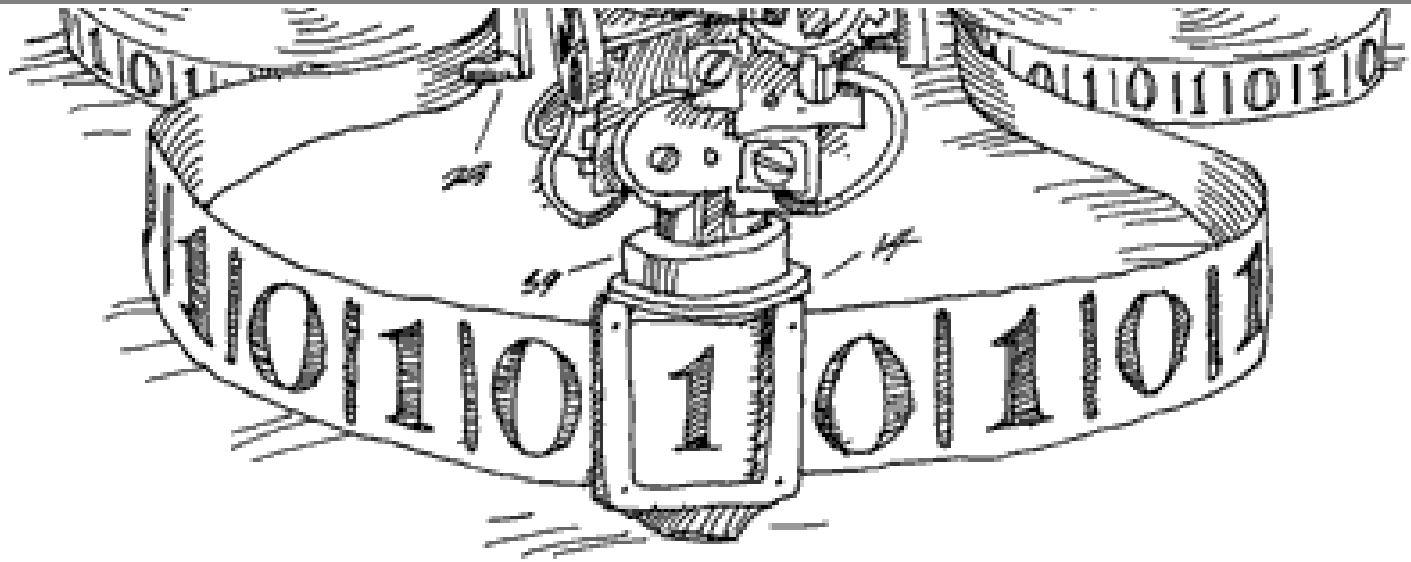
Karlsruher Institut für Technologie

Theoretische Grundlagen der Informatik

Tutorium 1

Institut für Kryptographie und Sicherheit



whois tutor

- **Michael Vollmer**
  Michael@trollbu.de
  Tutorium-Nummer: 20
  Mittwoch 15:45, SR -109

Organisatorisches – Zum Übungsbetrieb

- **Abgabe:** *Handschriftlich* in Gruppen
  - Bis zu 3 Personen als Gruppe
  - Erste Abgabe legt die Gruppe fest
  - Jede Person muss ein eigenes Blatt abgeben (mit Namen der Gruppenteilnehmer, falls vorhanden)
- **Schein:**
  - Klausurbonus (1 Notenschritt)
  - (Mindestens) Bei allen bis auf einem Blatt 50% Punkte
- korrigierte Übungsblätter gibt es im Tutorium
  - Bei Nichtabholung: Büro 274 Montags 14:00-15:00

