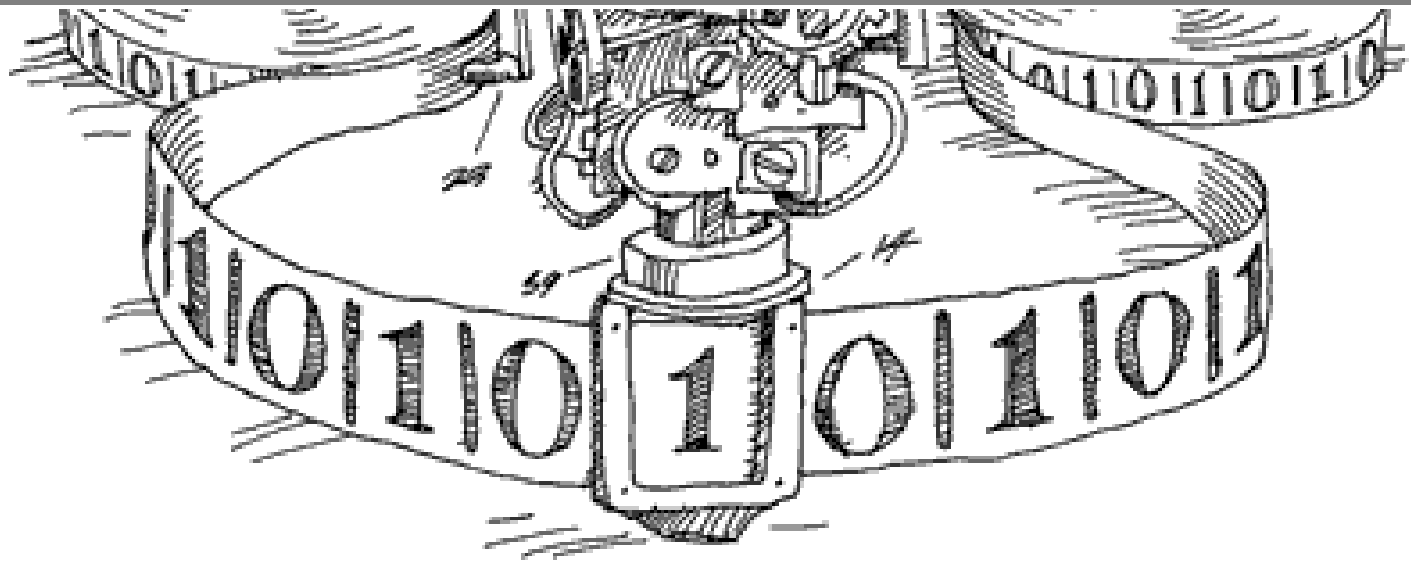
Karlsruher Institut für Technologie

Theoretische Grundlagen der Informatik

Tutorium 7

Institut für Kryptographie und Sicherheit



CH1 – Not even my final Form

Kontextfreie Grammatiken werden in dieser Vorlesung durch Produktionsmengen der folgenden Form charakterisiert:

- P = Menge der Produktionen mit Form $v \to w$
  - $v \in V^+$
  - $w \in ((V \setminus \{S\}) \bigcup T)^+$
  - $|v| \leq |w|$ oder $S \to \epsilon$

Grammatiken dieser Form lassen sich alle in Grammatiken dieser Form umwandeln (siehe Vorlesung bzw. Skript):

- P = Menge der Produktionen mit Form $\alpha A \beta \to \alpha B \beta$ oder $S \to A$ oder $A \to a$
  - $A \in V$
  - $\alpha, \beta, B \in V^*, B \neq \epsilon$
  - $a in T$

Das ist wichtig weil:

- Die untere Form ist geläufiger als Definition von kontextfreien Grammatiken
- Dazu konstruierte TM bei der unteren Form u.U. einfacher sind

Chompsky Abschlüsse

	Ch3	Ch2	Ch1	Ch0
Name	regulär	kontextfrei	kontextsensitiv	rekursiv aufzählba
Entscheidbar	✓	✓	✓	semi
„·“-Abschluss	✓	✓	✓	✓
„—“-Abschluss	✓	×	✓	×
„∪“-Abschluss	✓	✓	✓	✓
„∩“-Abschluss	✓	×	✓	✓
„∗“-Abschluss	✓	✓	✓	✓

- „—“-Abschluss = Abgeschlossenheit unter Komplementbildung
- Semientscheidbarkeit = ∃TM, die genau alle Wörter der Sprache akzeptiert, aber Wörter außerhalb der Sprache können Endlosschleifen erzeugen
- nicht entscheidbar = nichtentscheidbar = unentscheidbar = Kann nicht für jedes Wort sagen ob es in der Sprache liegt oder nicht, kann aber semi-entscheidbar sein

Reduktion

Aufgabe: Ist ein gegebenes *Problem* A *attribut*?

- Nehme an, A ist *attribut*
- Suche ein geeignetes *Problem* B, das bekanntermaßen (laut Vorlesung) *nicht attribut* ist
- Zeige: Wenn A *attribut* ist, dann wäre B auch *attribut*
  - Transformiere **alle** Instanzen von B zu Instanzen von A, wobei diese Transformation *attribut* **nicht beeinflussen** darf.
- Widerspruch!

Ist die Sprache
$L = \{\langle M \rangle \mid \text{TM M hat mind. einen nicht erreichbaren Zustand}\}$
entscheidbar?

