Computational Logic

Einführung in die Theoretische Informatik

Woche 7

Harald Zankl

Institut für Informatik @ UIBK
Wintersemester 2014/2015

Zusammenfassung der letzten LV

Beispiel

1. Wir betrachten die folgende Signatur $\mathsf{F} = \{+, \cdot, \overline{\ }, 0, 1\}$ sodass
   - Stelligkeit von 0, 1 ist 0
   - Stelligkeit von $\overline{\ }$ ist 1
   - Stelligkeit von $+$, $\cdot$ ist 2
2. $\mathsf{V} = \{x, y, \dots\}$
3. Wir betrachten die Gleichungen E

$$(x + y) + z \approx x + (y + z) \qquad \overline{x} + x \approx 1 \qquad x + x \approx x$$

4. Dann gilt $E \vdash 1 + x \approx 1$
5. Dann gilt $E \nvdash x + 1 \approx 1$

Satz (Satz von Birkhoff)

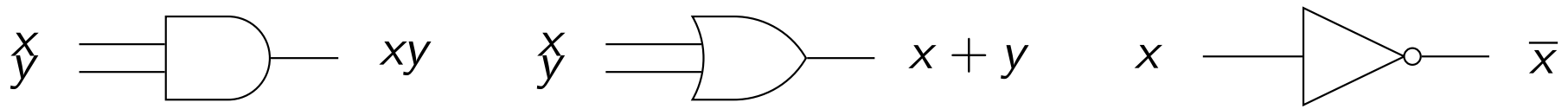
Für beliebige Terme s, t gilt: $E \models s \approx t$ *gdw.* $E \vdash s \approx t$.

Definition (Schaltalgebra)

Sei $\mathbb{B} = \{0, 1\}$, wir betrachten die Algebra

$$\langle \mathbb{B}; +, \cdot, \overline{\ }, 0, 1 \rangle$$

wobei die Operationen $+$, $\cdot$, $\overline{\ }$ wie folgt definiert sind:



Diese Algebra ist eine Boolesche Boolesche und heißt Schaltalgebra.

Definition (Schaltnetz)

- Ein logischer Schaltkreis (Schaltnetz) ist ein algebraischer Ausdruck der Schaltalgebra
- Die Operationen $+$, $\cdot$, $\overline{\ }$ werden als logische Gatter dargestellt

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare, Verschlüsselung und Sicherheit

Definition

Eine Teilmenge L von Σ^* heißt eine formale Sprache über Alphabet Σ

Beispiel

- Die Menge aller Wörter, die aus n Nullen gefolgt von n Einsen bestehen, wobei $n \geqslant 0$:

$$\{\epsilon, 01, 0011, 000111, \ldots\}$$

- Die Menge aller Wörter, die jeweils die selbe Anzahl Nullen und Einsen enthalten:

$$\{\epsilon, 01, 10, 0011, 0101, \ldots\}$$

- Für jedes Alphabet Σ ist
  - Σ^* eine formale Sprache
  - $\varnothing$ eine formale Sprache (die leere Sprache)
  - $\{\epsilon\}$ eine formale Sprache (beachte: $\varnothing \neq \{\epsilon\}$)

Definition

Seien L, M formale Sprachen über dem Alphabet Σ

- Die Vereinigung von L und M ist wie folgt definiert
$$L \cup M := \{x \mid x \in L \text{ oder } x \in M\}$$
- Wir definieren das Komplement von L:
$$\sim L = \Sigma^* \setminus L := \{x \in \Sigma^* \mid x \notin L\}$$
- Der Durchschnitt von L und M ist wie folgt definiert:
$$L \cap M := \{x \mid x \in L \text{ und } x \in M\}$$
- Das Produkt (oder die Verkettung) von L und M ist definiert als:
$$LM := \{xy \mid x \in L,\ y \in M\}$$

Lemma

Seien L, L_1, L_2, L_3 formale Sprachen, dann gilt

$$(L_1L_2)L_3 = L_1(L_2L_3) \qquad L\{\epsilon\} = \{\epsilon\}L = L \qquad L\varnothing = \varnothing L = \varnothing$$