Organisatorisches – Zum Tutorium

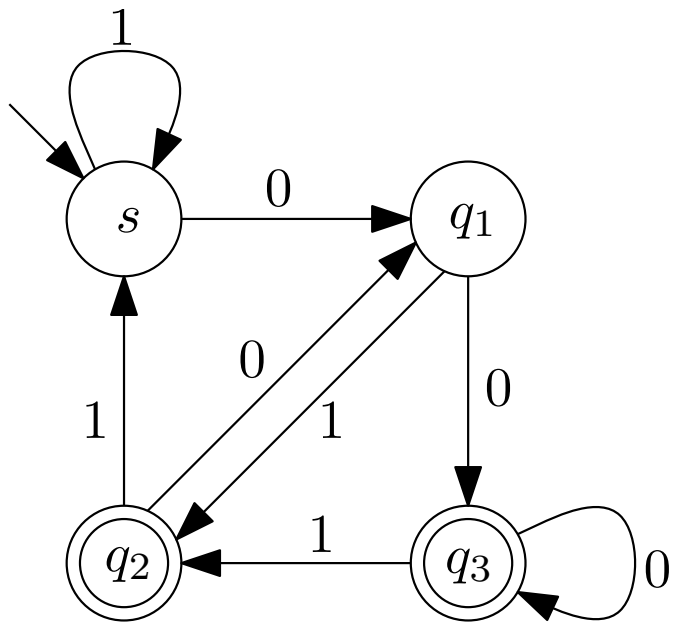
- Tutoriumsfolien
  - `http://tinyurl.com/tgitutws1314`
- E-Mail-Liste geht rum
- Stoff soll wiederholt werden
- Dabei Fokus auf Übungsbetrieb
- Fragen/Vorschläge/Anmerkungen willkommen!

Deterministische endliche Automaten

Ein deterministischer endlicher Automat M ist ein 5-Tupel

$$M = (Q, \Sigma, \delta, s, F).$$

- Q: endliche Zustandsmenge
- Σ: endliches Alphabet
- δ: Zustandsübergangsfunktion $Q \times \Sigma \to Q$
- s: Startzustand $\in Q$
- F: Endzustandsmenge $\subseteq Q$

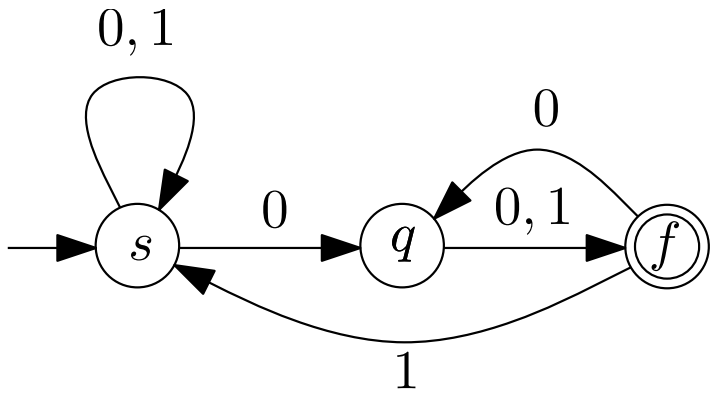


Nichtdeterministische endliche Automaten

Ein nichtdeterministischer endlicher Automat M ist ein 5-Tupel

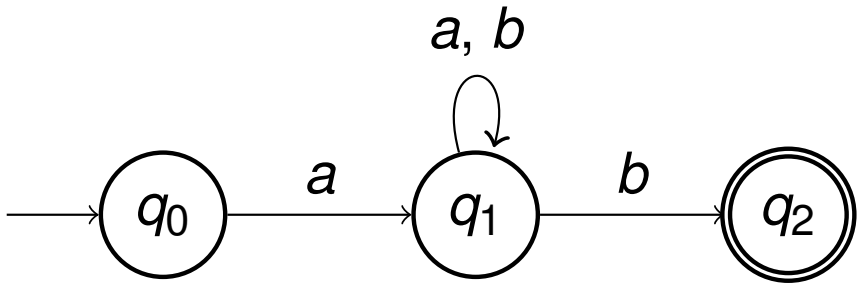
$$M = (Q, \Sigma, \delta, s, F).$$

- Q: endliche Zustandsmenge
- Σ: endliches Alphabet
- δ: Zustandsübergangsfunktion $Q \times (\Sigma \cup \varepsilon) \to \mathcal{P}(Q)$
- s: Startzustand $\in Q$
- F: Endzustandsmenge $\subseteq Q$



Damit der NEA ein Wort akzeptiert, muss es *einen* akzeptierenden Weg geben.

