Berechenbarkeit und Komplexität

Lecture #5: Das Halteproblem

Prof. Berthold Vöcking
präsentiert durch Prof. Joost-Pieter Katoen

4. November 2008

Wiederholung: Was bedeutet *berechenbar*?

Definition

Eine Funktion $f : \Sigma^* \longrightarrow \Sigma^*$ heißt *rekursiv (berechenbar)*, wenn es eine TM gibt, die aus der Eingabe x den Funktionswert $f(x)$ berechnet.

Definition

Eine Sprache $L \subseteq \Sigma^*$ heißt *rekursiv (entscheidbar)*, wenn es eine TM gibt, die auf allen Eingaben stoppt und die Eingabe w genau dann akzeptiert, wenn $w \in L$ ist.

Gibt es nicht-rekursive Probleme?

Ja, es gibt nicht rekursive Probleme,

denn die Mächtigkeit der Menge aller Sprachen ist größer

als die Mächtigkeit der Menge aller TM.

Exkursion: abzählbare und überabzählbare Mengen

Def: abzählbare Menge

Eine Menge M heißt *abzählbar*, wenn es eine surjektive Funktion $c : \mathrm{N} \to M$ gibt.

Jede endliche Menge M ist offensichtlich abzählbar.

Im Fall einer abzählbar unendlichen Menge M gibt es immer auch eine bijektive Abbildung $c : \mathrm{N} \to M$, denn Wiederholungen können bei der Abzählung offensichtlich ausgelassen werden. Die Elemente einer abzählbaren Menge können also *nummeriert* werden.

Abzählbar unendliche Mengen haben also dieselbe Mächtigkeit wie die Menge der natürlichen Zahlen N.

Exkursion: abzählbare und überabzählbare Mengen

Beispiele für abzählbar unendliche Mengen:

- die Menge der ganzen Zahlen $\mathbb{Z}$:

$$c(i) = \begin{cases} i/2 & \text{falls } i \text{ gerade} \\ -(i+1)/2 & \text{falls } i \text{ ungerade} \end{cases}$$

- die Menge der rationalen Zahlen $\mathbb{Q}$
- die Menge der Wörter über $\{0,1\}^*$:

$$\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, \ldots$$

- die Menge der TMn, weil jede TM durch eine eindeutige Gödelnummer beschrieben wird, und die Menge der Gödelnummern eine Teilmenge der Wörter über $\{0,1\}^*$ ist

Das *i-te Wort* gemäß der kanonischen Reihenfolge bezeichnen wir im Folgenden mit w_i und die *i-te TM* mit M_i.

Exkursion: abzählbare und überabzählbare Mengen

Die Menge aller Teilmengen von N, die Potenzmenge $\mathcal{P}(\mathrm{N})$, ist hingegen überabzählbar.

Satz:

Die Menge $\mathcal{P}(\mathrm{N})$ ist überabzählbar.

Beweis: (Diagonalisierung)

- Wir führen einen Widerspruchsbeweis
- Zum Zweck des Widerspruchs nehmen wir an, dass $\mathcal{P}(\mathrm{N})$ abzählbar ist.
- Mit S_i bezeichnen wir die i-te Menge aus $\mathcal{P}(\mathrm{N})$.
- Sei $(A_{i,j})_{i\in\mathrm{N},j\in\mathrm{N}}$ eine zwei-dimensionale unendliche Matrix mit

$$A_{i,j} = \begin{cases} 1 & \text{falls } j \in S_i \\ 0 & \text{sonst} \end{cases}$$

Exkursion: abzählbare und überabzählbare Mengen

Illustration: die Matrix A könnte etwa folgendermaßen aussehen

	0	1	2	3	4	5	6	
S_0	**0**	1	1	0	1	0	1	$\cdots$
S_1	1	**1**	1	0	1	0	1	$\cdots$
S_2	0	0	**1**	0	1	0	1	$\cdots$
S_3	0	1	1	**0**	0	0	1	$\cdots$
S_4	0	1	0	0	**1**	0	1	$\cdots$
S_5	0	1	1	0	1	**0**	0	$\cdots$
S_6	1	1	1	0	1	0	**1**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		

