# VL-04: Unentscheidbarkeit I

(Berechenbarkeit und Komplexität, WS 2018)

Gerhard Woeginger

WS 2018, RWTH

# Organisatorisches

Nächste Vorlesung:

Donnerstag, November 15, 12:30–14:00 Uhr, Aula

Achtung:

Keine Vorlesung am Donnerstag, November 8

Keine Vorlesung am Freitag, November 9

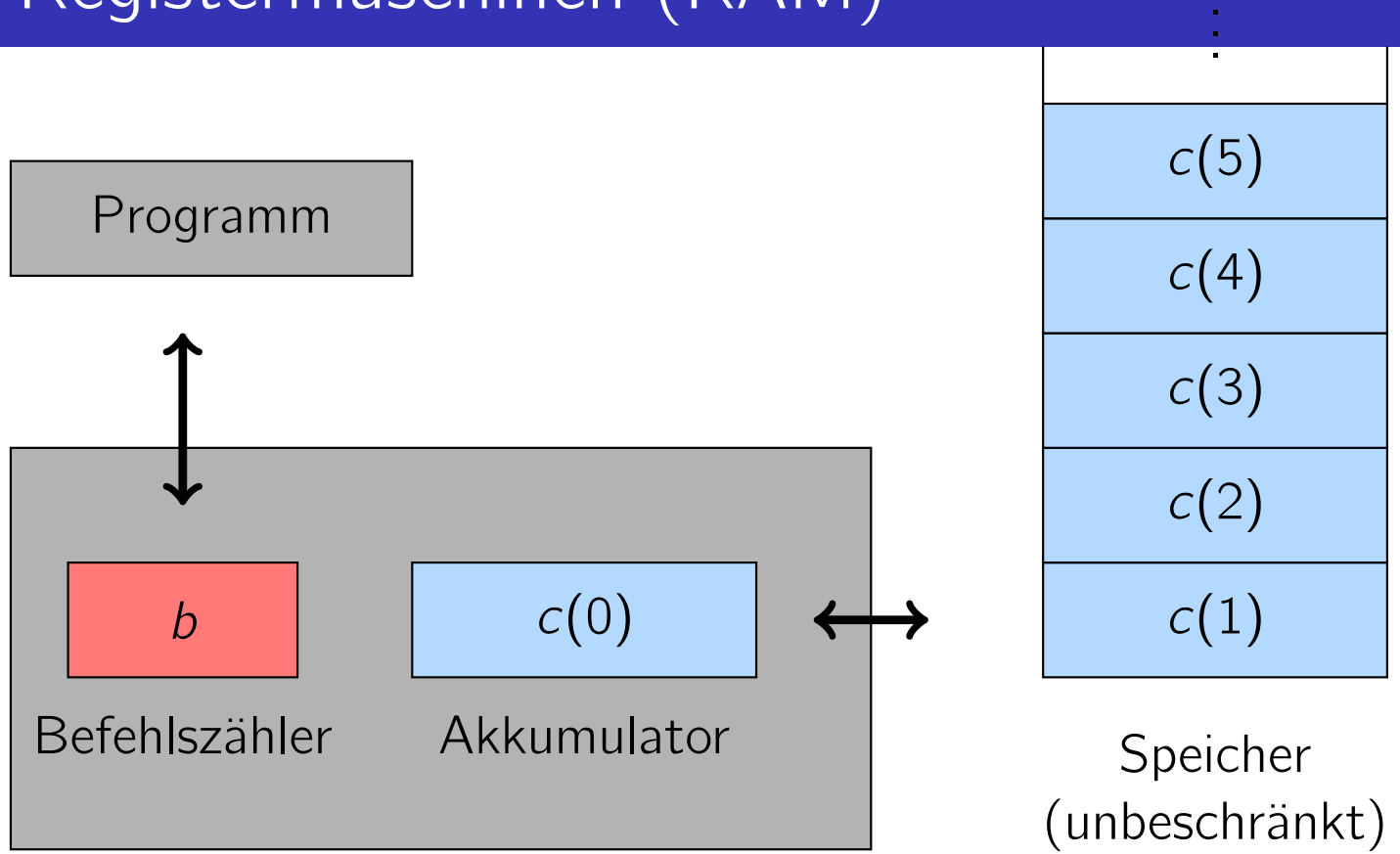
---

Webseite:

