Beweistechniken

Vorlesung Logik in der Informatik, HU Berlin

1. Übungsstunde

Was darf in einem Beweis verwendet werden?

- die Voraussetzungen des Satzes
- Definitionen und bereits bekannte Tatsachen und Sätze
- im Beweis selbst oder anderswo bereits als wahr bewiesene Aussagen
- logische Schlussregeln

Und was ist verboten?

- unzulässiges Argumentieren mit Beispielen
- Verwendung gleicher Symbole zur Bezeichnung verschiedener Dinge
- Hantieren mit nicht exakt oder gar widersprüchlich definierten Begriffsbildungen
- unzulässige Gedankensprünge beim Schlussfolgern
- Ausnutzung von bis dahin noch unbewiesenen Behauptungen zur Begründung von einzelnen Beweisschritten

Hilfreiche Beweistechniken

- direkter Beweis
- Beweis durch Kontraposition
- Beweis durch Widerspruch
- Beweis durch vollständige Induktion
  - ... über die natürlichen Zahlen
  - ... über rekursiv definierte Mengen

Direkter Beweis

Ansatz:

Die Behauptung wird "direkt" (d.h. "ohne Umwege") bewiesen.

Direkter Beweis

Ansatz:
Die Behauptung wird "direkt" (d.h. "ohne Umwege") bewiesen.

Notation/Erinnerung: Sei $\varphi \in \mathsf{AL}$ und $\mathcal{I} : \mathsf{AS} \to \{0,1\}$. Wir schreiben
$\mathcal{I} \models \varphi$, falls $[\![\varphi]\!]^{\mathcal{I}} = 1$ und $\mathcal{I} \not\models \varphi$, falls $[\![\varphi]\!]^{\mathcal{I}} = 0$.

Direkter Beweis

Ansatz:
Die Behauptung wird "direkt" (d.h. "ohne Umwege") bewiesen.

Notation/Erinnerung: Sei $\varphi \in \mathsf{AL}$ und $\mathcal{I} : \mathsf{AS} \to \{0,1\}$. Wir schreiben
$\mathcal{I} \models \varphi$, falls $[\![\varphi]\!]^{\mathcal{I}} = 1$ und $\mathcal{I} \not\models \varphi$, falls $[\![\varphi]\!]^{\mathcal{I}} = 0$.

Behauptung 1: Für alle $\varphi, \psi, \chi \in \mathsf{AL}$ und $\mathcal{I} : \mathsf{AS} \to \{0,1\}$ gilt:

$$\mathcal{I} \models (\varphi \land (\psi \lor \chi)) \iff \mathcal{I} \models ((\varphi \land \psi) \lor (\varphi \land \chi))$$

Direkter Beweis

Ansatz:
Die Behauptung wird "direkt" (d.h. "ohne Umwege") bewiesen.

Notation/Erinnerung: Sei $\varphi \in \mathrm{AL}$ und $\mathcal{I} : \mathrm{AS} \to \{0,1\}$. Wir schreiben
$\mathcal{I} \models \varphi$, falls $[\![\varphi]\!]^{\mathcal{I}} = 1$ und $\mathcal{I} \not\models \varphi$, falls $[\![\varphi]\!]^{\mathcal{I}} = 0$.

Behauptung 1: Für alle $\varphi, \psi, \chi \in \mathrm{AL}$ und $\mathcal{I} : \mathrm{AS} \to \{0,1\}$ gilt:

$$\mathcal{I} \models (\varphi \wedge (\psi \vee \chi)) \iff \mathcal{I} \models ((\varphi \wedge \psi) \vee (\varphi \wedge \chi))$$

Behauptung 2: Für alle $\varphi, \psi, \chi \in \mathrm{AL}$ und $\mathcal{I} : \mathrm{AS} \to \{0,1\}$ gilt:

$$\mathcal{I} \models (\varphi \vee (\psi \wedge \chi)) \iff \mathcal{I} \models ((\varphi \vee \psi) \wedge (\varphi \vee \chi))$$

Direkter Beweis

Ansatz:
Die Behauptung wird "direkt" (d.h. "ohne Umwege") bewiesen.

