Logik für Informatiker

1. Grundlegende Beweisstrategien: Teil 2

22.04.2012

Viorica Sofronie-Stokkermans

Universität Koblenz-Landau

e-mail: sofronie@uni-koblenz.de

Organisatorisches

Dienstags: M 001.

Letzte Vorlesung

1. Grundlegende Beweisstrategien

- Direkter Beweis
- Beweis durch Kontraposition:

  Um zu beweisen, dass $A \rightarrow B$, zeige dass $\neg B \rightarrow \neg A$.
- Beweis durch Widerspruch:

  Um zu beweisen, dass $A \rightarrow B$, zeige dass $A \wedge \neg B \rightarrow$ falsch
- Äquivalenzbeweis

  Um zu beweisen dass ($A \Leftrightarrow B$) (A genau dann, wenn B)

  Beweise dass $A \rightarrow B$ und dass $B \rightarrow A$.
- Beweis durch Fallunterscheidung

  Um B zu beweisen, beweise dass $A_1 \rightarrow B, \dots, A_n \rightarrow B$,

wobei $A_1 \vee \dots \vee A_n \equiv$ wahr

Letzte Vorlesung

Grundlegende Beweisstrategien

Aussagen mit Quantoren:

- $\forall x \in U : A(x)$

  Wähle a beliebig aus U.
  Beweise $A(a)$.
  Da a beliebig gewählt werden kann, folgt $\forall x \in U : A(x)$

- $\exists x \in U : A(x)$

  Sei a ein geeignetes Element aus U.
  Beweise, dass $A(a)$.
  Damit folgt $\exists x \in U : A(x)$.

- Ähnlich für $\forall x \in U \;\; \exists y \in U : A(x, y)$

Letzte Vorlesung

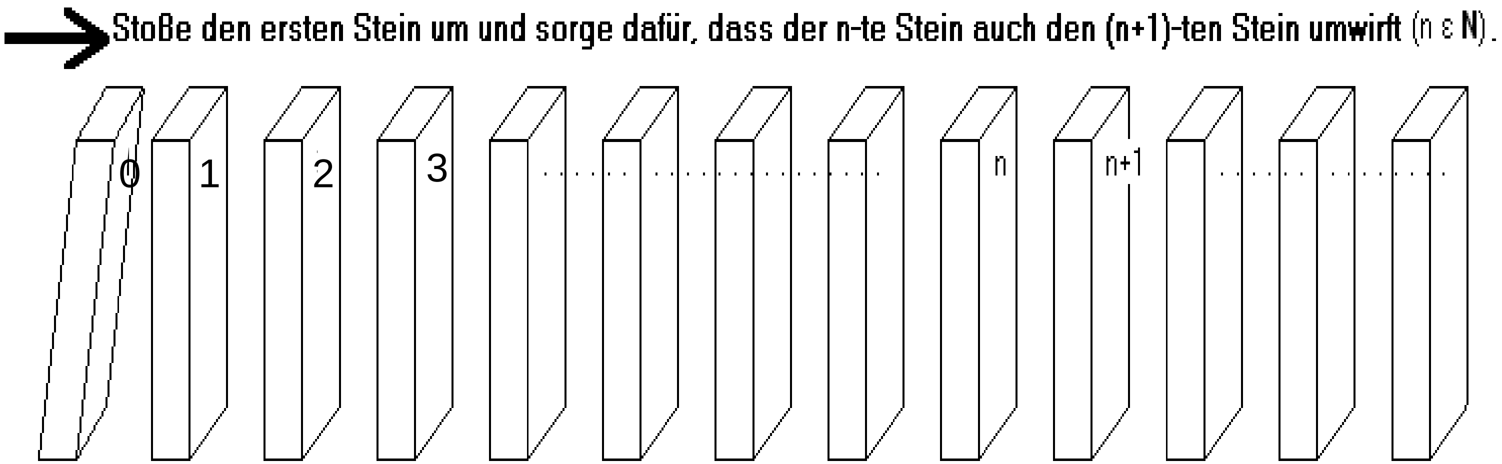
- **Induktion über die natürlichen Zahlen $\mathbb{N}$**