NEA: Beispiel



- Eingabe: abb
  - $q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_2 \xrightarrow{b} \emptyset$
  - $q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_1 \xrightarrow{b} q_2$
  - akzeptiert
- Eingabe: aba
  - $q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_1 \xrightarrow{a} \emptyset$
  - $q_0 \xrightarrow{a} q_1 \xrightarrow{b} q_2 \xrightarrow{a} \emptyset$
  - akzeptiert nicht

Rechtslineare Grammatiken

Eine Grammatik $G = (T, V, S, P)$

- T = Menge der Terminale (a.k.a. Alphabet der Sprache)
- V = Menge der Nichtterminale (zu T disjunkt)
- $S \in V$ = Startsymbol
- $P \subset V^+ \times (V \bigcup T)^*$ = Menge der Produktionen

bei der alle Produktionen so aussehen:

- $A \to \epsilon$
  - $A \in V$
  - ϵ ist leeres Wort (in der Vorlesung auch λ)
- $A \to bC$
  - $A, C \in V$
  - $b \in T$

heißt rechtslinear bzw. regulär.

Reguläre Ausdrücke

A ist ein regulärer Ausdruck über dem Alphabet Σ wenn:

- $A = \epsilon$
- $A = x \in \Sigma$
- $A = B^* = \{\epsilon, B, BB, BBB, \ldots\}$
- $A = B^+ = \{B, BB, BBB, \ldots\}$
- $A = B \cdot C = \{BC\}$
- $A = B \mid C = B + C = \{B, C\}$

Wobei B und C ebenfalls reguläre Ausdrücke über Σ sind.

Bitte deutlich schreiben:

$$B^+C \neq B + C$$

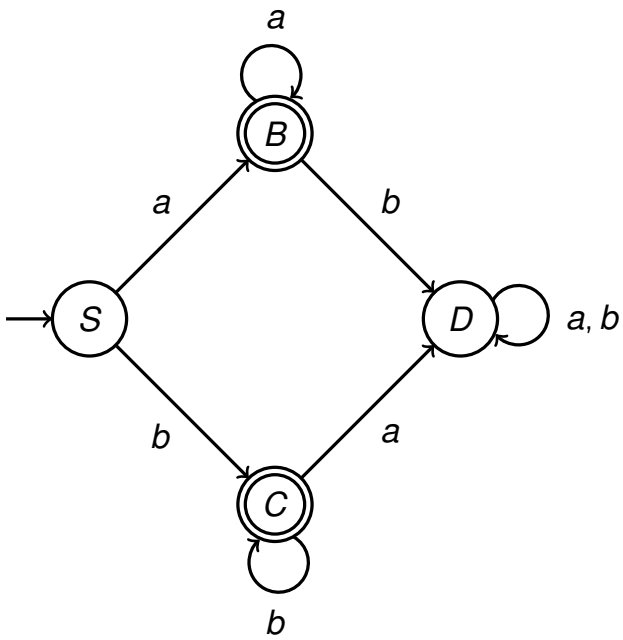
Chompsky Typ 3

Eine Sprache ist von Chompsky Typ 3, wenn...

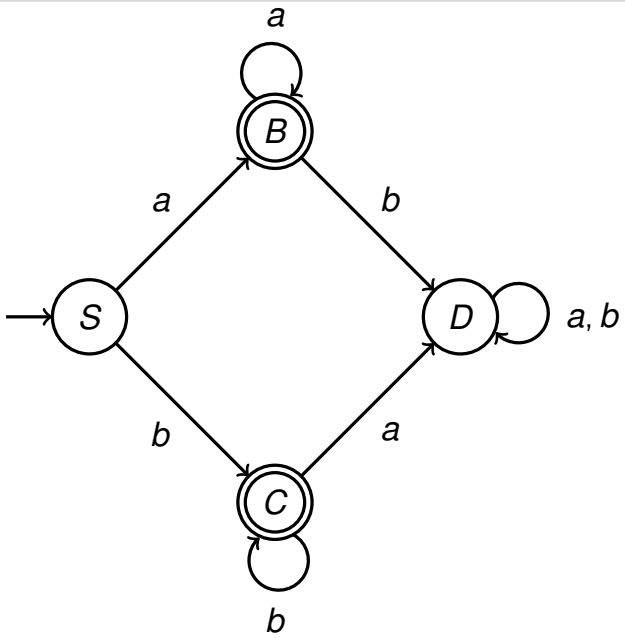
- ... sie durch eine reguläre, z.B. rechtslineare, Grammatik angegeben werden kann.
- ... sie durch einen regulären Ausdruck angegeben werden kann.
- ... ein endlicher Automat angegeben werden kann, der genau diese Sprache akzeptiert.