`http://algo.rwth-aachen.de/Lehre/WS1819/BuK.php`

# Wiederholung

# Wdh.: Registermaschinen (RAM)




Befehlssatz:

LOAD, STORE, ADD, SUB, MULT, DIV
INDLOAD, INDSTORE, INDADD, INDSUB, INDMULT, INDDIV
CLOAD, CADD, CSUB, CMULT, CDIV
IF c(0)?x THEN GOTO j (mit ? in {=,<,<=,>,>=})
GOTO, END

# Wdh.: RAM vs. TM

**Satz (RAM $\rightarrow$ TM)**

*Für jede im logarithmischen Kostenmass $t(n)$-zeitbeschränkte RAM $R$ gibt es ein Polynom $q$ und eine $q(n + t(n))$-zeitbeschränkte TM $M$, die $R$ simuliert.*

**Satz (TM $\rightarrow$ RAM)**

*Jede $t(n)$-zeitbeschränkte TM kann durch eine RAM simuliert werden, die zeitbeschränkt ist durch*

- $O(t(n) + n)$ *im uniformen Kostenmass und*
- $O((t(n) + n) \cdot \log(t(n) + n))$ *im logarithmischen Kostenmass.*

# Wdh.: Hintereinanderausführung von Polynomen

**Beobachtung**

Die Klasse der Polynome
ist unter Hintereinanderausführung abgeschlossen.

Wenn $p(x)$ und $q(x)$ Polynome sind,

- dann ist $p(q(x))$ ebenfalls ein Polynom;
- dann folgt aus $t(n) \in O(p(n))$ und $t'(n) \in O(q(n))$ immer auch $t(t'(n)) \in O(p(q(n)))$

# Wdh.: Das Collatz Problem

```
 1:  LOAD 1
 2:  IF c(0) > 1 THEN GOTO 4
 3:  END
 4:  CADD 1
 5:  CDIV 2
 6:  CMULT 2
 7:  SUB 1
 8:  IF c(0) > 0 THEN GOTO 13
 9:  LOAD 1
10:  CDIV 2
11:  STORE 1
12:  GOTO 1
13:  LOAD 1
14:  CMULT 3
15:  CADD 1
16:  STORE 1
17:  GOTO 1
```

$$x \leftarrow \begin{cases} x/2 & \text{wenn } x \text{ gerade} \\ 3x+1 & \text{wenn } x \text{ ungerade} \end{cases}$$

Ein 17-zeiliges Programm auf der RAM: Niemand weiss, ob dieses Programm für jede mögliche Eingabezahl in Register $c(1)$ terminiert.

# Vorlesung VL-04
# Unentscheidbarkeit I

- Exkurs: Abzählbare und überabzählbare Mengen
- Diagonalisierung
- Unentscheidbare Probleme

- Die Diagonalsprache
- Das Komplement der Diagonalsprache
- Die Unterprogrammtechnik
- Das Halteproblem

# Die zentrale Frage

**Frage**

Gibt es unentscheidbare Probleme?

Gibt es algorithmische Probleme, die kein Computer lösen kann?
Gibt es algorithmische Probleme, die keine TM lösen kann?
Gibt es algorithmische Probleme, die keine RAM lösen kann?

**Antwort**

Ja, es gibt unentscheidbare Probleme.

Grund: Es existieren mehr Sprachen/Probleme als TMs/Algorithmen.

# Exkurs: Abzählbare und überabzählbare Mengen

# Exkurs (1): Abzählbarkeit

**Definition: Abzählbare Menge**

Eine Menge $M$ heisst abzählbar,
wenn $M$ leer ist oder
wenn es eine surjektive Funktion $c : \mathbb{N} \to M$ gibt.