(1)	Induktionsbasis:	Beweise $p(0)$
(2)	Induktionsvoraussetzung:	Für ein beliebig gewähltes $n \in \mathbb{N}$ gilt $p(n)$
(3)	Induktionsschluss:	Folgere $p(n+1)$ aus der Induktionsvoraussetzung $p(n)$

Letzte Vorlesung

- **Induktion über die natürlichen Zahlen $\mathbb{N}$**

(1)	Induktionsbasis:	Beweise $p(0)$
(2)	Induktionsvoraussetzung:	Für ein beliebig gewähltes $n \in \mathbb{N}$ gilt $p(n)$
(3)	Induktionsschluss:	Folgere $p(n+1)$ aus der Induktionsvoraussetzung $p(n)$



Letzte Vorlesung

- **Induktion über die natürlichen Zahlen $\mathbb{N}$**

- **Verallgemeinerte vollständige Induktion**

  Gelten die beiden Aussagen:

  $$p(0) \quad \text{und}$$
  $$\forall n \in \mathbb{N} : p(0) \wedge p(1) \wedge \cdots \wedge p(n) \rightarrow p(n+1)$$

  dann gilt die Aussage $\forall n \in \mathbb{N} : p(n)$.

Induktionsvoraussetzung:	Für ein beliebig gewähltes $n \in \mathbb{N}$, gilt $p(k)$ für alle $k < n$
Induktionsschluss:	Folgere $p(n)$ aus der Induktionsvoraussetzung

Fehlerquellen

Häufige Fehler bei Induktionsbeweisen

- es gibt unendliche absteigende Ketten $x_1 > x_2 > \ldots$
- Induktionsanfäng inkorrekt
- Bei Induktionsschritt die Grenzfälle nicht bedacht

Fehlerquellen

Was ist hier falsch?

Behauptung: Alle Menschen haben die gleiche Haarfarbe

Fehlerquellen

Was ist hier falsch?

Behauptung: Alle Menschen haben die gleiche Haarfarbe

$p(n)$: In einer Menge von n Menschen haben alle die gleiche Haarfarbe

Fehlerquellen

Was ist hier falsch?

Behauptung: Alle Menschen haben die gleiche Haarfarbe

$p(n)$: In einer Menge von n Menschen haben alle die gleiche Haarfarbe

Induktionbasis: $n = 1$

Für eine Menge mit nur einem Menschen gilt die Behauptung trivial

Fehlerquellen

Was ist hier falsch?

Behauptung: Alle Menschen haben die gleiche Haarfarbe

$p(n)$: In einer Menge von n Menschen haben alle die gleiche Haarfarbe

Induktionsvoraussetzung: $p(n)$ wahr.

Induktionsschritt: Beweise, dass aus $p(n)$, $p(n+1)$ folgt.

$n+1$ Menschen werden in eine Reihe gestellt.

Der Mensch links außen wird rausgeschickt. Es bleiben nur n Menschen.

Nun kann die Induktionsbehauptung angewendet werden und alle verbliebenen haben die gleiche Haarfarbe (mit dem rechts außen).

Fehlerquellen

Was ist hier falsch?

Behauptung: Alle Menschen haben die gleiche Haarfarbe

$p(n)$: In einer Menge von n Menschen haben alle die gleiche Haarfarbe

Induktionsvoraussetzung: $p(n)$ wahr.

Induktionsschritt: Beweise, dass aus $p(n)$, $p(n+1)$ folgt.

$n+1$ Menschen werden in eine Reihe gestellt.

Der Mensch rechts außen wird rausgeschickt. Es bleiben nur n Menschen. Die Induktionsbehauptung kann angewendet werden und alle verbliebenen haben die gleiche Haarfarbe (mit dem links außen).

