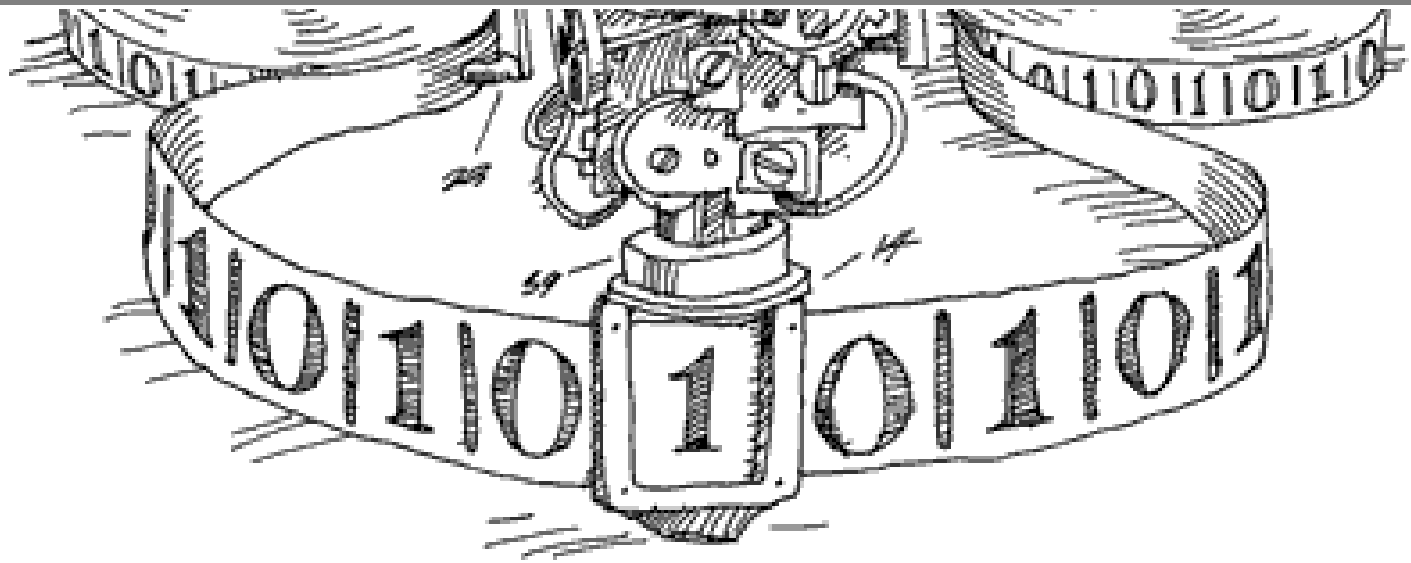
Karlsruher Institut für Technologie

Theoretische Grundlagen der Informatik

Tutorium 7

Institut für Kryptographie und Sicherheit



Das Rekursionstheorem 1.Form

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

Damit hat jede Programmtransformation einen Fixpunkt.

