

Theorie der Informatik

2. Beweistechniken

Malte Helmert Gabriele Röger

Universität Basel

18. Februar 2015

Beweis

Beweis

Ein **Beweis** leitet die Korrektheit einer mathematischen Aussage aus einer Menge von **Axiomen** und **bereits bewiesenen Aussagen** her. Er besteht aus einer Reihe von **Beweisschritten**, von denen jeder **unmittelbar** aus den gegebenen Voraussetzungen und den bisherigen Schritten einsehbar ist.

Beweis

Beweis

Ein **Beweis** leitet die Korrektheit einer mathematischen Aussage aus einer Menge von **Axiomen** und **bereits bewiesenen Aussagen** her. Er besteht aus einer Reihe von **Beweisschritten**, von denen jeder **unmittelbar** aus den gegebenen Voraussetzungen und den bisherigen Schritten einsehbar ist.

Beweistechniken

- Direkter Beweis
- Indirekter Beweis, Beweis durch Widerspruch
- Vollständige Induktion
- ...

Direkter Beweis

Direkter Beweis

Direkter Beweis

Direkte Ableitung der Aussage durch Folgern oder Umformen.

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis.

Wir zeigen zunächst, dass $x \in A \cap (B \cup C)$ impliziert, dass $x \in (A \cap B) \cup (A \cap C)$ (Hinrichtung, $\Rightarrow$):

...

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis.

Wir zeigen zunächst, dass $x \in A \cap (B \cup C)$ impliziert, dass $x \in (A \cap B) \cup (A \cap C)$ (Hinrichtung, $\Rightarrow$):

Sei $x \in A \cap (B \cup C)$. Dann gilt $x \in A$ und $x \in B \cup C$.

...

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis.

Wir zeigen zunächst, dass $x \in A \cap (B \cup C)$ impliziert, dass $x \in (A \cap B) \cup (A \cap C)$ (Hinrichtung, $\Rightarrow$):

Sei $x \in A \cap (B \cup C)$. Dann gilt $x \in A$ und $x \in B \cup C$.

Falls $x \in B$, so gilt mit $x \in A$, dass $x \in A \cap B$.

...

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis.

Wir zeigen zunächst, dass $x \in A \cap (B \cup C)$ impliziert, dass $x \in (A \cap B) \cup (A \cap C)$ (Hinrichtung, $\Rightarrow$):

Sei $x \in A \cap (B \cup C)$. Dann gilt $x \in A$ und $x \in B \cup C$.

Falls $x \in B$, so gilt mit $x \in A$, dass $x \in A \cap B$.

Sonst gilt wegen $x \in B \cup C$, dass $x \in C$ und daher mit $x \in A$, dass $x \in A \cap C$.

...

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis.

Wir zeigen zunächst, dass $x \in A \cap (B \cup C)$ impliziert, dass $x \in (A \cap B) \cup (A \cap C)$ (**Hinrichtung, $\Rightarrow$**):

Sei $x \in A \cap (B \cup C)$. Dann gilt $x \in A$ und $x \in B \cup C$.

Falls $x \in B$, so gilt mit $x \in A$, dass $x \in A \cap B$.

Sonst gilt wegen $x \in B \cup C$, dass $x \in C$ und daher mit $x \in A$, dass $x \in A \cap C$.

In jedem Fall gilt $x \in A \cap B$ oder $x \in A \cap C$ und wir schliessen, dass $x \in (A \cap B) \cup (A \cap C)$

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis (Fortsetzung).

Für die **Rückrichtung** ($\Leftarrow$) zeigen wir, dass aus $x \in (A \cap B) \cup (A \cap C)$ folgt, dass $x \in A \cap (B \cup C)$.

Sei $x \in (A \cap B) \cup (A \cap C)$.

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis (Fortsetzung).

Für die **Rückrichtung** ($\Leftarrow$) zeigen wir, dass aus $x \in (A \cap B) \cup (A \cap C)$ folgt, dass $x \in A \cap (B \cup C)$.

Sei $x \in (A \cap B) \cup (A \cap C)$.

