

Vorlesungstermin

WICHTIGE ÄNDERUNG !!!

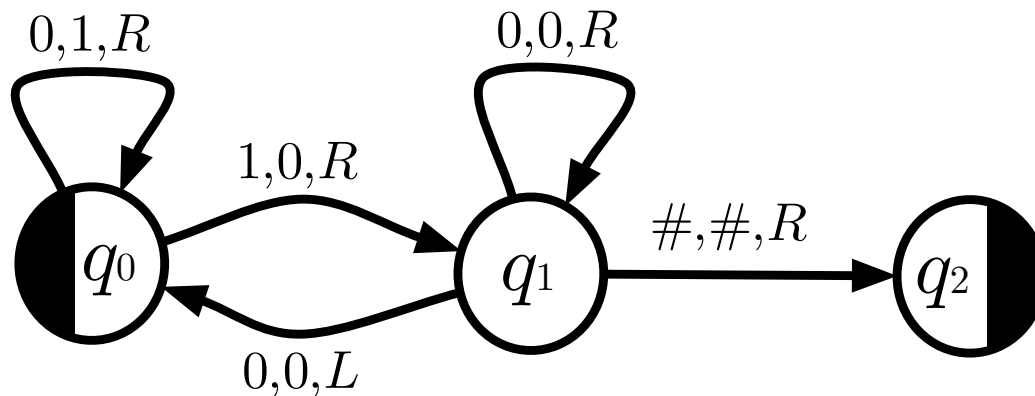
Am 13.11.2001 steht der Hörsaal wg. der Universitätstage nicht zur Verfügung!

Ersatztermin: Montag, 12.11.2001 um 16:15 Uhr (bis 17:45) im **Audi II**



Beispiel: NTM

$$M = (\{q_0, q_1, q_2\}, \{0, 1\}, \{0, 1, \#\}, \delta, q_0, \#, \{q_2\})$$

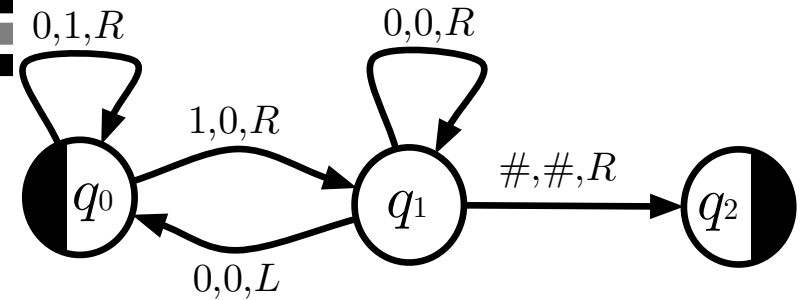


Zustand	0	1	#
q_0	$\{(1, R, q_0)\}$	$\{(0, R, q_1)\}$	$\emptyset$
q_1	$\{(0, R, q_1), (0, L, q_0)\}$	$\{(1, R, q_1), (1, L, q_0)\}$	$\{(\#, R, q_2)\}$
q_2	$\emptyset$	$\emptyset$	$\emptyset$

Aufgabe: Welche Konfigurationen sind bei Eingabe von 01 (bzw. 100) erreichbar?



Beispiel: NTM-Konfigurationen



Eingabe: 01 (bzw. 100)

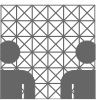
$$[q_0]01 \vdash_M 1[q_0]1 \vdash_M 10[q_1] \vdash_M 10\#[q_2]$$

$$[q_0]100 \vdash_M 0[q_1]00 \vdash_M 00[q_1]0 \vdash_M 000[q_1] \vdash_M 000\#[q_2]$$

$$[q_0]100 \vdash_M 0[q_1]00 \vdash_M [q_0]000 \vdash_M 1[q_0]00 \vdash_M 11[q_0]0 \vdash_M 111[q_0]$$

$$[q_0]100 \vdash_M 0[q_1]00 \vdash_M 00[q_1]0 \vdash_M 0[q_0]00 \vdash_M 01[q_0]0 \vdash_M 011[q_0]$$

$$[q_0]100 \vdash_M 0[q_1]00 \vdash_M 00[q_1]0 \vdash_M 000[q_1] \vdash_M 00[q_0]0 \vdash_M 001[q_0]$$



**Entscheidbare
vs.
rekursiv aufzählbare
Mengen**



Akzeptierung/Berechnung

... ein kurzer Rückblick:

- Sprache L wird durch eine TM M akzeptiert gdw. **nur** Wörter aus L eine Erfolgsrechnung auf M haben.
- Funktion f wird von DTM M berechnet, gdw. M für **jede** Eingabe w in einer Endkonfiguration $q_e f(w)$ hält bzw. nicht hält, falls $w \notin \text{Def}(f)$.

