Logik für Informatiker

1. Grundlegende Beweisstrategien

Viorica Sofronie-Stokkermans

Universität Koblenz-Landau

e-mail: sofronie@uni-koblenz.de

Mathematisches Beweisen

Mathematische Aussagen

- haben oft die Form: Wenn A, dann B.
- als Formel: $A \rightarrow B$

Mathematischer Beweis

- bzgl. eines vorgegebenen Axiomensystems
- mit Hilfe von Inferenzregeln

Grundlegende Beweisstrategien

Mathematische Aussagen der Form $A \to B$ (Wenn A, dann B)

- Direkter Beweis:

  Annahme: A gilt. Benutze A, Axiome, und Inferenzregeln
  um B zu beweisen.

Grundlegende Beweisstrategien

Mathematische Aussagen der Form $A \to B$ (Wenn A, dann B)

- Direkter Beweis:

  Annahme: A gilt. Benutze A, Axiome, und Inferenzregeln um B zu beweisen.

Behauptung: Das Quadrat einer ungeraden natürlichen Zahl n ist stets ungerade.

n ungerade $\to$ n^2 ungerade.

Grundlegende Beweisstrategien

Mathematische Aussagen der Form $A \to B$ (Wenn A, dann B)

- Direkter Beweis:

  Annahme: A gilt. Benutze A, Axiome, und Inferenzregeln um B zu beweisen.

Behauptung: Das Quadrat einer ungeraden natürlichen Zahl n ist stets ungerade.

Beweis: Es sei n eine ungerade natürliche Zahl. Dann lässt sich n als $n = 2k + 1$ darstellen, wobei $k \in \mathbb{N}$. Daraus folgt mit Hilfe der ersten binomischen Formel, dass:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1.$$

Aus der Möglichkeit, n^2 so darzustellen folgt, dass n^2 ungerade ist.

Grundlegende Beweisstrategien

Mathematische Aussagen der Form $A \to B$ (Wenn A, dann B)

- Beweis durch Kontraposition:

  Beweis von $\neg B \to \neg A$.

- Beweis durch Widerspruch:

  Beweise dass $A \wedge \neg B \to$ falsch

Grundlegende Beweisstrategien

Mathematische Aussagen der Form $A \to B$ (Wenn A, dann B)

- Beweis durch Kontraposition:

  Beweis von $\neg B \to \neg A$.

- Beweis durch Widerspruch:

  Beweise dass $A \wedge \neg B \to$ falsch

Behauptung: Ist die Wurzel aus einer geraden natürlichen Zahl n eine natürliche Zahl, so ist diese gerade.

$$n \text{ gerade und } \sqrt{n} = k \in \mathbb{N} \to k \text{ gerade}$$

Beweis durch Kontraposition: Zu zeigen:

$$\sqrt{n} = k \in \mathbb{N} \text{ und } k \text{ ungerade } \to n \text{ ungerade.}$$

Grundlegende Beweisstrategien

Mathematische Aussagen der Form $A \to B$ (Wenn A, dann B)

- Beweis durch Kontraposition:

  Beweis von $\neg B \to \neg A$.

- Beweis durch Widerspruch:

  Beweise dass $A \wedge \neg B \to$ falsch

Behauptung: Ist die Wurzel aus einer geraden natürlichen Zahl n eine natürliche Zahl, so ist diese gerade.

Beweis: Angenommen, $\sqrt{n} = k$ wäre ungerade. Dann ist wegen der bereits bewiesenen Behauptung auch $k^2 = n$ ungerade, und das ist ein Widerspruch zu der Voraussetzung, dass n gerade ist.
Also ist die getroffene Annahme falsch, d.h., $\sqrt{n}$ ist gerade.

Grundlegende Beweisstrategien

Mathematische Aussagen, die nicht die Form $A \to B$ haben

- Äquivalenzbeweis ($A \Leftrightarrow B$) (A genau dann, wenn B)

  Beweise dass $A \to B$ und dass $B \to A$.

  (Wenn A, dann B, und wenn B, dann A.)

Grundlegende Beweisstrategien

- Beweis durch Widerspruch

  Um A zu beweisen:

  Annahme: A ist falsch (die Negation von A ist wahr)

  Zeige, dass dies zu einem Widerspruch führt.

