

Script generated by TTT

Title: seidl: Theoretische_informatik (21.06.2012)

Date: Thu Jun 21 16:02:17 CEST 2012

Duration: 87:29 min

Pages: 85

4.9 Entscheidbarkeit und das Halteproblem

4.9 Entscheidbarkeit und das Halteproblem

Ziel: Es ist **unentscheidbar** ob ein Programm terminiert.

4.9 Entscheidbarkeit und das Halteproblem

Ziel: Es ist **unentscheidbar** ob ein Programm terminiert.

Definition 4.52

Eine Menge A ($\subseteq \mathbb{N}$ oder Σ^*) heißt **entscheidbar** gdw ihre charakteristische Funktion

$$\chi_A(x) := \begin{cases} 1 & \text{falls } x \in A \\ 0 & \text{falls } x \notin A \end{cases}$$

berechenbar ist.

4.9 Entscheidbarkeit und das Halteproblem

Ziel: Es ist **unentscheidbar** ob ein Programm terminiert.

Definition 4.52

Eine Menge $A (\subseteq \mathbb{N} \text{ oder } \Sigma^*)$ heißt **entscheidbar** gdw ihre charakteristische Funktion

$$\chi_A(x) := \begin{cases} 1 & \text{falls } x \in A \\ 0 & \text{falls } x \notin A \end{cases}$$

berechenbar ist.

Eine Eigenschaft/Problem $P(x)$ heißt **entscheidbar** gdw $\{x \mid P(x)\}$ entscheidbar ist.

4.9 Entscheidbarkeit und das Halteproblem

Ziel: Es ist **unentscheidbar** ob ein Programm terminiert.

Definition 4.52

Eine Menge $A (\subseteq \mathbb{N} \text{ oder } \Sigma^*)$ heißt **entscheidbar** gdw ihre charakteristische Funktion

$$\chi_A(x) := \begin{cases} 1 & \text{falls } x \in A \\ 0 & \text{falls } x \notin A \end{cases}$$

~~$\chi_{\bar{A}}(x) = 1 - \chi_A(x)$~~

berechenbar ist.

Eine Eigenschaft/Problem $P(x)$ heißt **entscheidbar** gdw $\{x \mid P(x)\}$ entscheidbar ist.

Fakt 4.53

Die entscheidbaren Mengen sind abgeschlossen unter Komplement: Ist A entscheidbar, dann auch \bar{A} .

Kodierung einer TM als Wort über $\Sigma = \{0, 1\}$, exemplarisch:

Kodierung einer TM als Wort über $\Sigma = \{0, 1\}$, exemplarisch:

- Sei $\Gamma = \{a_0, \dots, a_k\}$ und $Q = \{q_0, \dots, q_n\}$.
- $\delta(q_i, a_j) = (q_{i'}, a_{j'}, d)$ wird kodiert als

$$\#bin(i)\#bin(j)\#bin(i')\#bin(j')\#bin(d)$$

wobei $bin : \mathbb{N} \rightarrow \{0, 1\}^*$ die Binärcodierung einer Zahl ist und $d \in \{L/R/N\}$ falls $d = L/R/N$.

Kodierung einer TM als Wort über $\Sigma = \{0, 1\}$, exemplarisch:

- Sei $\Gamma = \{a_0, \dots, a_k\}$ und $Q = \{q_0, \dots, q_n\}$.
- $\delta(q_i, a_j) = (q_{i'}, a_{j'}, d)$ wird kodiert als

$$\#bin(i)\#bin(j)\#bin(i')\#bin(j')\#bin(m)$$

wobei $bin : \mathbb{N} \rightarrow \{0, 1\}^*$ die Binärkodierung einer Zahl ist und $m = 0/1/2$ falls $d = L/R/N$.

- Kodierung von δ : Konkatenation der Kodierungen aller $\delta(.,.) = (.,.,.)$, in beliebiger Reihenfolge.

Kodierung einer TM als Wort über $\Sigma = \{0, 1\}$, exemplarisch:

- Sei $\Gamma = \{a_0, \dots, a_k\}$ und $Q = \{q_0, \dots, q_n\}$.
- $\delta(q_i, a_j) = (q_{i'}, a_{j'}, d)$ wird kodiert als

$$\#bin(i)\#bin(j)\#bin(i')\#bin(j')\#bin(m)$$

wobei $bin : \mathbb{N} \rightarrow \{0, 1\}^*$ die Binärkodierung einer Zahl ist und $m = 0/1/2$ falls $d = L/R/N$.

