

Theoretische Grundlagen der Informatik

Tutorium 7

Institut für Kryptographie und Sicherheit



Das Rekursionstheorem 1.Form

Existiert eine TM M , die die Funktion $t: \Sigma^* \times \Sigma^* \rightarrow \Sigma^*$ berechnet, dann existiert eine TM R die $t(\langle R \rangle, w)$ berechnet, wobei w die Eingabe ist.

Dieses Theorem ist nicht nur auf Turingmaschinen beschränkt, sondern kann auch auf jede beliebige turingvollständige Codierungsform (wie z.B. Programmiersprachen) ausgedehnt werden.

Das Rekursionstheorem 2.Form

Für jede berechenbare Funktion $f: \Sigma^* \rightarrow \Sigma^*$ existiert eine TM F und eine TM G , wobei F und G die gleiche Funktion berechnen und $f(\langle F \rangle) = \langle G \rangle$.

Damit hat jede Programmtransformation einen Fixpunkt.

Eine SELF-Maschine (auch Quine genannt) ist eine Turingmaschine, die ihre eigene Gödelnummer ausgibt und dann hält. Sie realisiert demnach die Funktion $t(\langle SELF \rangle, w) = \langle SELF \rangle$.

Eine mögliche Art eine solche TM zu erstellen ist folgender:

- Man zerlegt die Turingmaschine in zwei Teile A und B.
- Teil A löscht die Eingabe und schreibt die Gödelnummer von Teil B aufs Band.
- Teil B liest die neue Eingabe w (seine eigene Gödelnummer) ein, schreibt die Gödelnummer der Turingmaschine aufs Band die bei beliebiger Eingabe das Wort w ausgibt, hängt daran w an und hält.

■ Quantoren

■ Existenzquantor $\exists x$:

Aussage muss für mindestens ein x aus dem Universum gelten.

■ Allquantor $\forall x$: Aussage muss für alle x aus dem Universum gelten.

■ Vorsicht bei Schachtelung von Quantoren:

$\forall x \exists y : x = y$ ist etwas völlig anderes als $\exists y \forall x : x = y$.

■ Ein Universum ist die Menge über der man eine Aussage betrachtet.

■ Eine Relation drückt aus, dass zwei Objekte zueinander in Beziehung stehen.

■ Sei R die Gleichheit, dann gilt $R(x, y) \Leftrightarrow x = y$.

■ Eine Theorie ist eine Menge $Th(U, R)$ induziert über dem Tupel (U, R) mit einem Universum U und einer Relation R .

Eine Formel ϕ ist Element einer Theorie, falls sie in Bezug auf U bzw. R wahr ist.

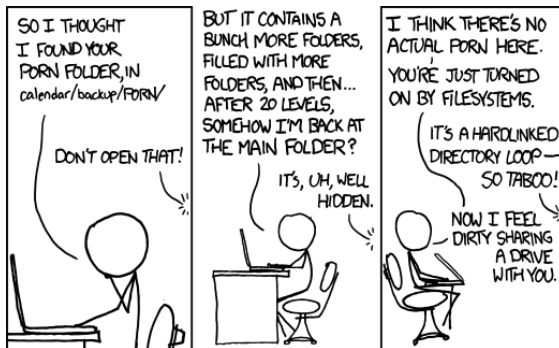
■ Sei $\phi = \forall x \exists y : R_1(x, y)$. Dann gilt $\phi \in Th(\mathbb{Z}, >)$ aber $\phi \notin Th(\mathbb{N}, >)$.

Geben Sie für folgendende Formeln an ob diese in den besagten Theorien liegen

1. Ist $\phi_1 = \forall x \exists y \forall z : x + y = z$ in $\text{Th}(\mathbb{N}, +)$?
2. Ist $\phi_2 = \forall x \exists y \forall z \exists w : (x + z = w) \wedge (x + y = w)$ in $\text{Th}(\mathbb{N}, +)$?
3. Ist
 $\phi_3 = \forall x \forall y \forall z \forall w \forall v \exists s : \neg(x + w = y) \vee \neg(y + v = z) \vee (x + s = z)$
in $\text{Th}(\mathbb{N}, +)$?
4. Sei $\text{Th}(\mathbb{N}, <)$ die Theorie der natürlichen Zahlen mit der Relation „echt kleiner“. Zeigen Sie: $\text{Th}(\mathbb{N}, <)$ ist entscheidbar.

Geben Sie Modelle für die folgenden prädikatenlogischen Formeln an!
Geben Sie dazu jeweils ein Universum \mathcal{U}
und eine Interpretation der Relationszeichen R_i an!

1. $\phi_1 = \quad \forall x (R_1(x, x))$ [K1.1]
 $\quad \wedge \forall x, y (R_1(x, y) \leftrightarrow R_1(y, x))$ [K1.2]
 $\quad \wedge \forall x, y, z ((R_1(x, y) \wedge R_1(y, z)) \rightarrow R_1(x, z))$ [K1.3]
2. $\phi_2 = \quad \phi_1$
 $\quad \wedge \forall x (R_1(x, x) \rightarrow \neg R_2(x, x))$ [K2.1]
 $\quad \wedge \forall x, y (\neg R_1(x, y) \rightarrow (R_2(x, y) \oplus R_2(y, x)))$ [K2.2]
 $\quad \wedge \forall x, y, z ((R_2(x, y) \wedge R_2(y, z)) \rightarrow R_2(x, z))$ [K2.3]
 $\quad \wedge \forall x \exists y (R_2(x, y))$ [K2.4]





Dieses Werk ist unter einem "Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 3.0 Deutschland"-Lizenzvertrag lizenziert. Um eine Kopie der Lizenz zu erhalten, gehen Sie bitte zu <http://creativecommons.org/licenses/by-sa/3.0/de/> oder schreiben Sie an Creative Commons, 171 Second Street, Suite 300, San Francisco, California 94105, USA.

Davon ausgenommen sind das Titelbild, welches aus der März-April 2002 Ausgabe von American Scientist erschienen ist und ohne Erlaubnis verwendet wird, sowie das KIT Beamer Theme. Hierfür gelten die Bestimmungen der jeweiligen Urheber.