- Die Elemente einer abzählbaren Menge können also der Reihe nach *durchnummeriert* werden.
- Jede endliche Menge $M$ ist abzählbar.
- Für eine abzählbar unendliche Menge $M$ gibt es immer auch eine bijektive (bijektiv = surjektiv+injektiv) Abbildung $c : \mathbb{N} \to M$: Wiederholungen von Elementen von $M$ können bei der Abzählung einfach weggelassen werden.
- Abzählbar unendliche Mengen haben somit dieselbe Mächtigkeit wie die Menge der natürlichen Zahlen $\mathbb{N}$.

# Exkurs (2a): Abzählbare Beispielmengen

## Beispiele für abzählbar unendliche Mengen

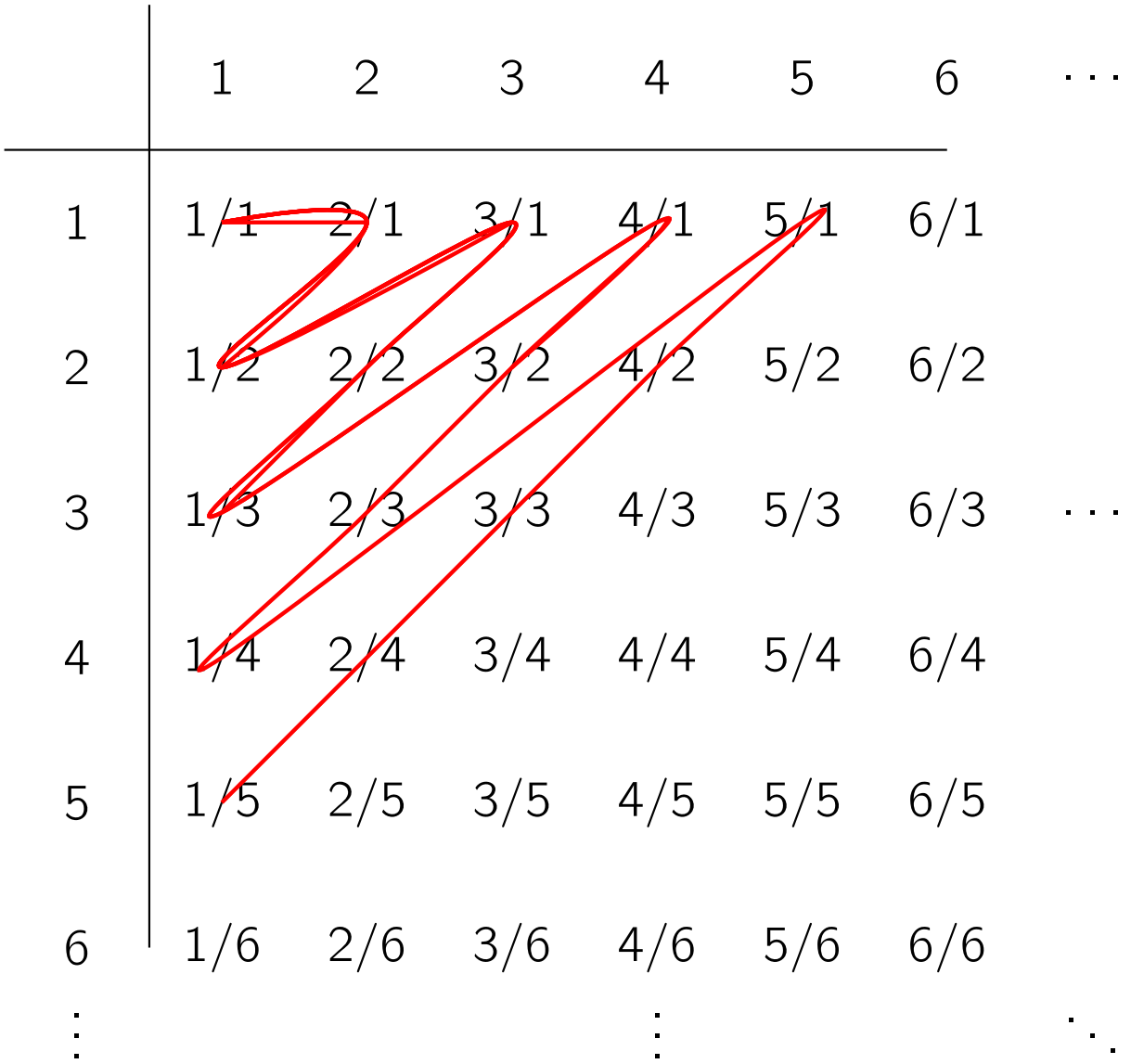
- die Menge der natürlichen Zahlen $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$ mit der Bijektion $c(i) = i$
- die Menge der ganzen Zahlen $\mathbb{Z} = \{0, -1, 1, -2, 2, -3, 3, -4, 4, \ldots\}$ mit der Bijektion