- Kodierung von δ : Konkatenation der Kodierungen aller $\delta(.,.) = (.,.,.)$, in beliebiger Reihenfolge.
- Kodierung von $\{0, 1, \#\}^*$ in $\{0, 1\}^*$:

$$0 \mapsto 00$$

$$1 \mapsto 01$$

$$\# \mapsto 11$$

Die Kodierung $TM \rightarrow \{0, 1\}^*$ ist nicht surjektiv,

Die Kodierung $TM \rightarrow \{0, 1\}^*$ ist nicht surjektiv,
dh nicht jedes Wort über $\{0, 1\}^*$ kodiert eine TM.

Die Kodierung $TM \rightarrow \{0, 1\}^*$ ist nicht surjektiv,
dh nicht jedes Wort über $\{0, 1\}^*$ kodiert eine TM.
Sei \hat{M} eine beliebige feste TM.

Die Kodierung $TM \rightarrow \{0, 1\}^*$ ist nicht surjektiv,
dh nicht jedes Wort über $\{0, 1\}^*$ kodiert eine TM.
Sei \hat{M} eine beliebige feste TM.

Definition 4.54

Die zu einem Wort $w \in \{0, 1\}^*$ gehörige TM M_w ist

$$M_w := \begin{cases} M & \text{falls } w \text{ Kodierung von } M \text{ ist} \\ \hat{M} & \text{sonst} \end{cases}$$

Die Kodierung $TM \rightarrow \{0, 1\}^*$ ist nicht surjektiv,
dh nicht jedes Wort über $\{0, 1\}^*$ kodiert eine TM.
Sei \hat{M} eine beliebige feste TM.

Definition 4.54

Die zu einem Wort $w \in \{0, 1\}^*$ gehörige TM M_w ist

$$M_w := \begin{cases} M & \text{falls } w \text{ Kodierung von } M \text{ ist} \\ \hat{M} & \text{sonst} \end{cases}$$

Die Kodierung von syntaktischen Objekten (Programmen,
Formeln, etc) als Zahlen nennt man [Gödelisierung](#) und die Zahlen
[Gödelnummern](#).

Definition 4.55

$M[w]$ ist Abk. für „Maschine M mit Eingabe w “

Definition 4.55

$M[w]$ ist Abk. für „Maschine M mit Eingabe w “
 $M[w]\downarrow$ bedeutet, dass $M[w]$ terminiert/hält.

Definition 4.55

$M[w]$ ist Abk. für „Maschine M mit Eingabe w “
 $M[w]\downarrow$ bedeutet, dass $M[w]$ terminiert/hält.

Definition 4.56 (Spezielles Halteproblem)

Gegeben: Ein Wort $w \in \{0, 1\}^*$.

Problem: Hält M_w bei Eingabe w ?

Definition 4.55

$M[w]$ ist Abk. für „Maschine M mit Eingabe w “
 $M[w]\downarrow$ bedeutet, dass $M[w]$ terminiert/hält.

Definition 4.56 (Spezielles Halteproblem)

Gegeben: Ein Wort $w \in \{0, 1\}^*$.

Problem: Hält M_w bei Eingabe w ?

Als Menge:

$$K := \{w \in \{0, 1\}^* \mid M_w[w]\downarrow\}$$

Satz 4.57

Das spezielle Halteproblem ist nicht entscheidbar.

Satz 4.57

Das spezielle Halteproblem ist nicht entscheidbar.

Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.

Satz 4.57

Das spezielle Halteproblem ist nicht entscheidbar.

Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.
Dann ist auch f berechenbar:

$$f(w) := \begin{cases} 1 & \text{falls } \chi_K(w) = 0 \\ \perp & \text{falls } \chi_K(w) = 1 \end{cases}$$

Satz 4.57

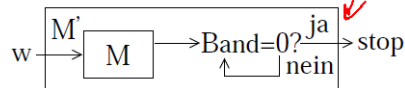
Das spezielle Halteproblem ist nicht entscheidbar.

Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.
Dann ist auch f berechenbar:

$$f(w) := \begin{cases} 1 & \text{falls } \chi_K(w) = 0 \\ \perp & \text{falls } \chi_K(w) = 1 \end{cases}$$

Berechnet die TM M_{χ_K} so berechnet $M' f$: *schick*



Satz 4.57

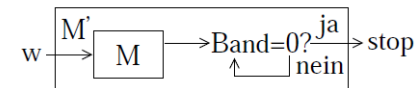
Das spezielle Halteproblem ist nicht entscheidbar.

Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.
Dann ist auch f berechenbar:

$$f(w) := \begin{cases} 1 & \text{falls } \chi_K(w) = 0 \\ \perp & \text{falls } \chi_K(w) = 1 \end{cases}$$

Berechnet die TM M_{χ_K} so berechnet $M' f$:



Dann gibt es ein w' mit $M_{w'} = M'$.

Satz 4.57

Das spezielle Halteproblem ist nicht entscheidbar.

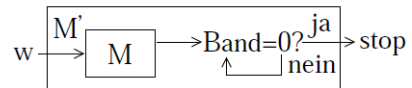
Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.

Dann ist auch f berechenbar:

$$f(w) := \begin{cases} 1 & \text{falls } \chi_K(w) = 0 \\ \perp & \text{falls } \chi_K(w) = 1 \end{cases}$$

Berechnet die TM M_{χ_K} so berechnet $M' f$:



Dann gibt es ein w' mit $M_{w'} = M'$.

$$f(w') = \perp \Leftrightarrow \chi_K(w') = 1$$

Satz 4.57

Das spezielle Halteproblem ist nicht entscheidbar.

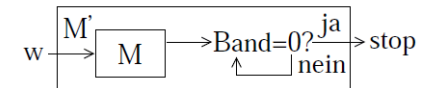
Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.

Dann ist auch f berechenbar:

$$f(w) := \begin{cases} 1 & \text{falls } \chi_K(w) = 0 \\ \perp & \text{falls } \chi_K(w) = 1 \end{cases}$$

Berechnet die TM M_{χ_K} so berechnet $M' f$:



Dann gibt es ein w' mit $M_{w'} = M'$.

$$\begin{aligned} f(w') = \perp &\Leftrightarrow \chi_K(w') = 1 \\ &\Leftrightarrow M_{w'}[w'] \downarrow \end{aligned}$$

Satz 4.57

Das spezielle Halteproblem ist nicht entscheidbar.

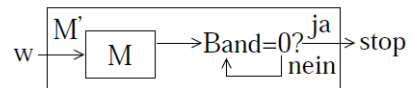
Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.

Dann ist auch f berechenbar:

$$f(w) := \begin{cases} 1 & \text{falls } \chi_K(w) = 0 \\ \perp & \text{falls } \chi_K(w) = 1 \end{cases}$$

Berechnet die TM M_{χ_K} so berechnet $M' f$:



Dann gibt es ein w' mit $M_{w'} = M'$.

$$\begin{aligned} f(w') = \perp &\Leftrightarrow \chi_K(w') = 1 \\ &\Leftrightarrow M_{w'}[w'] \downarrow \Leftrightarrow M'[w'] \downarrow \Leftrightarrow f(w') = 1 \end{aligned}$$

Satz 4.57

Das spezielle Halteproblem ist nicht entscheidbar.

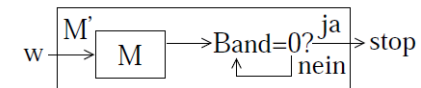
Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.

Dann ist auch f berechenbar:

$$f(w) := \begin{cases} 1 & \text{falls } \chi_K(w) = 0 \\ \perp & \text{falls } \chi_K(w) = 1 \end{cases}$$

Berechnet die TM M_{χ_K} so berechnet $M' f$:



Dann gibt es ein w' mit $M_{w'} = M'$.

$$\begin{aligned} f(w') = \perp &\Leftrightarrow \chi_K(w') = 1 \\ &\Leftrightarrow M_{w'}[w'] \downarrow \Leftrightarrow M'[w'] \downarrow \Leftrightarrow f(w') = 1 \quad \text{⚡} \quad \square \end{aligned}$$

Satz 4.57

Das spezielle Halteproblem ist nicht entscheidbar.

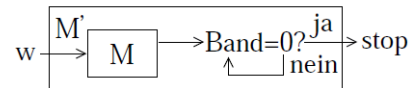
Beweis:

Angenommen, K sei entscheidbar, dh χ_K ist berechenbar.