Aufgabe 1

Gegeben sei der folgende endliche Automat:
$\mathcal{M} = (\mathcal{Q}, \Sigma, \delta, S, \mathcal{F})$ mit $\Sigma = \{a, b\}$, $\mathcal{Q} = \{S, B, C, D\}$, $\mathcal{F} = \{B, C\}$ und δ gegeben durch:



Aufgabe 1



1. Geben Sie die von diesem Automaten akzeptierte Sprache in einem regulären Ausdruck an!
2. Um was für einen Automaten handelt es sich?
3. Konstruieren Sie einen äquivalenten endlichen Automaten, der nur einen einzigen Endzustand besitzt!
4. Geben Sie eine linkslineare Grammatik für die Sprache dieses Automaten an, die keine überflüssigen Nichtterminale und Regeln enthält!

Aufgabe 2

1. Formulieren Sie einen regulären Ausdruck über dem Alphabet $\Sigma = \{0, 1\}$, der jedes beliebige Wort erfasst, wobei die vorletzte Ziffer 0 sein soll!
2. Geben Sie eine rechtslineare Grammatik an.
3. Geben Sie einen dazugehörigen Automaten an, der diese Sprache akzeptiert!

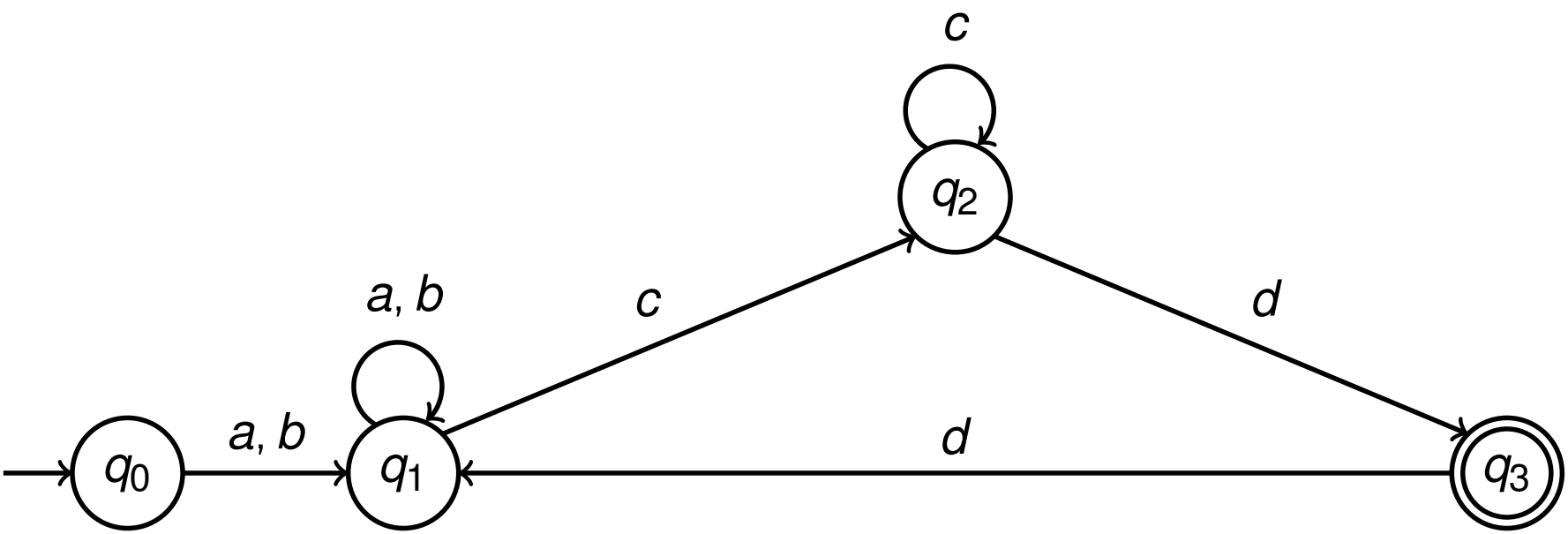
Akzeptor $\rightarrow$ Grammatik

Umwandlung von einem endlichen Akzeptor $M = (Q, \Sigma, \delta, q_0, F)$ in eine rechtslineare Grammatik $G = (T, V, S, P)$:

1. $T := \Sigma$.
2. $\forall q \in Q$ ein Nichtterminalsymbol in V definieren, wobei S q_0 zugeordnet ist.
3. $P := \{(X \rightarrow tY) \mid (q_X, t) = q_Y \in \delta\} \cup \{(Z \rightarrow \lambda) \mid q_Z \in F\}$.
   Wobei X, Y und Z jene Nichtterminalsymbole sind, welche q_X, q_Y, bzw. q_Z zugeordnet sind.

Aufgabe 3

Gegeben sei der folgende endliche Akzeptor $\mathcal{M}$ mit dem Eingabealphabet $\Sigma = \{a, b, c, d\}$:



1. Welche Sprache $\mathcal{L}(\mathcal{M})$ wird von dem Akzeptor $\mathcal{M}$ akzeptiert?
2. Konstruieren Sie aus $\mathcal{M}$ eine rechtslineare Grammatik, die $\mathcal{L}(\mathcal{M})$ erzeugt!

Konstruktion eines Akzeptors aus einer linearen Grammatik

Gegeben: rechtslineare Grammatik $G = (T, V, S, P)$
Gesucht: endlicher Akzeptor $M = (Q, \Sigma, \delta, q_0, F)$

1. $\Sigma := T$
2. $Q := \{q_X \mid X \in V\}$
   - $q_0 = q_S$
3. $\delta := \{(q_X, t) \to q_Y \mid (X \to tY) \in P\}$
4. $F := \{q_X \mid (X \to \lambda) \in P\}$

Aufgabe 4

Die Sprache $\mathcal{L}$ sei durch den regulären Ausdruck $(aa^*b^*)^*cc^*$ definiert.

1. Geben Sie eine rechtslineare Grammatik $\mathcal{G}$ an, die $\mathcal{L}$ erzeugt!
2. Konstruieren Sie aus $\mathcal{G}$ einen endlichen Akzeptor, der $\mathcal{L}$ akzeptiert!

Semi-Thue-Systeme

Ein Semi-Thue-System besteht aus

- einem nichtleeren Alphabet A

und

- einer Produktionsmenge $P \subset \{A^* \to A^*\}$

Beispiel:
$A = \{a, b, c\}$
$P = \{ab \to c, bc \to a, aa \to \epsilon, cc \to \epsilon\}$

Beispieleingaben:

$$\begin{aligned} \text{abc} &\Rightarrow \text{cc} \Rightarrow \epsilon \\ &\Rightarrow \text{aa} \Rightarrow \epsilon \\ \text{aab} &\Rightarrow \text{b} \\ &\Rightarrow \text{ac} \end{aligned}$$

Produktionen sind nicht immer eindeutig.

Scholtens Kaffeedosenspiel

Gegeben:

- Dose mit (endlich vielen) weißen und schwarzen Bohnen (mindestens einer).
- Spielregeln: Nehme zufällig 2 Bohnen aus der Dose
  - Falls die Bohnen die gleiche Farbe haben, so lege eine schwarze in die Dose zurück.
  - Falls die Bohnen verschiedene Farben haben, so lege nur die weiße Bohne zurück.

Behauptungen:

1. Spiel terminiert immer mit genau einer Bohne in der Dose.
2. Das Ergebnis ist nur von den Farben der Bohnen abhängig.

Kaffeebohnen in Semi-Thue

Semi-Thue-System:

- $A = \{ S, W \}$
- $P = \{ SW \to W, WS \to W, SS \to S, WW \to S \}$

Behauptungen:

- Die Ersetzungen terminieren immer mit Termlänge 1
- Das Ergebnis ist unabhängig von der Reihenfolge der Regelanwendungen