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

- die Menge der rationalen Zahlen $\mathbb{Q}$:

$$0, \frac{1}{1}, \frac{2}{1}, \frac{1}{2}, \frac{3}{1}, \ldots, \frac{i}{1}, \frac{i-1}{2}, \frac{i-2}{3}, \ldots, \frac{1}{i}, \ldots$$

# Exkurs (2b): Abzählbare Beispielmengen



# Exkurs (2c): Abzählbare Beispielmengen

## Weitere Beispiele für abzählbar unendliche Mengen

- Die Menge $\Sigma^*$ der Wörter über einem endlichen Alphabet $\Sigma$.
  Zum Beispiel: $\{0,1\}^*$ in kanonischer Reihenfolge lautet:

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

- Die Menge der Gödelnummern,
  da Gödelnummern Wörter über dem Alphabet $\{0,1\}$ sind
- Die Menge der TMen (in unserer Normalform),
  da jede TM durch eine eindeutige Gödelnummer beschrieben wird.

## Notation

- Über dem binären Alphabet $\Sigma = \{0,1\}$ bezeichnen wir
  das $i$-te Wort in der kanonischen Reihenfolge im Folgenden mit $w_i$.
- Die $i$-te TM in der kanonischen Reihenfolge der Gödelnummern
  bezeichnen wir mit $M_i$.

# Exkurs (3a): Überabzählbarkeit

Nun betrachten wir die Potenzmenge $\mathcal{P}(\mathbb{N})$,
die Menge aller Teilmengen von $\mathbb{N} = \{1, 2, 3, \ldots\}$.

**Satz**

Die Menge $\mathcal{P}(\mathbb{N})$ ist überabzählbar (= nicht abzählbar).

Beweis (durch Diagonalisierung)

- Zwecks Widerspruchs nehmen wir an, dass $\mathcal{P}(\mathbb{N})$ abzählbar ist.
- Es sei $S_0, S_1, S_2, S_3, \ldots$ eine Aufzählung von $\mathcal{P}(\mathbb{N})$.
- Wir definieren eine 2-dimensionale unendliche Matrix $(A_{i,j})_{i,j \in \mathbb{N}}$ mit

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

# Exkurs (3b): Überabzählbarkeit

Die Matrix $A$ könnte etwa folgendermassen aussehen:

| | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | |
|---|---|---|---|---|---|---|---|---|---|
| $\{1,2,4,6,\ldots\} =$ | $S_0$ | **0** | 1 | 1 | 0 | 1 | 0 | 1 | $\cdots$ |
| $\{0,1,2,4,6,\ldots\} =$ | $S_1$ | 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 | **0** | $\cdots$ |
| | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | | |

$S_{\text{diag}} = \{1, 2, 4, \ldots\}$
$\overline{S}_{\text{diag}} = \{0, 3, 5, 6 \ldots\}$

