Allgemeines Halteproblem
Hilberts 10. Problem

Prof. Dr. Berthold Vöcking
Lehrstuhl Informatik 1
Algorithmen und Komplexität
RWTH Aachen

November 2011

Wdh: Allgemeines Halteproblem

Das *allgemeine Halteproblem* ist definiert als

$$H_{\text{all}} = \{\langle M \rangle \mid M \text{ hält auf jeder Eingabe}\}$$

Wie kann man nachweisen, dass sowohl H_{all} als auch $\bar{H}_{\text{all}}$ nicht rekursiv aufzählbar sind?

Wdh: Allgemeines Halteproblem

Das *allgemeine Halteproblem* ist definiert als

$$H_{\text{all}} = \{\langle M \rangle \mid M \text{ hält auf jeder Eingabe}\}$$

Wie kann man nachweisen, dass sowohl H_{all} als auch $\bar{H}_{\text{all}}$ nicht rekursiv aufzählbar sind?

Wir verwenden eine spezielle Variante der Unterprgrammtechnik, die *Reduktion*.

Wdh: Die Reduktion

Definition

Es seien L_1 und L_2 Sprachen über einem Alphabet Σ. Dann heißt L_1 auf L_2 *reduzierbar*, Notation $L_1 \leq L_2$, wenn es eine berechenbare Funktion $f : \Sigma^* \to \Sigma^*$ gibt, so dass für alle $x \in \Sigma^*$ gilt

$$x \in L_1 \;\Leftrightarrow\; f(x) \in L_2 \;\;.$$

Wdh: Die Reduktion

Definition

Es seien L_1 und L_2 Sprachen über einem Alphabet Σ. Dann heißt L_1 auf L_2 *reduzierbar*, Notation $L_1 \leq L_2$, wenn es eine berechenbare Funktion $f : \Sigma^* \to \Sigma^*$ gibt, so dass für alle $x \in \Sigma^*$ gilt

$$x \in L_1 \;\Leftrightarrow\; f(x) \in L_2 \;\;.$$

Wir haben gezeigt:

Lemma

Falls $L_1 \leq L_2$ und L_2 rekursiv aufzählbar ist, so ist L_1 rekursiv aufzählbar.

Wdh: Die Reduktion

Im Umkehrschluss gilt:

Lemma

Falls $L_1 \leq L_2$ und L_1 nicht rekursiv aufzählbar ist, so ist L_2 nicht rekursiv aufzählbar.

Anwendung der Reduktion

H_ϵ ist nicht rekursiv, aber rekursiv aufzählbar. Folglich ist $\bar{H}_\epsilon$ nicht rekursiv aufzählbar.

Anwendung der Reduktion

H_ϵ ist nicht rekursiv, aber rekursiv aufzählbar. Folglich ist $\bar{H}_\epsilon$ nicht rekursiv aufzählbar.

Wir zeigen nun

Behauptung A

$$\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$$

Behauptung B

$$\bar{H}_\epsilon \leq H_{\text{all}}$$

Anwendung der Reduktion

H_ϵ ist nicht rekursiv, aber rekursiv aufzählbar. Folglich ist $\bar{H}_\epsilon$ nicht rekursiv aufzählbar.

Wir zeigen nun

Behauptung A

$$\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$$

Behauptung B

$$\bar{H}_\epsilon \leq H_{\text{all}}$$

Aus diesen Reduktionen folgt:

Satz

Sowohl $\bar{H}_{\text{all}}$ als auch H_{all} sind nicht rekursiv aufzählbar.

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$

Zur Durchführung der Reduktion gehen wir in zwei Schritten vor:

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$

Zur Durchführung der Reduktion gehen wir in zwei Schritten vor:

1) Wir beschreiben eine berechenbare Funktion f, die Ja-Instanzen von $\bar{H}_\epsilon$ auf Ja-Instanzen von $\bar{H}_{\text{all}}$ abbildet, und Nein-Instanzen von $\bar{H}_\epsilon$ auf Nein-Instanzen von $\bar{H}_{\text{all}}$ abbildet.