SELF-Maschine

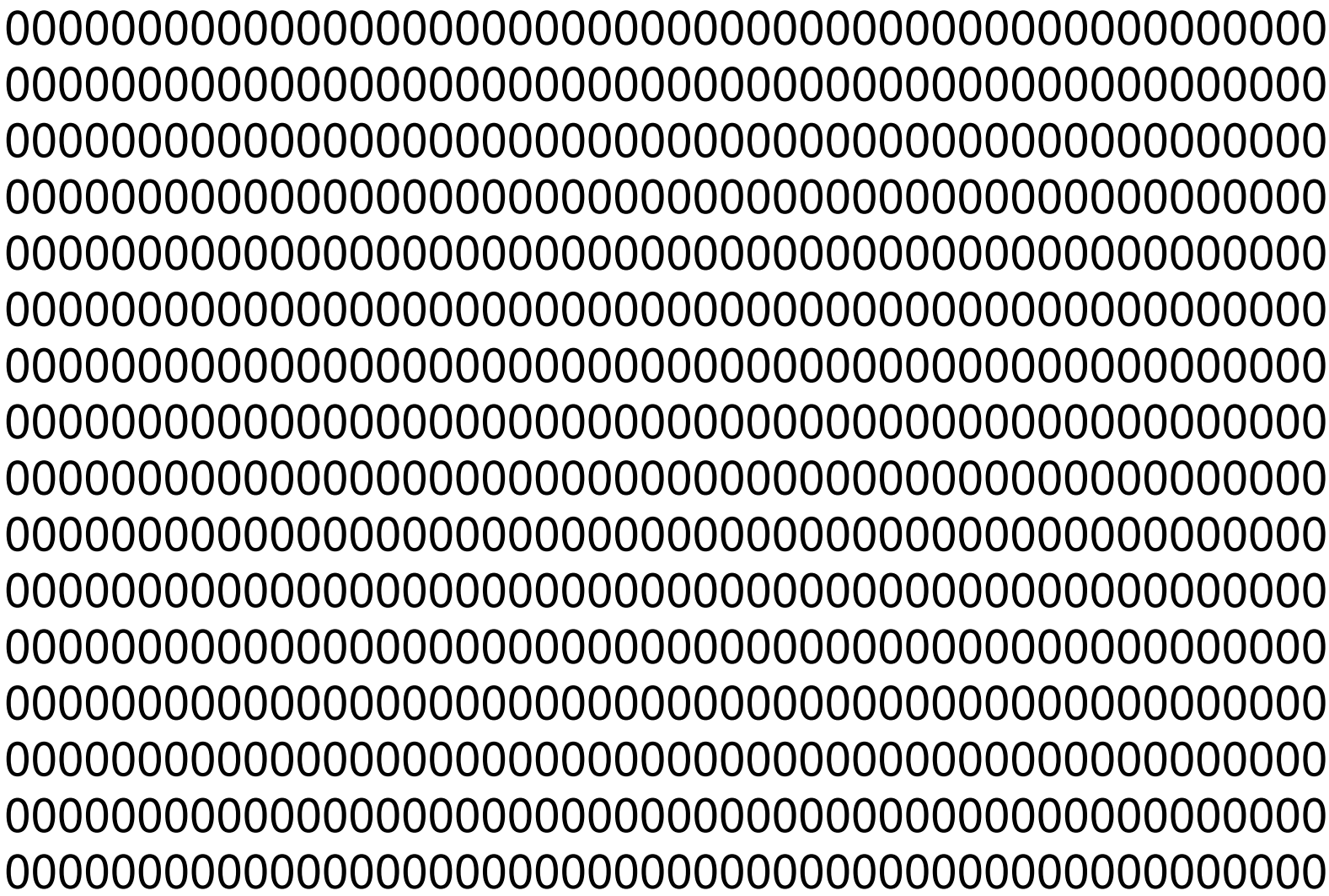
Eine SELF-Maschine (auch Quine genannt) ist eine Turingmaschine, die ihre eigene Gödelnummer ausgibt und dann hält. Sie realisiert demnach die Funktion $t(\langle SELF \rangle, w) = \langle SELF \rangle$.
Eine mögliche Art eine solche TM zu erstellen ist folgender:

- 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.

Kolmogorow

Beispiel: Das Wort, das aus 1000 Nullen besteht (Alphabet: ASCII)

Kolmogorow



Kolmogorow

Eine Beschreibung eines Wortes w ist ein Programm bei dessen Ausführung das Wort erzeugt wird. Die Länge dieses Programmes ist dann ein d(w).

```
Program Nullfolge (n)
 begin
  for i:= 1 to n
   print “0”
 end
```

Kolmogorow

Eine minimale Beschreibung eines Wortes w heißt Kolmogorow-Komplexität $K(w)$

- Also: $\forall d(w) : |d(w)| \geq |K(w)|$
- Die Länge von $K(w)$ ist abhängig von der Struktur von w

Falls $|K(w)| \geq |w|$ heißt das Wort unkomprimierbar.

Die Kolmogorow-Komplexität ist nicht entscheidbar aber semi-entscheidbar.

