# Einführung in die Theoretische Informatik


David Drexel
Julian Fodor
Alexander Lochmann
**Georg Moser**
Alexander Maringele
David Obwaller
Jonas Schöpf

cbr.uibk.ac.at


## Zusammenfassung

## Zusammenfassung der letzten LVA

**Beispiel**

1. Wir betrachten die folgende Signatur $F = \{\overline{\phantom{x}}, \cdot, +, 0, 1\}$ sodass
   - Stelligkeit von $0$, $1$ ist $0$
   - Stelligkeit von $\overline{\phantom{x}}$ ist $1$
   - Stelligkeit von $+$, $\cdot$ ist $2$
2. $V = \{x_1, x_2, \dots\}$
3. Wir betrachten die Identitäten $E$

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

4. Dann gilt $E \vdash 1 + x = 1$

**Satz (Satz von Birkhoff)**

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



## Wortmonoid

**Beispiel**

- Betrachten Sie $D$, die Sprache aller Dezimalzahlen mit optionalem Vorzeichen, wobei ganze Zahlen mit zumindest einer 0 hinter dem Dezimalpunkt dargestellt werden.
- Beschreiben Sie informell, welche Wörter in $\sim D$ enthalten sind.

**Antwort**

$\Sigma = \{+, -, ., 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$$V = \{+, -, \epsilon\}$$
$$Z = \{0, 1, \dots, 9\}$$
$$D = VZ^+.Z^+$$

$\sim D$ hängt von der Wahl von $\Sigma$ ab

**Einführung in die Logik**

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

**Einführung in die Algebra**

algebraische Strukturen, Beispiele von Algebren, Zusammenhang Boolesche Algebra und Aussagenlogik, Universelle Algebra, Satz von Birkhoff

**Einführung in die Theorie der Formalen Sprachen**

Grammatiken und Formale Sprachen, Chomsky-Hierarchie, Reguläre Sprachen, Kontextfreie Sprachen, Anwendungen von formalen Sprachen

**Einführung in die Berechenbarkeitstheorie**

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

**Einführung in die Programmverifikation**

Prinzipien der Analyse von Programmen, Verifikation nach Hoare



## Formale Sprachen

**Definition**

Eine Teilmenge L von $\Sigma^*$ heißt eine formale Sprache über Alphabet $\Sigma$

**Beispiel**

- Die Sprache aller Wörter, die aus $n$ 0en gefolgt von $n$ 1er bestehen, wobei $n \geqslant 0$:
$$\{\epsilon, 01, 0011, 000111, \cdots\}$$
- Die Menge der Wörter, die jeweils die selbe Anzahl 0en und 1er enthalten:
$$\{\epsilon, 01, 10, 0011, 0101, \cdots\}$$
- $\Sigma^*$ ist eine Sprache, $\varnothing$—die leere Sprache—ist eine Sprache, $\{\epsilon\}$ ist eine Sprache. Beachte $\{\epsilon\} \neq \varnothing$



**Definition**

Seien $L$, $M$ formale Sprachen über dem Alphabet $\Sigma$

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



**Definition**

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

Die $k$-te Potenz von $L$ 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:

$$L^+ = \bigcup_{k\geqslant 1} L^k = \{x_1 \cdots x_k \mid x_1, \dots, x_k \in L \text{ und } k \in \mathbb{N}, k > 0\}$$

### Beispiel

- Sei $\Sigma = \{0,1\}$ und betrachte die Sprache $L$ aller Wörter, die aus $n$ 0en gefolgt von $n$ 1er bestehen, wobei $n \geqslant 0$
- Wir können $L$ konzise in Mengennotation angeben:

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

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

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



## Grammatiken und Formale Sprachen

### Beispiel

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

Es gilt

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



### Definition

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

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

Eine Regel ist ein Paar $P \to Q$ von Wörtern, sodass $P, Q \in (V \cup \Sigma)^*$ und 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 $G = (V, \Sigma, R, \mathrm{S})$ 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 $x \Rightarrow y$

### Definition (Ableitbar)

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

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

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 $\Sigma^*$ heißen Terminalwörter
- Satzformen, die Terminalwörter sind, heißen Sätze

### Definition (Sprache einer Grammatik)

Die Menge aller Sätze

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

heißt die von der Grammatik $G$ erzeugte Sprache

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



## Klassen von Grammatiken

### Definition (rechtslinear)

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

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

### Beispiel

- Die Grammatik $G_1 = (\{B\}, \{0, 1\}, R, B)$ ist rechtslinear, wobei $R$ wie folgt definiert:

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

- Es gilt:

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



### Definition (kontextfrei)

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

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

### Beispiel

- Die Grammatik $G_2 = (\{K\}, \{(, )\}, R, K)$ ist kontextfrei, wobei $R$ wie folgt definiert:

$$K \to \epsilon \mid (K) \mid KK$$

- Es gilt:

$$K \Rightarrow KK \Rightarrow (K)K \Rightarrow (\epsilon)K = ()K \Rightarrow ()(K) \Rightarrow ()(KK) \overset{*}{\Rightarrow} ()(()(()))$$



### Definition (kontextsensitiv)

Grammatik $G = (V, \Sigma, R, \mathrm{S})$ 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 $P = \mathrm{S}$ und $Q = \epsilon$

Wenn $\mathrm{S} \to \epsilon \in G$, dann kommt S nicht in einer Konklusion vor

### Beispiel

$G_3 = (\{\mathrm{S}, B, C, H\}, \{\mathrm{a}, \mathrm{b}, \mathrm{c}\}, R, \mathrm{S})$ ist kontextsensitiv, wobei $R$:

$$\begin{array}{lll lll lll}
\mathrm{S} & \to & \mathrm{a}SBC \mid \mathrm{a}BC & HC & \to & BC & \mathrm{b}C & \to & \mathrm{bc} \\
CB & \to & HB & \mathrm{a}B & \to & \mathrm{ab} & \mathrm{c}C & \to & \mathrm{cc} \\
HB & \to & HC & \mathrm{b}B & \to & \mathrm{bb} & & &
\end{array}$$

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

### Definition (beschränkt)

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

1. entweder $|P| \leqslant |Q|$ oder
2. $P = \mathrm{S}$ und $Q = \epsilon$

Wenn $\mathrm{S} \to \epsilon \in G$, dann kommt S nicht in einer Konklusion vor

### Definition

Eine formale Sprache $L$ heißt

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



### Definition

Eine formale Sprache $L$ heißt

- beschränkt wenn $\exists$ beschränkte Grammatik $G$, $L = \mathrm{L}(G)$
- rekursiv aufzählbar (vom Typ 0)
  wenn $\exists$ Grammatik $G$, $L = \mathrm{L}(G)$

### Satz (Chomsky-Hierarchie)

*Es gelten die folgenden Inklusionen*

$$\mathcal{L}_3 \subsetneq \mathcal{L}_2 \subsetneq \mathcal{L}_1 \subsetneq \mathcal{L}_0 \subsetneq \mathcal{L}$$

- *$\mathcal{L}_i$ die Klasse der Sprachen von Typ $i$*
- *$\mathcal{L}$ Klasse der formalen Sprachen*

### Satz

*Eine Sprache L ist kontextsensitiv gdw. L beschränkt ist*



## Chomsky-Hierarchie