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$

Zur Durchführung der Reduktion gehen wir in zwei Schritten vor:

1) Wir beschreiben eine berechenbare Funktion f, die Ja-Instanzen von $\bar{H}_\epsilon$ auf Ja-Instanzen von $\bar{H}_{\text{all}}$ abbildet, und Nein-Instanzen von $\bar{H}_\epsilon$ auf Nein-Instanzen von $\bar{H}_{\text{all}}$ abbildet.

2) Für die Korrektheit zeigen wir:
   a) $w \in \bar{H}_\epsilon \;\Rightarrow\; f(w) \in \bar{H}_{\text{all}}$
   b) $w \notin \bar{H}_\epsilon \;\Rightarrow\; f(w) \notin \bar{H}_{\text{all}}$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$

Beschreibung der Funktion f :

Sei w die Eingabe für $\bar{H}_\epsilon$.

- Wenn w keine gültige Gödelnummer ist, so sei $f(w) = w$.

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$

Beschreibung der Funktion f :

Sei w die Eingabe für $\bar{H}_\epsilon$.

- Wenn w keine gültige Gödelnummer ist, so sei $f(w) = w$.
- Falls $w = \langle M \rangle$ für eine TM M, so sei $f(w)$ die Gödelnummer einer TM M^*_ϵ mit der folgenden Eigenschaft:

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$

Beschreibung der Funktion f :

Sei w die Eingabe für $\bar{H}_\epsilon$.

- Wenn w keine gültige Gödelnummer ist, so sei $f(w) = w$.
- Falls $w = \langle M \rangle$ für eine TM M, so sei $f(w)$ die Gödelnummer einer TM M^*_ϵ mit der folgenden Eigenschaft:

M^*_ϵ ignoriert die Eingabe und simuliert M mit der Eingabe ϵ.

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$

Beschreibung der Funktion f :

Sei w die Eingabe für $\bar{H}_\epsilon$.

- Wenn w keine gültige Gödelnummer ist, so sei $f(w) = w$.
- Falls $w = \langle M \rangle$ für eine TM M, so sei $f(w)$ die Gödelnummer einer TM M^*_ϵ mit der folgenden Eigenschaft:

M^*_ϵ ignoriert die Eingabe und simuliert M mit der Eingabe ϵ.

Die Funktion f ist offensichtlich berechenbar.

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

Korrektheit:

Falls w keine Gödelnummer ist, so ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) \in \bar{H}_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M^*_\epsilon \rangle$.

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

Korrektheit:

Falls w keine Gödelnummer ist, so ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) \in \bar{H}_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M^*_\epsilon \rangle$.

Es gilt

$$w \notin \bar{H}_\epsilon \quad \Rightarrow \quad M \text{ hält auf der Eingabe } \epsilon$$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

Korrektheit:

Falls w keine Gödelnummer ist, so ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) \in \bar{H}_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M^*_\epsilon \rangle$.

Es gilt

$$\begin{aligned} w \notin \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält auf der Eingabe } \epsilon \\ &\Rightarrow \quad M^*_\epsilon \text{ hält auf jeder Eingabe} \end{aligned}$$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

Korrektheit:

Falls w keine Gödelnummer ist, so ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) \in \bar{H}_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M^*_\epsilon \rangle$.

Es gilt

$$\begin{aligned} w \notin \bar{H}_\epsilon &\Rightarrow M \text{ hält auf der Eingabe } \epsilon \\ &\Rightarrow M^*_\epsilon \text{ hält auf jeder Eingabe} \\ &\Rightarrow \langle M^*_\epsilon \rangle \in H_{\text{all}} \end{aligned}$$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

Korrektheit:

Falls w keine Gödelnummer ist, so ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) \in \bar{H}_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M^*_\epsilon \rangle$.