Fortsetzung Beweis:

- Wir definieren die Menge $S_{diag} = \{i \in \mathrm{N} \mid A_{i,i} = 1\}$.
- Das Komplement dieser Menge ist

$$\bar{S}_{diag} = \mathrm{N} \setminus S_{diag} = \{i \in \mathrm{N} \mid A_{i,i} = 0\} .$$

Fortsetzung Beweis:

- Auch $\bar{S}_{diag}$ ist ein Element von $\mathcal{P}(\mathrm{N})$. In der Nummerierung von $\mathcal{P}(\mathrm{N})$ nehme $\bar{S}_{diag}$ den k-ten Platz ein, d.h. $\bar{S}_{diag} = S_k$.
- Jetzt gibt es zwei Fälle, die jeweils zum Widerspruch führen.
  - **Fall 1:**

$$A_{k,k} = 1 \overset{Def.\bar{S}_{diag}}{\Rightarrow} k \notin \bar{S}_{diag} \overset{\bar{S}_{diag}=S_k}{\Rightarrow} k \notin S_k \overset{Def.A}{\Rightarrow} A_{k,k} = 0$$

Widerspruch!

  - **Fall 2:**

$$A_{k,k} = 0 \overset{Def.\bar{S}_{diag}}{\Rightarrow} k \in \bar{S}_{diag} \overset{\bar{S}_{diag}=S_k}{\Rightarrow} k \in S_k \overset{Def.A}{\Rightarrow} A_{k,k} = 1$$

Widerspruch!

□

Exkursion: abzählbare und überabzählbare Mengen

Sei $\mathcal{L}$ die Menge aller Sprachen über $\{0,1\}^*$, d.h. $\mathcal{L} = \mathcal{P}(\{0,1\}^*)$.

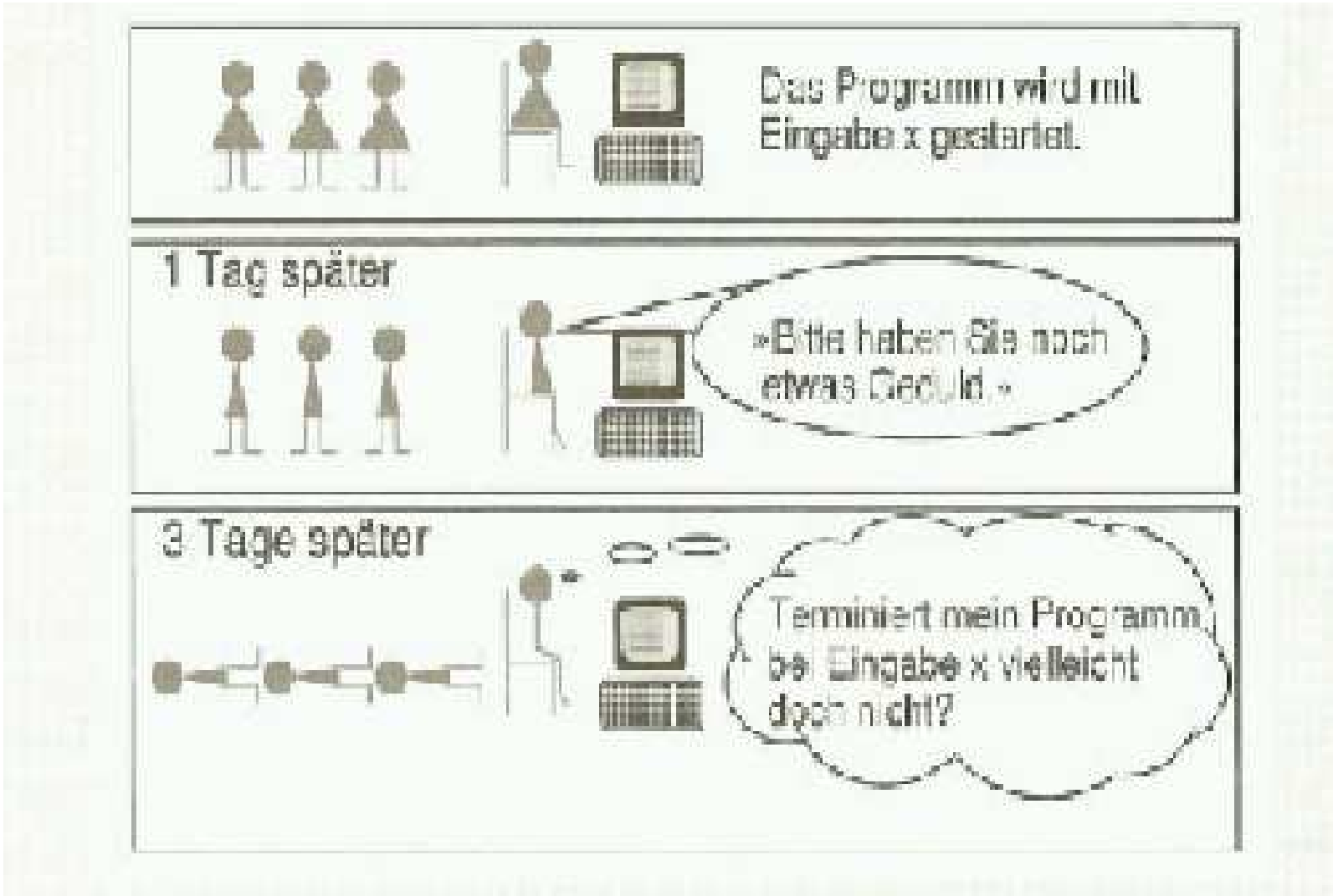
Die Menge $\{0,1\}^*$ hat dieselbe Mächtigkeit wie die Menge N.