Wir definieren die Diagonalmenge $S_{\text{diag}} = \{i \in \mathbb{N} \mid A_{i,i} = 1\}$
Komplement der Diagonalmenge $\overline{S}_{\text{diag}} = \mathbb{N} \setminus S_{\text{diag}} = \{i \in \mathbb{N} \mid A_{i,i} = 0\}$

# Exkurs (3c): Überabzählbarkeit

- Beachte: Auch $\overline{S}_{\text{diag}}$ ist eine Teilmenge von $\mathbb{N}$.
- $\overline{S}_{\text{diag}}$ kommt daher in der Aufzählung $S_1, S_2, \ldots$ von $\mathcal{P}(\mathbb{N})$ vor. Es gibt also eine Zeile $k \in \mathbb{N}$, sodass $\overline{S}_{\text{diag}} = S_k$.
- Jetzt gibt es zwei Fälle, die jeweils zum Widerspruch führen.

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

Widerspruch!

Fall 2: $A_{k,k} = 0 \overset{\text{Def. } \overline{S}_{\text{diag}}}{\Rightarrow} k \in \overline{S}_{\text{diag}} \Rightarrow k \in S_k \overset{\text{Def. } A}{\Rightarrow} A_{k,k} = 1$

Widerspruch!

- Folglich gibt es keine derartige Aufzählung von $\mathcal{P}(\mathbb{N})$.

# Unentscheidbare Probleme

# Wie viele verschiedene Entscheidungsprobleme gibt es?

Jedes Entscheidungsproblem mit binär kodierter Eingabe entspricht einer Sprache über dem Alphabet $\{0,1\}$ (und umgekehrt).

- Es sei $\mathcal{L}$ die Menge aller Entscheidungsprobleme über $\{0,1\}$.
- Ein Entscheidungsproblem $L \in \mathcal{L}$ ist eine Teilmenge von $\{0,1\}^*$.
- $\mathcal{L}$ ist somit die Menge aller Teilmengen von $\{0,1\}^*$.
  Also ist $\mathcal{L}$ die Potenzmenge von $\{0,1\}^*$.
  Also gilt $\mathcal{L} = \mathcal{P}(\{0,1\}^*)$.

Wir beobachten:

- $\{0,1\}^*$ hat dieselbe Mächtigkeit wie $\mathbb{N}$.
- $\mathcal{L} = \mathcal{P}(\{0,1\}^*)$ hat somit dieselbe Mächtigkeit wie $\mathcal{P}(\mathbb{N})$.
- Die Menge $\mathcal{L}$ der Entscheidungsprobleme ist also überabzählbar.

# Die Existenz unentscheidbarer Probleme

Zusammengefasst:

- Es gibt überabzählbar viele Sprachen.
- Es gibt nur abzählbar viele TMen/Gödelnummern.

**Triviale Schlussfolgerung**

Es existieren unentscheidbare Sprachen.

- Die reine Existenz von unentscheidbaren Problemen ist eigentlich nicht bedrohlich: Es könnte sich dabei ja ausschliesslich um völlig uninteressante, künstliche, nicht praxis-relevante Probleme handeln.
- Wir werden aber sehen, dass sich diese Hoffnung nicht bestätigt.

# Die Diagonalsprache

# Die Diagonalsprache (1)

**Definition (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 $w_i$ (in kanonischer Reihenfolge von $\{0,1\}^*$)
ist genau dann in der Diagonalsprache $D$,
wenn die $i$-te TM $M_i$ (in kanonischer Reihenfolge der Gödelnummern)
dieses Wort $w_i$ **nicht** akzeptiert.

# Die Diagonalsprache (2): Intuition

Warum trägt diese Sprache den Namen *Diagonalsprache*?

Betrachte eine unendliche binäre Matrix $A$ mit

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

| | $w_0$ | $w_1$ | $w_2$ | $w_3$ | $w_4$ | |
|---|---|---|---|---|---|---|
| $M_0$ | **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** | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | | |

Die Diagonalsprache lässt sich von der Diagonale der Matrix ablesen. Es gilt

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

# Die Diagonalsprache (3): Der Beweis

**Satz**

Die Diagonalsprache $D$ ist unentscheidbar.