Grundlegende Beweisstrategien

- Beweis durch Widerspruch

  Um A zu beweisen:

  Annahme: A ist falsch (die Negation von A ist wahr)

  Zeige, dass dies zu einem Widerspruch führt.

Behauptung: $\sqrt{2} \notin \mathbb{Q}$.

Beweis: Wir nehmen an dass $\sqrt{2} \in \mathbb{Q}$ und somit $\sqrt{2} = \frac{p}{q}$ wobei der Bruch p/q in gekürzter Form vorliegt (d.h. p und q teilerfremde ganze Zahlen sind). Dann $\left(\frac{p}{q}\right)^2 = 2$, d.h: $p^2 = 2q^2$. Da $2q^2$ eine gerade Zahl ist, ist auch p^2 gerade. Daraus folgt, dass auch p gerade ist, d.h. $p = 2r$ (wobei $r \in \mathbb{Z}$). Damit erhält man mit obiger Gleichung: $2q^2 = p^2 = (2r)^2 = 4r^2$, und hieraus nach Division durch 2: $q^2 = 2r^2$. Mit der gleichen Argumentation wie zuvor folgt, dass q^2 und damit auch q eine gerade Zahl ist. Da p und q durch 2 teilbar sind, erhalten wir einen Widerspruch zur Teilerfremdheit von p und q. Dieser Widerspruch zeigt, dass die Annahme, $\sqrt{2}$ sei eine rationale Zahl, falsch ist und daher das Gegenteil gelten muss. Damit ist die Behauptung, dass $\sqrt{2}$ irrational ist, bewiesen.

Grundlegende Beweisstrategien

- Beweis durch Fallunterscheidung

  Um B zu beweisen, beweise dass $A_1 \to B, \ldots, A_n \to B$,

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

Grundlegende Beweisstrategien

- Beweis durch Fallunterscheidung

  Um B zu beweisen, beweise dass $A_1 \to B, \ldots, A_n \to B$,

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

Behauptung: Jede Primzahl $p \geq 3$ hat die Form $p = 4 \cdot k + 1$ oder $p = 4 \cdot k - 1$ mit $k \in \mathbb{N}$.

Beweis: Man unterscheidet folgende vier Fälle für p, von denen immer genau einer eintritt:

Fall 1: $p = 4k$
Fall 2: $p = 4k + 1$
Fall 3: $p = 4k + 2$
Fall 4: $p = 4k + 3 = 4(k + 1) - 1$

Im ersten dieser Fälle ist p durch 4 teilbar und damit keine Primzahl,
im dritten Fall ist p durch 2 teilbar und somit ebenfalls keine Primzahl.
Also muss einer der Fälle zwei oder vier eintreten, das heißt p hat die Form $p = 4 \cdot k + 1$ oder $p = 4 \cdot k - 1$ mit $k \in \mathbb{N}$.

Grundlegende Beweisstrategien

- Beweis durch Fallunterscheidung

  Um B zu beweisen, beweise dass $A_1 \to B, \ldots, A_n \to B$,
  wobei $A_1 \vee \cdots \vee A_n \equiv$ wahr

Es sei angemerkt, dass die Fallunterscheidung zwar vollständig sein muss, aber die untersuchten Fälle sich nicht gegenseitig ausschließen müssen.

Grundlegende Beweisstrategien

Aussagen mit Quantoren

$\forall x \in U : (p(x) \to q(x))$

Wähle a beliebig aus U.

Beweise, dass $p(a) \to q(a)$.

Da a beliebig gewählt werden kann, folgt

$$\forall x \in U : p(x) \to q(x)$$

Grundlegende Beweisstrategien

Aussagen mit Quantoren

$\forall x \in U : (p(x) \to q(x))$

Wähle a beliebig aus U.

Beweise, dass $p(a) \to q(a)$.

Da a beliebig gewählt werden kann, folgt

$$\forall x \in U : p(x) \to q(x)$$

Behauptung: $\forall n \in \mathbb{N} : (\underbrace{n \text{ ist gerade und } \sqrt{n} \text{ ist eine natürliche Zahl}}_{p(n)} \to \underbrace{\sqrt{n} \text{ ist gerade}}_{q(n)})$.