Notation/Erinnerung: Sei $\varphi \in \mathrm{AL}$ und $\mathcal{I} : \mathrm{AS} \to \{0,1\}$. Wir schreiben
$\mathcal{I} \models \varphi$, falls $[\![\varphi]\!]^{\mathcal{I}} = 1$ und $\mathcal{I} \not\models \varphi$, falls $[\![\varphi]\!]^{\mathcal{I}} = 0$.

Behauptung 1: Für alle $\varphi, \psi, \chi \in \mathrm{AL}$ und $\mathcal{I} : \mathrm{AS} \to \{0,1\}$ gilt:

$$\mathcal{I} \models (\varphi \land (\psi \lor \chi)) \iff \mathcal{I} \models ((\varphi \land \psi) \lor (\varphi \land \chi))$$

Behauptung 2: Für alle $\varphi, \psi, \chi \in \mathrm{AL}$ und $\mathcal{I} : \mathrm{AS} \to \{0,1\}$ gilt:

$$\mathcal{I} \models (\varphi \lor (\psi \land \chi)) \iff \mathcal{I} \models ((\varphi \lor \psi) \land (\varphi \lor \chi))$$

Behauptung 3:
Es gilt für jede Formel $\varphi \in \mathrm{AL}$:

$$\varphi \text{ ist erfüllbar} \iff \neg\varphi \text{ ist nicht allgemeingültig.}$$

Beweis durch Kontraposition

Seien V und A beliebige Aussagen. Dann gilt:

“Falls V gilt, so auch A” ist wahr.

$\iff$ “A gilt oder V gilt nicht” ist wahr.

$\iff$ “Falls A nicht gilt, so gilt auch V nicht” ist wahr.

Beweis durch Kontraposition

Seien V und A beliebige Aussagen. Dann gilt:

“Falls V gilt, so auch A” ist wahr.

$\iff$ “A gilt oder V gilt nicht” ist wahr.

$\iff$ “Falls A <u>nicht</u> gilt, so gilt auch V <u>nicht</u>” ist wahr.

Ansatz: Beweise einen Satz der Form

“Falls V gilt, so auch A.”

dadurch, zu zeigen dass folgendes gilt:

“Falls A <u>nicht</u> gilt, so kann auch V <u>nicht</u> gelten.”

Beweis durch Kontraposition

Seien V und A beliebige Aussagen. Dann gilt:

“Falls V gilt, so auch A” ist wahr.

$\iff$ “A gilt oder V gilt nicht” ist wahr.

$\iff$ “Falls A nicht gilt, so gilt auch V nicht” ist wahr.

Ansatz: Beweise einen Satz der Form

“Falls V gilt, so auch A.”

dadurch, zu zeigen dass folgendes gilt:

“Falls A nicht gilt, so kann auch V nicht gelten.”

Behauptung: Sei $n \in \mathbb{N}_{\geq 1}$ und seien $M_1, \ldots, M_n$ endliche Mengen. Dann gilt für jedes $k \in \mathbb{N}$: Falls

$$|M_1| + \cdots + |M_n| \quad > \quad k,$$

so existiert eine Menge $M \in \{M_1, \ldots, M_n\}$ mit $|M| > \frac{k}{n}$.

Beweis durch Widerspruch

Ziel:

Beweise einen Satz der Form

Falls die Voraussetzungen V erfüllt sind, so gilt auch Aussage A.

Beweis durch Widerspruch

Ziel:

Beweise einen Satz der Form

> Falls die Voraussetzungen V erfüllt sind, so gilt auch Aussage A.

Ansatz:

1. Nimm an, dass die Voraussetzungen V erfüllt sind,
   jedoch die Aussage A nicht gilt.
2. Leite daraus einen Widerspruch her.

Beweis durch Widerspruch

Ziel:

Beweise einen Satz der Form

Falls die Voraussetzungen V erfüllt sind, so gilt auch Aussage A.

Ansatz:

1. Nimm an, dass die Voraussetzungen V erfüllt sind,
   jedoch die Aussage A nicht gilt.
2. Leite daraus einen Widerspruch her.

Behauptung:

Sei ψ eine aussagenlogische Formel.