Abschluss einer Formalen Sprache

Definition

Sei L eine formale Sprache und $k \in \mathbb{N}$

Die k-te Potenz von L ist definiert als:

$$L^k = \begin{cases} \{\epsilon\} & \text{falls } k = 0 \\ L & \text{falls } k = 1 \\ \underbrace{LL \cdots L}_{k\text{-mal}} & \text{falls } k > 1 \end{cases}$$

Definition

Der Kleene-Stern * oder Abschluss von L ist wie folgt definiert:

$$L^* = \bigcup_{k \geqslant 0} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k \in \mathbb{N}, k \geqslant 0\}$$

Definition

Schließlich definieren wir:

$$L^+ = \bigcup_{k \geqslant 1} L^k = \{x_1 \cdots x_k \mid x_1, \ldots, x_k \in L \text{ und } k \in \mathbb{N}, k \geqslant 1\}$$

Beispiel

- Sei $\Sigma = \{0, 1\}$ und betrachte die formale Sprache L aller Wörter, die aus n Nullen gefolgt von n Einsen bestehen, wobei $n \geqslant 0$, also

$$L = \{0^n 1^n \mid n \geqslant 0\}$$

- Es gilt $010101 \notin L$, aber $010011 \in L^2$
- Allgemein erhalten wir:

$$L^2 = \{0^n 1^n 0^k 1^k \mid n, k \geqslant 0\}$$

Grammatiken und Formale Sprachen

Beispiel

$$
\begin{aligned}
S &\to \text{Pronomen Nomen Verb Adjektiv} \\
\text{Nomen} &\to \text{Lehrveranstaltungsleiter} \\
\text{Nomen} &\to \text{Vortragender} \\
\text{Pronomen} &\to \text{Unser} \mid \text{Mein} \\
\text{Verb} &\to \text{ist} \\
\text{Adjektiv} &\to \text{lästig} \mid \text{nett} \mid \text{streng} \mid \text{monoton} \mid \text{anspruchsvoll}
\end{aligned}
$$

Es gilt:

$$S \stackrel{*}{\Rightarrow} \text{Unser Lehrveranstaltungsleiter ist anspruchsvoll}$$

Definition

Eine Grammatik G ist ein Quadrupel $G = (V, \Sigma, R, S)$, wobei

1. V eine endliche Menge von Variablen (oder Nichtterminale)
2. Σ ein Alphabet, die Terminale, $V \cap \Sigma = \varnothing$
3. R eine endliche Menge von Regeln
4. $S \in V$ das Startsymbol

Eine Regel ist ein Paar $P \to Q$ von Wörtern $P, Q \in (V \cup \Sigma)^*$, sodass in P mindestens eine Variable vorkommt

P nennen wir auch die Prämisse und Q die Konklusion der Regel

Konvention

- Variablen werden groß geschrieben, Terminale klein
- Statt $P \to Q_1$, $P \to Q_2$, $P \to Q_3$ schreiben wir $P \to Q_1 \mid Q_2 \mid Q_3$

Sei $G = (V, \Sigma, R, S)$ eine Grammatik und seien $x, y \in (V \cup \Sigma)^*$

Definition

1. Wir sagen y ist aus x in G direkt ableitbar, wenn gilt:

   $$\exists\, u, v \in (V \cup \Sigma)^*,\ \exists\, (P \to Q) \in R \text{ sodass } (x = uPv \text{ und } y = uQv)$$

2. In diesem Fall schreiben wir kurz $x \underset{G}{\Rightarrow} y$
3. Wenn G aus dem Kontext folgt schreiben wir $x \Rightarrow y$

▸ Beispiel

Definition (Ableitbar)

Wir sagen y ist aus x in G ableitbar, wenn $k \in \mathbb{N}$ und $w_0, w_1, \ldots, w_k \in (V \cup \Sigma)^*$ existieren, sodass

$$x = w_0 \Rightarrow w_1 \Rightarrow \ldots \Rightarrow w_k = y$$

Wir schreiben $x \overset{*}{\underset{G}{\Rightarrow}} y$, beziehungsweise $x \overset{*}{\Rightarrow} y$

Sprache einer Grammatik

Definition

- Die vom Startsymbol S ableitbaren Wörter heißen Satzformen
- Elemente von Σ^* heißen Terminalwörter
- Satzformen, die Terminalwörter sind, heißen Sätze

Definition (Sprache einer Grammatik)