Kolmogorow

Eine minimale Beschreibung eines Wortes w heißt Kolmogorow-Komplexität $K(w)$

- Also: $\forall d(w) : |d(w)| \geq |K(w)|$
- Die Länge von $K(w)$ ist abhängig von der Struktur von w

Falls $|K(w)| \geq |w|$ heißt das Wort unkomprimierbar.

Die Kolmogorow-Komplexität ist nicht berechenbar aber rekursiv aufzählbar.

Kolmogorow Komplexität: Aufgabe (B7 A1)

1. Beweisen Sie, dass $K(x)$ nicht berechenbar ist!
2. Beweisen Sie, dass die Menge der nichtkomprimierbaren Strings $\mathcal{L}$ nicht rekursiv aufzählbar ist!
3. Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität von 0^n an!
4. Geben Sie eine möglichst gute obere Schranke für die Kolmogorow-Komplexität der Binärdarstellung der n-ten Primzahl p an!
5. Sei x ein Palindrom. Geben sie eine möglichst gute obere Schranke für $K(x)$ an!
6. Sei π_n die Kreiszahl π bis zur n-ten Nachkommastelle entwickelt. Geben Sie eine möglichst gute obere Schranke für π_n an.

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.

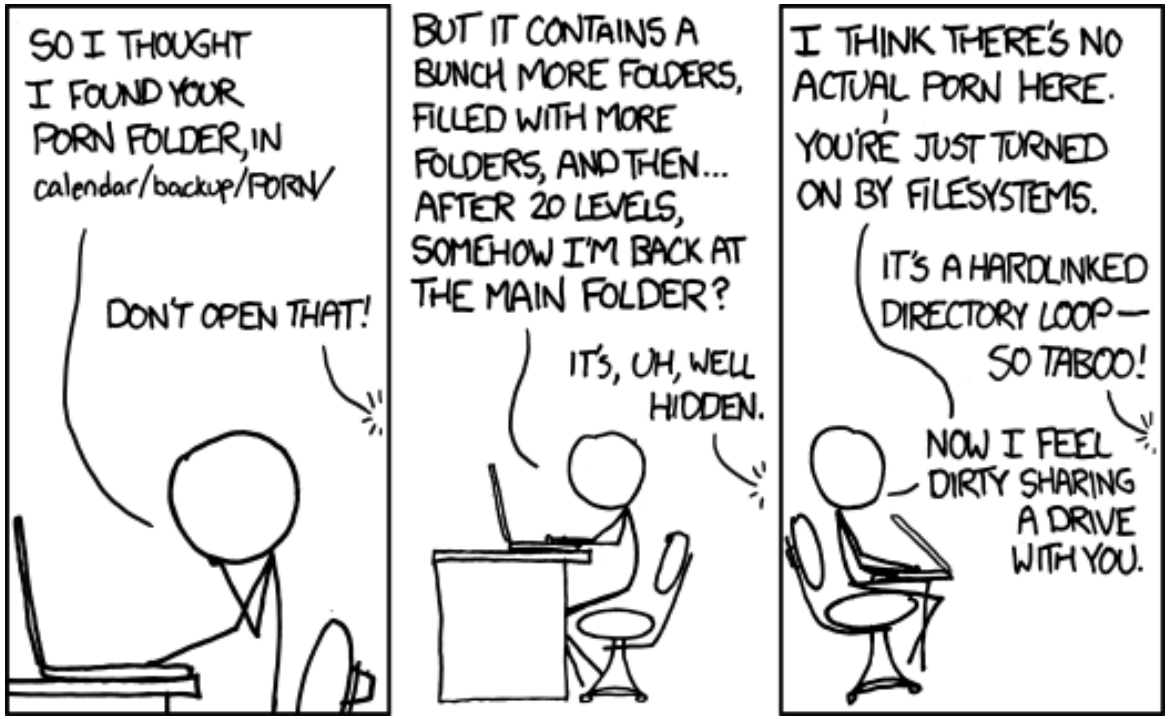
Weitere Aufgaben: B7 A3

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