Falls $\varphi := (\psi \wedge \neg\psi)$, dann
gibt es keine Interpretation $\mathcal{I} : \mathsf{AS} \to \{0,1\}$ mit $\mathcal{I} \models \varphi$.

Beweis durch vollständige Induktion über $\mathbb{N}$: Grundidee

Für $n \in \mathbb{N}$ sei $A(n)$ eine Aussage über die Zahl n.

Ziel: Zeige, dass für jedes $n \in \mathbb{N}$ die Aussage $A(n)$ gilt.

Beweis durch vollständige Induktion über $\mathbb{N}$: Grundidee

Für $n \in \mathbb{N}$ sei $A(n)$ eine Aussage über die Zahl n.

Ziel: Zeige, dass für jedes $n \in \mathbb{N}$ die Aussage $A(n)$ gilt.

Ansatz: Nutze das Induktionsprinzip:

Induktionsanfang:
Zeige, dass $A(n)$ für die Zahl $n = 0$ gilt.

Induktionsschritt:
Zeige, dass für jede Zahl $n \in \mathbb{N}$ gilt:

$$\text{Falls } \underbrace{A(0), \ldots, A(n)}_{\text{Induktionsannahme}} \text{ gelten, so auch } A(n+1).$$

Beweis durch vollständige Induktion über $\mathbb{N}$: Grundidee

Induktionsanfang:

Zeige, dass $A(n)$ für die Zahl $n = 0$ gilt.

Induktionsschritt:

Zeige, dass für jede Zahl $n \in \mathbb{N}$ gilt:

Falls $A(0), \ldots, A(n)$ gelten, so auch $A(n+1)$.

Dann gilt:

$A(0)$ ist wahr gemäß Induktionsanfang.

Beweis durch vollständige Induktion über $\mathbb{N}$: Grundidee

Induktionsanfang:
Zeige, dass $A(n)$ für die Zahl $n = 0$ gilt.

Induktionsschritt:
Zeige, dass für jede Zahl $n \in \mathbb{N}$ gilt:

Falls $A(0), \ldots, A(n)$ gelten, so auch $A(n+1)$.

Dann gilt:

$A(0)$ ist wahr gemäß Induktionsanfang.

$A(1)$ ist wahr da $A(0)$ gilt und wegen dem Induktionsschritt für $n = 0$.

Beweis durch vollständige Induktion über $\mathbb{N}$: Grundidee

Induktionsanfang:
Zeige, dass $A(n)$ für die Zahl $n = 0$ gilt.

Induktionsschritt:
Zeige, dass für jede Zahl $n \in \mathbb{N}$ gilt:

Falls $A(0), \ldots, A(n)$ gelten, so auch $A(n+1)$.

Dann gilt:

$A(0)$ ist wahr gemäß Induktionsanfang.

$A(1)$ ist wahr da $A(0)$ gilt und wegen dem Induktionsschritt für $n = 0$.

$A(2)$ ist wahr da $A(0)$ und $A(1)$ gelten
und wegen dem Induktionsschritt für $n = 1$.

Beweis durch vollständige Induktion über $\mathbb{N}$: Grundidee

Induktionsanfang:
Zeige, dass $A(n)$ für die Zahl $n = 0$ gilt.

Induktionsschritt:
Zeige, dass für jede Zahl $n \in \mathbb{N}$ gilt:

$$\text{Falls } A(0), \ldots, A(n) \text{ gelten, so auch } A(n+1).$$

Dann gilt:

$A(0)$ ist wahr gemäß Induktionsanfang.

$A(1)$ ist wahr da $A(0)$ gilt und wegen dem Induktionsschritt für $n = 0$.

$A(2)$ ist wahr da $A(0)$ und $A(1)$ gelten
und wegen dem Induktionsschritt für $n = 1$.

$A(3)$ ist wahr da $A(0), A(1)$ und $A(2)$ gelten
und wegen dem Induktionsschritt für $n = 2$.

Beweis durch vollständige Induktion über $\mathbb{N}$: Grundidee

Induktionsanfang:
Zeige, dass $A(n)$ für die Zahl $n = 0$ gilt.

Induktionsschritt:
Zeige, dass für jede Zahl $n \in \mathbb{N}$ gilt:

Falls $A(0), \dots, A(n)$ gelten, so auch $A(n+1)$.

