FSK
Zentralübung 1

Prof. Dr. Jasmin Blanchette

Lehr- und Forschungseinheit für
Theoretische Informatik

Stand: 19. April 2023
Folien ursprünglich von PD Dr. David Sabel

Fragen, Probleme?

Inhaltliches

Kapitel 2 Grundlagen aus dem Skript selbst lesen

Wird nur teilweise in Vorlesung und Übung behandelt

Plan für Heute

- Notation zu Wörtern, Sprachen: Beispiele und Hinweise
- Chomsky-Hierarchie: Beispiele
- Wiederholung zum formalen Argumentieren
- Beweise und Beweistechniken

Notationen (und Probleme)

Für Sprachen L haben wir eingeführt:

$$L^0 := \{\varepsilon\} \qquad L^* := \bigcup_{i \in \mathbb{N}} L^i$$

$$L^i := L \circ L^{i-1} \text{ für } i > 0 \qquad L^+ := \bigcup_{i \in \mathbb{N}_{>0}} L^i$$

Später verwenden wir manchmal soetwas wie L_i^j:
Hier sind i und j Indizes, und keine Potenzen.
Gerne nachfragen, wenn es mehrdeutig ist.

Quiz

Sei $\Sigma = \{a, d, e, h, k, m, n, s, u, t, z\}$ und $L = \{hund, katze, maus\}$.

Welche der Antworten ist richtig?

a) $katzemaushund \in L^2$

b) $haus \in L^*$

c) $tatze \in \Sigma^*$

d) $hundhundhund \in L^4$

Quiz

Sei $\Sigma = \{a, d, e, h, k, m, n, s, u, t, z\}$ und $L = \{hund, katze, maus\}$.

Welche der Antworten ist richtig?

a) $katzemaushund \in L^2$

b) $haus \in L^*$

c) $tatze \in \Sigma^*$

d) $hundhundhund \in L^4$

Korrekt: c)

Definition einer Grammatik

Definition (Grammatik)

Eine Grammatik ist ein 4-Tupel $G = (V, \Sigma, P, S)$ mit

- V ist eine endliche Menge von Variablen
  (alternativ Nichtterminale, Nichtterminalsymbole)
- Σ (mit $V \cap \Sigma = \emptyset$) ist ein Alphabet von Zeichen
  (alternativ Terminale, Terminalsymbole)
- P ist eine endliche Menge von Produktionen von der Form $\ell \to r$ wobei $\ell \in (V \cup \Sigma)^+$ und $r \in (V \cup \Sigma)^*$
  (alternativ Regeln)
- $S \in V$ ist das Startsymbol
  (alternativ Startvariable)

Ableitung

Sei $G = (V, \Sigma, P, S)$ eine Grammatik.

Ableitungsschritt $\Rightarrow_G$

Für Satzformen u, v: u geht unter Grammatik G unmittelbar in v über, $u \Rightarrow_G v$, wenn

$$u = w_1 \ell w_2 \Rightarrow_G w_1 r w_2 = v \text{ mit } (\ell \to r) \in P$$

Ableitung

Eine Folge $(w_0, w_1, \ldots, w_n)$ mit $w_0 = S$, $w_n \in \Sigma^*$ und $w_{i-1} \Rightarrow w_i$ für $i = 1, \ldots, n$ heißt Ableitung von w_n.

Erzeugte Sprache einer Grammatik

Die von einer Grammatik $G = (V, \Sigma, P, S)$ **erzeugte Sprache** $L(G)$ ist

$$L(G) := \{w \in \Sigma^* \mid S \Rightarrow_G^* w\}.$$

Quiz

Sei $G = (\{A, B, C\}, \{d, e\}, P, A)$ mit

$$P = \{A \to BBCC,\ B \to d,\ C \to e,\ dC \to Cd,\ ed \to \varepsilon\}$$

Welches Wort liegt in $L(G)$?

a) ε

b) $BBdd$

c) e

Quiz

Sei $G = (\{A, B, C\}, \{d, e\}, P, A)$ mit

$$P = \{A \to BBCC,\ B \to d,\ C \to e,\ dC \to Cd,\ ed \to \varepsilon\}$$

Welches Wort liegt in $L(G)$?

a) ε

b) $BBdd$

c) e

Korrekt: a), da $A \Rightarrow BBCC \Rightarrow^2 ddCC \Rightarrow^3 CCdd \Rightarrow^2 eedd \Rightarrow ed \Rightarrow \varepsilon$

Die Chomsky-Hierarchie

Sei $G = (V, \Sigma, P, S)$ eine Grammatik.

