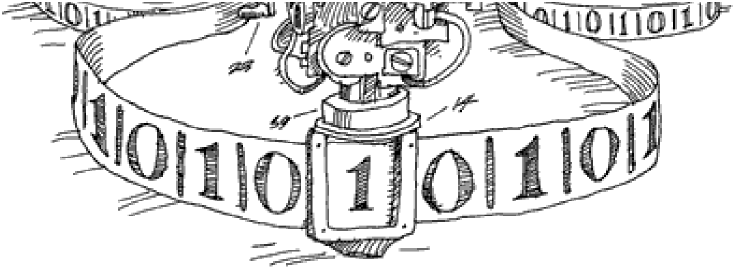
Karlsruher Institut für Technologie

Tutorium Theoretische Grundlagen der Informatik

Simon Bischof

Institut für Kryptographie und Sicherheit



Zum Übungsblatt

Karlsruher Institut für Technologie

- beim ”Simulieren” alle Konfigurationen angeben, außer es steht explizit was anderes da
- Zwischenschritte beim Umformen in Chomsky-NF machen es dem Tutor einfacher

Gödels Unvollständigkeitssatz

- Jedes ”hinreichend mächtige” formale System ist entweder widersprüchlich oder unvollständig.

Gödels Unvollständigkeitssatz

- Jedes ”hinreichend mächtige” formale System ist entweder widersprüchlich oder unvollständig.
- Bsp. für hinreichend mächtig: $\mathbb{N}$ mit $+$ und $*$ (Th$(\mathbb{N}, +, *)$)

(Nicht-)Entscheidbarkeit von wichtigen Theorien

- $\mathrm{Th}(\mathbb{N}, +)$ ist entscheidbar.

(Nicht-)Entscheidbarkeit von wichtigen Theorien

- $\mathrm{Th}(\mathbb{N}, +)$ ist entscheidbar.
- $\mathrm{Th}(\mathbb{N}, +, *)$ ist unentscheidbar.

Was ist ein Beweis?

- Ein Beweis ist (maschinen-)überprüfbar.
- Alle beweisbaren Aussagen sind wahr (”Soundness”).

Was ist ein Beweis?

- Ein Beweis ist (maschinen-)überprüfbar.
- Alle beweisbaren Aussagen sind wahr (”Soundness”).
- Die Menge der beweisbaren Aussagen in $\mathrm{Th}(\mathbb{N}, +, *)$ ist rekursiv aufzählbar.

$\Rightarrow$ Es existieren nicht beweisbare Aussagen in $\mathrm{Th}(\mathbb{N}, +, *)$.

Was ist ein Beweis?

- Ein Beweis ist (maschinen-)überprüfbar.
- Alle beweisbaren Aussagen sind wahr (”Soundness”).
- Die Menge der beweisbaren Aussagen in $\mathrm{Th}(\mathbb{N}, +, *)$ ist rekursiv aufzählbar.

$\Rightarrow$ Es existieren nicht beweisbare Aussagen in $\mathrm{Th}(\mathbb{N}, +, *)$.

- Für jedes Kalkül (mit ”Soundness” und Turingentscheidbarkeit der Gültigkeit von Ableitungen) gibt es eine Aussage, die im Kalkül nicht beweisbar ist.

Turingreduzierbarkeit

- Ein Orakel für eine Sprache L ist ein ”externes Gerät”, das als Hilfe für eine TM entscheidet, ob ein Wort $w \in L$ ist.
- $TM^O :=$ Turingmaschine mit Zugriff auf Orakel O.

Turingreduzierbarkeit

- Ein Orakel für eine Sprache L ist ein ”externes Gerät”, das als Hilfe für eine TM entscheidet, ob ein Wort $w \in L$ ist.
- $TM^O :=$ Turingmaschine mit Zugriff auf Orakel O.
- $A \leq_T B :=$ es existiert eine Orakel-TM TM^O, die A entscheidet, wobei O Orakel für B (Turingreduzierbarkeit).

Turingreduzierbarkeit

- Ein Orakel für eine Sprache L ist ein ”externes Gerät”, das als Hilfe für eine TM entscheidet, ob ein Wort $w \in L$ ist.
- $TM^O :=$ Turingmaschine mit Zugriff auf Orakel O.
- $A \leq_T B :=$ es existiert eine Orakel-TM TM^O, die A entscheidet, wobei O Orakel für B (Turingreduzierbarkeit).
- $A \leq_T B$ und B entscheidbar $\Rightarrow A$ entscheidbar
- Halteproblem für TM mit Orakel O nicht durch Turingmaschinen mit Orakel O entscheidbar.

ein kleiner Versuch...

Karlsruher Institut für Technologie

ein kleiner Versuch...

Karlsruher Institut für Technologie

37498693208414903274912470912926919689532787419749816298460714862583214188 84

ein kleiner Versuch...

Karlsruher Institut für Technologie

ein kleiner Versuch...

Karlsruher Institut für Technologie

012345678910111213141516171819202122232425
262728293031323334353637383940414 2

ein kleiner Versuch...

Karlsruher Institut für Technologie

Kolmogorow-Komplexität

- stelle Wort w durch $\langle M \rangle 01 w'$ dar, wobei
  - 01 ist ”Trennzeichen”
  - M bei Eingabe w' hält und w aufs Band schreibt

Kolmogorow-Komplexität

- stelle Wort w durch $\langle M \rangle 01 w'$ dar, wobei
  - 01 ist ”Trennzeichen”
  - M bei Eingabe w' hält und w aufs Band schreibt
- $K(w)$ ist die Länge der kürzesten Codierung für $w \in \{0,1\}^*$ nach obiger Form (Kolmogorow-Komplexität)