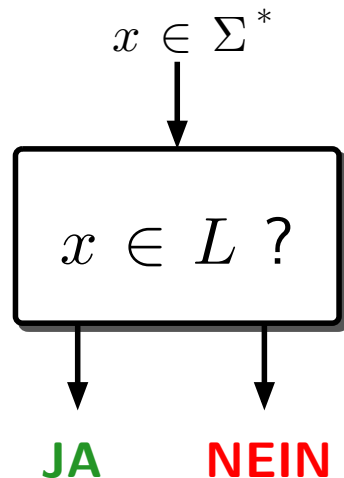


Definition: rekursiv

Eine Menge $L \subseteq \Sigma^*$ heißt (relativ zu Σ^*) **entscheidbar** oder **rekursiv** gdw. ihre charakteristische Funktion $\chi_L : \Sigma^* \rightarrow \{0, 1\}$ berechenbar ist.

Die *Klasse aller entscheidbaren Mengen* wird mit $\mathcal{REC}$ (*recursive sets*) bezeichnet.

Entscheidbarkeit

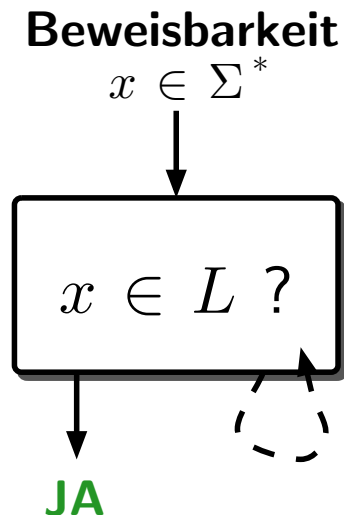


Definition: rekursiv aufzählbar

Eine Menge $L \subseteq \Sigma^*$ heißt **beweisbar** oder **rekursiv aufzählbar** gdw. $L = \emptyset$ ist, oder eine totale Turing-berechenbare Funktion $g : \mathbb{N} \rightarrow \Sigma^*$ existiert, für die $g(\mathbb{N}) = L$ ist.

Die *Klasse aller aufzählbaren Mengen* wird mit $\mathcal{RE}$ (*recursively enumerable sets*) bezeichnet.

... oder
anders dar-
gestellt:



Eigenschaften

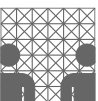
Theorem: L ist *rekursiv aufzählbar* gdw. eine TM M mit $L = L(M)$ existiert. **Beweisidee:** $L = L(M) \Rightarrow \exists$ TM A , die alle Wörter aus L auf die Ausgabe schreibt:

- Generiere sukzessive Paare aus $(i, j) \in \mathbb{N}^2$.
- Simuliere M auf dem i -ten Wort w_i .
- Falls M nach j Schritten hält, schreibe w_i und ein Trennsymbol.

$\exists$ TM A , die alle Wörter aus L schreibt $\Rightarrow L = L(M)$

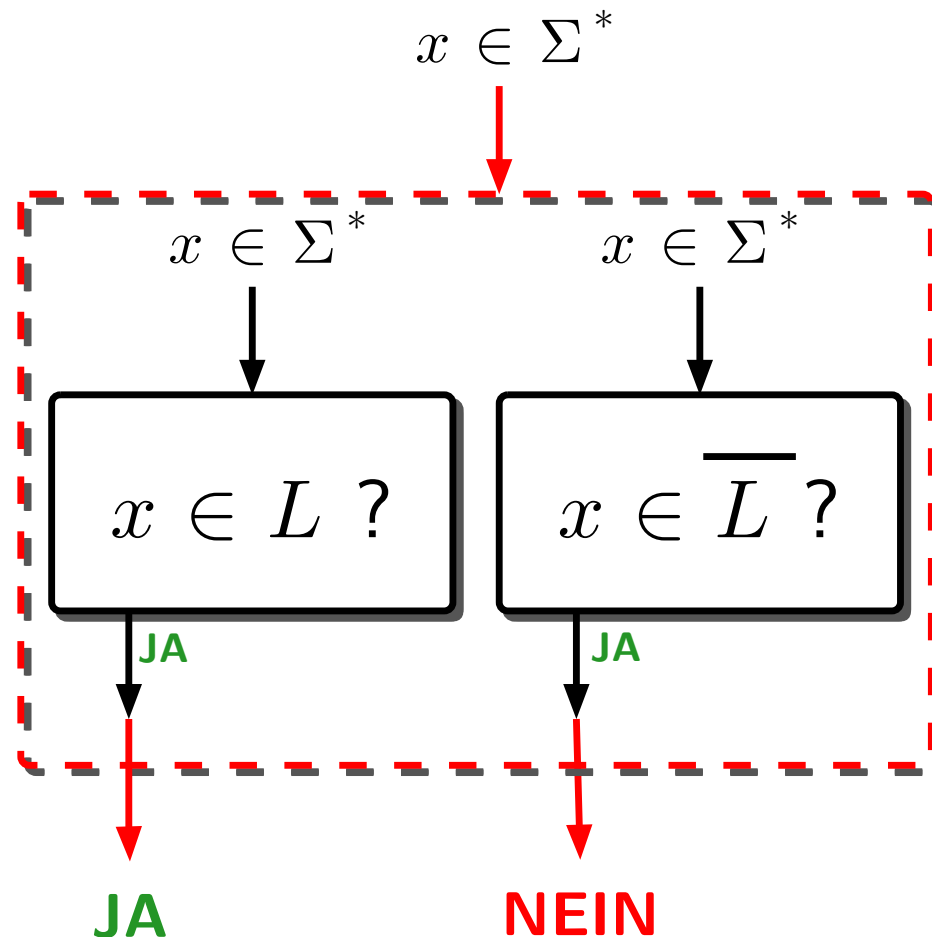
- Verwende Zähler i
- Kontrolliere, ob w_i (Ausgabe von A) das Eingabewort w ist? Ja: akzeptiere! Nein: inkrementiere i .