Dann ist auch f berechenbar:

$$f(w) := \begin{cases} 1 & \text{falls } \chi_K(w) = 0 \\ \perp & \text{falls } \chi_K(w) = 1 \end{cases}$$

Berechnet die TM M_{χ_K} so berechnet $M' f$:



Dann gibt es ein w' mit $M_{w'} = M'$.

$$\begin{aligned} f(w') = \perp &\Leftrightarrow \chi_K(w') = 1 \\ &\Leftrightarrow M_{w'}[w'] \downarrow \Leftrightarrow M'[w'] \downarrow \Leftrightarrow f(w') = 1 \quad \text{↯} \quad \square \end{aligned}$$

Definition 4.58 ((Allgemeines) Halteproblem)

Gegeben: Wörter $w, x \in \{0, 1\}^*$.

Problem: Hält M_w bei Eingabe x ?

Definition 4.58 ((Allgemeines) Halteproblem)

Gegeben: Wörter $w, x \in \{0, 1\}^*$.

Problem: Hält M_w bei Eingabe x ?

Definition 4.58 ((Allgemeines) Halteproblem)

Gegeben: Wörter $w, x \in \{0, 1\}^*$.

Problem: Hält M_w bei Eingabe x ?

Als Menge:

$$H := \{w\#x \mid M_w[x] \downarrow\}$$

Definition 4.58 ((Allgemeines) Halteproblem)

Gegeben: Wörter $w, x \in \{0, 1\}^*$.

Problem: Hält M_w bei Eingabe x ?

Als Menge:

$$H := \{w\#x \mid M_w[x]\downarrow\}$$

Satz 4.59

Das Halteproblem H ist nicht entscheidbar.

Definition 4.58 ((Allgemeines) Halteproblem)

Gegeben: Wörter $w, x \in \{0, 1\}^*$.

Problem: Hält M_w bei Eingabe x ?

Als Menge:

$$H := \{w\#x \mid M_w[x]\downarrow\}$$

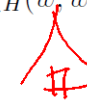
Satz 4.59

Das Halteproblem H ist nicht entscheidbar.

Beweis:

Wäre H entscheidbar, dann trivialerweise auch K :

$$\chi_K(w) = \chi_H(w, w)$$



□

Definition 4.60 (Reduktion)

Eine Menge $A \subseteq \Sigma^*$ ist **reduzierbar** auf eine Menge $B \subseteq \Gamma^*$

Definition 4.60 (Reduktion)

Eine Menge $A \subseteq \Sigma^*$ ist **reduzierbar** auf eine Menge $B \subseteq \Gamma^*$ gdw es eine totale und berechenbare Funktion $f : \Sigma^* \rightarrow \Gamma^*$ gibt mit

$$\forall w \in \Sigma^*. w \in A \Leftrightarrow f(w) \in B$$

Definition 4.60 (Reduktion)

Eine Menge $A \subseteq \Sigma^*$ ist **reduzierbar** auf eine Menge $B \subseteq \Gamma^*$ gdw es eine totale und berechenbare Funktion $f : \Sigma^* \rightarrow \Gamma^*$ gibt mit

$$\forall w \in \Sigma^*. w \in A \Leftrightarrow f(w) \in B$$

Wir schreiben dann $A \leq B$.

Definition 4.60 (Reduktion)

Eine Menge $A \subseteq \Sigma^*$ ist **reduzierbar** auf eine Menge $B \subseteq \Gamma^*$ gdw es eine totale und berechenbare Funktion $f : \Sigma^* \rightarrow \Gamma^*$ gibt mit

$$\forall w \in \Sigma^*. w \in A \Leftrightarrow f(w) \in B$$

Wir schreiben dann $A \leq B$.

Intuition:

- B ist mindestens so schwer zu lösen wie A .

Lemma 4.61

Falls $A \leq B$ und B ist entscheidbar, so ist auch A entscheidbar.

Lemma 4.61

Falls $A \leq B$ und B ist entscheidbar, so ist auch A entscheidbar.

Beweis:

Es gelte $A \leq B$ mittels f und χ_B sei berechenbar.

Lemma 4.61

Falls $A \leq B$ und B ist entscheidbar, so ist auch A entscheidbar.

Beweis:

Es gelte $A \leq B$ mittels f und χ_B sei berechenbar.

Dann ist $\chi_B \circ f$ berechenbar und $\chi_A = \chi_B \circ f$:

Lemma 4.61

Falls $A \leq B$ und B ist entscheidbar, so ist auch A entscheidbar.

Beweis:

Es gelte $A \leq B$ mittels f und χ_B sei berechenbar.