Also haben die beiden außen die gleiche Haarfarbe, wie die in der Mitte, und die haben auch alle die gleiche Haarfarbe

Also haben alle $n+1$ Menschen die gleiche Haarfarbe.

Strukturelle Induktion

Bei der vollständigen Induktion werden Eigenschaften der natürlichen Zahlen bewiesen.

Bei der strukturellen Induktion werden Eigenschaften für Mengen bewiesen, deren Elemente aus Grundelementen durch eine endliche Anzahl von Konstruktionsschritten (unter Verwendung bereits konstruierter Elemente) bzw. mittels eines Erzeugungssystems entstehen.

Induktive Definitionen

Induktive Definition von Mengen:

Induktive Definition einer Menge M aus einer Basismenge B mit "Konstruktoren" in Σ.

(Konstruktoren sind Funktionssymbole; für $f \in \Sigma$, $a(f) \in \mathbb{N}$ ist die Stelligkeit von f.)

Basismenge:	B
Erzeugungsregel:	Wenn $f \in \Sigma$ mit Stelligkeit n und $e_1, \dots, e_n \in M$, dann gilt $f(e_1, \dots, e_n) \in M$.

M ist die kleinste Menge,

- die die Basismenge B enthält,
- mit der Eigenschaft, dass für alle $f \in \Sigma$ mit Stelligkeit n und alle $e_1, \dots, e_n \in M$: $f(e_1, \dots, e_n) \in M$.

Induktive Definitionen: Beispiele

(1) Menge $\mathbb{N}$ aller natürlichen Zahlen

Basismenge:	0
Erzeugungsregel:	Wenn $n \in \mathbb{N}$, dann gilt $n + 1 \in \mathbb{N}$

$\mathbb{N}$ ist die kleinste aller Mengen A mit folgenden Eigenschaften:

(1) A enthält 0;

(2) für alle Elemente n, falls $n \in A$ so $n + 1 \in A$.

Das bedeutet, dass:

(1) $0 \in \mathbb{N}$

(2) Falls $n \in \mathbb{N}$ so $n + 1 \in \mathbb{N}$.

(3) Für jede Menge A mit Eigenschaften (1) und (2) gilt: $\mathbb{N} \subseteq A$.

Induktive Definitionen: Beispiele

(2) Menge Σ^* aller Wörter über ein Alphabet Σ

Basismenge:	Das leere Wort $\epsilon \in \Sigma^*$
Erzeugungsregel:	Wenn $w \in \Sigma^*$ und $a \in \Sigma$,
	dann gilt $wa \in \Sigma^*$

Σ^* ist die kleinste aller Mengen A mit folgenden Eigenschaften:

(1) A enthält das leere Wort ϵ

(2) für alle Elemente w, falls $w \in A$ und $a \in \Sigma$, so $wa \in A$.

Das bedeutet, dass:

(1) $\epsilon \in \Sigma^*$

(2) Falls $w \in \Sigma^*$ und $a \in \Sigma$ so $wa \in \Sigma^*$.

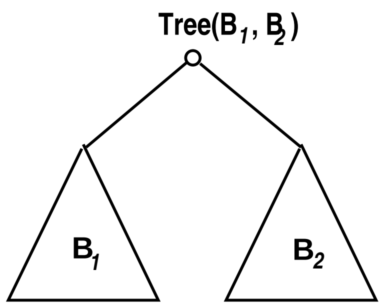
(3) Für jede Menge A mit Eigenschaften (1) und (2) gilt: $\Sigma^* \subseteq A$.