Analog: L *rekursiv aufzählbar* $\Rightarrow \exists$ TMM $L = L(M)$



Eigenschaften

Theorem: Ist eine Menge L und ihr Komplement $\overline{L}$ rekursiv aufzählbar, so ist L auch rekursiv.



Hierarchie

Folgende Beziehungen wollen wir zeigen:

Klasse der **regulären Mengen**

$\subsetneq$ Klasse der **kontextfreien Mengen**

$\subsetneq$ Klasse der **kontextsensitiven Mengen**

$\subsetneq$ Klasse der **entscheidbaren Mengen**

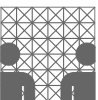
$\subsetneq$ Klasse der **aufzählbaren Mengen**

$\subsetneq$ Klasse der **abzählbaren Mengen**

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

Existenz überabzählbarer Mengen ist bekannt.

(z.B. aus Diagonalbeweis).



Abschlußeigenschaften

Theorem: Die Klasse der entscheidbaren Mengen bildet eine *boolesche Mengen-Algebra*.

Beweisidee: Z.z. ist der Abschluß gegen

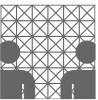
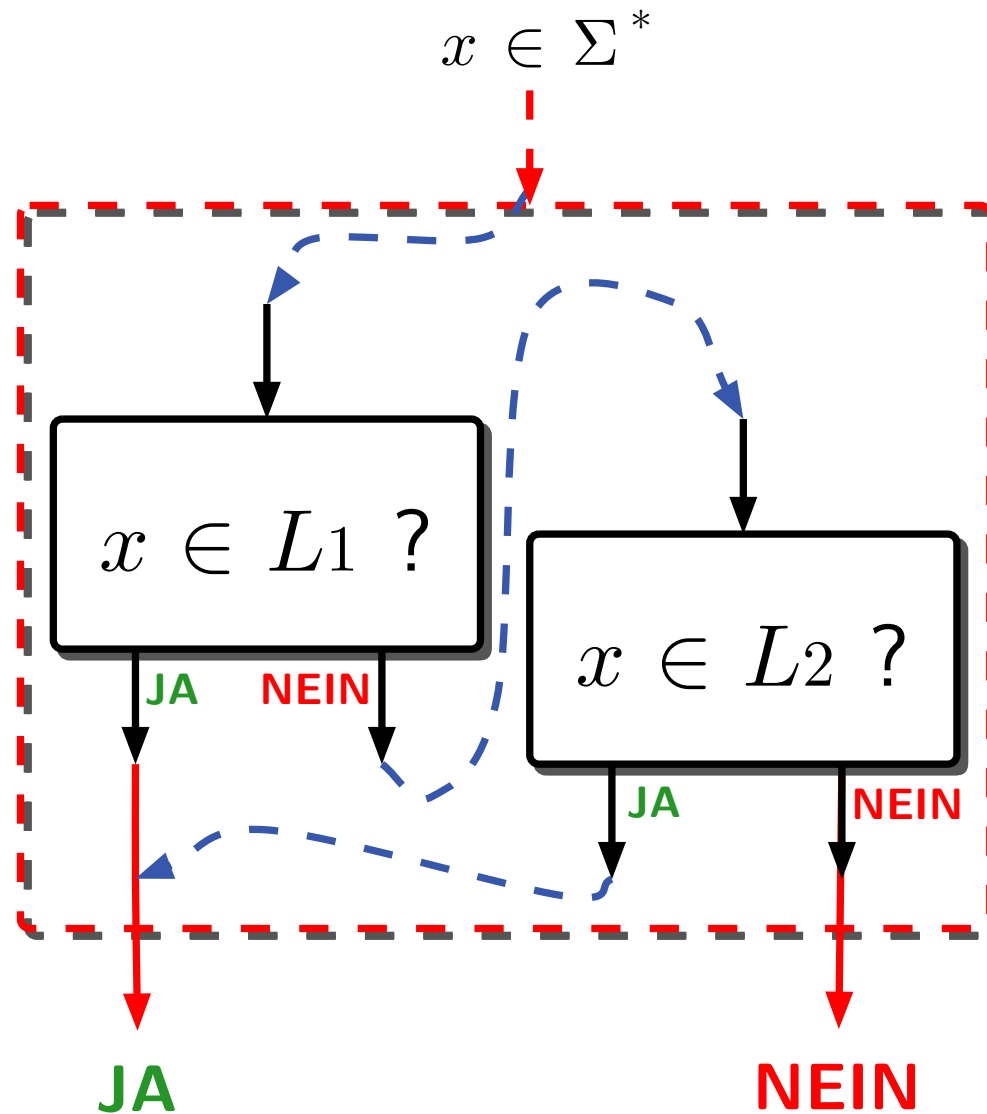
- Komplementbildung,
- Durchschnitt,
- Vereinigung.