Es gilt

$$\begin{aligned} w \notin \bar{H}_\epsilon &\Rightarrow M \text{ hält auf der Eingabe } \epsilon \\ &\Rightarrow M^*_\epsilon \text{ hält auf jeder Eingabe} \\ &\Rightarrow \langle M^*_\epsilon \rangle \in H_{\text{all}} \\ &\Rightarrow f(w) \notin \bar{H}_{\text{all}} \ . \end{aligned}$$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

$$w \in \bar{H}_\epsilon \quad \Rightarrow \quad M \text{ hält nicht auf Eingabe } \epsilon$$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf Eingabe } \epsilon \\
&\Rightarrow \quad M^*_\epsilon \text{ hält auf keiner Eingabe}
\end{aligned}
$$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf Eingabe } \epsilon \\
&\Rightarrow \quad M_\epsilon^* \text{ hält auf keiner Eingabe} \\
&\Rightarrow \quad \langle M_\epsilon^* \rangle \notin H_{\text{all}}
\end{aligned}
$$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf Eingabe } \epsilon \\
&\Rightarrow \quad M_\epsilon^* \text{ hält auf keiner Eingabe} \\
&\Rightarrow \quad \langle M_\epsilon^* \rangle \notin H_{\text{all}} \\
&\Rightarrow \quad f(w) \in \bar{H}_{\text{all}} \ .
\end{aligned}
$$

Beweis von Behauptung A: $\bar{H}_\epsilon \leq \bar{H}_{\text{all}}$ — Korrektheit

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf Eingabe } \epsilon \\
&\Rightarrow \quad M_\epsilon^* \text{ hält auf keiner Eingabe} \\
&\Rightarrow \quad \langle M_\epsilon^* \rangle \notin H_{\text{all}} \\
&\Rightarrow \quad f(w) \in \bar{H}_{\text{all}} \ .
\end{aligned}
$$

Also gilt $w \in \bar{H}_\epsilon \ \Leftrightarrow \ f(w) \in \bar{H}_{\text{all}}$ und somit ist die Funktion f korrekt konstruiert. □

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Wir gehen wiederum in zwei Schritten vor:

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Wir gehen wiederum in zwei Schritten vor:

1) Wir beschreiben eine berechenbare Funktion f, die Ja-Instanzen von $\bar{H}_\epsilon$ auf Ja-Instanzen von H_{all} abbildet, und Nein-Instanzen von $\bar{H}_\epsilon$ auf Nein-Instanzen von H_{all} abbildet.

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Wir gehen wiederum in zwei Schritten vor:

1) Wir beschreiben eine berechenbare Funktion f, die Ja-Instanzen von $\bar{H}_\epsilon$ auf Ja-Instanzen von H_{all} abbildet, und Nein-Instanzen von $\bar{H}_\epsilon$ auf Nein-Instanzen von H_{all} abbildet.

2) Für die Korrektheit zeigen wir:
   a) $w \in \bar{H}_\epsilon \Rightarrow f(w) \in H_{\text{all}}$
   b) $w \notin \bar{H}_\epsilon \Rightarrow f(w) \notin H_{\text{all}}$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Beschreibung der Funktion f:

Sei w die Eingabe für $\bar{H}_\epsilon$. Sei w' irgendein Wort aus H_{all}.

- Wenn w keine gültige Gödelnummer ist, so sei $f(w) = w'$.

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Beschreibung der Funktion f :

Sei w die Eingabe für $\bar{H}_\epsilon$. Sei w' irgendein Wort aus H_{all}.

- Wenn w keine gültige Gödelnummer ist, so sei $f(w) = w'$.
- Falls $w = \langle M \rangle$ für eine TM M, so sei $f(w)$ die Gödelnummer einer TM M'_M, die sich auf Eingaben der Länge i wie folgt verhält:

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Beschreibung der Funktion f :

Sei w die Eingabe für $\bar{H}_\epsilon$. Sei w' irgendein Wort aus H_{all}.

- Wenn w keine gültige Gödelnummer ist, so sei $f(w) = w'$.
- Falls $w = \langle M \rangle$ für eine TM M, so sei $f(w)$ die Gödelnummer einer TM M'_M, die sich auf Eingaben der Länge i wie folgt verhält:

M'_M simuliert die ersten i Schritte von M auf der Eingabe ϵ. Wenn M innerhalb dieser i Schritte hält, dann geht M'_M in eine Endlosschleife, ansonsten hält M'_M.