Induktive Definitionen: Beispiele

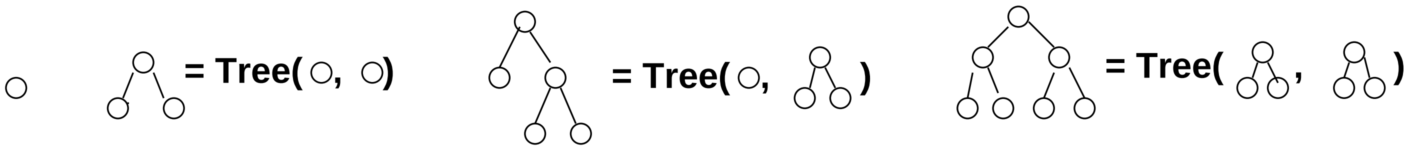
(3) Bin : die Menge aller (vollständigen) binären Bäume

Basismenge: $\circ$ Baum mit nur einem Knoten.

Erzeugungsregel: Wenn $B_1, B_2 \in$ Bin, dann ist auch
Tree$(B_1, B_2) \in$ Bin.



Beispiele:



Induktive Definitionen: Beispiele

(3) Bin : die Menge aller (vollständigen) binären Bäume

Basismenge: $\circ$ Baum mit nur einem Knoten.

Erzeugungsregel: Wenn $B_1, B_2 \in$ Bin, dann ist auch
Tree$(B_1, B_2) \in$ Bin.

Bin ist die kleinste aller Mengen A mit folgenden Eigenschaften:

(1) A enthält der Baum mit nur einem Knoten $\circ$.

(2) für alle Elemente B_1, B_2, falls $B_1, B_2 \in A$ so Tree$(B_1, B_2) \in A$.

Das bedeutet, dass:

(1) $\circ \in$ Bin

(2) Falls $B_1, B_2 \in$ Bin so Tree$(B_1, B_2) \in$ Bin.

(3) Für jede Menge A mit Eigenschaften (1) und (2) gilt: Bin $\subseteq A$.

Induktive Definitionen: Beispiele

(4) Menge aller aussagenlogischen Formeln

Basismenge: $\perp$ (falsch), $\top$ (wahr), $P_0, P_1, P_2, \ldots$ sind aussagenlogische Formeln (atomare Formeln)

Erzeugungsregel: Wenn F_1, F_2 aussagenlogische Formeln sind, dann sind auch $\neg F_1$, $F_1 \wedge F_2$, $F_1 \vee F_2$, $F_1 \rightarrow F_2$, $F_1 \leftrightarrow F_2$ aussagenlogische Formeln

Induktive Definitionen

Induktive Definition von Mengen:

Induktive Definition einer Menge M aus einer Basismenge B mit Operationssymbole ("Konstruktoren") Σ (wobei $a(f)$ Stelligkeit von f für $f \in \Sigma$).

Basismenge:	B
Erzeugungsregel:	Wenn $f \in \Sigma$ mit Stelligkeit n und $e_1, \dots, e_n \in M$, dann gilt $f(e_1, \dots, e_n) \in M$.

M ist die kleinste aller Mengen A mit folgenden Eigenschaften:

(1) A enthält die Basismenge B

(2) für alle Elemente $e_1, \dots, e_n \in A$, und alle $f \in \Sigma$ (mit Stelligkeit n), ist auch $f(e_1, \dots, e_n)$ in A.

Dass bedeutet, dass:

(1) $B \subseteq M$

(2) Falls $e_1, \dots, e_n \in M$ und $f \in \Sigma$ (mit Stelligkeit n), so $f(e_1, \dots, e_n) \in M$.

(3) Für jede Menge A mit Eigenschaften (1) und (2) gilt: $M \subseteq A$.

Strukturelle Induktion

Zu zeigen: $\forall x \in M : P(x)$

(1) **Induktionsbasis:** Beweise, dass für alle $b \in \mathrm{B}$, $P(b)$ gilt.

(2) Sei $e \in M$, $e \notin B$.

Dann $e = f(e_1, \ldots, e_n)$, mit $f \in \Sigma$ und $e_1, \ldots, e_n \in M$.