Falls $x \in A \cap B$, gilt $x \in A$ und $x \in B$. Aus letzterem folgt, dass $x \in B \cup C$ und damit insgesamt, dass $x \in A \cap (B \cup C)$.

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis (Fortsetzung).

Für die **Rückrichtung** ($\Leftarrow$) zeigen wir, dass aus $x \in (A \cap B) \cup (A \cap C)$ folgt, dass $x \in A \cap (B \cup C)$.

Sei $x \in (A \cap B) \cup (A \cap C)$.

Falls $x \in A \cap B$, gilt $x \in A$ und $x \in B$. Aus letzterem folgt, dass $x \in B \cup C$ und damit insgesamt, dass $x \in A \cap (B \cup C)$.

Falls $x \notin A \cap B$, gilt wegen $x \in (A \cap B) \cup (A \cap C)$, dass $x \in A \cap C$. Dann gilt (analog zu vorher) $x \in A$ und $x \in B \cup C$ und somit $x \in A \cap (B \cup C)$.

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis (Fortsetzung).

Für die **Rückrichtung** ($\Leftarrow$) zeigen wir, dass aus $x \in (A \cap B) \cup (A \cap C)$ folgt, dass $x \in A \cap (B \cup C)$.

Sei $x \in (A \cap B) \cup (A \cap C)$.

Falls $x \in A \cap B$, gilt $x \in A$ und $x \in B$. Aus letzterem folgt, dass $x \in B \cup C$ und damit insgesamt, dass $x \in A \cap (B \cup C)$.

Falls $x \notin A \cap B$, gilt wegen $x \in (A \cap B) \cup (A \cap C)$, dass $x \in A \cap C$. Dann gilt (analog zu vorher) $x \in A$ und $x \in B \cup C$ und somit $x \in A \cap (B \cup C)$.

In jedem Fall impliziert $x \in (A \cap B) \cup (A \cap C)$, dass $x \in A \cap (B \cup C)$.

...

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis (Fortsetzung).

Wir haben gezeigt, dass jedes Element von $A \cap (B \cup C)$ auch Element von $(A \cap B) \cup (A \cap C)$ ist und umgekehrt. Damit sind die Mengen gleich. □

Direkter Beweis: Beispiel

Satz

Für beliebige Mengen A, B, C gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Beweis.

Alternativ:

$$\begin{aligned} A \cap (B \cup C) &= \{x \mid x \in A \text{ und } x \in B \cup C\} \\ &= \{x \mid x \in A \text{ und } (x \in B \text{ oder } x \in C)\} \\ &= \{x \mid (x \in A \text{ und } x \in B) \text{ oder } (x \in A \text{ und } x \in C)\} \\ &= \{x \mid x \in A \cap B \text{ oder } x \in A \cap C\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned}$$



Fragen



Fragen?

Indirekter Beweis

Indirekter Beweis

Indirekter Beweis

- **Annahme**: Gegenteil der Behauptung ist wahr
- Herleitung eines **Widerspruchs** aus Annahme, Axiomen und bewiesenen Aussagen durch Folgern oder Umformen
- Da Annahme falsch ist, ist ursprüngliche Aussage korrekt.

Indirekter Beweis: Beispiel

Eine Primzahl ist eine Zahl $p \in \mathbb{N}_1$, die genau zwei natürliche Zahlen als Teiler hat.

Satz

Es gibt unendlich viele Primzahlen.

Indirekter Beweis: Beispiel

Eine Primzahl ist eine Zahl $p \in \mathbb{N}_1$, die genau zwei natürliche Zahlen als Teiler hat.

Satz

Es gibt unendlich viele Primzahlen.

Beweis.

Annahme: Es gibt nur endlich viele Primzahlen.



Indirekter Beweis: Beispiel

Eine Primzahl ist eine Zahl $p \in \mathbb{N}_1$, die genau zwei natürliche Zahlen als Teiler hat.

Satz

Es gibt unendlich viele Primzahlen.

Beweis.

Annahme: Es gibt nur endlich viele Primzahlen.