G **ist vom Typ 0**
G ist automatisch vom Typ 0
G **ist vom Typ 1 (kontextsensitive Grammatik), wenn ...**
für alle $(\ell \to r) \in P$: $\lvert\ell\rvert \leq \lvert r\rvert$
G **ist vom Typ 2 (kontextfreie Grammatik), wenn ...**
G ist vom Typ 1 und für alle $(\ell \to r) \in P$ gilt: $\ell \in V$
G **ist vom Typ 3 (reguläre Grammatik), wenn ...**
G ist vom Typ 2 und für alle $(A \to r) \in P$ gilt: $r = a$ oder $r = aA'$ für $a \in \Sigma, A' \in V$ (die rechten Seiten sind Wörter aus $\Sigma \cup \Sigma V$)

Quiz 1

Sei $G = (\{A, B, C\}, \{d, e\}, P, A)$ mit

$$P = \{A \to BBCC,\ B \to d,\ C \to e,\ dC \to Cd\}$$

Welchen Typ hat G?

a) 0

b) 1

c) 2

d) 3

Quiz 1

Sei $G = (\{A, B, C\}, \{d, e\}, P, A)$ mit

$$P = \{A \to BBCC,\ B \to d,\ C \to e,\ dC \to Cd\}$$

Welchen Typ hat G?

a) 0

b) 1

c) 2

d) 3

Korrekt: a) und b)

Quiz 2

Sei $G = (\{A, B, C\}, \{d, e\}, P, A)$ mit

$$P = \{A \to BBCC,\ B \to dCCC,\ CdC \to d,\ dC \to Cd\}$$

Welchen Typ hat G?

a) 0

b) 1

c) 2

d) 3

Quiz 2

Sei $G = (\{A, B, C\}, \{d, e\}, P, A)$ mit

$$P = \{A \to BBCC,\ B \to dCCC,\ CdC \to d,\ dC \to Cd\}$$

Welchen Typ hat G?

a) 0

b) 1

c) 2

d) 3

Korrekt: a)

Quiz 3

Sei $G = (\{A, B, C\}, \{a, d, e\}, P, A)$ mit

$$P = \{A \to a,\ A \to aB,\ B \to d,\ C \to e,\ C \to dC\}$$

Welchen Typ hat G?

a) 0

b) 1

c) 2

d) 3

Quiz 3

Sei $G = (\{A, B, C\}, \{a, d, e\}, P, A)$ mit

$$P = \{A \to a,\ A \to aB,\ B \to d,\ C \to e,\ C \to dC\}$$

Welchen Typ hat G?

a) 0

b) 1

c) 2

d) 3

Korrekt: a), b), c), d)

Quiz: Sprachtyp

Sei $G = (\{A, B, C\}, \{d, e\}, P, A)$ mit

$$P = \{A \to BBCC,\ B \to d,\ C \to e,\ dC \to Cd\}$$

Welchen Typ hat $L(G)$?

a) 0

b) 1

c) 2

d) 3

Quiz: Sprachtyp

Sei $G = (\{A, B, C\}, \{d, e\}, P, A)$ mit

$$P = \{A \to BBCC,\ B \to d,\ C \to e,\ dC \to Cd\}$$

Welchen Typ hat $L(G)$?

a) 0

b) 1

c) 2

d) 3

Korrekt: d), da $L(G) = \{ddee, dede, deed, edde, eded, eedd\}$ und es reguläre Grammatiken gibt, die $L(G)$ erzeugen.
Z.B. $L(G) = (\{S, D, E, A_{DEE}, A_{DDE}, A_{DD}, A_{DE}, A_{EE}\}, \{d, e\}, P', S)$ mit
$P' = \{S \to dA_{DEE} \mid eA_{DDE}, A_{DDE} \to dA_{DE} \mid eA_{DD}, A_{DEE} \to dA_{EE} \mid eA_{DE},$
$A_{DE} \to dE \mid eD, A_{DD} \to dD, A_{EE} \to eE, D \to d, E \to e\}$