Dann gilt:

$A(0)$ ist wahr gemäß Induktionsanfang.

$A(1)$ ist wahr da $A(0)$ gilt und wegen dem Induktionsschritt für $n = 0$.

$A(2)$ ist wahr da $A(0)$ und $A(1)$ gelten
und wegen dem Induktionsschritt für $n = 1$.

$A(3)$ ist wahr da $A(0), A(1)$ und $A(2)$ gelten
und wegen dem Induktionsschritt für $n = 2$.

$A(4)$ ... *... und so weiter.*

Beweis durch vollständige Induktion über $\mathbb{N}$: Grundidee

Induktionsanfang:
Zeige, dass $A(n)$ für die Zahl $n = 0$ gilt.

Induktionsschritt:
Zeige, dass für jede Zahl $n \in \mathbb{N}$ gilt:

Falls $A(0), \ldots, A(n)$ gelten, so auch $A(n+1)$.

Dann gilt:

$A(0)$ ist wahr gemäß Induktionsanfang.

$A(1)$ ist wahr da $A(0)$ gilt und wegen dem Induktionsschritt für $n = 0$.

$A(2)$ ist wahr da $A(0)$ und $A(1)$ gelten
und wegen dem Induktionsschritt für $n = 1$.

$A(3)$ ist wahr da $A(0), A(1)$ und $A(2)$ gelten
und wegen dem Induktionsschritt für $n = 2$.

$A(4)$ ... *... und so weiter.*

Für alle $n \in \mathbb{N}$ gilt also:

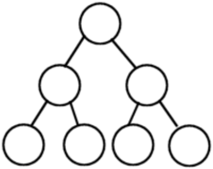
$A(n+1)$ ist wahr da $A(0), \ldots, A(n)$ gelten
und wegen dem Induktionsschritt für n.

Beweis durch vollständige Induktion über $\mathbb{N}$

Aufgabe 1

Zeige, dass für alle $n \in \mathbb{N}$ gilt:

$$\sum_{i=0}^{n} 2^i \quad = \quad 2^{n+1} - 1.$$

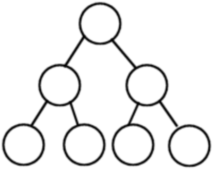


Beweis durch vollständige Induktion über $\mathbb{N}$

Aufgabe 1

Zeige, dass für alle $n \in \mathbb{N}$ gilt:

$$\sum_{i=0}^{n} 2^i \quad = \quad 2^{n+1} - 1.$$



Aufgabe 2

Zeige, dass für alle $x \in \mathbb{R}$ mit $x \geq -1$ und alle $n \in \mathbb{N}$ mit $n \geq 1$ gilt:

$$(1 + x)^n \quad \geq \quad 1 + n \cdot x.$$

Rekursive Definition von Mengen

Eine rekursive Definition einer Menge M besteht aus:

Basisregeln der Form "$m \in M$" und

Rekursive Definition von Mengen

Eine rekursive Definition einer Menge M besteht aus:

Basisregeln der Form "$m \in M$" und

Rekursiven Regeln der Form

"Sind $m_1, \ldots, m_k \in M$, dann ist auch $m \in M$",

wobei m von $m_1, \ldots, m_k$ abhängt.

Rekursive Definition von Mengen

Die Menge L aller Zeichenketten über dem Alphabet

$$A := \{\mathbf{x}, :=, +, -, \neq, ;, \mathbf{while}, \mathbf{do}, \mathbf{end}\} \cup \mathbb{N},$$

die syntaktisch korrekte WHILE-Programme sind, ist wie folgt definiert:

Rekursive Definition von Mengen

Die Menge L aller Zeichenketten über dem Alphabet

$$A \;:=\; \{\mathbf{x}, :=, +, -, \neq, ;, \mathbf{while}, \mathbf{do}, \mathbf{end}\} \cup \mathbb{N},$$

die syntaktisch korrekte WHILE-Programme sind, ist wie folgt definiert:

Basisregeln:

(B1) Für Zahlen $i, j, c \in \mathbb{N}$ gilt: $\mathbf{x}i := \mathbf{x}j + c \;\in L$.