Dann ist $\chi_B \circ f$ berechenbar und $\chi_A = \chi_B \circ f$:

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases} = \begin{cases} 1, & f(x) \in B \\ 0, & f(x) \notin B \end{cases} = \chi_B(f(x)) \quad \square$$

Lemma 4.61

Falls $A \leq B$ und B ist entscheidbar, so ist auch A entscheidbar.

Beweis:

Es gelte $A \leq B$ mittels f und χ_B sei berechenbar.

Dann ist $\chi_B \circ f$ berechenbar und $\chi_A = \chi_B \circ f$:

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases} = \begin{cases} 1, & f(x) \in B \\ 0, & f(x) \notin B \end{cases} = \chi_B(f(x)) \quad \square$$

Lemma 4.61

Falls $A \leq B$ und B ist entscheidbar, so ist auch A entscheidbar.

Beweis:

Es gelte $A \leq B$ mittels f und χ_B sei berechenbar.

Dann ist $\chi_B \circ f$ berechenbar und $\chi_A = \chi_B \circ f$:

$$\chi_A(x) = \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases} = \begin{cases} 1, & f(x) \in B \\ 0, & f(x) \notin B \end{cases} = \chi_B(f(x)) \quad \square$$

Korollar 4.62

Falls $A \leq B$ und A ist unentscheidbar, dann ist auch B unentscheidbar.

Korollar 4.62

Falls $A \leq B$ und A ist unentscheidbar, dann ist auch B unentscheidbar.

Beispiel 4.63

Da $K \leq H$ (mit Reduktion $f(w) := w\#w$) und K unentscheidbar ist, ist auch H unentscheidbar.

Satz 4.64

Das Halteproblem auf leerem Band, H_0 , ist unentscheidbar.

$$H_0 := \{w \in \{0, 1\}^* \mid M_w[\epsilon]\downarrow\}$$

Satz 4.64

Das Halteproblem auf leerem Band, H_0 , ist unentscheidbar.

$$H_0 := \{w \in \{0, 1\}^* \mid M_w[\epsilon]\downarrow\}$$

Beweis:

Wir zeigen $K \leq H_0$ mit einer Funktion $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$.

Satz 4.64

Das Halteproblem auf leerem Band, H_0 , ist unentscheidbar.

$$H_0 := \{w \in \{0, 1\}^* \mid M_w[\epsilon]\downarrow\}$$

Beweis:

Wir zeigen $K \leq H_0$ mit einer Funktion $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$.
 $f(w)$ ist die Gödelnummer folgender TM:

Überschreibe die Eingabe mit w ; führe M_w aus.

Satz 4.64

Das Halteproblem auf leerem Band, H_0 , ist unentscheidbar.

$$H_0 := \{w \in \{0, 1\}^* \mid M_w[\epsilon]\downarrow\}$$

Beweis:

Wir zeigen $K \leq H_0$ mit einer Funktion $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$.
 $f(w)$ ist die Gödelnummer folgender TM:

Überschreibe die Eingabe mit w ; führe M_w aus.

Dh f berechnet aus w die Kodierung w_1 einer TM, die w schreibt,

Satz 4.64

Das Halteproblem auf leerem Band, H_0 , ist unentscheidbar.

$$H_0 := \{w \in \{0, 1\}^* \mid M_w[\epsilon] \downarrow\}$$

Beweis:

Wir zeigen $K \leq H_0$ mit einer Funktion $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$.
 $f(w)$ ist die Gödelnummer folgender TM:

Überschreibe die Eingabe mit w ; führe M_w aus.

Dh f berechnet aus w die Kodierung w_1 einer TM, die w schreibt,
und gibt die Kodierung von " $w_1; w$ " zurück.

Damit ist f total und berechenbar.

Es gilt:

$$w \in K \Leftrightarrow M_w[w] \downarrow \Leftrightarrow M_{f(w)}[\epsilon] \downarrow \Leftrightarrow f(w) \in H_0$$

□

Fazit:

Es gibt keine allgemeine algorithmische Methode, um zu entscheiden, ob ein Programm terminiert.

Fazit:

Es gibt keine allgemeine algorithmische Methode, um zu entscheiden, ob ein Programm terminiert.

Die Unentscheidbarkeit vieler Fragen über die Ausführung von Programmen folgt durch Reduktion des Halteproblems:

Fazit:

Es gibt keine allgemeine algorithmische Methode, um zu entscheiden, ob ein Programm terminiert.

