

Einführung in die Theoretische Informatik

Woche 7

Harald Zankl

Institut für Informatik @ UIBK
Wintersemester 2014/2015



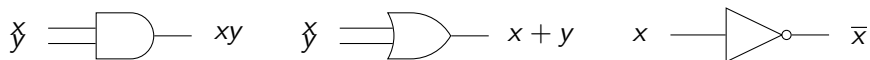
Zusammenfassung

Definition (Schaltalgebra)

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

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

wobei die Operationen $+$, \cdot , $\bar{}$ 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 , $\bar{}$ werden als **logische Gatter** dargestellt

Zusammenfassung der letzten LV

Beispiel

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

$$(x + y) + z \approx x + (y + z) \quad \bar{x} + x \approx 1 \quad x + x \approx x$$
- 4 Dann gilt $E \vdash 1 + x \approx 1$
- 5 Dann gilt $E \not\vdash x + 1 \approx 1$

Satz (Satz von Birkhoff)

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

Überblick

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 $n \geq 0$:

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

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

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

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

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

$$(L_1 L_2) L_3 = L_1 (L_2 L_3) \quad L\{\epsilon\} = \{\epsilon\}L = L \quad L\emptyset = \emptyset L = \emptyset$$

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:

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

Definition

Schließlich definieren wir:

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

Beispiel

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

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

- Es gilt $010101 \notin L$, aber $010011 \in L^2$

- Allgemein erhalten wir:

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

Grammatiken und Formale Sprachen

Beispiel

$S \rightarrow$ Pronomen Nomen Verb Adjektiv
 Nomen \rightarrow Lehrveranstaltungsleiter
 Nomen \rightarrow Vortragender
 Pronomen \rightarrow Unser | Mein
 Verb \rightarrow ist
 Adjektiv \rightarrow lästig | nett | streng | monoton | anspruchsvoll

Es gilt:

$S \xrightarrow{*}$ Unser Lehrveranstaltungsleiter ist anspruchsvoll

Ableitungen in einer Grammatik

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

Definition

- Wir sagen y ist aus x in G **direkt ableitbar**, wenn gilt:
 $\exists u, v \in (V \cup \Sigma)^*, \exists (P \rightarrow Q) \in R$ sodass $(x = uPv$ und $y = uQv)$
- In diesem Fall schreiben wir kurz $x \xrightarrow[G]{*} y$
- 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 $w_0, w_1, \dots, w_k \in (V \cup \Sigma)^*$ existieren, sodass

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

Wir schreiben $x \xrightarrow[G]{*} y$, beziehungsweise $x \Rightarrow y$

Definition

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

- V eine endliche Menge von **Variablen** (oder **Nichtterminale**)
- Σ ein Alphabet, die **Terminale**, $V \cap \Sigma = \emptyset$
- R eine endliche Menge von **Regeln**
- $S \in V$ das **Startsymbol**

Eine Regel ist ein Paar $P \rightarrow Q$ 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 $P \rightarrow Q_1, P \rightarrow Q_2, P \rightarrow Q_3$ schreiben wir $P \rightarrow Q_1 \mid Q_2 \mid Q_3$

Sprache einer Grammatik

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

$$L(G) = \{x \in \Sigma^* \mid S \xrightarrow[G]{*} x\}$$

heißt die von der Grammatik G **erzeugte Sprache**

Definition (Äquivalenz)

Zwei Grammatiken G_1 und G_2 heißen **äquivalent**, wenn $L(G_1) = L(G_2)$

Klassen von Grammatiken

Definition (rechtslinear)

Grammatik $G = (V, \Sigma, R, S)$ heißt **rechtslinear**, wenn für alle Regeln

$P \rightarrow Q$ gilt:

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

Beispiel

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

$$B \rightarrow 0 \mid 1 \mid 0B \mid 1B$$

Es gilt:

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

► zurück

Definition (kontextfrei)

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

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

Beispiel

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

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

Es gilt:

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

Definition (beschränkt)

Grammatik $G = (V, \Sigma, R, S)$ heißt **beschränkt**, wenn für alle Regeln

$P \rightarrow Q$ gilt:

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

Beispiel

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

$$S \rightarrow aSBC \mid aBC$$

$$CB \rightarrow BC$$

$$aB \rightarrow ab \quad bB \rightarrow bb \quad bC \rightarrow bc \quad cC \rightarrow cc$$

Es gilt

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

Definition (kontextsensitiv)

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

- 1 entweder es existieren $u, v, w \in (V \cup \Sigma)^*$ und $A \in V$, sodass

$$P = uAv \text{ und } Q = uwv \text{ wobei } |w| \geq 1$$

- 2 oder $P = S$, $Q = \epsilon$ und S kommt in keiner Konklusion einer Regel vor

Beispiel

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

$$S \rightarrow aSBC \mid aBC$$

$$CB \rightarrow BC$$

$$aB \rightarrow ab \quad bB \rightarrow bb \quad bC \rightarrow bc \quad cC \rightarrow cc$$

Es gilt:

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

Definition (kontextsensitiv)

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

1 entweder es existieren $u, v, w \in (V \cup \Sigma)^*$ und $A \in V$, sodass

$$P = uAv \text{ und } Q = uwv \text{ wobei } |w| \geq 1$$

2 oder $P = S$, $Q = \epsilon$ und S kommt in keiner Konklusion einer Regel vor

Beispiel

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

$$S \rightarrow aSBC \mid aBC$$

$$CB \rightarrow HB \quad HB \rightarrow HC \quad HC \rightarrow BC$$

$$aB \rightarrow ab \quad bB \rightarrow bb \quad bC \rightarrow bc \quad cC \rightarrow cc$$

Es gilt:

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

Beispiel

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

$$S \rightarrow YST \mid a \quad Ya \rightarrow aaY \quad YaT \rightarrow aa$$

Es gilt:

- G_5 ist nicht beschränkt
- $L(G_5) = \{a^{2^n} \mid n \geq 0\} = \{a, aa, aaaa, aaaaaaaaa, \dots\}$

Beispiel

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

$$S \rightarrow YST \mid a \mid aa \quad Ya \rightarrow aaY \quad YaaT \rightarrow aaaa$$

Es gilt:

- G_6 ist beschränkt
- $L(G_6) = \{a^{2^n} \mid n \geq 0\} = \{a, aa, aaaa, aaaaaaaaa, \dots\}$

Beobachtung

Grammatik G_2 ist kontextfrei, aber nicht kontextsensitiv, wegen der Regeln $S \rightarrow \epsilon$ und $S \rightarrow (S)$. 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 $L = L(G)$
- **kontextfrei** (vom Typ 2)
wenn \exists kontextfreie Grammatik G mit $L = L(G)$
- **kontextsensitiv** (vom Typ 1)
wenn \exists kontextsensitive Grammatik G mit $L = L(G)$
- **rekursiv aufzählbar** (vom Typ 0)
wenn \exists Grammatik G mit $L = L(G)$

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

