Zentralübung 1

Prof. Dr. Jasmin Blanchette

Lehr- und Forschungseinheit für
Theoretische Informatik und Theorembeweisen

Stand: 23. April 2024
Basiert auf Folien von PD Dr. David Sabel

Plan für heute

1. Wörter und Sprachen
2. Beweise und Beweistechniken
3. Grammatiken
4. Die Chomsky-Hierarchie

1. Wörter und Sprachen

Notationen

Für Sprachen L haben wir eingeführt:

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

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) $hundhundhund \in L^4$

Antwort: c)

2. Beweise und Beweistechniken

Begriffe in mathematischen Texten

- Axiome sind Grundaussagen. Sie müssen nicht bewiesen werden.
- Definitionen führen neue Begriffe bzw. Notation ein.
  Sie Enthalten keine Aussagen und müssen nicht bewiesen werden.
- Sätze formulieren Aussagen, die bewiesen werden müssen.
  Je nach Wichtigkeit: Theorem, Satz, Lemma.
  Korollare sind direkte Folgerungen aus anderen Sätzen, daher ohne Beweis.
- Beweise zeigen die Korrektheit von Sätzen.
- Bemerkungen erläutern, motivieren usw.
- Beispiele illustrieren Begriffe, Aussagen oder Algorithmen.

Atomare 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)

Zusammengesetzte Aussagen

Verknüpfungen bilden zusammengesetzte Aussagen:

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

Wichtige Umformungsregeln für Verknüpfungen

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

Aussageformen (Prädikate)

Aussageformen (Prädikate) sind Aussagen mit Variablen.
Z.B. *Wenn* $w \in \{a^j b^{2j} \mid 0 < j < 10\}$, *dann gilt* $\#_a(w) < \#_b(w)$.
Hier ist w eine Variable.

Aussageformen (Prädikate)

Aussageformen (Prädikate) sind Aussagen mit Variablen.
Z.B. *Wenn* $w \in \{a^j b^{2j} \mid 0 < j < 10\}$, *dann gilt* $\#_a(w) < \#_b(w)$.
Hier ist w eine Variable.

Allgemein kann eine solche Aussageform $P(w)$

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

Aussageformen (Prädikate)

Aussageformen (Prädikate) sind Aussagen mit Variablen.
Z.B. *Wenn* $w \in \{a^j b^{2j} \mid 0 < j < 10\}$, *dann gilt* $\#_a(w) < \#_b(w)$.
Hier ist w eine Variable.

Allgemein kann eine solche Aussageform $P(w)$

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

Es kommt auf die Quantifizierung der Variablen an. Quantoren sind:

- Allquantor, „für alle ...“, $\forall w.\ P(w)$ ist nur wahr, wenn für jedes konkrete Wort u die Aussage $P(u)$ wahr ist, sonst falsch.
- Existenzquantor, „Es existiert ...“, $\exists w.\ P(w)$ ist nur wahr, wenn es (mindestens) ein Wort u gibt, sodass die Aussage $P(u)$ wahr ist, sonst falsch.

Wichtige Umformungsregeln für Quantoren

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

Implizite Allquantifizierung

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

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

  Sei L *eine Sprache . . .*

  ist L beliebig und daher wird über alle L quantifiziert.

Was macht einen Beweis zum Beweis

- Ein Beweis ist eine vollständige, nachvollziehbare, folgerichtige Argumentation, dass die zu zeigende Aussage wahr ist.
- Aussagen bestehen meist aus Voraussetzungen und Folgerungen.
  Die Argumentation muss zeigen, dass die Folgerungen stets gelten, falls die Voraussetzungen erfüllt sind.
- Vollständigkeit: Die 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
- Fallunterscheidung
- Vollständige Induktion
- Widerlegen durch Gegenbeispiel

Direkter Beweis

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

Beispiel für einen direkten Beweis

Satz

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

Beispiel für einen direkten Beweis

Satz

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

Beweis

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

Umgang mit Verknüpfungen und Quantoren

Die folgende Tabelle fasst zusammen, wie man mit Aussagen, die bestimmte logische Operationen enthalten, umgeht.

	Um eine Aussage dieser Form zu beweisen ...	Wenn eine Aussage dieser Form angenommen wird ...
$P \wedge Q$		
$P \vee Q$		
$\neg P$		
$P \Longrightarrow Q$		
$\forall x,\ P(x)$		
$\exists x,\ P(x)$		

Umgang mit Verknüpfungen und Quantoren

Die folgende Tabelle fasst zusammen, wie man mit Aussagen, die bestimmte logische Operationen enthalten, umgeht.

	Um eine Aussage dieser Form zu beweisen ...	Wenn eine Aussage dieser Form angenommen wird ...
$P \wedge Q$	beweise sowohl P als auch Q	
$P \vee Q$	beweise entweder P oder Q	
$\neg P$	beweise, dass unter der Annahme P ein Widerspruch folgt	
$P \Longrightarrow Q$	beweise, dass unter der Annahme P Q folgt	
$\forall x,\ P(x)$	beweise, dass $P(a)$ für ein beliebiges a gilt	
$\exists x,\ P(x)$	gib ein konkretes a an und beweise $P(a)$	

Umgang mit Verknüpfungen und Quantoren

Die folgende Tabelle fasst zusammen, wie man mit Aussagen, die bestimmte logische Operationen enthalten, umgeht.