Beweis: Sei n beliebig aus $\mathbb{N}$.
Wir zeigen, dass wenn n gerade ist und $\sqrt{n}$ eine natürliche Zahl ist, dann $\sqrt{n}$ gerade ist.
(Dies wurde auf Seite 8 bewiesen.)

Grundlegende Beweisstrategien

Aussagen mit Quantoren

$\exists x \in U\, A(x)$

Sei a ein geeignetes Element aus U.

Beweise, dass $A(a)$ wahr ist. Damit folgt $\exists x \in U : A(x)$.

Grundlegende Beweisstrategien

Aussagen mit Quantoren

$\exists x \in U\, A(x)$

Sei a ein geeignetes Element aus U.

Beweise, dass $A(a)$ wahr ist. Damit folgt $\exists x \in U : A(x)$.

Behauptung: $\exists x \in \mathbb{N} : x^2 - 2x + 1 = 0$

Beweis: $A(x): \quad x^2 - 2x + 1 = 0$
Sei $a = 1$. Wir zeigen, dass $A(a)$ wahr ist: $a^2 - 2a + 1 = 1^2 - 2 + 1 = 0$.
Damit folgt $\exists x \in \mathbb{N} : A(x)$

Grundlegende Beweisstrategien

Aussagen mit Quantoren

$\exists x \in U\, A(x)$

Sei a ein geeignetes Element aus U.

Beweise, dass $A(a)$ wahr ist. Damit folgt $\exists x \in U : A(x)$.

$\exists x \in U\, (p(x) \to q(x))$

Sei a ein geeignetes Element aus U.

Beweis der Implikation $p(a) \to q(a)$.

Damit folgt $\exists x \in U : p(x) \to q(x)$.

Grundlegende Beweisstrategien

Beweise mittels Vollständiger Induktion

Induktion

Wesentliches Beweisprinzip in Mathematik und Logik

Induktion

Wesentliches Beweisprinzip in Mathematik und Logik

Einfache Version

Induktion über die natürlichen Zahlen $\mathbb{N}$
(natural induction)

Induktion

Wesentliches Beweisprinzip in Mathematik und Logik

Einfache Version

Induktion über die natürlichen Zahlen $\mathbb{N}$
(natural induction)

Generalization

Noethersche Induktion
(noetherian induction/
induction over well-founded partially ordered sets)

Hier: Strukturelle Induktion

Induktion über die natürlichen Zahlen

Idee: Definition der natürlichen Zahlen

(A1) 0 ist eine natürliche Zahl

(A2) Jede natürliche Zahl n hat einen Nachfolger $S(n)$

(A3) Aus $S(n) = S(m)$ folgt $n = m$

(A4) 0 ist nicht Nachfolger einer natürlichen Zahl

(A5) Jede Menge X, die 0 und mit jeder natürlichen Zahl n auch deren Nachfolger $S(n)$ enthält, umfasst alle natürlichen Zahlen.

Induktion über die natürlichen Zahlen

(A5) Jede Menge X, die 0 und mit jeder natürlichen Zahl n auch deren Nachfolger $S(n)$ enthält, umfasst alle natürlichen Zahlen.

$\forall X$ Menge: Falls $0 \in X$, und

$$\forall n \in \mathbb{N} : n \in X \rightarrow n + 1 \in X$$

so $\forall n \in \mathbb{N} : n \in X$

Induktion über die natürlichen Zahlen

(A5) Jede Menge X, die 0 und mit jeder natürlichen Zahl n auch deren Nachfolger $S(n)$ enthält, umfasst alle natürlichen Zahlen.

$\forall X$ Menge: Falls $0 \in X$, und

$$\forall n \in \mathbb{N} : n \in X \rightarrow n + 1 \in X$$

so $\forall n \in \mathbb{N} : n \in X$

Induktionssatz

Gelten die beiden Aussagen:

- $p(0)$ und
- $\forall n \in \mathbb{N} : p(n) \rightarrow p(n + 1)$,

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

Induktion über die natürlichen Zahlen

(A5) Jede Menge X, die 0 und mit jeder natürlichen Zahl n auch deren Nachfolger $S(n)$ enthält, umfasst alle natürlichen Zahlen.