Die Unentscheidbarkeit vieler Fragen über die Ausführung von Programmen folgt durch Reduktion des Halteproblems:

- Kann ein WHILE-Programm mit einer bestimmten Eingabe einen bestimmten Programmpunkt erreichen?

Fazit:

Es gibt keine allgemeine algorithmische Methode, um zu entscheiden, ob ein Programm terminiert.

Die Unentscheidbarkeit vieler Fragen über die Ausführung von Programmen folgt durch Reduktion des Halteproblems:

- Kann ein WHILE-Programm mit einer bestimmten Eingabe einen bestimmten Programmpunkt erreichen?
Der Spezialfall Programmpunkt=Programmende ist das Halteproblem.

Fazit:

Es gibt keine allgemeine algorithmische Methode, um zu entscheiden, ob ein Programm terminiert.

Die Unentscheidbarkeit vieler Fragen über die Ausführung von Programmen folgt durch Reduktion des Halteproblems:

- Kann ein WHILE-Programm mit einer bestimmten Eingabe einen bestimmten Programmpunkt erreichen?
Der Spezialfall Programmpunkt=Programmende ist das Halteproblem.
- Kann Variable x_7 bei einer bestimmten Eingabe je den Wert 2^{32} erreichen?

Fazit:

Es gibt keine allgemeine algorithmische Methode, um zu entscheiden, ob ein Programm terminiert.

Die Unentscheidbarkeit vieler Fragen über die Ausführung von Programmen folgt durch Reduktion des Halteproblems:

- Kann ein WHILE-Programm mit einer bestimmten Eingabe einen bestimmten Programmpunkt erreichen?
Der Spezialfall Programmpunkt=Programmende ist das Halteproblem.
- Kann Variable x_7 bei einer bestimmten Eingabe je den Wert 2^{32} erreichen?
Reduktion: Ein Programm P hält gdw während der Ausführung von
$$P; x_7 := 2^{32}$$
Variable x_7 den Wert 2^{32} erreicht.

Quiz

Ist es entscheidbar, ob eine TM

- ① mehr als 314 Zustände hat?

Quiz

Ist es entscheidbar, ob eine TM

- 2 bei Eingabe ϵ mehr als 314 Schritte macht?

Quiz

Ist es entscheidbar, ob eine TM

- 3 bei *irgendeiner* Eingabe mehr als 314 Schritte macht?

Quiz

Ist es entscheidbar, ob eine TM

- 4 bei *allen* Eingaben mehr als 314 Schritte macht?

Quiz

Ist es entscheidbar, ob eine TM

- 5 bei Eingabe ϵ ihren Kopf mehr als 314 Felder von der 0-Position entfernen kann?

Quiz

Ist es entscheidbar, ob eine TM

- 6 bei Eingabe ϵ einen bestimmten Zustand erreichen kann?

Quiz

Ist es entscheidbar, ob eine TM

- 7 irgendeine Eingabe akzeptieren kann?

Es müssen nicht immer TM sein:

Satz 4.65 (Matiyasevich 1970, Hilberts 10. Problem)

Es ist unentscheidbar, ob ein Polynom in n Variablen mit ganzzahligen Koeffizienten eine ganzzahlige Nullstelle hat ($\in \mathbb{Z}^n$).

Es müssen nicht immer TM sein:

Satz 4.65 (Matiyasevich 1970, Hilberts 10. Problem)

Es ist unentscheidbar, ob ein Polynom in n Variablen mit ganzzahligen Koeffizienten eine ganzzahlige Nullstelle hat ($\in \mathbb{Z}^n$).

Beweis:

$$H \leq H_{10}$$

□

Es müssen nicht immer TM sein:

Satz 4.65 (Matiyasevich 1970, Hilberts 10. Problem)

Es ist unentscheidbar, ob ein Polynom in n Variablen mit ganzzahligen Koeffizienten eine ganzzahlige Nullstelle hat ($\in \mathbb{Z}^n$).