Wiederholung zum formalen Argumentieren, Beweise und Beweistechniken

Wiederholung zum formalen Argumentieren

Begriffe in formalen / mathematischen Texten

- **Axiome**: Grundaussagen; werden nicht bewiesen.
- **Definitionen**: führt neue Begriffe / Notation ein. Enthalten keine Aussagen / werden nicht bewiesen.
- **Sätze**: Formuliert Aussagen, diese müssen bewiesen werden. Je nach Wichtigkeit: Theorem, Satz, Lemma, Korollar. Korollar oft direkte Folgerung aus anderen Sätzen, daher ohne Beweis.
- **Beweise**: Zeigen Korrektheit von Sätzen.
- **Bemerkungen:** Erläuterungen, Motivationen usw.
- **Beispiele:** Illustration von Begriffen und Aussagen, Algorithmen.

Aussagen

Atomare Aussagen: sind wahr oder falsch, z.B.

- *Die Sprache* $L = \{a^j b^{2j} \mid 0 < j < 10\}$ *ist endlich.* (wahr)
- *Es gilt* $aaabbb \in \{a^j b^{2j} \mid 0 < j < 10\}$. (falsch)

Verknüpfungen bilden zusammengesetzte Aussagen:

- Konjunktion, „und“, $A \wedge B$: wahr wenn A und B beide wahr sind, sonst falsch
  Z.B. $aabbb \in L$ *und* $abb \in L$.
- Disjunktion, „oder“, $A \vee B$: nur falsch, wenn A und B falsch sind, sonst wahr
  Z.B. $aabb \in L$ *oder* $abb \in L$.
- Negation, „nicht“, $\neg A$: wahr, wenn A falsch ist, und falsch, wenn A wahr ist
  Z.B. *Die Sprache* L *ist nicht endlich.*
- Implikation, „wenn . . . , dann . . . “, $A \implies B$: wahr wenn A falsch, oder B wahr ist
  Z.B. *Wenn* $abbb \in L$, *dann ist auch* $abb \in L$.
- Äquivalenz, „. . . genau dann, wenn . . . “, $A \Leftrightarrow B$: $(A \implies B) \wedge (B \implies A)$
  Z.B. $aaabbb \in L$ *genau dann, wenn* $aaabbb \notin \overline{L}$.

Umformungsregeln

$$
\begin{aligned}
\neg\neg F &\equiv F \\
F \vee G &\equiv G \vee F \\
F \wedge G &\equiv G \wedge F \\
\neg(F \vee G) &\equiv \neg F \wedge \neg G \\
\neg(F \wedge G) &\equiv \neg F \vee \neg G \\
F \vee (G \wedge H) &\equiv (F \vee G) \wedge (F \vee H) \\
F \wedge (G \vee H) &\equiv (F \wedge G) \vee (F \wedge H) \\
F \implies G &\equiv \neg F \vee G \\
F \implies G &\equiv \neg G \implies \neg F
\end{aligned}
$$

(wobei $\equiv$ die Äquivalenz von Formeln)

Aussageformen / Prädikate

Aussageformen = Aussagen mit **Variablen**

z.B. *Wenn* $w \in \{a^j b^{2j} \mid 0 < j < 10\}$ *und* $\#_b(w) = k$, *dann gilt* $\#_a(w) < k$.
Hier ist w eine Variable.

Allgemein kann eine solche Aussageform / Prädikat $P(w)$

- für alle Wörter w wahr sein
- für manche Wörter w (mindestens eins) wahr sein
- für kein Wort w wahr sein.

Es kommt auf die **Quantifzierung der Variablen** an: Quantoren sind:

- **Allquantor**, Für alle, $\forall w.P(w)$: für jedes konkrete Wort u ist $P(u)$ wahr.
- **Existenzquantor**, „Es existiert“, $\exists w.P(w)$: es gibt ein Wort u, sodass $P(u)$ wahr ist.

