Widerspruch!

M. Jantzen, FGI-1, SoSe 2009: 20

Montag, 6. Juli 2009

20

# Folgerung

Alle Inklusionen dieser Sprachfamilien wurden nun als  
echte Inklusionen erkannt:  
keine zwei Sprachfamilien sind identisch!

Folgende Beziehungen sind nun bewiesen:

- Familie der **regulären Mengen**
- $\subsetneq$  Familie der **kontextfreien Mengen**
- $\subsetneq$  Familie der **kontextsensitiven Mengen**
- $\subsetneq$  Familie der **entscheidbaren Mengen**
- $\subsetneq$  Familie der **aufzählbaren Mengen**
- $\subsetneq$  Familie der **abzählbaren Mengen**
- $\neq$  Familie der **überabzählbaren Mengen**

## Halteproblem und $L_d$

- Kodieren wir  $H$  und  $L_d$  über dem Alphabet  $\{0,1\}$
- Unentscheidbarkeit von  $H$  kann durch Reduktion von  $L_d$  auf  $H$  gezeigt werden:

$$w \in L_d \iff \langle w \rangle \langle w \rangle \notin H$$

- D.h.: wenn  $H$  entscheidbar ist, dann ist auch  $L_d$  entscheidbar. Letzteres ist aber nicht der Fall!

# Wichtige / interessante Unentscheidbarkeitsresultate:

 Schon als unentscheidbar kennen wir:

1. Sprache  $L_d$
2. Komplement von  $L_d$
3. Halteproblem, d.h., Sprache  $H$

 außerdem unentscheidbar:

1. Kachelprobleme
2. 10. Hilbertsches Problem
3. Vorkommen einer 1 als Bild einer Funktion
4. jedes nichttriviale Problem über Turingmaschinen!

M. Jantzen, FGI-1, SoSe 2008: 23

Montag, 6. Juli 2009

23

## Postsches Korrespondenzproblem

### Definition 64:

Sei  $P \subseteq \Sigma^* \times \Sigma^*$  eine endliche Menge von Wortpaaren

$$P := \{(u_i, v_i) \mid 1 \leq i \leq |P|, u_i, v_i \in \Sigma^*\}.$$

Als Post'sches Korrespondenzproblem (PCP) bezeichnet man folgendes Problem:

### PCP:

<b>Gegeben:</b>	Eine beliebige, endliche Menge $P = \{(u_i, v_i) \mid 1 \leq i \leq  P , u_i, v_i \in \Sigma^*\} \subseteq \Sigma^* \times \Sigma^*$
<b>Gesucht:</b>	Indexfolge $i_1 i_2 \dots i_k$ mit $\forall_{j=1}^k : 1 \leq i_j \leq  P $ und $u_{i_1} u_{i_2} \dots u_{i_k} = v_{i_1} v_{i_2} \dots v_{i_k}$
<b>Antwort:</b>	JA oder NEIN

M. Jantzen, FGI-1, SoSe 2009: 24

Montag, 6. Juli 2009

24

## Beispiel

Die Paare: 1:  $\begin{bmatrix} a \\ ba \end{bmatrix}$ , 2:  $\begin{bmatrix} aa \\ a \end{bmatrix}$ , 3:  $\begin{bmatrix} ab \\ aa \end{bmatrix}$ . Gibt es Lösung?

## Beispiel

Die Paare: 1:  $\begin{bmatrix} a \\ ba \end{bmatrix}$ , 2:  $\begin{bmatrix} aa \\ a \end{bmatrix}$ , 3:  $\begin{bmatrix} ab \\ aa \end{bmatrix}$ . Gibt es Lösung?

Ja: eine Indexfolge ist 231, mit:  $\begin{bmatrix} aa \\ a \end{bmatrix} \begin{bmatrix} ab \\ aa \end{bmatrix} \begin{bmatrix} a \\ ba \end{bmatrix}$

# Unentscheidbarkeit des *PCP*

## Satz 38:

Es gibt keinen Algorithmus, der für ein beliebiges *PCP* entscheidet, ob es eine Lösung besitzt!

Wenn das Alphabet nur ein Symbol enthält, dann ist jedes (endliche) *PCP* entscheidbar.

Es konnte mit sehr komplizierten Beweis gezeigt werden, dass jedes *PCP* mit höchstens zwei Wortpaaren entscheidbar ist!

Das bisher kleinste, unentscheidbare *PCP* besitzt 7 Wortpaare!

# Der Satz von Rice

## Satz 40:

Jede nichttriviale Eigenschaft  $\mathcal{S}$  der aufzählbaren Sprachen ist unentscheidbar.

Nichttriviale Eigenschaften zeichnen sich dadurch aus, dass es sowohl Mengen gibt, die sie erfüllen, wie auch andere, die diese Eigenschaft nicht erfüllen.

Viele der bisherigen und noch folgenden Unentscheidbarkeitsresultate folgen aus diesem allgemeinen Theorem!

# Kommt 1 als Funktionswert vor?

## Definition 63:

Mit  $M_T$  sei die Menge aller (Kodierungen von) Turing-Maschinen  $M$  bezeichnet, die totale Funktionen  $f_M : \Sigma^* \rightarrow \{0, 1\}$  berechnen.

## Problem:

<b>Gegeben:</b>	Eine beliebige stets haltende Turing-Maschine
<b>Gesucht:</b>	Wird bei allen Eingaben stets die Ausgabe 0 berechnet?
<b>Antwort:</b>	JA oder NEIN

Das Problem, ob eine Funktion irgendwann den Wert 1 als Resultat erhält, ist **UNENTSCHEIDBAR** !

M. Jantzen, FGI-1, SoSe 2009: 28

Montag, 6. Juli 2009

28

## Unentscheidbarkeitsresultate

### Satz 39:

Es gibt keinen Algorithmus, der für eine beliebige Funktion

$$f_M \in M_T$$

entscheidet, ob

$$f_M(w) = 1 \text{ für mindestens ein } w \in \Sigma^* \text{ gilt.}$$

### Korollar:

Es ist unentscheidbar, ob eine beliebige, durch eine TM definierte, entscheidbare Menge  $M$  leer ist.

M. Jantzen, FGI-1, SoSe 2009: 29

Montag, 6. Juli 2009

29

# weitere Unentscheidbare Fragen

Folgende Probleme sind unentscheidbar:

Ist  $L$  endliche Menge?

Ist  $L$  leere Menge?

Ist  $L$  unendliche Menge?

Ist  $L$  reguläre Menge?

Ist  $L$  kontextfreie Sprache?

Ist  $L$  entscheidbare Sprache?

Ist  $L$  eine Menge mit genau einem Element?