$\forall X$ Menge: Falls $0 \in X$, und

$$\forall n \in \mathbb{N} : n \in X \rightarrow n+1 \in X$$

so $\forall n \in \mathbb{N} : n \in X$

Induktionssatz

Gelten die beiden Aussagen:

- $p(0)$ und — Induktionsbasis
- $\forall n \in \mathbb{N} : p(n) \rightarrow p(n+1)$, — Induktionsschritt

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

Induktion über die natürlichen Zahlen

Struktur eines Induktionsbeweises

(1)	Induktionsbasis:	Beweise $p(0)$
(2)	Induktionsschritt:	Beweise $p(n) \to p(n+1)$
		für ein beliebiges $n \in \mathbb{N}$

Induktion über die natürlichen Zahlen

Struktur eines Induktionsbeweises

(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 $p(n)$

Beispiel

Behauptung: Die Summe der ersten n ungeraden Zahlen ist n^2.

Für alle $n \in \mathbb{N}$, $\sum_{i=0}^{n-1}(2i+1) = n^2$.

Beispiel

Behauptung: Die Summe der ersten n ungeraden Zahlen ist n^2.

Für alle $n \in \mathbb{N}$, $\sum_{i=0}^{n-1}(2i+1) = n^2$.

$$p(n): \quad \sum_{i=0}^{n-1}(2i+1) = n^2$$

(1) Induktionsbasis: Beweise $p(0)$

$n = 0$: $0 = 0^2$

Beispiel

Behauptung: Die Summe der ersten n ungeraden Zahlen ist n^2.

Für alle $n \in \mathbb{N}$, $\sum_{i=0}^{n-1}(2i+1) = n^2$.

$$p(n): \quad \sum_{i=0}^{n-1}(2i+1) = n^2$$

(1) Induktionsbasis: Beweise $p(0)$ OK

(2) Induktionsvoraussetzung: Für ein beliebig gewähltes $n \in \mathbb{N}$ gilt $p(n)$: $\sum_{i=0}^{n-1}(2i+1) = n^2$

Beispiel

Behauptung: Die Summe der ersten n ungeraden Zahlen ist n^2.

Für alle $n \in \mathbb{N}$, $\sum_{i=0}^{n-1}(2i+1) = n^2$.

$$p(n): \quad \sum_{i=0}^{n-1}(2i+1) = n^2$$

(1)	Induktionsbasis:	Beweise $p(0)$ OK
(2)	Induktionsvoraussetzung:	Für ein beliebig gewähltes $n \in \mathbb{N}$ gilt $p(n)$: $\sum_{i=0}^{n-1}(2i+1) = n^2$
(3)	Induktionsschluss:	Folgere $p(n+1)$ aus $p(n)$ $p(n+1): \sum_{i=0}^{n}(2i+1) = (n+1)^2$.

Beweis: $\sum_{i=0}^{n}(2i+1) = (\sum_{i=0}^{n-1}(2i+1)) + (2n+1) \overset{p(n)}{=} n^2 + (2n+1) = (n+1)^2$.

Verallgemeinerte vollständige Induktion

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 $\forall n \in \mathbb{N} : p(n)$.

Wohlfundierte (Noethersche) Induktion

Verallgemeinerte vollständige Induktion

Gelten die beiden Aussagen:

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

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

Äquivalent

Gelten die beiden Aussagen:

$p(0)$ und
$\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : (k < n+1 \rightarrow p(k)) \rightarrow p(n+1))$

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

Wohlfundierte (Noethersche) Induktion

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 $\forall n \in \mathbb{N} : p(n)$.

Äquivalent

Gilt die Aussage:

$$\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : (k < n \rightarrow p(k)) \rightarrow p(n))$$

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

Vollständige Induktion

Zu zeigen: $\forall n \geq n_0 : P(n)$

Sei $n \in \mathbb{N}, n \geq n_0$.

Induktionsvoraussetzung: $p(k)$ gilt für alle $k < n$

Induktionsschluss: Folgere $p(n)$ aus der Induktionsvoraussetzung.