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Beschreibung der Funktion f :

Sei w die Eingabe für $\bar{H}_\epsilon$. Sei w' irgendein Wort aus H_{all}.

- Wenn w keine gültige Gödelnummer ist, so sei $f(w) = w'$.
- Falls $w = \langle M \rangle$ für eine TM M, so sei $f(w)$ die Gödelnummer einer TM M'_M, die sich auf Eingaben der Länge i wie folgt verhält:

M'_M simuliert die ersten i Schritte von M auf der Eingabe ϵ. Wenn M innerhalb dieser i Schritte hält, dann geht M'_M in eine Endlosschleife, ansonsten hält M'_M.

Die Funktion f ist offensichtlich berechenbar.

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Korrektheit

Falls w keine Gödelnummer ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) = w' \in H_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M'_M \rangle$.

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Korrektheit

Falls w keine Gödelnummer ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) = w' \in H_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M'_M \rangle$.

Es gilt

$$w \notin \bar{H}_\epsilon \quad \Rightarrow \quad M \text{ hält auf der Eingabe } \epsilon$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Korrektheit

Falls w keine Gödelnummer ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) = w' \in H_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M'_M \rangle$.

Es gilt

$$\begin{aligned} w \notin \bar{H}_\epsilon &\Rightarrow M \text{ hält auf der Eingabe } \epsilon \\ &\Rightarrow \exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon \end{aligned}$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Korrektheit

Falls w keine Gödelnummer ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) = w' \in H_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M'_M \rangle$.

Es gilt

$$\begin{aligned} w \notin \bar{H}_\epsilon &\Rightarrow M \text{ hält auf der Eingabe } \epsilon \\ &\Rightarrow \exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon \\ &\Rightarrow \exists i\text{: } M'_M \text{ hält nicht auf Eingaben der Länge } i \end{aligned}$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Korrektheit

Falls w keine Gödelnummer ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) = w' \in H_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M'_M \rangle$.

Es gilt

$$
\begin{aligned}
w \notin \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält auf der Eingabe } \epsilon \\
&\Rightarrow \quad \exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon \\
&\Rightarrow \quad \exists i\text{: } M'_M \text{ hält nicht auf Eingaben der Länge } i \\
&\Rightarrow \quad M'_M \text{ hält nicht auf jeder Eingabe}
\end{aligned}
$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

Korrektheit

Falls w keine Gödelnummer ist die Korrektheit klar, denn in diesem Fall gilt $w \in \bar{H}_\epsilon$ und $f(w) = w' \in H_{\text{all}}$.

Sei nun $w = \langle M \rangle$ für eine TM M, so dass $f(w) = \langle M'_M \rangle$.

Es gilt

$$
\begin{aligned}
w \notin \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält auf der Eingabe } \epsilon \\
&\Rightarrow \quad \exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon \\
&\Rightarrow \quad \exists i\text{: } M'_M \text{ hält nicht auf Eingaben der Länge } i \\
&\Rightarrow \quad M'_M \text{ hält nicht auf jeder Eingabe} \\
&\Rightarrow \quad f(w) = \langle M'_M \rangle \notin H_{\text{all}} \ .
\end{aligned}
$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

$$w \in \bar{H}_\epsilon \quad \Rightarrow \quad M \text{ hält nicht auf der Eingabe } \epsilon$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf der Eingabe } \epsilon \\
&\Rightarrow \quad \neg\exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon
\end{aligned}
$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf der Eingabe } \epsilon \\
&\Rightarrow \quad \neg\exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon \\
&\Rightarrow \quad \forall i\text{: } M'_M \text{ hält auf Eingaben der Länge } i
\end{aligned}
$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf der Eingabe } \epsilon \\
&\Rightarrow \quad \neg\exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon \\
&\Rightarrow \quad \forall i\text{: } M'_M \text{ hält auf Eingaben der Länge } i \\
&\Rightarrow \quad M'_M \text{ hält auf jeder Eingabe}
\end{aligned}
$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf der Eingabe } \epsilon \\
&\Rightarrow \quad \neg\exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon \\
&\Rightarrow \quad \forall i\text{: } M'_M \text{ hält auf Eingaben der Länge } i \\
&\Rightarrow \quad M'_M \text{ hält auf jeder Eingabe} \\
&\Rightarrow \quad f(w) = \langle M'_M \rangle \in H_{\text{all}} \ .
\end{aligned}
$$