	Um eine Aussage dieser Form zu beweisen ...	Wenn eine Aussage dieser Form angenommen wird ...
$P \wedge Q$	beweise sowohl P als auch Q	nimm P und Q an
$P \vee Q$	beweise entweder P oder Q	beweise die gewünschte Aussage einmal unter der Annahme P und nocheinmal unter der Annahme Q (Fallunterscheidung)
$\neg P$	beweise, dass unter der Annahme P ein Widerspruch folgt	beweise P, um einen Widerspruch herzuleiten
$P \Longrightarrow Q$	beweise, dass unter der Annahme P Q folgt	beweise P und nimm dann Q an
$\forall x,\ P(x)$	beweise, dass $P(a)$ für ein beliebiges a gilt	nimm $P(a)$ für jedes konkrete a an
$\exists x,\ P(x)$	gib ein konkretes a an und beweise $P(a)$	nimm ein beliebiges a an, für das $P(a)$ gilt

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)“.

Beispiel für einen Beweis durch Widerspruch

Satz

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

Beispiel für einen Beweis durch Widerspruch

Satz

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

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 $m \in \mathbb{N}$.
Sei $|u| = k \in \mathbb{N}$.
Dann gilt $|uu| = |u| + [u| = k + k = 2k = 2m + 1$ und damit $m = k - 1/2$.
Daraus folgt $m \notin \mathbb{N}$.
Widerspruch.
(Daher war die Annahme falsch, und die Aussage muss wahr sein.) □

Beispiel für einen Beweis durch Kontraposition

Satz

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

Beispiel für einen Beweis durch Kontraposition

Satz

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

Beweis Durch Kontraposition.
Zeige: Wenn $a^6 \notin L^*$, dann $a^5 \notin L^*$.
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 für einen Beweis durch Fallunterscheidung

Satz

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

Beispiel für einen Beweis durch Fallunterscheidung

Satz

Sei L eine 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 Durch Fallunterscheidung:

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

Vollständige Induktion

Prinzip: Beweis, um Gültigkeit für alle natürlichen Zahlen zu zeigen.
Zeige zwei Fälle:

- Induktionsbasis: Die Aussage gilt für $n = 0$.
- Induktionsschritt: Wenn die Aussage für alle m mit $m < n$ gilt, folgt daraus, dass die Aussage für n gilt.

Beispiel für einen Beweis durch vollständige Induktion

Satz

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

Beispiel für einen Beweis durch vollständige Induktion

Satz

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

Beweis Durch Induktion über $|u|$:

- Fall $|u| = 0$: Dann $\#_a(u) = 0$, $\#_b(u) = 0$.
  Mit $0 + 0 = 0$ folgt die Aussage.
- Fall $|u| > 0$: Dann ist u von der Form aw oder bw, wobei $w \in \{a, b\}^*$.
  Als Induktionshypothese (IH) nehmen wir an, dass die Behauptung für w gilt:
  $|w| = \#_a(w) + \#_b(w)$.
  Wir zeigen, dass sie für aw und bw dann ebenfalls gilt:
  - Fall $u = aw$: Es gilt $\#_a(aw) = 1 + \#_a(w)$ und $\#_b(aw) = \#_b(w)$ und zusammen mit der IH gilt $\#_a(aw) + \#_b(aw) = 1 + \#_a(w) + \#_b(w) = 1 + |w| = |aw|$.
  - Fall $u = bw$: Es gilt $\#_a(bw) = \#_a(w)$ und $\#_b(bw) = 1 + \#_b(w)$ und zusammen mit der IH gilt $\#_a(bw) + \#_b(bw) = 1 + \#_a(w) + \#_b(w) = 1 + |w| = |bw|$. □

Widerlegung durch Gegenbeispiel

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

Beispiel für eine Widerlegung durch Gegenbeispiel

Aussage

Sei L eine 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 $a^2 \notin L^*$.

3. Grammatiken

Definition einer Grammatik

Definition

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

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

Ableitungen

Definition

Sei $G = (V, \Sigma, P, S)$ eine Grammatik.
Eine Satzform ist ein Wort aus $(V \cup \Sigma)^*$.
Satzform u geht unter Grammatik G unmittelbar in Satzform v über, $u \Rightarrow_G v$, wenn

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

Definition

Sei $G = (V, \Sigma, P, S)$ eine Grammatik.
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.
Statt $(w_0, \ldots, w_n)$ schreiben wir auch $w_0 \Rightarrow \cdots \Rightarrow w_n$.

Erzeugte Sprache

Definition

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

Antwort: a), da $A \Rightarrow BBCC \Rightarrow^2 ddCC \Rightarrow^4 CCdd \Rightarrow^2 eedd \Rightarrow ed \Rightarrow \varepsilon$

4. Die Chomsky-Hierarchie

Die Chomsky-Hierarchie

Definition

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

- G ist automatisch vom Typ 0.
- G ist vom Typ 1 (alternativ kontextsensitiv), wenn:
  für alle $\ell \to r \in P$ gilt $|\ell| \leq |r|$.
- G ist vom Typ 2 (alternativ kontextfrei), wenn:
  G ist vom Typ 1 und für alle $\ell \to r \in P$ gilt $\ell \in V$.
- G ist vom Typ 3 (alternativ regulär), wenn:
  G ist vom Typ 2 und für alle $A \to r \in P$ gilt $r = a$ oder $r = aA'$ für $a \in \Sigma, A' \in V$ (d.h. die rechten Seiten sind Satzformen aus $\Sigma \cup \Sigma V$).

1. Quiz

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

1. Quiz

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

Antwort: a) und b)

2. Quiz

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

2. Quiz

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

Antwort: a)

3. Quiz

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

3. Quiz

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

Antwort: a), b), c), d)

4. Quiz

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

4. Quiz

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

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