Komplementabschluß:

... einfach **JA** und **NEIN** vertauschen.

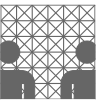
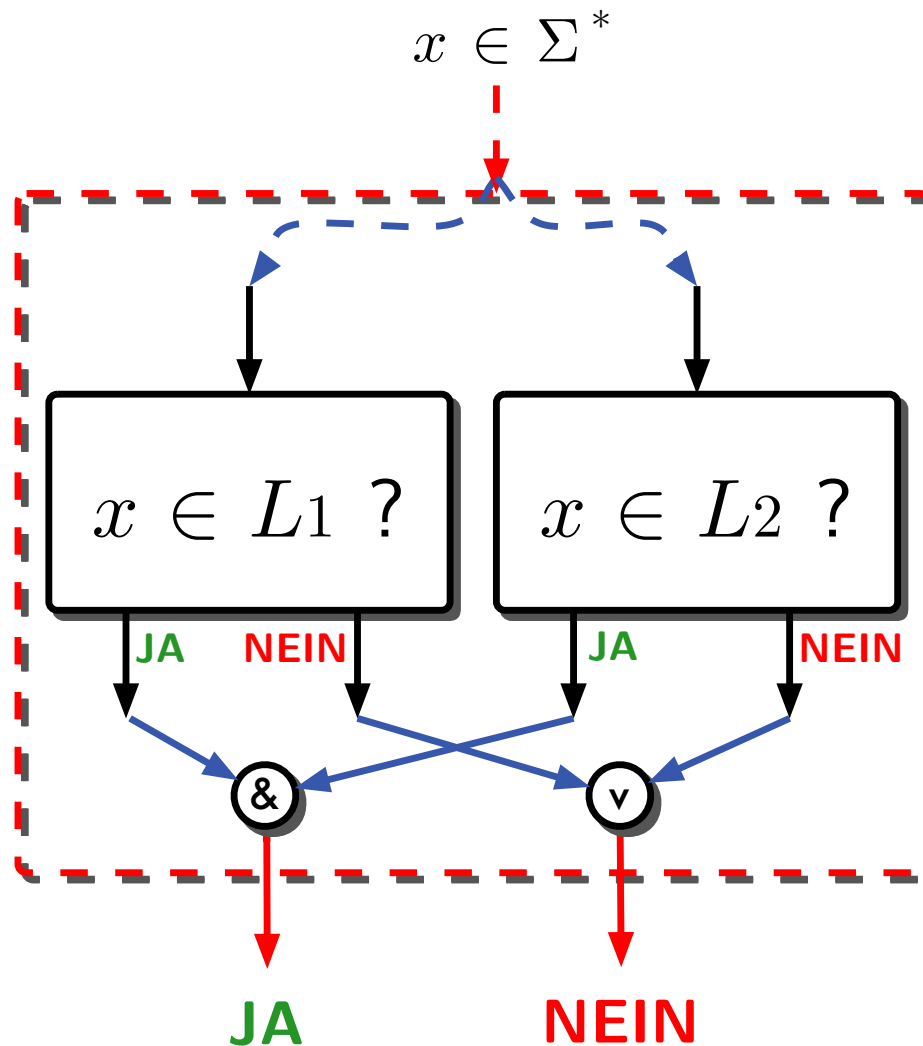


Vereinigung

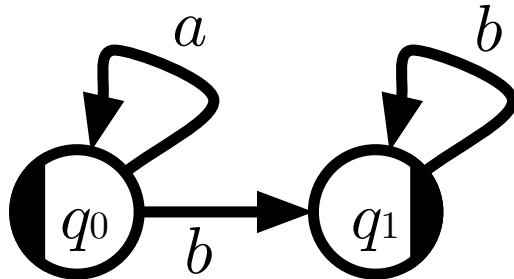


Durchschnitt

... folgt nach De Morgan, oder direkt:



Gödelisierung von FA's



... wird kodiert durch:

a	X
b	XX
q_0	Z
q_1	ZZ

Kante (q_0, b, q_1) :

-ZXXZZ

Insgesamt:

-ZXZ-ZXXZZ+ZZXXZZ

... ähnlich auch für Turing-Maschinen!



nicht aufzählbare Menge

- Wir zeigen, daß es Mengen gibt, die nicht rekursiv aufzählbar sind:

Theorem: Sei G ein Alphabet zur Kodierung von Turing-Maschinen bzw. Wörtern, sowie w_i das i -te Wort und M_i die i -te DTM in der lexikalischen Aufzählung der Wörter $\langle M_i \rangle \in G^*$.