Wohlfundierte (Noethersche) Induktion

Theorem:

Falls	$\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : (k < n \to p(k)) \to p(n))$	P
dann gilt	$\forall n \in \mathbb{N} : p(n)$	Q

Beweis: Zu zeigen: $P \to Q$

Kontrapositionsbeweis: Wir zeigen, dass $\neg Q \to \neg P$

Annahme: $\neg Q := \neg(\forall n \in \mathbb{N} : p(n)) \equiv \exists n \in \mathbb{N} : \neg p(n)$.

$>$ **wohlfundierte Ordnung auf** $\mathbb{N}$**:** es gibt keine unendliche Folge $x_1, \ldots, x_n, \ldots$ mit $x_1 > x_2 > \cdots > x_n > \ldots$.

Sei $Y = \{n \in \mathbb{N} \mid \neg p(n)\} \neq \emptyset$. Dann hat Y ein minimales Element m, d.h. $\exists m(m \in Y \wedge (\forall k \in \mathbb{N} : (k < m \to k \notin Y))) = \neg P$.

Wohlfundierte (Noethersche) Induktion

Theorem:

Falls	$\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : (k < n \to p(k)) \to p(n))$	P
dann gilt	$\forall n \in \mathbb{N} : p(n)$	Q

Beweis: Zu zeigen: $P \to Q$

Kontrapositionsbeweis: Wir zeigen, dass $\neg Q \to \neg P$

Annahme: $\neg Q := \neg(\forall n \in \mathbb{N} : p(n)) \equiv \exists n \in \mathbb{N} : \neg p(n)$.

$>$ **wohlfundierte Ordnung auf** $\mathbb{N}$**:** es gibt keine unendliche Folge $x_1, \ldots, x_n, \ldots$ mit $x_1 > x_2 > \cdots > x_n > \ldots$.

Sei $Y = \{n \in \mathbb{N} \mid \neg p(n)\} \neq \emptyset$. Dann hat Y ein minimales Element m, d.h. $\exists m(m \in Y \wedge (\forall k \in \mathbb{N} : (k < m \to k \notin Y))) = \neg P$.

Wohlfundierte (Noethersche) Induktion

Theorem:

Falls	$\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : (k < n \to p(k)) \to p(n))$	P
dann gilt	$\forall n \in \mathbb{N} : p(n)$	Q

Verallgemeinerung

- beliebige Menge A statt $\mathbb{N}$

- $<$ Ordnung auf A

- $<$ wohlfundiert (es gibt keine unendliche Folge $x_1, \ldots, x_n, \ldots$ mit $x_1 > x_2 > \cdots > x_n > \ldots$)

Beispiel

Satz: Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen darstellen.

$p(n)$: $n \geq 2 \rightarrow n$ lässt sich als Produkt von Primzahlen darstellen.

Beispiel

Satz: Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen darstellen.
$p(n)$: $n \geq 2 \rightarrow n$ lässt sich als Produkt von Primzahlen darstellen.

Beweis: Sei $n \in \mathbb{N}$, $n \geq 2$ beliebig gewählt.

Induktionsvoraussetzung: $p(k)$ gilt für alle $k < n$
Induktionsschluss: Folgere $p(n)$ aus der Induktionsvoraussetzung

Beispiel

Satz: Jede natürliche Zahl $n \geq 2$ lässt sich als Produkt von Primzahlen darstellen.
$p(n)$: $n \geq 2 \rightarrow n$ lässt sich als Produkt von Primzahlen darstellen.

Beweis: Sei $n \in \mathbb{N}$, $n \geq 2$, beliebig gewählt.

Induktionsvoraussetzung: $p(k)$ gilt für alle $k < n$
Induktionsschluss: Folgere $p(n)$ aus der Induktionsvoraussetzung.

Fallunterscheidung:

Fall 1: n **Primzahl.** Dann lässt sich n als Produkt von Primzahlen darstellen ($n = n$)

Fall 2: n **keine Primzahl.** Dann $n = k_1 \cdot k_2$, mit $k_1, k_2 \in \mathbb{N}$, $k_1, k_2 \geq 2$.

Da aber $k_i < n$, $i = 1, 2$ ist nach Induktionsvoraussetzung bereits eine Darstellung als Produkt von Primzahlen für k_i bekannt.

Multipliziert man diese beiden Produkte miteinander, so erhält man eine Darstellung für n.