Sei $P = \{p_1, \dots, p_n\}$ die Menge aller Primzahlen.

Definiere $m = p_1 \cdot \dots \cdot p_n + 1$.



Indirekter Beweis: Beispiel

Eine Primzahl ist eine Zahl $p \in \mathbb{N}_1$, die genau zwei natürliche Zahlen als Teiler hat.

Satz

Es gibt unendlich viele Primzahlen.

Beweis.

Annahme: Es gibt nur endlich viele Primzahlen.

Sei $P = \{p_1, \dots, p_n\}$ die Menge aller Primzahlen.

Definiere $m = p_1 \cdot \dots \cdot p_n + 1$.

Da $m \notin P$, ist m keine Primzahl und hat daher einen Primteiler p .



Indirekter Beweis: Beispiel

Eine Primzahl ist eine Zahl $p \in \mathbb{N}_1$, die genau zwei natürliche Zahlen als Teiler hat.

Satz

Es gibt unendlich viele Primzahlen.

Beweis.

Annahme: Es gibt nur endlich viele Primzahlen.

Sei $P = \{p_1, \dots, p_n\}$ die Menge aller Primzahlen.

Definiere $m = p_1 \cdot \dots \cdot p_n + 1$.

Da $m \notin P$, ist m keine Primzahl und hat daher einen Primteiler p .

Da p eine Primzahl ist, muss p in P sein.



Indirekter Beweis: Beispiel

Eine Primzahl ist eine Zahl $p \in \mathbb{N}_1$, die genau zwei natürliche Zahlen als Teiler hat.

Satz

Es gibt unendlich viele Primzahlen.

Beweis.

Annahme: Es gibt nur endlich viele Primzahlen.

Sei $P = \{p_1, \dots, p_n\}$ die Menge aller Primzahlen.

Definiere $m = p_1 \cdot \dots \cdot p_n + 1$.

Da $m \notin P$, ist m keine Primzahl und hat daher einen Primteiler p .

Da p eine Primzahl ist, muss p in P sein.

Die Zahl m ist durch keines der $p_1, \dots, p_n$ ohne Rest teilbar.

$\rightsquigarrow$ **Widerpruch**



Fragen



Fragen?

Vollständige und strukturelle Induktion

Vollständige Induktion über die natürlichen Zahlen

Vollständige Induktion (über die natürlichen Zahlen)

Beweis einer Aussage für alle natürlichen Zahlen n mit $n \geq m$

- **Induktionsanfang** (IA): Beweis der Aussage für $n = m$
- **Induktionsvoraussetzung** (IV):
Aussage gilt für alle k mit $m \leq k \leq n$
- **Induktionsschritt** (IS): Beweis der Aussage für $n + 1$ unter Verwendung der Induktionsannahme

Vollständige Induktion: Beispiel I

Satz

Für alle natürlichen Zahlen $n \geq 1$ gilt $\sum_{k=1}^n (2k - 1) = n^2$.

Vollständige Induktion: Beispiel I

Satz

Für alle natürlichen Zahlen $n \geq 1$ gilt $\sum_{k=1}^n (2k - 1) = n^2$.

Beweis.

Vollständige Induktion über n :

IA $n = 1$: $\sum_{k=1}^1 (2k - 1) = 2 - 1 = 1 = 1^2$



Vollständige Induktion: Beispiel I

Satz

Für alle natürlichen Zahlen $n \geq 1$ gilt $\sum_{k=1}^n (2k - 1) = n^2$.

Beweis.

Vollständige Induktion über n :

IA $n = 1$: $\sum_{k=1}^1 (2k - 1) = 2 - 1 = 1 = 1^2$

IV: Für $1 \leq m \leq n$ gilt $\sum_{k=1}^m (2k - 1) = m^2$



Vollständige Induktion: Beispiel I

Satz

Für alle natürlichen Zahlen $n \geq 1$ gilt $\sum_{k=1}^n (2k - 1) = n^2$.

Beweis.