(B2) Für Zahlen $i, j, c \in \mathbb{N}$ gilt: $\mathbf{x}i := \mathbf{x}j - c \;\in L$.

Rekursive Definition von Mengen

Die Menge L aller Zeichenketten über dem Alphabet

$$A := \{\mathbf{x}, :=, +, -, \neq, ;, \mathbf{while}, \mathbf{do}, \mathbf{end}\} \cup \mathbb{N},$$

die syntaktisch korrekte WHILE-Programme sind, ist wie folgt definiert:

Basisregeln:

(B1) Für Zahlen $i, j, c \in \mathbb{N}$ gilt: $\mathbf{x}i := \mathbf{x}j + c \in L$.

(B2) Für Zahlen $i, j, c \in \mathbb{N}$ gilt: $\mathbf{x}i := \mathbf{x}j - c \in L$.

Rekursive Regeln:

(R1) Sind $w_1 \in L$ und $w_2 \in L$, so ist auch $w_1; w_2 \in L$.

(R2) Ist $w \in L$ und $i \in \mathbb{N}$, so ist $\mathbf{while}\ \mathbf{x}i \neq \mathbf{0}\ \mathbf{do}\ w\ \mathbf{end} \in L$.

Rekursive Definition von Mengen

Zur Erinnerung: Definition von L:

Basisregeln:

(B1) Für Zahlen $i, j, c \in \mathbb{N}$ gilt:
$\mathbf{x}i := \mathbf{x}j + c \quad \in L$.

(B2) Für Zahlen $i, j, c \in \mathbb{N}$ gilt:
$\mathbf{x}i := \mathbf{x}j - c \quad \in L$.

Rekursive Regeln:

(R1) Sind $w_1 \in L$ und $w_2 \in L$, so ist auch
$w_1 ; w_2 \quad \in L$.

(R2) Ist $w \in L$ und $i \in \mathbb{N}$, so ist
$\mathbf{while}\ \mathbf{x}i \neq \mathbf{0}\ \mathbf{do}\ w\ \mathbf{end} \quad \in L$.

Aufgabe 3:

Welche der folgenden Zeichenketten gehört zur Menge L aller syntaktisch korrekten WHILE-Programme, welche nicht?

(1) $\mathbf{x}3 := \mathbf{x}7 - 2$

(2) $\mathbf{x}3 + 1; \mathbf{x}2 := \mathbf{x}3 + 5$

(3) $\mathbf{while}\ \mathbf{x}1 \neq 0\ \mathbf{do}\ \mathbf{x}0 := \mathbf{x}0 + 1; \mathbf{x}1 := \mathbf{x}1 - 1\ \mathbf{end}$

(4) $\mathbf{x}1 := \mathbf{x}1 + 42; \mathbf{while}\ \mathbf{x}1 \neq 0\ \mathbf{do}\ \mathbf{x}1 := \mathbf{x}1 - 1$

Rekursive Definition von Funktionen

Sei M eine rekursiv definierte Menge und sei P eine beliebige Menge.

Die rekursive Definition einer Funktion $f : M \to P$ sieht folgendermaßen aus:

Rekursive Definition von Funktionen

Sei M eine rekursiv definierte Menge und sei P eine beliebige Menge.

Die rekursive Definition einer Funktion $f: M \to P$ sieht folgendermaßen aus:

Rekursionsanfang:
Für jede Basisregel der Form "$m \in M$" in der Definition von M, definiere $f(m) \in P$.

Rekursive Definition von Funktionen

Sei M eine rekursiv definierte Menge und sei P eine beliebige Menge.

Die rekursive Definition einer Funktion $f\colon M \to P$ sieht folgendermaßen aus:

Rekursionsanfang:
Für jede Basisregel der Form "$m \in M$" in der Definition von M, definiere $f(m) \in P$.

Rekursionsschritt:
Für jede rekursive Regel der Form

"Sind $m_1, \ldots, m_k \in M$, dann ist auch $m \in M$"

in der Definition von M, definiere $f(m) \in P$ aus $f(m_1), \ldots, f(m_k)$.

Rekursive Definition von Funktionen

Zur Erinnerung: *Definition von L:*

Basisregeln:

(B1) Für Zahlen $i, j, c \in \mathbb{N}$ gilt:
$\mathbf{x}i := \mathbf{x}j + c \;\in L$.