Die Menge aller Sätze

$$\mathrm{L}(G) = \{x \in \Sigma^* \mid S \overset{*}{\underset{G}{\Rightarrow}} x\}$$

heißt die von der Grammatik G erzeugte Sprache

Definition (Äquivalenz)

Zwei Grammatiken G_1 und G_2 heißen äquivalent, wenn $\mathrm{L}(G_1) = \mathrm{L}(G_2)$

Klassen von Grammatiken

Definition (rechtslinear)

Grammatik $G = (V, \Sigma, R, S)$ heißt rechtslinear, wenn für alle Regeln $P \to Q$ gilt:

1. $P \in V$
2. $Q \in \Sigma^* \cup \Sigma^+ V$

Beispiel

Grammatik $G_1 = (\{B\}, \{0, 1\}, R, B)$ mit Regeln R:

$$B \to 0 \mid 1 \mid 0B \mid 1B$$

Es gilt:

- $B \underset{G}{\Rightarrow} 0B \underset{G}{\Rightarrow} 01B \underset{G}{\Rightarrow} 010$
- G_1 ist rechtslinear
- $\mathrm{L}(G_1) = \{0, 1\}^+$

zurück

Definition (kontextfrei)

Grammatik $G = (V, \Sigma, R, S)$ heißt kontextfrei, wenn für alle Regeln $P \to Q$ gilt:

1. $P \in V$
2. $Q \in (V \cup \Sigma)^*$

Beispiel

Grammatik $G_2 = (\{S\}, \{(,)\}, R, S)$ mit Regeln R:

$$S \to \epsilon \mid (S) \mid SS$$

Es gilt:

- G_2 ist kontextfrei
- $S \Rightarrow SS \Rightarrow (S)S \Rightarrow (\epsilon)S = ()S \Rightarrow ()(S) \Rightarrow ()(SS) \overset{*}{\Rightarrow} ()((())(()))$
- $\mathrm{L}(G_2)$ beschreibt die Menge der *balancierten Klammerausdrücke*

Definition (beschränkt)

Grammatik $G = (V, \Sigma, R, S)$ heißt beschränkt, wenn für alle Regeln $P \to Q$ gilt:

1. entweder $|P| \leqslant |Q|$
2. oder $P = S$, $Q = \epsilon$ und S kommt in keiner Konklusion einer Regel vor

Beispiel

$G_3 = (\{S, B, C\}, \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}, R, S)$ mit Regeln R:

$$S \to \mathrm{a}SBC \mid \mathrm{a}BC$$

$$CB \to BC$$

$$\mathrm{a}B \to \mathrm{ab} \qquad \mathrm{b}B \to \mathrm{bb} \qquad \mathrm{b}C \to \mathrm{bc} \qquad \mathrm{c}C \to \mathrm{cc}$$

Es gilt

- G_3 ist beschränkt
- $\mathrm{L}(G_3) = \{\mathrm{a}^n\mathrm{b}^n\mathrm{c}^n \mid n \geqslant 1\}$

Definition (kontextsensitiv)

Grammatik $G = (V, \Sigma, R, S)$ heißt kontextsensitiv, wenn für alle Regeln $P \to Q$ gilt:

1. entweder es existieren $u, v, w \in (V \cup \Sigma)^*$ und $A \in V$, sodass
$$P = uAv \text{ und } Q = uwv \text{ wobei } |w| \geqslant 1$$
2. oder $P = S$, $Q = \epsilon$ und S kommt in keiner Konklusion einer Regel vor

Beispiel

$G_3 = (\{S, B, C\}, \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}, R, S)$ mit Regeln R:

$$S \to \mathrm{a}SBC \mid \mathrm{a}BC$$

$$CB \to BC$$

$$\mathrm{a}B \to \mathrm{ab} \qquad \mathrm{b}B \to \mathrm{bb} \qquad \mathrm{b}C \to \mathrm{bc} \qquad \mathrm{c}C \to \mathrm{cc}$$

Es gilt:

- G_3 ist nicht kontextsensitiv
- $\mathrm{L}(G_3) = \{\mathrm{a}^n\mathrm{b}^n\mathrm{c}^n \mid n \geqslant 1\}$

Definition (kontextsensitiv)

Grammatik $G = (V, \Sigma, R, S)$ heißt kontextsensitiv, wenn für alle Regeln $P \to Q$ gilt:

1. entweder es existieren $u, v, w \in (V \cup \Sigma)^*$ und $A \in V$, sodass
$$P = uAv \text{ und } Q = uwv \text{ wobei } |w| \geqslant 1$$
2. oder $P = S$, $Q = \epsilon$ und S kommt in keiner Konklusion einer Regel vor

Beispiel

$G_4 = (\{S, B, C, H\}, \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}, R, S)$ mit Regeln R:

$$S \to \mathrm{a}SBC \mid \mathrm{a}BC$$

$$CB \to HB \qquad HB \to HC \qquad HC \to BC$$

$$\mathrm{a}B \to \mathrm{ab} \qquad \mathrm{b}B \to \mathrm{bb} \qquad \mathrm{b}C \to \mathrm{bc} \qquad \mathrm{c}C \to \mathrm{cc}$$

Es gilt:

- G_4 ist kontextsensitiv
- $\mathrm{L}(G_4) = \{\mathrm{a}^n\mathrm{b}^n\mathrm{c}^n \mid n \geqslant 1\}$

Beispiel

Grammatik $G_5 = (\{S, Y, T\}, \{\mathrm{a}\}, R, S)$ mit Regeln R:

$$S \to YST \mid \mathrm{a} \qquad Y\mathrm{a} \to \mathrm{a}\mathrm{a}Y \qquad Y\mathrm{a}T \to \mathrm{a}\mathrm{a}$$

Es gilt:

- G_5 ist nicht beschränkt
- $\mathrm{L}(G_5) = \{\mathrm{a}^{2^n} \mid n \geqslant 0\} = \{\mathrm{a}, \mathrm{a}\mathrm{a}, \mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}, \mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}, \ldots\}$

Beispiel

Grammatik $G_6 = (\{S, Y, T\}, \{\mathrm{a}\}, R, S)$ mit Regeln R:

$$S \to YST \mid \mathrm{a} \mid \mathrm{a}\mathrm{a} \qquad Y\mathrm{a} \to \mathrm{a}\mathrm{a}Y \qquad Y\mathrm{a}\mathrm{a}T \to \mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}$$

Es gilt:

- G_6 ist beschränkt
- $\mathrm{L}(G_6) = \{\mathrm{a}^{2^n} \mid n \geqslant 0\} = \{\mathrm{a}, \mathrm{a}\mathrm{a}, \mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}, \mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}\mathrm{a}, \ldots\}$

Beobachtung

Grammatik G_2 ist kontextfrei, aber nicht kontextsensitiv, wegen der Regeln $S \to \epsilon$ und $S \to (S)$. G_2 kann in eine äquivalente kontextsensitive Grammatik umgeschrieben werden.

Satz

Für jede kontextfreie Grammatik gibt es eine äquivalente kontextsensitive Grammatik.

Beobachtung

Grammatik G_3 ist nicht beschränkt, aber die äquivalente Grammatik G_4 ist beschränkt.

Satz

- *Jede kontextsensitive Grammatik ist beschränkt.*
- *Für jede beschränkte Grammatik gibt es eine äquivalente kontextsensitive Grammatik.*