$\mathcal{L} = \mathcal{P}(\{0,1\}^*)$ hat somit dieselbe Mächtigkeit wie $\mathcal{P}(\mathrm{N})$ und ist deshalb überabzählbar.

Fazit:

- Die Menge aller TMn ist abzählbar.
- Die Menge aller Sprachen ist überabzählbar.
- Also gibt es Sprachen, die nicht rekursiv sind.

Das Halteproblem



Das Halteproblem

Die reine Existenz unentscheidbarer Probleme ist noch nicht dramatisch, denn es könnte sich ja um uninteressante, nicht praxis-relevante Probleme handeln. Leider werden wir sehen, dass diese Hoffnung sich nicht bestätigt.

Beim *Halteproblem* geht es darum, zu entscheiden, ob ein Programm auf einer bestimmten Eingabe w terminiert. In der Notation der TM ergibt sich die folgende formale Problemdefinition.

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

Es wäre äußerst hilfreich, wenn Compiler das Halteproblem entscheiden könnten. Wir werden jedoch sehen, dass dieses elementare Problem nicht entscheidbar ist.

Unentscheidbarkeit der Diagonalsprache

Zum Beweis der Unentscheidbarkeit des Halteproblems machen wir einen Umweg über die sogenannte *Diagonalsprache*.

$$D = \{ w \in \{0,1\}^* \mid w = w_i \text{ und } M_i \text{ akzeptiert } w \text{ nicht} \} .$$

Anders gesagt, das i-te Wort bzgl. der kanonischen Reihenfolge, also w_i, ist genau dann in D, wenn die i-te TM, also M_i, dieses Wort nicht akzeptiert.

Satz:

Die Diagonalsprache D ist nicht rekursiv.