Beweis von Behauptung B: $\bar{H}_\epsilon \leq H_{\text{all}}$

$$
\begin{aligned}
w \in \bar{H}_\epsilon \quad &\Rightarrow \quad M \text{ hält nicht auf der Eingabe } \epsilon \\
&\Rightarrow \quad \neg\exists i\text{: } M \text{ hält innerhalb von } i \text{ Schritten auf } \epsilon \\
&\Rightarrow \quad \forall i\text{: } M'_M \text{ hält auf Eingaben der Länge } i \\
&\Rightarrow \quad M'_M \text{ hält auf jeder Eingabe} \\
&\Rightarrow \quad f(w) = \langle M'_M \rangle \in H_{\text{all}} \ .
\end{aligned}
$$

Also gilt $w \in \bar{H}_\epsilon \ \Leftrightarrow \ f(w) \in H_{\text{all}}$ und somit ist die Funktion f korrekt konstruiert. □

Anmerkung zur Reduktion

Es gilt übrigens auch

Lemma

Falls $L_1 \leq L_2$ und L_2 rekursiv ist, so ist L_1 rekursiv.

Beziehungsweise

Lemma

Falls $L_1 \leq L_2$ und L_1 nicht rekursiv ist, so ist L_2 nicht rekursiv.

Beweis: analog zur rekursiven Aufzählbarkeit. □

Hilberts zehntes Problem

Im Jahr 1900 präsentierte der Mathematiker David Hilbert 23 mathematische Probleme auf einem Kongress in Paris.

Hilberts zehntes Problem

Im Jahr 1900 präsentierte der Mathematiker David Hilbert 23 mathematische Probleme auf einem Kongress in Paris.

Hilberts zehntes Problem (im Originalwortlaut)

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlenkoeffizienten sei vorgelegt: *Man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in den ganzen rationalen Zahlen lösbar ist.*

Hilberts zehntes Problem

Im Jahr 1900 präsentierte der Mathematiker David Hilbert 23 mathematische Probleme auf einem Kongress in Paris.

Hilberts zehntes Problem (im Originalwortlaut)

Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlenkoeffizienten sei vorgelegt: *Man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in den ganzen rationalen Zahlen lösbar ist.*

Die „ganzen rationalen Zahlen“, von denen in diesem Problem die Rede ist, sind die ganzen Zahlen aus $\mathbb{Z}$, wie wir sie kennen.

„Diophantische Gleichungen“ bezeichnen Gleichungen über Polynomen in mehreren Variablen.

Diophantische Gleichungen

- Ein *Term* ist ein Produkt aus Variablen mit einem konstanten Koeffizienten, z.B. ist

$$6 \cdot x \cdot x \cdot x \cdot y \cdot z \cdot z \quad \text{bzw.} \quad 6x^3yz^2$$

ein Term über den Variablen x, y, z mit dem Koeffizienten 6.

Diophantische Gleichungen

- Ein *Term* ist ein Produkt aus Variablen mit einem konstanten Koeffizienten, z.B. ist

$$6 \cdot x \cdot x \cdot x \cdot y \cdot z \cdot z \quad \text{bzw.} \quad 6x^3yz^2$$

ein Term über den Variablen x, y, z mit dem Koeffizienten 6.

- Ein *Polynom* ist eine Summe von Termen, z.B.

$$6x^3yz^2 + 3xy^2 - x^3 - 10 \ .$$

Diophantische Gleichungen

- Ein *Term* ist ein Produkt aus Variablen mit einem konstanten Koeffizienten, z.B. ist

$$6 \cdot x \cdot x \cdot x \cdot y \cdot z \cdot z \quad \text{bzw.} \quad 6x^3yz^2$$

ein Term über den Variablen x, y, z mit dem Koeffizienten 6.