Dann ist die Menge $L_d := \{w_i \mid w_i \notin L(M_i)\}$ nicht aufzählbar.

(Selbstanwendbarkeitsproblem)



Beweis: $L_d \notin \mathcal{RE}$

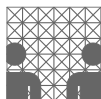
Charakteristische Funktion für $L(M_i)$ und L_d :

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

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

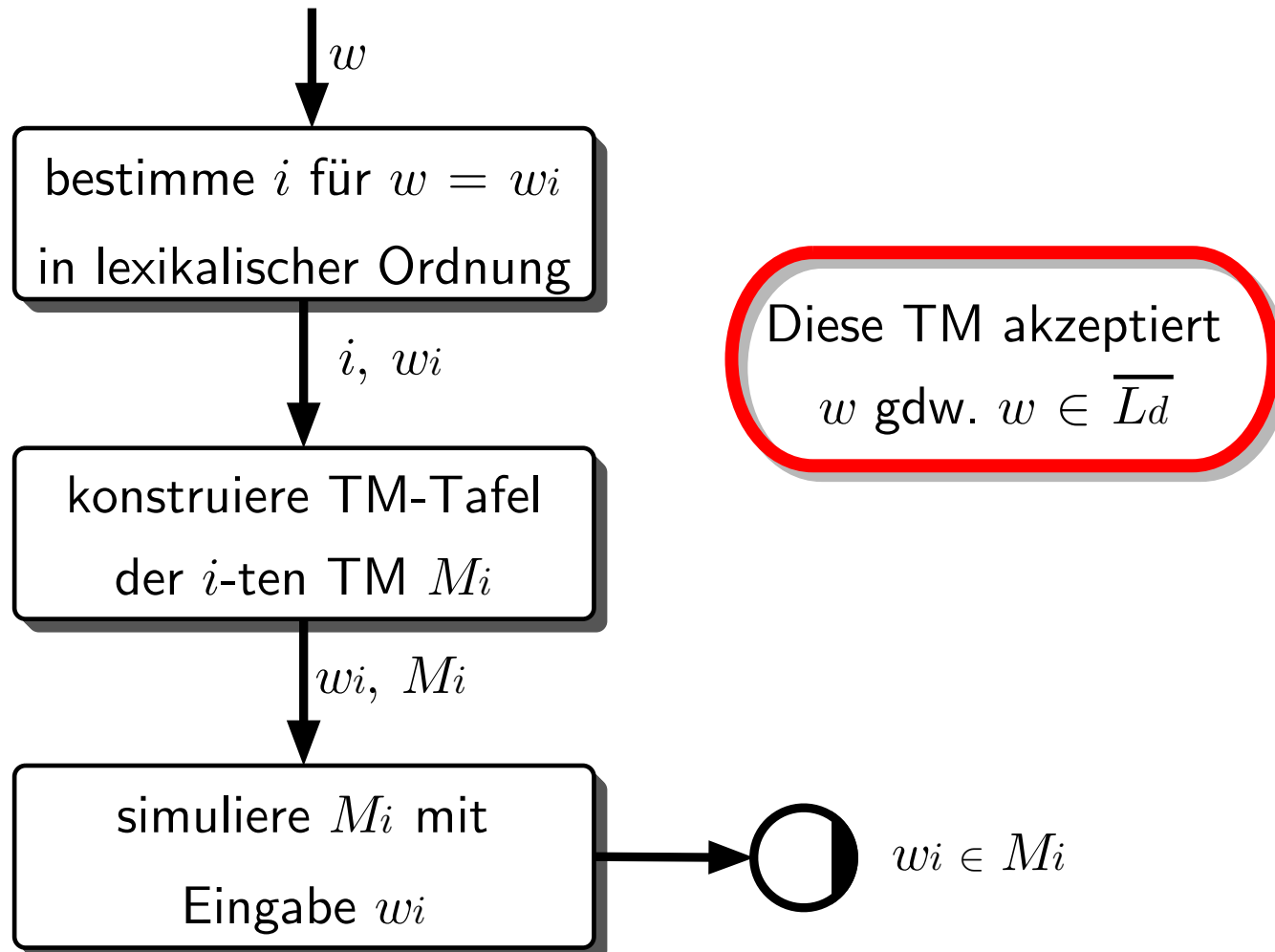
Somit $\forall i \in \mathbb{N}. L(M_i) \neq L_d$

und L_d nicht aufzählbar!