Beweis:

$$H \leq H_{10}$$

□

Bemerkungen

- Nicht alle unentscheidbaren Probleme sind gleich schwer

Bemerkungen

- Nicht alle unentscheidbaren Probleme sind gleich schwer
- ZB gilt: Das Äquivalenzproblem

$$Eq := \{u\#v \mid M_u \text{ berechnet die gleiche Funktion wie } M_v\}$$

Bemerkungen

- Nicht alle unentscheidbaren Probleme sind gleich schwer
- ZB gilt: Das Äquivalenzproblem

$$Eq := \{u\#v \mid M_u \text{ berechnet die gleiche Funktion wie } M_v\}$$

ist schwerer als das Halteproblem:

$$H \leq Eq \quad \text{aber} \quad Eq \not\leq H$$

Bemerkungen

- Nicht alle unentscheidbaren Probleme sind gleich schwer
- ZB gilt: Das Äquivalenzproblem

$$Eq := \{u\#v \mid M_u \text{ berechnet die gleiche Funktion wie } M_v\}$$

ist schwerer als das Halteproblem:

$$H \leq Eq \quad \text{aber} \quad Eq \not\leq H$$

- Es gibt sogar eine unendliche Folge

$$A_0 \leq A_1 \leq A_2 \leq \dots$$

4.10 Semi-Entscheidbarkeit

Definition 4.66

Eine Menge A ($\subseteq \mathbb{N}$ oder Σ^*) heißt **semi-entscheidbar (s-e)** gdw

$$\chi'_A(x) := \begin{cases} 1 & \text{falls } x \in A \\ \perp & \text{falls } x \notin A \end{cases}$$

berechenbar ist.

4.10 Semi-Entscheidbarkeit

Definition 4.66

Eine Menge A ($\subseteq \mathbb{N}$ oder Σ^*) heißt **semi-entscheidbar (s-e)** gdw

$$\chi'_A(x) := \begin{cases} 1 & \text{falls } x \in A \\ \perp & \text{falls } x \notin A \end{cases}$$

berechenbar ist.

Satz 4.67

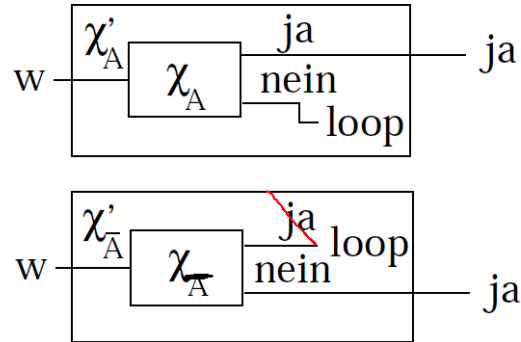
Eine Menge A ist **entscheidbar** gdw sowohl A als auch \overline{A} s-e sind.

Satz 4.67

Eine Menge A ist entscheidbar gdw sowohl A als auch \bar{A} s-e sind.

Beweis:

„ \Rightarrow “: Wandle TM für χ_A in TM für χ'_A und $\chi'_{\bar{A}}$ um:

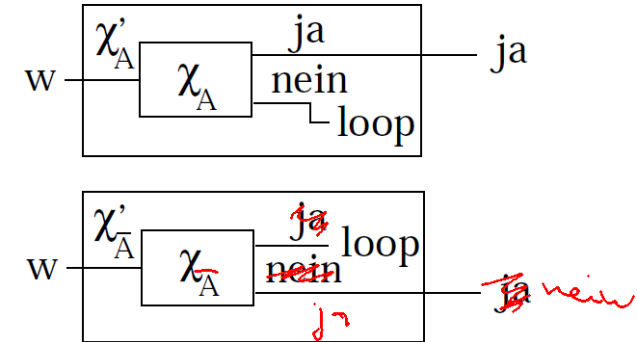


Satz 4.67

Eine Menge A ist entscheidbar gdw sowohl A als auch \bar{A} s-e sind.

Beweis:

„ \Rightarrow “: Wandle TM für χ_A in TM für χ'_A und $\chi'_{\bar{A}}$ um:



Beweis (Forts.):

„ \Leftarrow “:

Wandle TM M_1 für χ'_A und TM M_2 für $\chi'_{\bar{A}}$ in TM für χ_A um:

Beweis (Forts.):

„ \Leftarrow “:

Wandle TM M_1 für χ'_A und TM M_2 für $\chi'_{\bar{A}}$ in TM für χ_A um:

```
input(x);  
for  $s := 0, 1, 2, \dots$  do  
  if  $M_1[x]$  hält in  $s$  Schritten then output(1); halt fi ;  
  if  $M_2[x]$  hält in  $s$  Schritten then output(0); halt fi
```

Formulierung mit Parallelismus:



Beweis (Forts.):