(B2) Für Zahlen $i, j, c \in \mathbb{N}$ gilt:
$\mathbf{x}i := \mathbf{x}j - c \;\in L$.

Rekursive Regeln:

(R1) Sind $w_1 \in L$ und $w_2 \in L$, so ist auch
$w_1; w_2 \;\in L$.

(R2) Ist $w \in L$ und $i \in \mathbb{N}$, so ist
$\textbf{while } \mathbf{x}i \neq \mathbf{0} \textbf{ do } w \textbf{ end} \;\in L$.

Aufgabe 4:

Definiere Funktionen $f : L \to \mathbb{N}$ und $g : L \to \mathbb{N}$ rekursiv, so dass für alle $w \in L$ gilt:

$$f(w) := \text{Anzahl der “:=” in } w,$$

$$g(w) := \text{Anzahl der “;” in } w.$$

Rekursive Definition von Funktionen

Zur Erinnerung: Definition von L:

Basisregeln:

(B1) Für Zahlen $i, j, c \in \mathbb{N}$ gilt:
$\mathbf{x}i := \mathbf{x}j + c \;\; \in L$.

(B2) Für Zahlen $i, j, c \in \mathbb{N}$ gilt:
$\mathbf{x}i := \mathbf{x}j - c \;\; \in L$.

Rekursive Regeln:

(R1) Sind $w_1 \in L$ und $w_2 \in L$, so ist auch
$w_1 ; w_2 \;\; \in L$.

(R2) Ist $w \in L$ und $i \in \mathbb{N}$, so ist
$\textbf{while } \mathbf{x}i \neq \mathbf{0} \textbf{ do } w \textbf{ end} \;\; \in L$.

Aufgabe 4:

Definiere Funktionen $f : L \to \mathbb{N}$ und $g : L \to \mathbb{N}$ rekursiv, so dass für alle $w \in L$ gilt:

$$f(w) \; := \; \text{Anzahl der “$:=$” in } w,$$

$$g(w) \; := \; \text{Anzahl der “;” in } w.$$

Aufgabe 5:

Zeige, dass für alle $w \in L$ gilt:

$$f(w) \; = \; g(w) + 1.$$

Hinweis: Damit zeigen wir auch, dass (2) in Aufgabe 3 nicht in L ist.

Rekursive Definition von Funktionen

Notation:
Für eine Menge M schreiben wir 2^M oder $\mathcal{P}(M)$ um die Potenzmenge von M zu bezeichnen, d.h. die Menge aller Teilmengen von M.

Aufgabe 6:

Gib die rekursive Definition einer Funktion $as\colon \mathrm{AL} \to \mathcal{P}(\mathrm{AS})$ an, so dass für alle $\varphi \in \mathrm{AL}$ gilt:

$$as(\varphi) \;= \{X : X \text{ ist ein Aussagensymbol, das in } \varphi \text{ vorkommt}\}.$$

Rekursive Definition von Funktionen

Notation:
Für eine Menge M schreiben wir 2^M oder $\mathcal{P}(M)$ um die Potenzmenge von M zu bezeichnen, d.h. die Menge aller Teilmengen von M.

Aufgabe 6:
Gib die rekursive Definition einer Funktion $as\colon \mathrm{AL} \to \mathcal{P}(\mathrm{AS})$ an, so dass für alle $\varphi \in \mathrm{AL}$ gilt:

$$as(\varphi) = \{X : X \text{ ist ein Aussagensymbol, das in } \varphi \text{ vorkommt}\}.$$

Aufgabe 7: *("Koinzidenzlemma für AL")*
Zeige, dass für alle $\varphi \in \mathrm{AL}$ gilt:
Sind $\mathcal{I}_1, \mathcal{I}_2 \colon \mathrm{AS} \to \{0,1\}$ Interpretationen mit

$$\mathcal{I}_1(X) \quad = \quad \mathcal{I}_2(X) \quad \text{für alle } X \in as(\varphi),$$

dann ist $[\![\varphi]\!]^{\mathcal{I}_1} = [\![\varphi]\!]^{\mathcal{I}_2}$.