Vollständige Induktion über n :

IA $n = 1$: $\sum_{k=1}^1 (2k - 1) = 2 - 1 = 1 = 1^2$

IV: Für $1 \leq m \leq n$ gilt $\sum_{k=1}^m (2k - 1) = m^2$

IS $n \rightarrow n + 1$:

$$\begin{aligned}\sum_{k=1}^{n+1} (2k - 1) &= \left(\sum_{k=1}^n (2k - 1) \right) + 2(n + 1) - 1 \\ &\stackrel{\text{IV}}{=} n^2 + 2(n + 1) - 1 \\ &= (n + 1)^2\end{aligned}$$



Vollständige Induktion: Beispiel II

Satz

Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen darstellen, also als $n = p_1 \cdot p_2 \cdot \dots \cdot p_m$ mit Primzahlen $p_1, \dots, p_m$.

Vollständige Induktion: Beispiel II

Satz

Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen darstellen, also als $n = p_1 \cdot p_2 \cdot \dots \cdot p_m$ mit Primzahlen $p_1, \dots, p_m$.

Beweis.

Vollständige Induktion über n :

IA $n = 2$: Trivial erfüllt, da 2 Primzahl

...

Vollständige Induktion: Beispiel II

Satz

Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen darstellen, also als $n = p_1 \cdot p_2 \cdot \dots \cdot p_m$ mit Primzahlen $p_1, \dots, p_m$.

Beweis.

Vollständige Induktion über n :

IA $n = 2$: Trivial erfüllt, da 2 Primzahl

IV: Jede natürliche Zahl k mit $2 \leq k \leq n$ lässt sich als Produkt von Primzahlen darstellen. ...

Vollständige Induktion: Beispiel II

Satz

Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen darstellen, also als $n = p_1 \cdot p_2 \cdot \dots \cdot p_m$ mit Primzahlen $p_1, \dots, p_m$.

Beweis (Fortsetzung).

IS $n \rightarrow n + 1$:

- Fall 1: $n + 1$ ist Primzahl $\rightsquigarrow$ trivial



Vollständige Induktion: Beispiel II

Satz

Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen darstellen, also als $n = p_1 \cdot p_2 \cdot \dots \cdot p_m$ mit Primzahlen $p_1, \dots, p_m$.

Beweis (Fortsetzung).

IS $n \rightarrow n + 1$:

- Fall 1: $n + 1$ ist Primzahl $\rightsquigarrow$ trivial
- Fall 2: $n + 1$ ist keine Primzahl.

Es gibt natürliche Zahlen $2 \leq q, r \leq n$ mit $n + 1 = q \cdot r$.

Nach IV gibt es Primzahlen $q_1, \dots, q_s$ mit $q = q_1 \cdot \dots \cdot q_s$ und $r_1, \dots, r_t$ mit $r = r_1 \cdot \dots \cdot r_t$.

Insgesamt gilt $n + 1 = q_1 \cdot \dots \cdot q_s \cdot r_1 \cdot \dots \cdot r_t$.



Induktive Definition einer Menge: Beispiele

Beispiel (Natürliche Zahlen)

Die Menge $\mathbb{N}_0$ der natürlichen Zahlen ist wie folgt induktiv definiert:

- 0 ist eine natürliche Zahl.
- Ist n eine natürliche Zahl, so ist $n + 1$ eine natürliche Zahl.

Induktive Definition einer Menge: Beispiele

Beispiel (Natürliche Zahlen)

Die Menge $\mathbb{N}_0$ der natürlichen Zahlen ist wie folgt induktiv definiert:

- 0 ist eine natürliche Zahl.
- Ist n eine natürliche Zahl, so ist $n + 1$ eine natürliche Zahl.

Beispiel (Binärbaum)

Die Menge $\mathcal{B}$ der Binärbäume ist induktiv wie folgt definiert:

- $\square$ ist ein Binärbaum (ein **Blatt**)
- Sind B_L und B_R Binärbäume, so ist auch $(B_L, \bigcirc, B_R)$ ein Binärbaum (mit **innerem Knoten** $\bigcirc$).