- Ein *Polynom* ist eine Summe von Termen, z.B.

$$6x^3yz^2 + 3xy^2 - x^3 - 10 \ .$$

- Eine *diophantische Gleichung* setzt ein Polynom gleich Null. Die Lösungen der Gleichung entsprechen also den Nullstellen des Polynoms. Obiges Polynom hat beispielsweise die Nullstelle

$$(x, y, z) = (5, 3, 0) \ .$$

Formulierung als Entscheidungsproblem

Hilberts zehntes Problem (in unseren Worten)

Beschreibe einen Algorithmus, der entscheidet, ob ein gegebenes Polynom mit ganzzahligen Koeffizienten eine ganzzahlige Nullstelle hat.

Formulierung als Entscheidungsproblem

Hilberts zehntes Problem (in unseren Worten)

Beschreibe einen Algorithmus, der entscheidet, ob ein gegebenes Polynom mit ganzzahligen Koeffizienten eine ganzzahlige Nullstelle hat.

Die diesem Entscheidungsproblem zugrundeliegende Sprache ist

$$N = \{ p \mid p \text{ ist ein Polynom mit einer ganzzahligen Nullstelle} \} .$$

Rekursive Aufzählbarkeit von N

Gegeben sei ein Polynom p mit ℓ Variablen.

Der Wertebereich von p entspricht der abzählbar unendlichen Menge $\mathbb{Z}^\ell$.

Rekursive Aufzählbarkeit von N

Gegeben sei ein Polynom p mit ℓ Variablen.

Der Wertebereich von p entspricht der abzählbar unendlichen Menge $\mathbb{Z}^\ell$.

Der folgende Algorithmus erkennt N:

- Zähle die ℓ-Tupel aus $\mathbb{Z}^\ell$ in kanonischer Reihenfolge auf und werte p für jedes dieser Tupel aus.
- Akzeptiere sobald eine der Auswertungen den Wert *Null* ergibt.

Rekursive Aufzählbarkeit von N

Gegeben sei ein Polynom p mit ℓ Variablen.

Der Wertebereich von p entspricht der abzählbar unendlichen Menge $\mathbb{Z}^\ell$.

Der folgende Algorithmus erkennt N:

- Zähle die ℓ-Tupel aus $\mathbb{Z}^\ell$ in kanonischer Reihenfolge auf und werte p für jedes dieser Tupel aus.
- Akzeptiere sobald eine der Auswertungen den Wert *Null* ergibt.

Fazit: N ist rekursiv aufzählbar.

Ist N entscheidbar? – Diskussion

- Falls wir eine obere Schranke für die Absolutwerte der Nullstellen hätten, so bräuchten wir nur eine endliche Menge von ℓ-Tupeln aufzählen, und N wäre somit entscheidbar.

Ist N entscheidbar? – Diskussion

- Falls wir eine obere Schranke für die Absolutwerte der Nullstellen hätten, so bräuchten wir nur eine endliche Menge von ℓ-Tupeln aufzählen, und N wäre somit entscheidbar.
- Für Polynome über nur einer Variable gibt es tatsächlich eine derartige obere Schranke: Für ein Polynom der Form

$$p(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$$

mit ganzzahligen Koeffizienten gilt

$$p(x) = 0, x \in \mathbb{Z} \Rightarrow x \text{ teilt } a_0. \text{ (Warum?)}$$

Also gibt es keine Nullstelle mit Absolutwert größer als $|a_0|$.

Ist N entscheidbar? – Diskussion

- Falls wir eine obere Schranke für die Absolutwerte der Nullstellen hätten, so bräuchten wir nur eine endliche Menge von ℓ-Tupeln aufzählen, und N wäre somit entscheidbar.
- Für Polynome über nur einer Variable gibt es tatsächlich eine derartige obere Schranke: Für ein Polynom der Form

$$p(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0$$

mit ganzzahligen Koeffizienten gilt

$$p(x) = 0, x \in \mathbb{Z} \Rightarrow x \text{ teilt } a_0. \text{ (Warum?)}$$

Also gibt es keine Nullstelle mit Absolutwert größer als $|a_0|$.

