

Logik für Informatiker

1. Grundlegende Beweisstrategien

Viorica Sofronie-Stokkermans

Universität Koblenz-Landau

e-mail: sofronie@uni-koblenz.de

Organisatorisches

- Übungen: Start 8:00 s.t. bzw. 9:00 s.t.
- Nächste Woche:
 - Do, 18.04.19 die Übungen finden statt
 - Fr, 19.04.19: Karfreitag (keine Übung)

Mathematisches Beweisen

Beweise in der Mathematik (und in der Informatik) haben viele Funktionen:

- Erkenntnissicherung
- Begründung/Veranschaulichung
- Überzeugen und Kommunizieren
- Finden von neuen Sätzen und Begriffen

“Was beweisbar ist, soll in der Wissenschaft nicht ohne Beweis geglaubt werden.”

Richard Dedekind

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 $A \rightarrow B$ (Wenn A , dann B)

- Direkter Beweis:

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

Dazu zeigt man oft Zwischenresultate, also

$$A \rightarrow A_1 \rightarrow A_2 \rightarrow \dots \rightarrow A_n \rightarrow B.$$

Wir nehmen A an, folgern daraus A_1 , dann A_2, \dots , dann A_n und daraus folgern wir B .

Grundlegende Beweisstrategien

Mathematische Aussagen der Form $A \rightarrow B$ (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.

$$n \text{ ungerade} \rightarrow n^2 \text{ ungerade.}$$

Grundlegende Beweisstrategien

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

- Beweis durch Kontraposition:
Beweis von $\neg B \rightarrow \neg A$.
- Beweis durch Widerspruch:
Beweise dass $A \wedge \neg B \rightarrow$ falsch

Grundlegende Beweisstrategien

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

- Beweis durch Kontraposition:
Beweis von $\neg B \rightarrow \neg A$.
- Beweis durch Widerspruch:
Beweise dass $A \wedge \neg B \rightarrow$ falsch

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

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

Beweis durch Kontraposition: Zu zeigen:

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

Grundlegende Beweisstrategien

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

- Beweis durch Kontraposition:
Beweis von $\neg B \rightarrow \neg A$.
- Beweis durch Widerspruch:
Beweise dass $A \wedge \neg B \rightarrow$ falsch

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

Beweis durch Kontraposition: Angenommen, $\sqrt{n} = k$ wäre ungerade.
Dann ist wegen der bereits bewiesenen Behauptung auch $k^2 = n$ ungerade.

Grundlegende Beweisstrategien

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

- Beweis durch Kontraposition:
Beweis von $\neg B \rightarrow \neg A$.
- Beweis durch Widerspruch:
Beweise dass $A \wedge \neg B \rightarrow$ falsch

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

Beweis durch Widerspruch: Sei n eine gerade natürliche Zahl.

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} muss gerade sein.

Grundlegende Beweisstrategien

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

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

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

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

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).

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: $p^2 = 2q^2$.

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 $r \in \mathbb{Z}$).

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: $q^2 = 2r^2$.

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.

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 haben wir bewiesen, dass $\sqrt{2}$ irrational ist.

Grundlegende Beweisstrategien

- Beweis durch Fallunterscheidung

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

wobei $A_1 \vee \dots \vee A_n \equiv \text{wahr}$

Grundlegende Beweisstrategien

- Beweis durch Fallunterscheidung

Um B zu beweisen, beweise dass $A_1 \rightarrow B, \dots, A_n \rightarrow B$,
wobei $A_1 \vee \dots \vee A_n \equiv \text{wahr}$

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 $A_1 \rightarrow B, \dots, A_n \rightarrow B$,
wobei $A_1 \vee \dots \vee A_n \equiv \text{wahr}$

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

Grundlegende Beweisstrategien

Aussagen mit Quantoren

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

Wähle a beliebig aus U .

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

Da a beliebig gewählt werden kann, folgt

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

Grundlegende Beweisstrategien

Aussagen mit Quantoren

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

Wähle a beliebig aus U .

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

Da a beliebig gewählt werden kann, folgt

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

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

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 Seiten 9 / 10 / 11 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: $A(x) : x^2 - 2x + 1 = 0$

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

$$\exists x \in U (p(x) \rightarrow q(x))$$

Sei a ein geeignetes Element aus U .