Das Komplement von L_d

... ist aufzählbar:



Definition: UTM

- Sei M eine DTM mit Anfangskonfiguration k_0 .
- Sei $\langle M \rangle$ die Kodierung über dem Alphabet $G := \{0, 1\}$ von M und $\langle k_0 \rangle$ jene von k_0 .

Eine DTM $U := (Z, \Sigma, \Gamma, \delta, q_0, Z_{\text{end}})$ heißt **universelle Turing-Maschine (UTM)**, wenn für die Anfangskonfiguration $q_0 \langle M \rangle \langle k_0 \rangle$ gilt:

- $k_i \vdash_M k_j \Rightarrow \langle A \rangle \langle k_i \rangle \vdash_U^* \langle A \rangle \langle k_j \rangle$, wobei hier nur die relevante Bandinschrift von U gemeint ist, ohne die Stellungen ihres LSK und der Zustände.



Existenz einer UTM

Definition der **universellen Turing-Maschine** macht noch keine Aussage darüber, ob so etwas auch tatsächlich existiert!

Lemma: Es gibt universelle Turing-Maschinen.

- Lesen der Kodierung einer TM und eines Eingabewortes,
- Simulation der Einzelschritte der kodierten TM.
- hier **kein Beweis** (durch Angabe einer UTM)



Das Halteproblem

Das Halteproblem lautet:

Gegeben:	Ein Computerprogramm P und ein Eingabe x für P .
Gesucht:	Kommt P für x jemals in einen Stop- bzw. Endzustand?
Antwort:	?

- Darstellung als Menge:

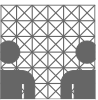
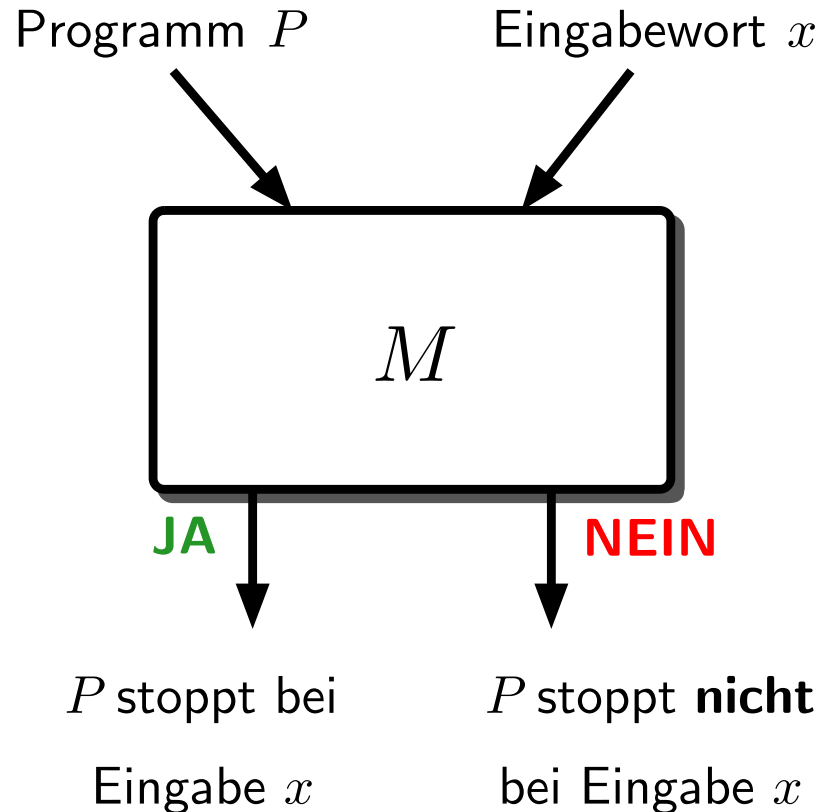
$$H = \{ \langle M \rangle \langle w \rangle \mid \text{TM } M \text{ hält auf } w \}$$

- Wichtig zur Erkennung von Endlosschleifen!
- **Aber:** H ist unentscheidbar.