- Eingeschränkt auf Polynome mit nur einer Variable ist das Nullstellenproblem damit entscheidbar.

Ist N entscheidbar? – Diskussion

- Für Polynome mit mehreren Variablen gibt es leider keine obere Schranke für die Absolutwerte der Nullstellen. Um das einzusehen, betrachte beispielsweise das Polynom $x + y$.

Ist N entscheidbar? – Diskussion

- Für Polynome mit mehreren Variablen gibt es leider keine obere Schranke für die Absolutwerte der Nullstellen. Um das einzusehen, betrachte beispielsweise das Polynom $x + y$.
- Aber vielleicht gibt es ja immer eine Nullstelle mit kleinen Absolutwerten und somit eine obere Schranke für die Nullstelle mit den kleinsten Absolutwerten?

Ist N entscheidbar? – Diskussion

- Für Polynome mit mehreren Variablen gibt es leider keine obere Schranke für die Absolutwerte der Nullstellen. Um das einzusehen, betrachte beispielsweise das Polynom $x + y$.
- Aber vielleicht gibt es ja immer eine Nullstelle mit kleinen Absolutwerten und somit eine obere Schranke für die Nullstelle mit den kleinsten Absolutwerten?
- Oder vielleicht gibt es ganz andere Möglichkeiten einem Polynom anzusehen, ob es eine ganzzahlige Nullstelle hat?

Ist N entscheidbar? – Diskussion

- Für Polynome mit mehreren Variablen gibt es leider keine obere Schranke für die Absolutwerte der Nullstellen. Um das einzusehen, betrachte beispielsweise das Polynom $x + y$.
- Aber vielleicht gibt es ja immer eine Nullstelle mit kleinen Absolutwerten und somit eine obere Schranke für die Nullstelle mit den kleinsten Absolutwerten?
- Oder vielleicht gibt es ganz andere Möglichkeiten einem Polynom anzusehen, ob es eine ganzzahlige Nullstelle hat?
- Erst knapp siebzig Jahre nachdem Hilbert sein Problem präsentiert hat, konnte Yuri Matijasevič all' diese Fragen beantworten, und zwar negativ!

Unentscheidbarkeit des Nullstellenproblems

Hilbert hat die folgende Antwort nicht erwartet.

Unentscheidbarkeit des Nullstellenproblems

Hilbert hat die folgende Antwort nicht erwartet.

Satz von Matijasevič (1970)

Das Problem, ob ein ganzzahliges Polynom eine ganzzahlige Nullstelle hat, ist unentscheidbar.

Unentscheidbarkeit des Nullstellenproblems

Hilbert hat die folgende Antwort nicht erwartet.

Satz von Matijasevič (1970)

Das Problem, ob ein ganzzahliges Polynom eine ganzzahlige Nullstelle hat, ist unentscheidbar.

Damit ist Hilberts Aufgabenstellung unlösbar.

Unentscheidbarkeit des Nullstellenproblems

Der Beweis des Satzes von Matijasevič beruht auf einer Kette von Reduktionen durch die letztendlich das Halteproblem H auf das Nullstellenproblem N reduziert wird. Yuri Matijasevič hat „lediglich“ das letzte Glied dieser Kette geschlossen. Andere wichtige Beiträge zu diesem Ergebnis wurden zuvor von Martin Davis, Julia Robinson und Hilary Putnan erbracht.

Unentscheidbarkeit des Nullstellenproblems

Der Beweis des Satzes von Matijasevič beruht auf einer Kette von Reduktionen durch die letztendlich das Halteproblem H auf das Nullstellenproblem N reduziert wird. Yuri Matijasevič hat „lediglich“ das letzte Glied dieser Kette geschlossen. Andere wichtige Beiträge zu diesem Ergebnis wurden zuvor von Martin Davis, Julia Robinson und Hilary Putnan erbracht.

Leider ist der Beweis zu komplex, um ihn im Rahmen dieser Vorlesung präsentieren zu können.