Beweis:

- Wir nehmen zwecks Widerspruchs an, dass $D$ entscheidbar ist. Dann gibt es eine TM $M_j$, die $D$ entscheidet.
- Wir starten die TM $M_j$ mit der Eingabe $w_j$. Es ergeben sich zwei Fälle, die jeweils direkt zum Widerspruch führen.

  Fall 1: $w_j \in D \overset{M_j \text{ entsch. } D}{\Rightarrow} M_j$ akzeptiert $w_j \overset{\text{Def. von } D}{\Rightarrow} w_j \notin D$

  Fall 2: $w_j \notin D \overset{M_j \text{ entsch. } D}{\Rightarrow} M_j$ akzeptiert $w_j$ nicht $\overset{\text{Def. von } D}{\Rightarrow} w_j \in D$

- Somit ist $D$ unentscheidbar.

# Unentscheidbarkeit des Diagonalsprachenkomplements

# Diagonalsprachenkomplement (1)

**Definition**

Das Komplement der Diagonalsprache ist

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

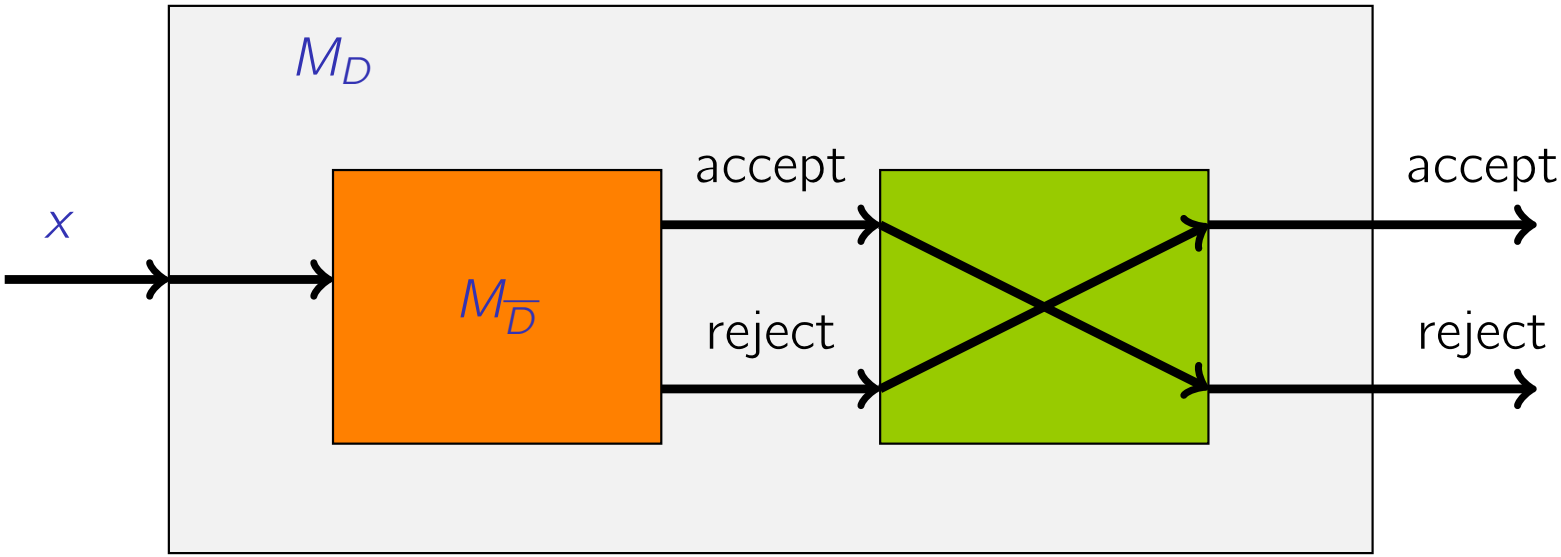
**Satz**

Das Komplement $\overline{D}$ der Diagonalsprache ist nicht entscheidbar.