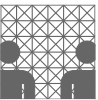
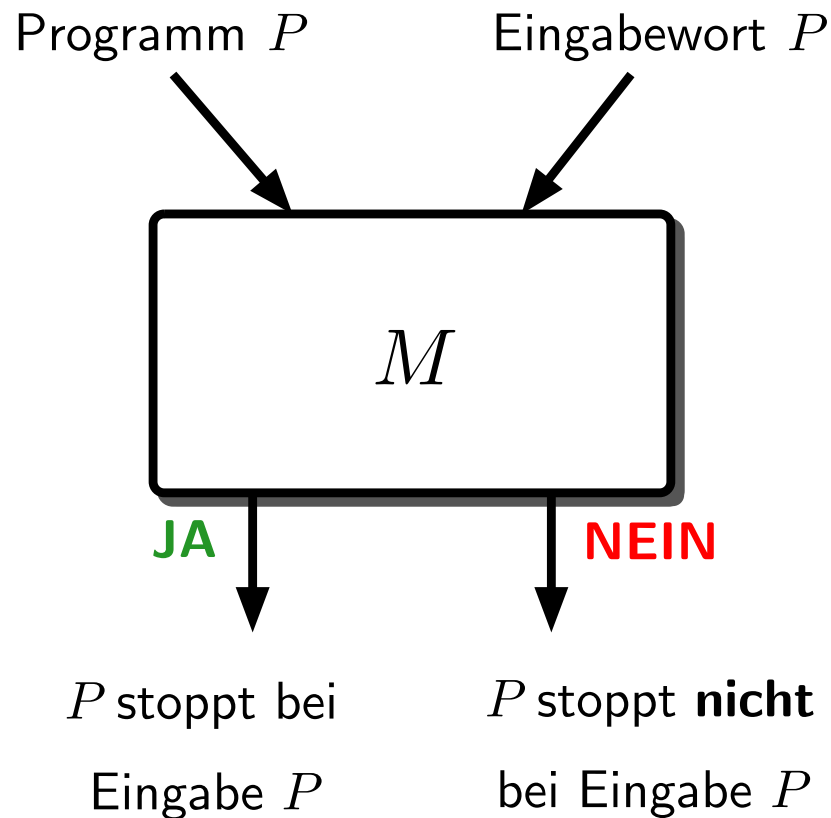
Beweis: Halteproblem $\notin \mathcal{REC}$

Erster Beweis: Konstruktion mit Widerspruch
Angenommen M löst das Halteproblem:



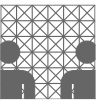
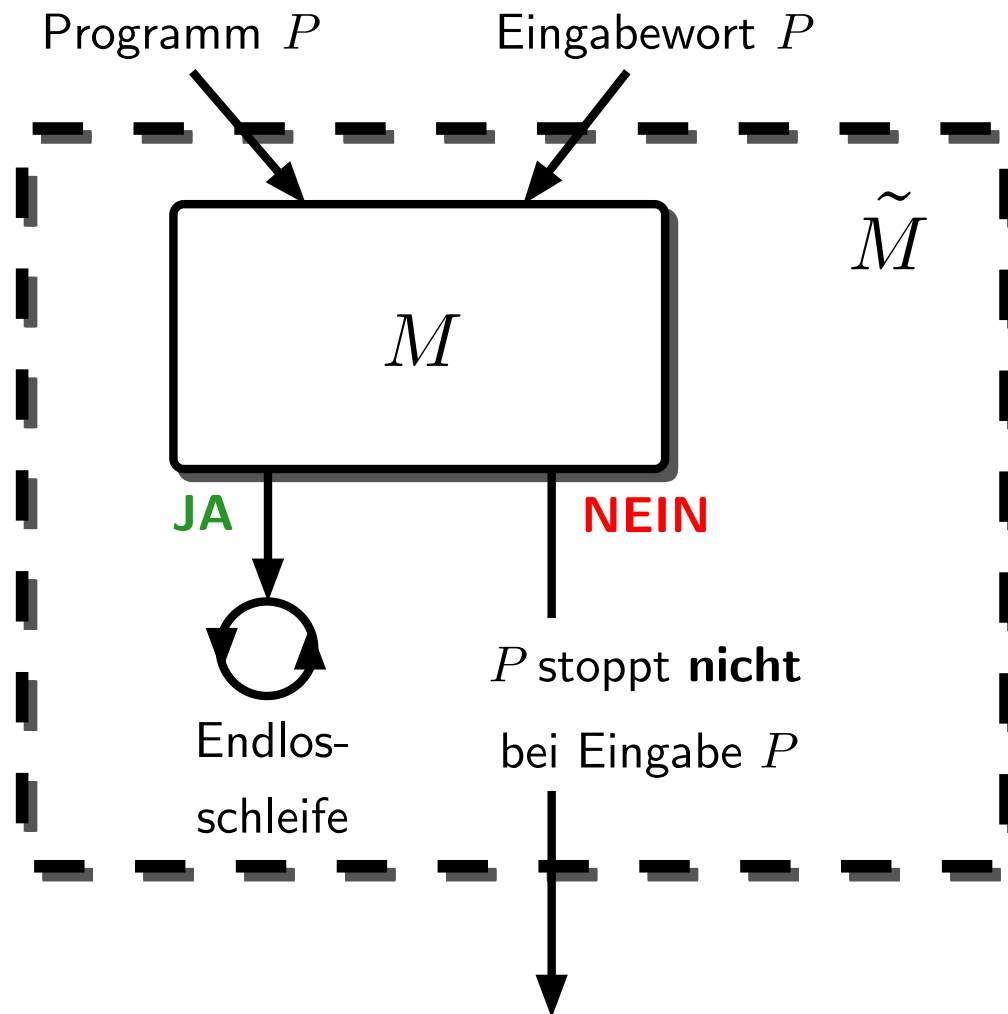
Halteproblem (2)