Induktionsvoraussetzung: Wir nehmen an, dass $P(e_1), \ldots, P(e_n)$ gelten.

Induktionsschluss: Folgere, dass $P(e)$ gilt.

Strukturelle Induktion

Satz. Falls:

(1) bewiesen werden kann, dass für alle $b \in \mathrm{B}$, $P(b)$ gilt. (Induktionsbasis)

(2) falls $e = f(e_1, \dots, e_n)$ mit $f \in \Sigma$
unter der Annahme dass $P(e_1), \dots, P(e_n)$ gelten (Induktionsvoraussetzung)
wir beweisen können, dass auch $P(e)$ gilt (Induktionsschritt)

Dann gilt $P(m)$ für alle $m \in M$.

Beweis: Sei $A = \{e \mid P(e) \text{ wahr }\}$.

(1) Da bewiesen werden kann, dass für alle $b \in \mathrm{B}$, $P(b)$ gilt, wissen wir, dass A die Basismenge B enthält.

(2) Da wir, aus der Annahme dass $P(e_1), \dots, P(e_n)$ wahr sind, beweisen können, dass auch $P(e)$ wahr ist, wissen wir, dass
falls $e_1, \dots, e_n \in A$, und $f \in \Sigma$ (mit Stelligkeit n), so $f(e_1, \dots, e_n)$ in A.

Da M die kleinste aller Mengen mit Eigenschaften (1) und (2) ist, folgt, dass $M \subseteq A = \{e \mid P(e) \text{ wahr }\}$, d.h. $\forall m \in M, P(m)$ wahr.

Beispiel

Σ^* : die Menge aller Wörter über ein Alphabet Σ

Basismenge:	Das leere Wort $\epsilon \in \Sigma^*$
Erzeugungsregel:	Wenn $w \in \Sigma^*$ und $a \in \Sigma$,
	dann gilt $wa \in \Sigma^*$

Sei die Umkehrung (Reverse) eines Wortes wie folgt definiert:

$\text{rev}(\epsilon) = \epsilon$

$\text{rev}(wa) = a\ \text{rev}(w)$ mit $w \in \Sigma^*$ und $a \in \Sigma$.

Beispiel

Zu zeigen: $\forall w_1, w_2 \in \Sigma^*, \text{rev}(w_1 w_2) = \text{rev}(w_2) rev(\text{w}_1)$

Sei $w_1 \in \Sigma^*$, beliebig.

Zu zeigen: $\forall w_2 \in \Sigma^*, p(w_2)$ wobei: $p(w_2)$: $\text{rev}(w_1 w_2) = \text{rev}(w_2)\text{rev}(w_1)$

Induktion über die Struktur von w_2.

(1) **Induktionsbasis:** Wir zeigen, dass die Eigenschaft gilt für $w_2 = \epsilon$
(d.h. dass $P(\epsilon) : \text{rev}(w_1\epsilon) = \text{rev}(\epsilon)\text{rev}(w_1)$ wahr ist).

Beweis: $\text{rev}(w_1\epsilon) = \text{rev}(w_1) = \epsilon rev(w_1) = \text{rev}(\epsilon) rev(w_1)$.

Beispiel

Zu zeigen: $\forall w_1, w_2 \in \Sigma, \text{rev}(w_1 w_2) = \text{rev}(w_2) rev(\text{w}_1)$

Sei $w_1 \in \Sigma^*$, beliebig.

$\boxed{\text{Zu zeigen: } \forall w_2 \in \Sigma, p(w_2) \qquad \text{wobei: } p(w_2): \quad \text{rev}(w_1 w_2) = \text{rev}(w_2)\text{rev}(w_1)}$

(2) Sei $w_2 \in \Sigma^*$, $w_2 \neq \epsilon$. Dann $w_2 = wa$.

Induktionsvoraussetzung: Wir nehmen an, dass $p(w)$ gilt,
d.h. dass $\text{rev}(w_1 w) = \text{rev}(w) rev(\text{w}_1)$.