Wichtige Umformungen für quantifiziert Formeln

$$
\begin{aligned}
\neg\forall w.P(w) &\equiv \exists w.\neg P(w) \\
\neg\exists w.P(w) &\equiv \forall w.\neg P(w) \\
\forall w.(P(w) \wedge Q(w)) &\equiv (\forall w.P(w)) \wedge (\forall w.Q(w)) \\
\exists w.(P(w) \vee Q(w)) &\equiv (\exists w.P(w)) \vee (\exists w.Q(w))
\end{aligned}
$$

Implizite Allquantifizierung

Wenn $w \in \{a^j b^{2j} \mid 0 < j < 10\}$ *und* $\#_b(w) = k$*, dann gilt* $\#_a(w) < k$*.*

- Hier ist kein Quantor explizit angegeben.
- Dann ist die Variable w allquantifizert.
- Auch in

  Sei L *eine formale Sprache . . .*

  ist L beliebig und daher wird über alle L quantifiziert.

Beweise: Was macht einen Beweis zum Beweis

- **Beweis** = vollständige, nachvollziehbare, folgerichtige Argumentation, dass die zu zeigende Aussage wahr ist.
- Aussagen bestehen meist aus Voraussetzungen und Konsequenzen. Die Argumentation muss zeigen, dass die Konsequenzen stets gelten, falls die Voraussetzungen erfüllt sind.
- **Vollständigkeit:** Argumentation muss jeden möglichen Fall abdecken.
- **Folgerichtigkeit:** Jedes einzelne Argument muss korrekt, nachvollziehbar und akzeptabel sein (auch von kritischen Lesenden).

Beweistechniken

- Direkter Beweis
- Indirekter Beweis
- Vollständige Fallunterscheidung
- Vollständige Induktion
- Widerlegen durch Gegenbeispiel

Direkter Beweis

Prinzip: Aussage wird durch logische Schlüsse aus bekannten Aussagen hergeleitet.

Beispiel:

Satz

Sei u ein Wort über einem Alphabet Σ. Dann ist die Wortlänge des Wortes uu gerade.

Direkter Beweis:

Sei u ein Wort über Σ.
Sei $|u| = m \in \mathbb{N}$.
Dann ist uu doppelt so lang wie $|u|$ und daher $|uu| = 2 \cdot m$.
Daher ist 2 ein Teiler von $|uu|$.
Daher ist $|uu|$ eine gerade Zahl. □

Indirekter Beweis

Prinzip: Statt der eigentlichen Aussage wird eine logisch-äquivalente Aussage gezeigt.

Varianten:

Beweis durch Kontraposition:

Um „aus Aussage A folgt Aussage B“ zu zeigen, zeige
„Wenn Aussage B nicht gilt, dann gilt auch Aussage A nicht“

Beweis durch Widerspruch:

Um Aussage A zu zeigen, zeige:
Gilt A nicht, so folgt daraus ein Widerspruch (d.h. Falsch)

Beachte: Wenn A selbst eine Implikation ist ($C \implies D$), dann zeigt man: Wenn C gilt, aber D nicht gilt, dann folgt ein Widerspruch.

Beispiel: Beweis durch Widerspruch

Satz

Sei u ein Wort über einem Alphabet Σ. Dann ist die Wortlänge des Wortes uu gerade.

Indirekter Beweis (Beweis durch Widerspruch):

Nehme an die Aussage ist falsch.
Dann gibt es ein Wort u über Σ, sodass $|uu|$ keine gerade Zahl ist.
Dann ist $|uu| = 2m + 1$ für ein $m \in \mathbb{N}_0$.
Sei $|u| = k \in \mathbb{N}_0$.
Dann gilt $|uu| = |u| + [u| = k + k = 2k = 2m + 1$ und damit $m = k - \frac{1}{2}$.
Daraus folgt $m \notin \mathbb{N}$.
Widerspruch.
Daher war die Annahme falsch, und die Aussage muss wahr sein. □

Beispiel: Beweis durch Kontraposition

Satz

Sei L eine formale Sprache über $\{a\}$, sodass für alle $w \in L$: $1 < |w| < 5$.
Wenn $a^5 \in L^*$, dann ist auch $a^6 \in L^*$.