Eingabewort x ersetzt durch das Programm P :



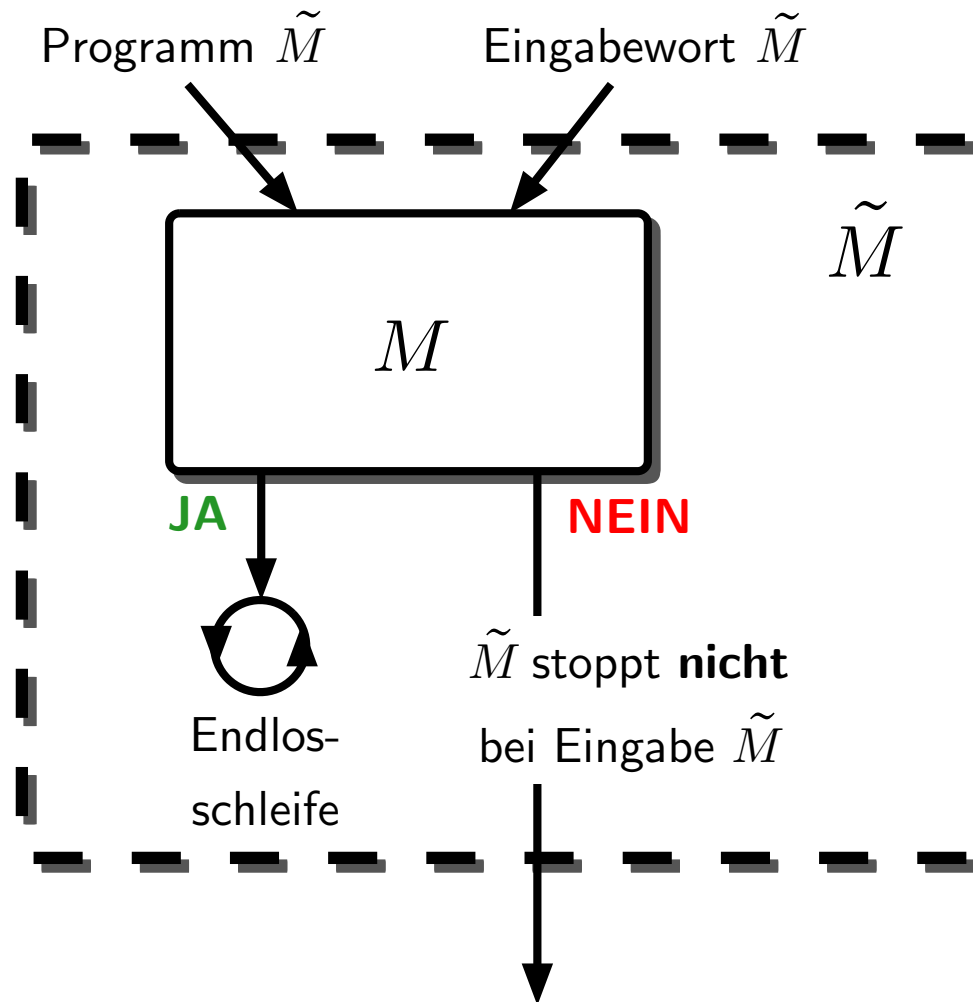
Halteproblem (3)

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



Halteproblem (4)

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



Halteproblem und L_d

- Kodieren wir L_d und H mit dem Alphabet $\{0, 1\}$.
- Die Unentscheidbarkeit des Halteproblems H kann dann durch Reduktion von $L_d^{\{0,1\}}$ auf H gezeigt werden (bei geeigneter Kodierung):

$$w \in L_d^{\{0,1\}} \iff \langle w \rangle \langle w \rangle \notin H$$

ALSO: Wenn H entscheidbar, dann auch $L_d^{\{0,1\}}$.

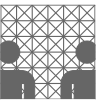


Halteproblem ist aufzählbar

$H = \{ \langle M \rangle \langle w \rangle \mid \text{TM } M \text{ hält auf } w \}$ ist rekursiv aufzählbar.

- Wir nehmen eine UTM.
- Diese simuliert M auf der Eingabe w
 - solange, bis M hält,
 - oder unendlich lange, falls M nicht auf w hält.

Mithin akzeptiert die UTM das Wort $\langle M \rangle \langle w \rangle$ gdw. M auf dem Wort w hält.



- Weitere wichtige Unentscheidbarkeitsresultate
- Weitere Berechenbarkeitsmodelle
- Realistische Maschinenmodelle

... am **Montag, 12.11.2001**
um **16:15 Uhr** im **Audi II**