- Zwecks Widerspruchs nehmen wir an, dass es eine TM $M_{\overline{D}}$ gibt, die die Sprache $\overline{D}$ entscheidet. Diese TM $M_{\overline{D}}$ hält dann auf jeder Eingabe $w$, und akzeptiert $w$ genau dann, wenn $w \in \overline{D}$.
- Wir konstruieren nun eine neue TM $M$, die $M_{\overline{D}}$ als Unterprogramm verwendet: $M$ startet $M_{\overline{D}}$ auf der vorliegenden Eingabe und negiert anschliessend die Ausgabe von $M_{\overline{D}}$.
- Diese TM $M$ entscheidet dann offensichtlich $D$.
  Ein Widerspruch zur Unentscheidbarkeit von $D$.

# Diagonalsprachenkomplement (2)

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




Die Existenz von $M_D$ widersprucht der Unentscheidbarkeit von $D$.
Daher kann es das Programm $M_{\overline{D}}$ nicht geben.
Daher ist $\overline{D}$ nicht entscheidbar.

# Die Unterprogrammtechnik

# Unterprogrammtechnik (1)

Die Beweistechnik aus dem vorhergehenden Satz (über die Unentscheidbarkeit von $\overline{D}$) lässt sich wie folgt zusammenfassen:

**Unterprogrammtechnik zum Beweis von Unentscheidbarkeiten**

- Es sei $L'$ eine bereits analysierte, nicht-entscheidbare Sprache.
- Es sei $L$ eine neue Sprache, die wir untersuchen wollen.

Um nachzuweisen, dass $L$ nicht entscheidbar ist, genügt es zu zeigen, dass man mit Hilfe von Unterprogrammaufrufen einer TM $M_L$ (zum Entscheiden von $L$) auch die Sprache $L'$ entscheiden kann.

# Unterprogrammtechnik (2)

**Beobachtung**

Wenn die Sprache $L \subseteq \{0,1\}^*$ unentscheidbar ist,
dann ist auch ihr Komplement $\overline{L}$ unentscheidbar.

**Beobachtung**

Wenn die Sprache $L \subseteq \{0,1\}^*$ entscheidbar ist,
dann ist auch ihr Komplement $\overline{L}$ entscheidbar.

# Das Halteproblem

# Das Halteproblem

Das Halteproblem besteht darin, zu entscheiden,
ob ein gegebenes Programm mit einer gegebenen Eingabe terminiert.

In unserer Notation mit TMen ergibt sich die folgende formale Problemdefinition:

**Definition (Halteproblem)**

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

Es wäre sehr nützlich, wenn Compiler das Halteproblem entscheiden könnten. Wir werden jedoch sehen, dass dieses grundlegende Problem unentscheidbar ist.

# Das Halteproblem (2)

**Satz**

Das Halteproblem $H$ ist nicht entscheidbar.

Beweisidee: Wir benutzen die Unterprogrammtechnik:

- Es sei $M_H$ eine TM, die $H$ entscheidet:
  $M_H$ hält auf jeder Eingabe und akzeptiert nur Eingaben der Form $\langle M \rangle w$, bei denen $M$ auf $w$ hält.
- Wir konstruieren eine neue TM $M_{\overline{D}}$ mit $M_H$ als Unterprogramm, die $\overline{D}$ entscheidet.
- Dies steht im Widerspruch zur Nicht-Berechenbarkeit von $\overline{D}$.
  Dieser Widerspruch impliziert die Nicht-Existenz der TM $M_H$.

# Beweis (1)

Der ausgearbeitete Beweis:

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

(1) Auf Eingabe $w$ berechne zuerst Index $i$ mit $w = w_i$.

(2) Berechne dann die Gödelnummer der $i$-ten TM $M_i$, also $\langle M_i \rangle$.