- Annahme: L entscheidbar ($\Leftrightarrow \overline{L}$ entscheidbar)
- Bekannt: Das Halteproblem ist nicht entscheidbar
- Transformation f von (allen) Instanzen $\in$ Halt zu Instanzen von $\overline{L}$
  $f : (\langle M \rangle, w) \rightarrow \langle M' \rangle$
- Konstruiere M': M' hat folgende Funktionsweise:
  1. Leere das Band
  2. Schreibe w auf das Band
  3. Simuliere M
  4. Gehe in einen zusätzlichen Zustand q_s
- Folgerung:
  - $\langle M' \rangle = f((\langle M \rangle, w)) \in \overline{L}$
  - $\Leftrightarrow M'$ hat keinen nicht erreichbaren Zustand
  - $\Leftrightarrow M'$ geht in Zustand q_s
  - $\Leftrightarrow M$ hält bei Eingabe w
  - $\Leftrightarrow (\langle M \rangle, w) \in HALT$
- Also: L entscheidbar $\Rightarrow \overline{L}$ entscheidbar $\Rightarrow$ HALT entscheidbar ↯

Mehr Übungen

Ist die Sprache

$L_1 = \{\langle M \rangle \mid \text{TM } M \text{ akzeptiert keine Eingabe}\}$

$L_2 = \{\langle M \rangle \mid \text{TM } M \text{ akzeptiert die Eingabe } \langle M \rangle \text{ nicht}\}$

$L_3 = \{\langle M \rangle \mid \text{TM } M \text{ ist minimal}\}$

d.h. es gibt keine funktionsäquivalente Turingmaschine N mit $|\langle N \rangle| < |\langle M \rangle|$

- Beweis siehe Skript und/oder Tutorium 8

entscheidbar?

Aufgabe B6 A3 rekursiv aufzählbare Mengen

Welche der folgenden Mengen sind rekursiv aufzählbar?
Beweisen Sie Ihre Aussage!

1. $M_2 := \{r \in \mathbb{R} \mid 0 < r < 1\}$

Das Rekursionstheorem 1.Form

Existiert eine TM M, die die Funktion t: $\Sigma^* \times \Sigma^* \to \Sigma^*$ 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: $\Sigma^* \to \Sigma^*$ existiert eine TM F und eine TM G, wobei F und G die gleiche Funktion berechnen und $f(\langle F \rangle) = \langle G \rangle$.

SELF-Maschine

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.

„Übung“

Beweisen Sie, dass es eine Gödelnummer $n = \langle \mathcal{M} \rangle \in \mathbb{N}_0$ zu einer Turingmaschine $\mathcal{M}$ gibt, die die Funktion $f_n(x) = (n + x)^2$ für alle $x \in \mathbb{N}_0$ berechnet!

Wiederholung einiger Begriffe

- 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 $\phi \notin Th(\mathbb{N}, >)$.

Weitere Aufgaben: B7 A2

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

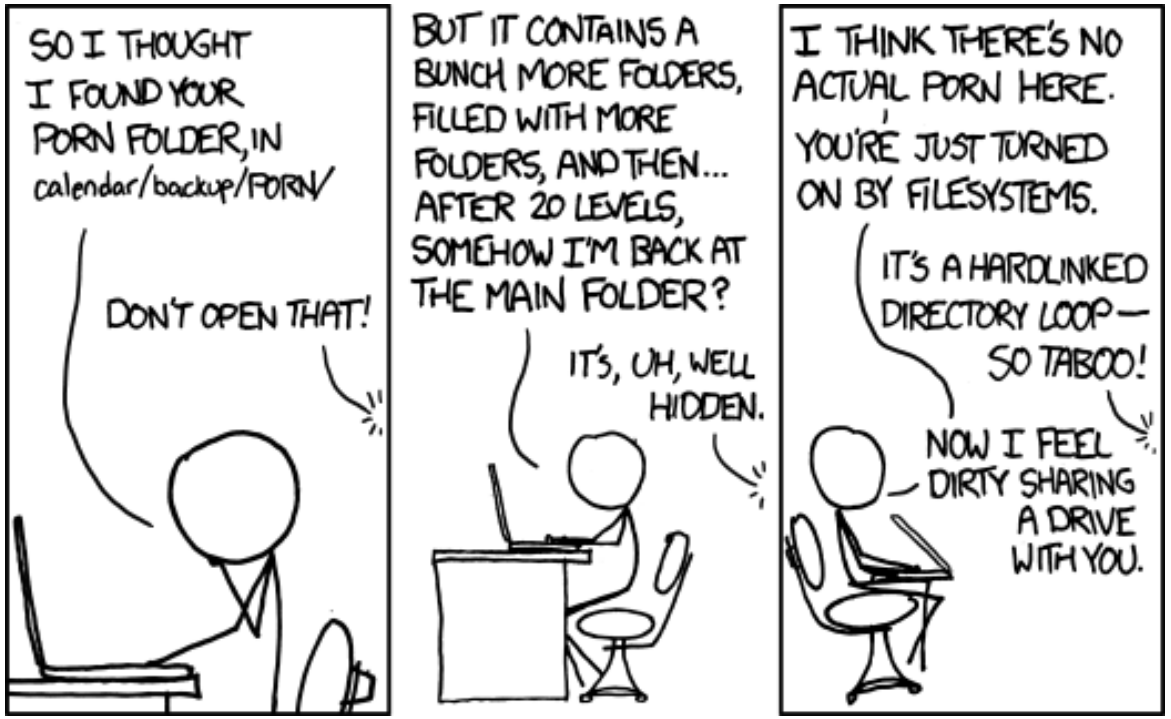
Weitere Aufgaben: B7 A3

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]
$\wedge \forall\, x,y\, (R_1(x,y) \leftrightarrow R_1(y,x))$ [K1.2]
$\wedge \forall\, x,y,z\, ((R_1(x,y) \wedge R_1(y,z)) \rightarrow R_1(x,z))$ [K1.3]

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

Bis zum nächsten Mal!



Lizenzen