Indirekter Beweis (Beweis durch Kontraposition):

Sei L wie im Satz verlangt.
Zeige: Wenn $a^6 \notin L^*$, dann $a^5 \notin L^*$.
(Es folgt dann $a^5 \in L^* \implies a^6 \in L^*$.)
Nehme also an $a^6 \notin L^*$.
Dann gilt auch $a^2 \notin L$ (sonst wäre $a^6 \in L^3 \subseteq L^*$).
Dann gilt auch $a^3 \notin L$ (sonst wäre $a^6 \in L^2 \subseteq L^*$).
Die Anforderungen an L zeigen $a^1 \notin L$ und $a^i \notin L$ mit $i \geq 5$.
Daher ist $L = \{\}$ oder $L = \{a^4\}$.
Damit folgt $a^5 \notin L^*$, denn $L^* = \{\varepsilon\}$ oder $L^* = \{a^{4i} \mid i \in \mathbb{N}\}$. □

Beweis durch Fallunterscheidung

Prinzip: Im Beweis werden alle möglichen Fälle diskutiert und für jeden Fall gezeigt, dass er die Aussage erfüllt.

Beispiel:

Satz

Sei L formale Sprache über $\{a\}$, sodass für alle $w \in L$: $1 < |w| < 5$.
Wenn $a^7 \in L^*$, dann ist auch $a^6 \in L^*$.

Beweis: Da $L \subseteq \{a^2, a^3, a^4\}$ ist folgende Fallunterscheidung vollständig:

- $a^2 \in L$: Dann ist $a^6 \in L^3 \subseteq L^*$
- $a^3 \in L$. Dann ist $a^6 \in L^2 \subseteq L^*$
- weder $a^2 \in L$ noch $a^3 \in L$: Dann ist $a^7 \notin L^*$, da $L \subseteq \{a^4\}$ □

Vollständige Induktion

Prinzip: Beweis, um Gültigkeit für alle natürlichen Zahlen zu zeigen.
Zeige Induktionsbasis ($n = 0$) und Induktionsschritt (wenn Aussage für $n - 1$ gilt, folgt daraus, dass Aussage für n gilt).
Geht auch für andere rekursive definierte Strukturen, z.B. Wörter
(Basis: leeres Wort, Schritt: $w \to aw$ für alle Zeichen a).

Beispiel: Vollständige Induktion

Satz

Sei $u \in \{a, b\}^*$. Dann gilt $|u| = \#_a(u) + \#_b(u)$

Beweis durch vollständige Induktion über die Struktur von u:

Induktionsbasis $u = \varepsilon$:

Es gilt $|u| = 0$, $\#_a(u) = 0$, $\#_b(u) = 0$.

Mit $0 + 0 = 0$ folgt die Aussage.

Induktionsschritt:

Als Induktionshypothese nehmen wir an, dass die Behauptung für w gilt ($|w| = \#_a(w) + \#_b(w)$) und zeigen, dass sie für aw und bw dann ebenfalls gilt:

- Fall aw: Es gilt $\#_a(aw) = 1 + \#_a(w)$ und $\#_b(aw) = \#_b(w)$ und damit $\#_a(aw) + \#_b(aw) = 1 + \#_a(w) + \#_b(w) = 1 + |w| = |aw|$.
- Fall bw: Es gilt $\#_a(bw) = \#_a(w)$ und $\#_b(bw) = 1 + \#_b(w)$ und damit $\#_a(bw) + \#_b(bw) = 1 + \#_a(w) + \#_b(w) = 1 + |w| = |bw|$. □

Widerlegung durch Gegenbeispiel

Prinzip: Widerlege eine allquantifizerte Aussage, indem eine Belegung angegeben wird, welche die Aussage falsch macht

Beispiel:

Aussage

Sei L formale Sprache über $\{a\}$, sodass für alle $w \in L$: $1 < |w| < 5$.
Wenn $a^7 \in L^*$, dann ist auch $a^2 \in L^*$.

Die Aussage ist falsch.

Widerlegung durch Gegenbeispiel:
Für $L = \{aaa, aaaa\}$ gilt die Aussage nicht,
da $a^7 \in L^*$, aber $a^2 \notin L^*$.