Unentscheidbarkeit der Diagonalsprache – Intuition

Warum trägt die Sprache den Namen *Diagonalsprache*? – Betrachte eine unendliche binäre Matrix A mit

$$A_{i,j} = \begin{cases} 1 & \text{falls } M_i \text{ akzeptiert } w_j \\ 0 & \text{sonst} \end{cases}$$

Beispiel:

	w_0	w_1	w_2	w_3	w_4	
M_0	**0**	1	1	0	1	$\cdots$
M_1	1	**0**	1	0	1	$\cdots$
M_2	0	0	**1**	0	1	$\cdots$
M_3	0	1	1	**1**	0	$\cdots$
M_4	0	1	0	0	**0**	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Die Diagonalsprache läßt sich auf der Diagonale der Matrix ablesen. Es ist

$$D = \{w_i \mid A_{i,i} = 0\} .$$

Unentscheidbarkeit der Diagonalsprache – Beweis

Beweis:

Wir führen einen Widerspruchsbeweis und nehmen an, D ist rekursiv. Dann gibt es eine TM M_j, die D entscheidet.

Wir wenden M_j auf w_j an. Es ergeben sich zwei Fälle, die jeweils direkt zum Widerspruch führen.

- **Fall 1:**

$$w_j \in D \overset{M_j \text{ entsch. } D}{\Rightarrow} M_j \text{ akzeptiert } w_j \overset{\text{Def. von } D}{\Rightarrow} w_j \notin D$$

Widerspruch!

- **Fall 2:**

$$w_j \notin D \overset{M_j \text{ entsch. } D}{\Rightarrow} M_j \text{ akzeptiert } w_j \text{ nicht } \overset{\text{Def. von } D}{\Rightarrow} w_j \in D$$

Widerspruch!

□

Unentscheidbarkeit des Komplements der Diagonalsprache

Das Komplement zur Diagonalsprache ist

$$\bar{D} = \{ w \in \{0,1\}^* \mid w = w_i \text{ und } M_i \text{ akzeptiert } w \}$$

Satz:

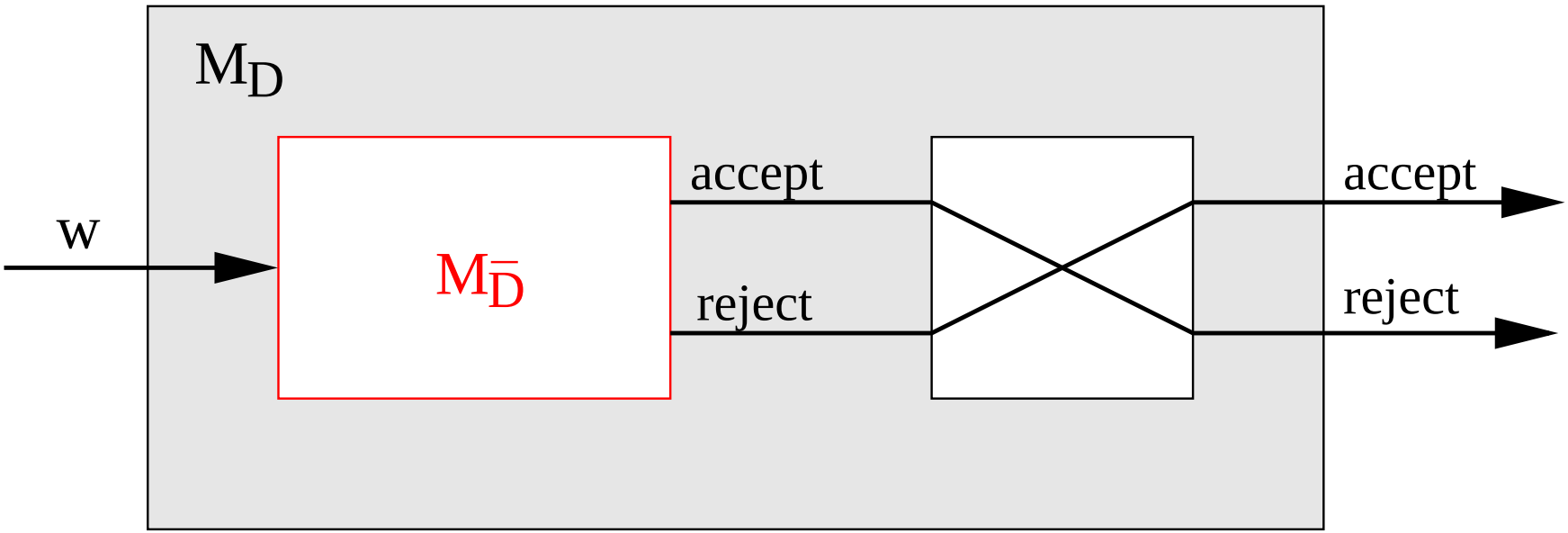
Das Komplement $\bar{D}$ der Diagonalsprache ist nicht rekursiv.