Definition

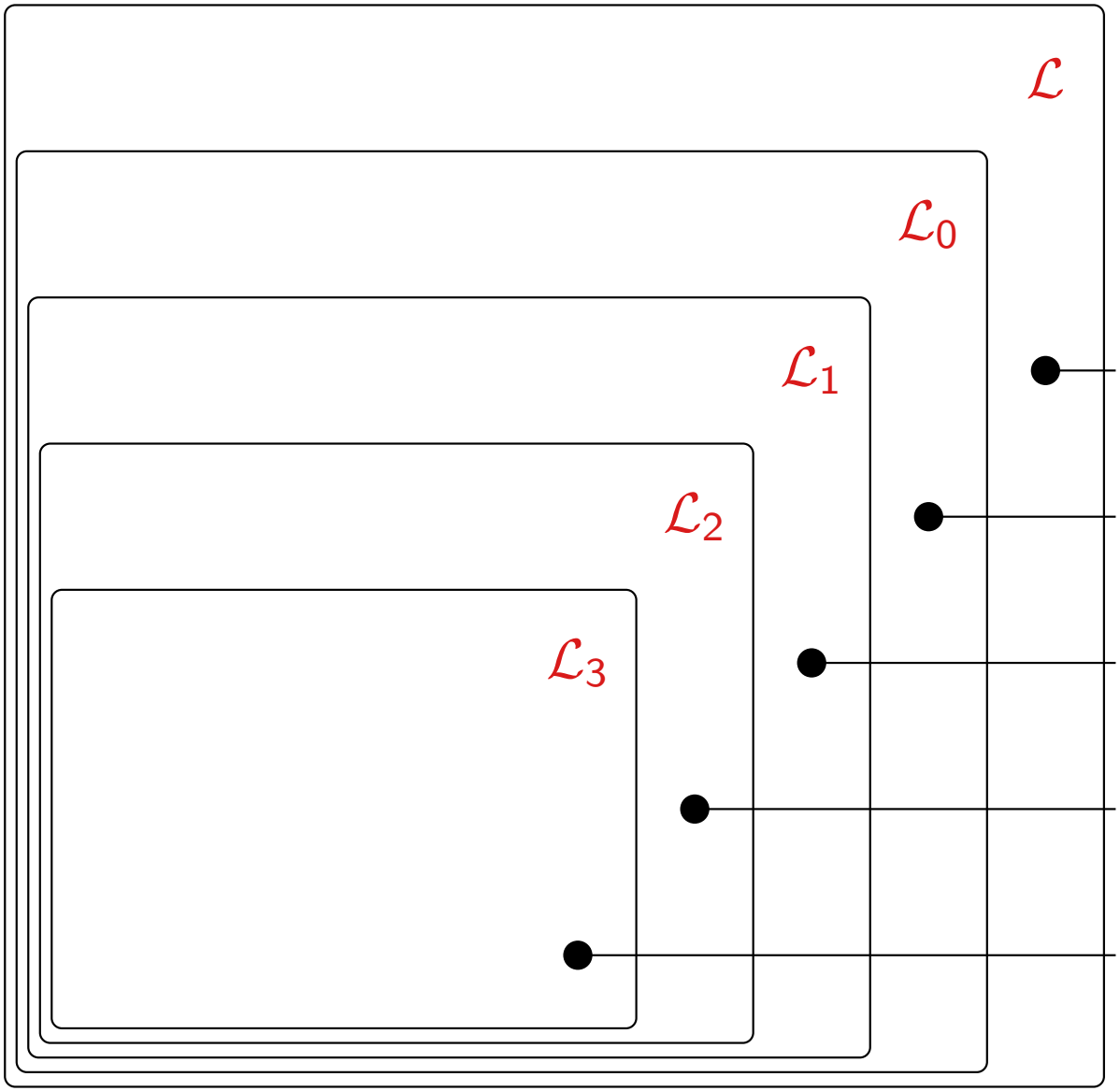
Eine formale Sprache L heißt

- regulär (vom Typ 3)
  wenn $\exists$ rechtslineare Grammatik G mit $L = \mathrm{L}(G)$
- kontextfrei (vom Typ 2)
  wenn $\exists$ kontextfreie Grammatik G mit $L = \mathrm{L}(G)$
- kontextsensitiv (vom Typ 1)
  wenn $\exists$ kontextsensitive Grammatik G mit $L = \mathrm{L}(G)$
- rekursiv aufzählbar (vom Typ 0)
  wenn $\exists$ Grammatik G mit $L = \mathrm{L}(G)$

Satz (Chomsky-Hierarchie)

Sei $\mathcal{L}_i$ die Klasse der Sprachen vom Typ i und $\mathcal{L}$ die Klasse aller Sprachen.
Dann gilt: $\mathcal{L}_3 \subsetneq \mathcal{L}_2 \subsetneq \mathcal{L}_1 \subsetneq \mathcal{L}_0 \subsetneq \mathcal{L}$

Chomsky-Hierarchie



$\{(E, s, t) \mid E \nvdash s \approx t\}$

$\{(E, s, t) \mid E \vdash s \approx t\}$

$\mathrm{L}(G_4) = \{\mathrm{a}^n\mathrm{b}^n\mathrm{c}^n \mid n \geqslant 1\}$

$\mathrm{L}(G_2) =$ „Klammerausdrücke“

$\mathrm{L}(G_1) = \{0, 1\}^+$