Induktionsschluss: Wir beweisen, dass dann $p(w_2)$ gilt.

$$
\begin{aligned}
\text{rev}(w_1 w_2) &= \text{rev}(w_1(wa)) = \text{rev}((w_1 w)a) = a\ \text{rev}(w_1 w) && \text{(Definition von rev)}\\
&= a\ \text{rev}(w)\text{rev}(w_1) && \text{(Induktionsvoraussetzung)}\\
&= (a\ \text{rev}(w))\text{rev}(w_1) = \text{rev}(wa)\text{rev}(w_1) && \text{(Definition von rev)}\\
&= \text{rev}(w_2)\text{rev}(w_1)
\end{aligned}
$$

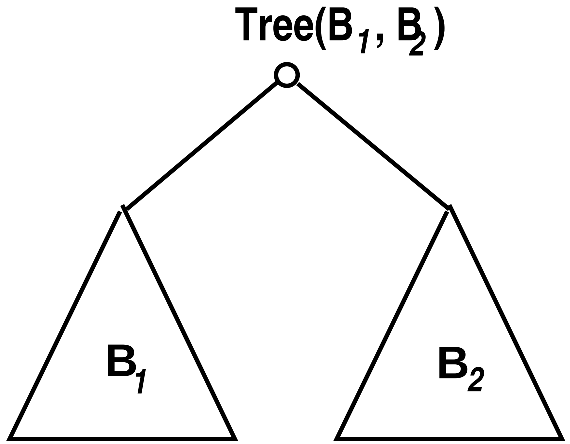
Beispiel 2

Bin : Menge allen (vollständigen) binären Bäume

Basismenge: $\circ$ Baum mit nur einem Knoten.

Erzeugungsregel: Wenn $B_1, B_2 \in$ Bin, dann ist auch

Tree$(B_1, B_2) \in$ Bin.



Beispiel 2

Behauptung:
Für alle $B \in \text{Bin}$, falls B n Blätter hat, so besitzt B genau $n-1$ innere Knoten.

$P(B)$:	Falls B $n \geq 1$ Blätter hat, dann besitzt B genau $n-1$ innere Knoten.

(1) **Induktionsbasis:** Wir zeigen, dass $P(B)$ gilt wenn B nur aus einem Knoten $\circ$ besteht.

Beweis: Sei B Baum, der nur aus einem Knoten besteht.
Dann besteht T nur aus einem Blatt, und B hat keinen inneren Knoten. d.h. $P(B)$ gilt.

Beispiel 2 ... ctd.

(2) Sei $B \in \text{Bin}$, B nicht in der Basismenge, d.h. $B = \mathit{Tree}(B_1, B_2)$.

Induktionsvoraussetzung: Wir nehmen an, dass $P(B_1), P(B_2)$ gelten.

Induktionsschluss: Wir beweisen, dass $P(B)$ gilt.

Beweis: Sei $B = \mathit{Tree}(B_1, B_2)$. Dann gilt:

- $n = n_1 + n_2$, wobei n, n_1, n_2 Anzahl der Blätter von B, B_1 bzw. B_2 sind.
- mit m, m_1, m_2 als Anzahl innerer Knoten von B, B_1 bzw. B_2:

$$\begin{array}{lcll} m & = & 1 + m_1 + m_2 & \text{nach Definition von } B = \mathit{Tree}(B_1, B_2) \\ & = & 1 + (n_1 - 1) + (n_2 - 1) & \text{nach Induktionsvoraussetzung} \\ & = & (n_1 + n_2) - 1 = n - 1. & \end{array}$$

Somit ist es bewiesen, dass $\forall B \in \text{Bin}, P(B)$ gilt.

Zusammenfassung

- Grundlegende Beweisstrategien
- Induktion über die natürlichen Zahlen
- Fehlerquellen
- Strukturelle Induktion