Beweis:

- Zum Widerspruch nehmen wir an, es gibt eine TM $M_{\bar{D}}$, die die Sprache $\bar{D}$ entscheidet.
- Gemäß der Def *rekursiver Sprachen* hält $M_{\bar{D}}$ auf jeder Eingabe w und akzeptiert genau dann, wenn $w \in \bar{D}$.
- Wir konstruieren nun eine TM M, die $M_{\bar{D}}$ als Unterprogramm verwendet: M startet $M_{\bar{D}}$ auf der vorliegenden Eingabe und negiert anschließend die Ausgabe von $M_{\bar{D}}$.
- Die TM M entscheidet nun offensichtlich D. Ein Widerspruch zur Unentscheidbarkeit von D. □

Unentscheidbarkeit des Komplement der Diagonalsprache

Illustration: Aus $M_{\bar{D}}$ konstruieren wir M_D.



Aber die Existenz von M_D steht im Widerspruch zur Unentscheidbarkeit von D. Damit kann es $M_{\bar{D}}$ nicht geben, und $\bar{D}$ ist nicht entscheidbar.

Unterprogrammtechnik

Die Beweistechnik aus diesem Satz lässt sich allgemein wie folgt zusammenfassen:

Unterprogrammtechnik zum Nachweis von Unentscheidbarkeit

Um nachzuweisen, dass eine Sprache L nicht rekursiv ist, genügt es zu zeigen, dass man durch Unterprogrammaufruf einer TM M_L, die L entscheidet, ein anderes Problem L' entscheiden kann, dass bereits als nicht rekursiv bekannt ist.

Im Folgenden üben wir die Unterprogrammtechnik an einigen Beispielsprachen, die auch das Halteproblem umfassen.

Unentscheidbarkeit des Halteproblems

Satz:

Das Halteproblem H ist nicht rekursiv.

Beweis:

Wir nutzen die Unterprogrammtechnik:

- Sei M_H eine TM die H entscheidet, also eine TM, die auf jede Eingabe hält, und nur Eingaben der Form $\langle M \rangle w$ akzeptiert, bei denen M auf w hält.
- Wir konstruieren eine TM $M_{\bar{D}}$ mit M_H als Unterprogramm, die $\bar{D}$ entscheidet, was im Widerspruch zur Nicht-Berechenbarkeit von $\bar{D}$ steht.

Aus diesem Widerspruch ergibt sich die Unmöglichkeit der TM M_H.