Beweis der Terminierung durch Induktion

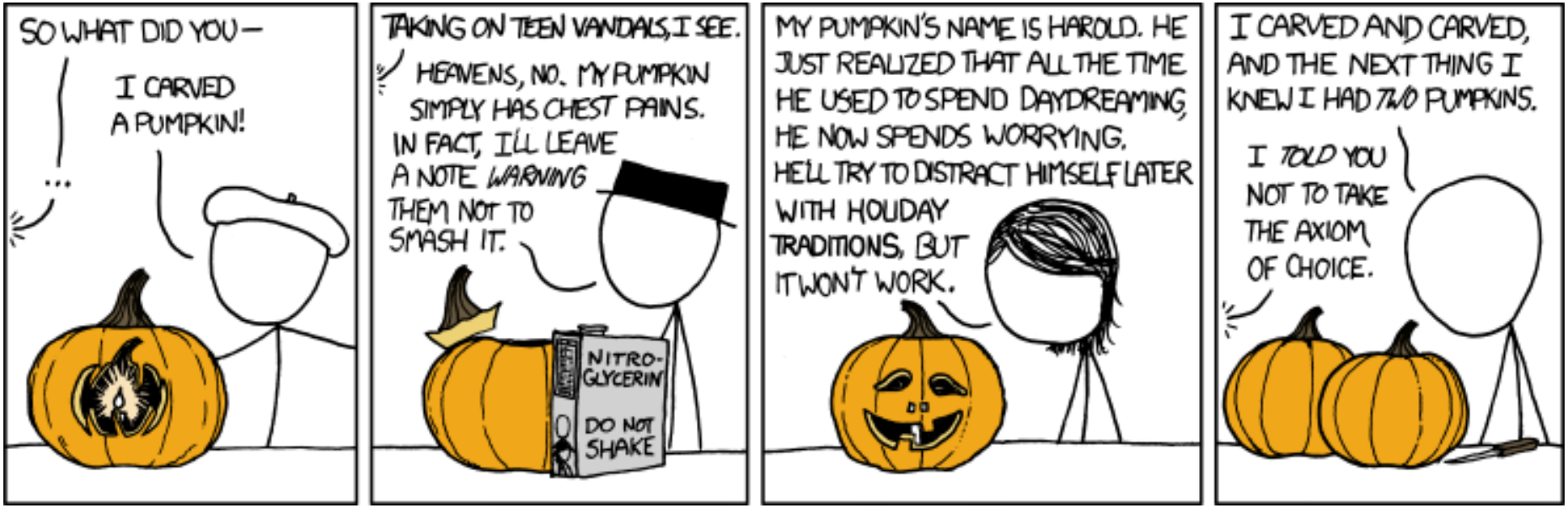
- Induktionsanfang: Term der Länge 1
  Keine Regel anwendbar, also terminiert mit Länge 1
- Induktionsvoraussetzung: Jeder Term mit einer beliebig aber festen Länge n terminiert mit Länge 1.
- Induktionsschritt: Term mit Länge $n + 1$
  - Da n mindestens 1 ist, besitzt der Term mindestens Länge 2. Also ist auf jeden Fall eine Regel anwendbar
  - Jede Regel ersetzt einen Subterm der Länge 2 mit einem Term der Länge 1. Nach einer Regelanwendung besitzt der Restterm also nun die Länge n.
  - Nach Induktionsvoraussetzung terminiert dieser Restterm mit Länge 1.

Beweis der Unabhängigkeit durch Induktion

- Behauptung: Wenn der Term eine ungerade Anzahl an W enthält, terminiert die Term mit W als letztes Zeichen.
- Beweis:
  - Induktionsanfang: Term ist Länge 1. Falls der Term eine ungerade Anzahl an W enthält, terminiert der Term mit W.
  - Induktionsvoraussetzung: Behauptung gilt für alle Terme mit einer beliebig aber festen Länge n.
  - Induktionsschritt: Term mit Länge $n + 1$:
    - Die Regeln $\{ \text{SW} \rightarrow \text{W}, \text{WS} \rightarrow \text{W}, \text{SS} \rightarrow \text{S} \}$ erhalten die Anzahl von W im Term.
    - Die Regel $\{ \text{WW} \rightarrow \text{S} \}$ veringert die Anzahl von W im Term um 2.
    - Falls die Anzahl W im Term ungerade war, bleibt dies auch nach Regelanwendung erhalten. Nach Regelanwendung besitzt der Term die Restlänge n und es gilt die Induktionsvoraussetzung.

Analoger Beweis: Bei gerade Anzahl an W im Term, ist S das letzte Zeichen im Term.

Bis zum nächsten Mal!



Lizenzen