„ \Leftarrow “:

Wandle TM M_1 für χ'_A und TM M_2 für $\chi'_{\bar{A}}$ in TM für χ_A um:

Definition 4.69

Eine Menge A heißt **rekursiv aufzählbar** (*recursively enumerable*)
gdw $A = \emptyset$ oder es eine berechenbare totale Funktion $f : \mathbb{N} \rightarrow A$
gibt, so dass

$$A = \{f(0), f(1), f(2), \dots\}$$

Definition 4.69

Eine Menge A heißt **rekursiv aufzählbar** (*recursively enumerable*)
gdw $A = \emptyset$ oder es eine berechenbare totale Funktion $f : \mathbb{N} \rightarrow A$
gibt, so dass

$$A = \{f(0), f(1), f(2), \dots\}$$

Bemerkung:

- Es dürfen Elemente doppelt auftreten ($f(i) = f(j)$ für $i \neq j$)
- Die Reihenfolge ist beliebig.

Warnung: Rekursiv aufzählbar \neq abzählbar!

Definition 4.69

Eine Menge A heißt **rekursiv aufzählbar** (*recursively enumerable*)
gdw $A = \emptyset$ oder es eine berechenbare totale Funktion $f : \mathbb{N} \rightarrow A$
gibt, so dass

$$A = \{f(0), f(1), f(2), \dots\}$$

$$\omega \mapsto \omega \cup \{f(i) \mid f(i) = \omega\}$$

Bemerkung:

- Es dürfen Elemente doppelt auftreten ($f(i) = f(j)$ für $i \neq j$)
- Die Reihenfolge ist beliebig.

Warnung: Rekursiv aufzählbar \neq abzählbar!

- Rekursiv aufzählbar \implies abzählbar

Definition 4.69

Eine Menge A heißt **rekursiv aufzählbar** (*recursively enumerable*)
gdw $A = \emptyset$ oder es eine berechenbare totale Funktion $f : \mathbb{N} \rightarrow A$
gibt, so dass

$$A = \{f(0), f(1), f(2), \dots\}$$

Bemerkung:

- Es dürfen Elemente doppelt auftreten ($f(i) = f(j)$ für $i \neq j$)
- Die Reihenfolge ist beliebig.

Warnung: Rekursiv aufzählbar \neq abzählbar!

- Rekursiv aufzählbar \implies abzählbar
- Aber nicht umgekehrt:
 $\overline{K} \subseteq \{0, 1\}^*$ ist abzählbar aber nicht rekursiv aufzählbar (s.u.)

Lemma 4.70

Eine Menge A ist rekursiv aufzählbar gdw sie semi-entscheidbar ist.

Lemma 4.70

Eine Menge A ist rekursiv aufzählbar gdw sie semi-entscheidbar ist.

Lemma 4.70

Eine Menge A ist rekursiv aufzählbar gdw sie semi-entscheidbar ist.

Beweis:

Der Fall $A = \emptyset$ ist trivial. Sei $A \neq \emptyset$.

Lemma 4.70

Eine Menge A ist rekursiv aufzählbar gdw sie semi-entscheidbar ist.

Beweis:

Der Fall $A = \emptyset$ ist trivial. Sei $A \neq \emptyset$.

„ \Rightarrow “:

Sei A rekursiv aufzählbar mit f . Dann ist A semi-entscheidbar:

input(x);

for $i := 0, 1, 2, \dots$ **do**

if $f(i) = x$ **then** output(1); **halt fi**

„ \Leftarrow “: Wir nehmen an $A \subseteq \mathbb{N}$.

Sei A semi-entscheidbar durch (zB) GOTO-Programm P .

Lemma 4.70

Eine Menge A ist rekursiv aufzählbar gdw sie semi-entscheidbar ist.

Beweis:

Der Fall $A = \emptyset$ ist trivial. Sei $A \neq \emptyset$.

„ \Rightarrow “:

Sei A rekursiv aufzählbar mit f . Dann ist A semi-entscheidbar:

input(x);

for $i := 0, 1, 2, \dots$ **do**

if $f(i) = x$ **then** output(1); **halt fi**

„ \Leftarrow “: Wir nehmen an $A \subseteq \mathbb{N}$.

Sei A semi-entscheidbar durch (zB) GOTO-Programm P .

Problem: $P[i]$ muss nicht halten und darf daher nur

„zeitbeschränkt“ ausgeführt werden.