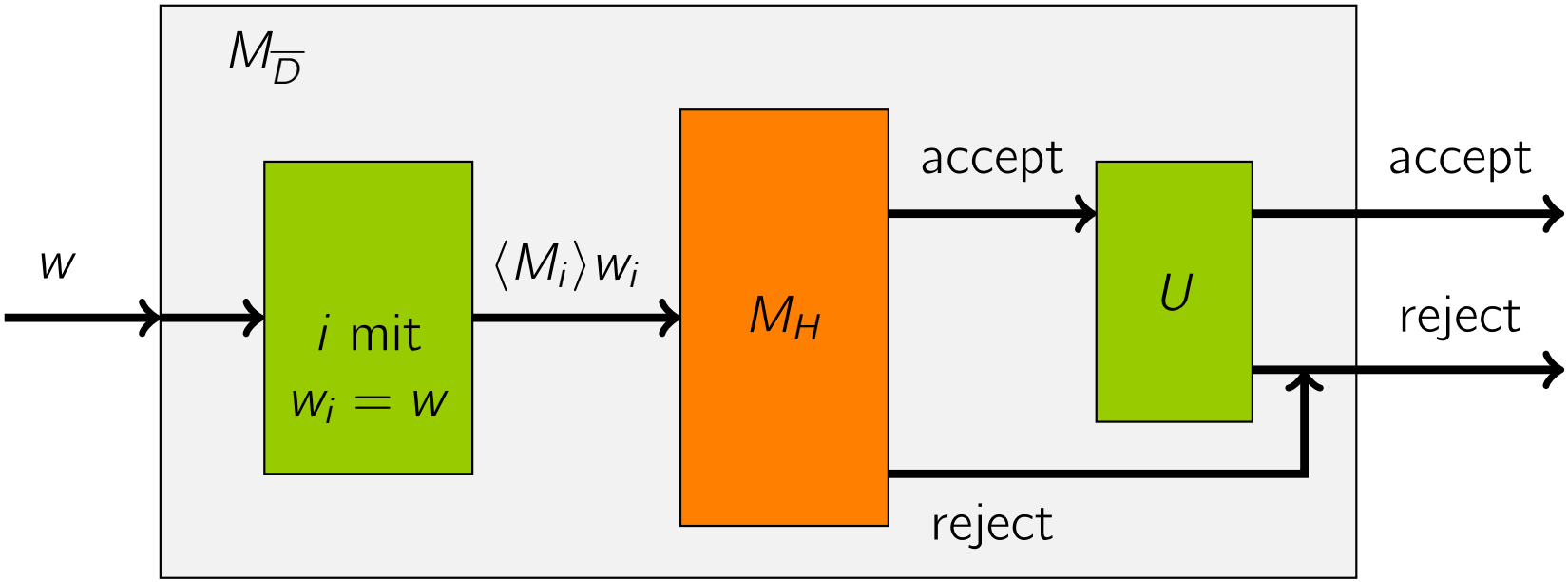
(3) Starte $M_H$ als Unterprogramm mit Eingabe $\langle M_i \rangle w_i$.

  (3.1) Falls $M_H$ akzeptiert, so simuliere das Verhalten von $M_i$ auf $w_i$ (mit Hilfe der universellen TM $U$).

  (3.2) Falls $M_H$ verwirft, so verwirf die Eingabe.

# Beweis (2)

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




Existenz von $M_{\overline{D}}$ steht im Widerspruch zur Unentscheidbarkeit von $\overline{D}$.
Daher gibt es $M_H$ nicht, und das Halteproblem $H$ ist nicht entscheidbar.

# Beweis (3)

**Für die Korrektheit ist zu zeigen:**

1. $w \in \overline{D} \Rightarrow M_{\overline{D}}$ akzeptiert $w$
2. $w \notin \overline{D} \Rightarrow M_{\overline{D}}$ verwirft $w$

Es sei $w = w_i$. Dann gilt:

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

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