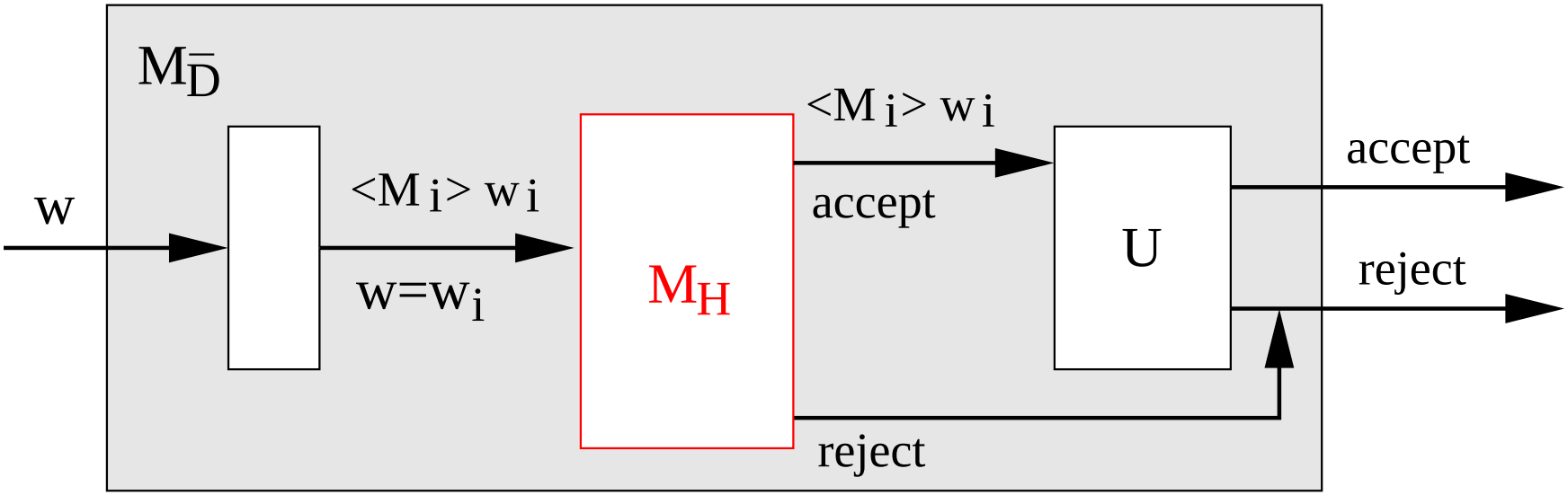
Unentscheidbarkeit des Halteproblems – Forts. Beweis

Algorithmus der TM $M_{\bar{D}}$ mit Unterprogramm M_H:

1) Auf Eingabe w, berechne i, so dass gilt $w = w_i$.
2) Berechne nun die Gödelnummer der i-ten TM, also $\langle M_i \rangle$.
3) Jetzt starte M_H als Unterprogramm mit Eingabe $\langle M_i \rangle w$.
   - 3.1) Falls M_H akzeptiert, so simuliere das Verhalten von M_i auf w (genau wie die universelle TM U dies tun würde).
   - 3.2) Falls M_H verwirft, so verwirf die Eingabe.

Unentscheidbarkeit des Halteproblems

Illustration: Aus M_H konstruieren wir $M_{\bar{D}}$.



Aber die Existenz von $M_{\bar{D}}$ steht im Widerspruch zur Unntscheidbarkeit von $\bar{D}$.

Damit kann es M_H nicht geben, und das Halteproblem H ist nicht entscheidbar.

Unentscheidbarkeit des Halteproblems – Forts. Beweis

Terminierung: $M_{\bar{D}}$ hält auf jede Eingabe, da die univers. TM U nur aufgerufen wird, wenn M_H garantiert, dass M_i auf w_i hält.

Partielle Korrektheit: Sei $w = w_i$. Es gilt

$$\begin{aligned} w \in \bar{D} &\Rightarrow M_i \text{ akzeptiert } w_i \\ &\Rightarrow M_H \text{ und } U \text{ akzeptieren } \langle M_i \rangle w_i \\ &\Rightarrow M_{\bar{D}} \text{ akzeptiert } w \ . \end{aligned}$$

$$\begin{aligned} w \notin \bar{D} &\Rightarrow M_i \text{ akzeptiert } w_i \text{ nicht} \\ &\Rightarrow (\, M_i \text{ hält nicht auf } w_i \,) \text{ oder } (\, M_i \text{ verwirft } w_i \,) \\ &\Rightarrow (\, M_H \text{ verwirft } \langle M_i \rangle w_i \,) \text{ oder} \\ &\qquad (\, M_H \text{ akzeptiert und } U \text{ verwirft } \langle M_i \rangle w_i \,) \\ &\Rightarrow M_{\bar{D}} \text{ verwirft } w \ . \end{aligned}$$

□