Induktive Definition einer Menge: Beispiele

Beispiel (Natürliche Zahlen)

Die Menge $\mathbb{N}_0$ der natürlichen Zahlen ist wie folgt induktiv definiert:

- 0 ist eine natürliche Zahl.
- Ist n eine natürliche Zahl, so ist $n + 1$ eine natürliche Zahl.

Beispiel (Binärbaum)

Die Menge $\mathcal{B}$ der Binärbäume ist induktiv wie folgt definiert:

- $\square$ ist ein Binärbaum (ein **Blatt**)
- Sind B_L und B_R Binärbäume, so ist auch $(B_L, \bigcirc, B_R)$ ein Binärbaum (mit **innerem Knoten** $\bigcirc$).

Implizit: Menge enthält kein Element, das nicht nach diesen Regeln gebildet werden kann

Induktive Definition einer Menge: Allgemein

Induktive Definition

Eine Menge M definiert man **induktiv** durch

- Angabe von Basiselementen, die in der Menge enthalten sind
- Konstruktionsregeln der Art
„Für $M' \subseteq M$, ist auch $K(M')$ in M .“

Strukturelle Induktion

Strukturelle Induktion

Beweis einer Aussage für eine induktiv definierte Menge

- **Induktionsanfang** (IA): Beweis der Aussage für alle Basiselemente.
- **Induktionsvoraussetzung** (IV):
Aussage gilt für Elemente von M' (aus Konstruktionsregel).
- **Induktionsschritt** (IS): Beweis der Aussage für $K(M')$
unter Verwendung der Induktionsannahme
(für jede Konstruktionsregel)

Strukturelle Induktion: Beispiel

Satz

Ein Binärbaum mit b Blättern hat $b - 1$ innere Knoten.

Strukturelle Induktion: Beispiel

Satz

Ein Binärbaum mit b Blättern hat $b - 1$ innere Knoten.

Beweis.

IA: Ein Baum $\square$ hat ein Blatt und keinen inneren Knoten.



Strukturelle Induktion: Beispiel

Satz

Ein Binärbaum mit b Blättern hat $b - 1$ innere Knoten.

Beweis.

IA: Ein Baum $\square$ hat ein Blatt und keinen inneren Knoten.

IV: Satz gilt für B_L und B_R .



Strukturelle Induktion: Beispiel

Satz

Ein Binärbaum mit b Blättern hat $b - 1$ innere Knoten.

Beweis.

IA: Ein Baum $\square$ hat ein Blatt und keinen inneren Knoten.

IV: Satz gilt für B_L und B_R .

IS für $B = (B_L, \bigcirc, B_R)$:

Wir bezeichnen die Anzahl der inneren Knoten eines Baumes B' mit $inner(B')$ und die der Blätter mit $blätter(B')$.

$$\begin{aligned} inner(B) &= inner(B_L) + inner(B_R) + 1 \\ &\stackrel{IV}{=} (blätter(B_L) - 1) + (blätter(B_R) - 1) + 1 \\ &= blätter(B_L) + blätter(B_R) - 1 = blätter(B) - 1 \end{aligned}$$



Fragen



Fragen?

Zusammenfassung

Zusammenfassung

- Ein **Beweis** basiert auf Axiomen und bereits bewiesenen Aussagen.
- Einzelne **Beweisschritte** müssen unmittelbar einsehbar sein.
- **Direkter Beweis**: Ableitung der Aussage durch Folgern und/oder Umformen
- **Indirekter Beweis**: Widerlegung der verneinten Aussage
- **Vollständige und strukturelle Induktion**: Beweis der Aussage für Induktionsanfang und Erhaltung der Aussage in Induktionsschritt

Vorbereitung für nächstes Mal

Worin besteht das Geheimnis Ihres langen Lebens?



Ich halte mich streng an Diätregeln: Wenn ich kein Bier zu einer Mahlzeit trinke, dann habe ich immer Fisch. Immer wenn ich Fisch und Bier zur selben Mahlzeit habe, verzichte ich auf Eiscreme. Wenn ich Eiscreme habe oder Bier meide, dann rühre ich Fisch nicht an.

Vereinfachen Sie diesen Ratschlag!