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

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

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 $p(n) \rightarrow p(n + 1)$
für ein beliebiges $n \in \mathbb{N}$

Induktion über die natürlichen Zahlen

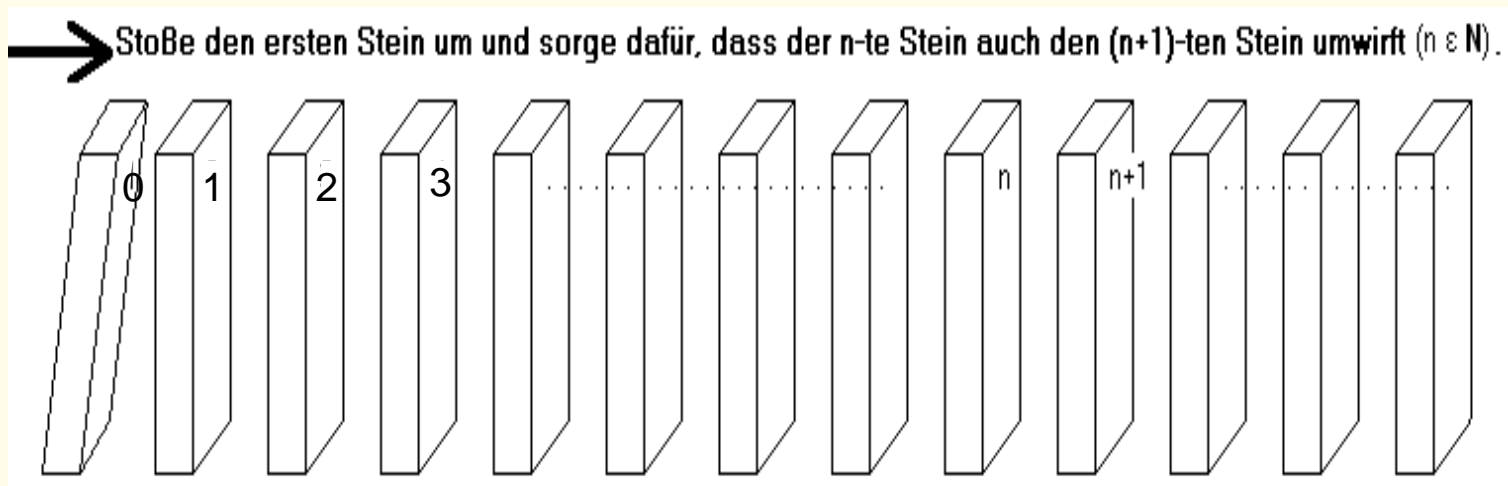
Struktur eines Induktionsbeweises

- (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 $p(n)$

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

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

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

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

Beispiel

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

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

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

(1) Induktionsbasis:

Beweise $p(0)$ OK

(2) Induktionsvoraussetzung:

Für ein beliebig gewähltes

$$n \in \mathbb{N} \text{ gilt } p(n): \sum_{i=0}^{n-1} (2i + 1) = n^2$$

Beispiel

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

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

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

(1) Induktionsbasis:

Beweise $p(0)$ OK

(2) Induktionsvoraussetzung:

Für ein beliebig gewähltes

$$n \in \mathbb{N} \text{ gilt } p(n): \sum_{i=0}^{n-1} (2i + 1) = n^2$$

(3) Induktionsschluss:

Folgere $p(n+1)$ aus $p(n)$

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

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

Induktion über die natürlichen Zahlen

Struktur eines Induktionsbeweises

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

- (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 $p(n)$

Induktion über die natürlichen Zahlen

Struktur eines Induktionsbeweises

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

- (1) Induktionsbasis: Beweise $p(n_0)$
- (2) Induktionsvoraussetzung: Für ein beliebig gewähltes $n \geq n_0$ gilt $p(n)$
- (3) Induktionsschluss: Folgere $p(n + 1)$ aus der Induktionsvoraussetzung $p(n)$

Verallgemeinerte vollständige Induktion

Verallgemeinerte vollständige Induktion

Gelten die beiden Aussagen:

$p(0)$ und

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

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

Wohlfundierte (Noethersche) Induktion

Verallgemeinerte vollständige Induktion

Gelten die beiden Aussagen:

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

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

Äquivalent

Gelten die beiden Aussagen:

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

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

Wohlfundierte (Noethersche) Induktion

Verallgemeinerte vollständige Induktion

Gelten die beiden Aussagen:

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

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 $n_0 \leq k < n$

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

Wohlfundierte (Noethersche) Induktion

Theorem:

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

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

Beweis: Zu zeigen: $P \rightarrow Q$

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

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, \dots, x_n, \dots mit $x_1 > x_2 > \dots > x_n > \dots$

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

Wohlfundierte (Noethersche) Induktion

Theorem:

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

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

Beweis: Zu zeigen: $P \rightarrow Q$

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

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, \dots, x_n, \dots mit $x_1 > x_2 > \dots > x_n > \dots$

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

Wohlfundierte (Noethersche) Induktion

Theorem:

Falls $\forall n \in \mathbb{N} : (\forall k \in \mathbb{N} : (k < n \rightarrow p(k)) \rightarrow p(n))$ 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, \dots, x_n, \dots mit $x_1 > x_2 > \dots > x_n > \dots$)

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 .

Fehlerquellen

Häufige Fehler bei Induktionsbeweisen

- Ordnung ist nicht noethersch
- Induktionsanfang 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.

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.

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.

Fehlerquellen

Was ist hier falsch?

Bei Induktionsschritt Grenzfall $n = 2$
nicht bedacht.

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.

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.

Fehlerquellen

Was ist hier falsch?

Paradox des Haufens

Wir gehen davon aus, dass jede Menge mit mehr als 100.000 Sandkörner ein Haufen Sand bildet.

Axiom: Wenn wir von einem Haufen Sand ein Sandkorn entfernen, dann bilden die restlichen Sandkörner weiterhin einen Haufen.

Fehlerquellen

Was ist hier falsch?

Paradox des Haufens

Wir gehen davon aus, dass jede Menge mit mehr als 100.000 Sandkörner ein Haufen Sand bildet.

Axiom: Wenn wir von einem Haufen Sand ein Sandkorn entfernen, dann bilden die restlichen Sandkörner weiterhin einen Haufen.

Somit lässt sich folgern:

Wenn n Körner ein Haufen sind, dann sind $(n - 1)$ Körner ein Haufen;

$n - 1$ Körner sind ein Haufen, also sind $n - 2$ ein Haufen;

Wenn $(n - (n - 2))$ Körner ein Haufen sind, dann ist 1 Korn ein Haufen.

Letztendlich gelangen wir so zu der Aussage, dass bereits ein Sandkorn ein Haufen ist.

Fehlerquellen

Was ist hier falsch?

Paradox des Haufens

Wir gehen davon aus, dass jede Anzahl von Sandkörnern ein Haufen Sand bildet.

Axiom: Wenn wir von einem Haufen Sand ein Sandkorn entfernen, dann bilden die restlichen Sandkörner weiterhin einen Haufen.

Somit lässt sich folgern:

Wenn n Körner ein Haufen sind, dann sind $(n - 1)$ Körner ein Haufen;

$n - 1$ Körner sind ein Haufen, also sind $n - 2$ ein Haufen;

Wenn $(n - (n - 2))$ Körner ein Haufen sind, dann ist 1 Korn ein Haufen.

Letztendlich gelangen wir so zu der Aussage, dass bereits ein Sandkorn ein Haufen ist.

Falsch:

Das Axiom und die Definition des Begriffs "Haufen" passen nicht zusammen.

Zusammenfassung

- Grundlegende Beweisstrategien
- Induktion über die natürlichen Zahlen
- Fehlerquellen

Strukturelle Induktion

Bei der vollständigen Induktion werden Eigenschaften der natürlichen Zahlen bewiesen.

Bei der strukturellen Induktion werden Eigenschaften für Elemente in induktiv definierten Mengen bewiesen

d.h. Mengen, die 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:

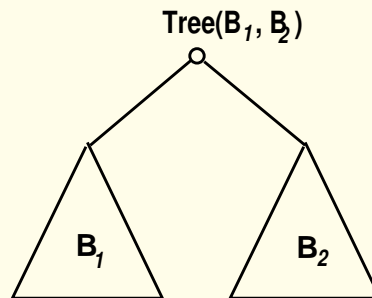
- (1) $\epsilon \in \Sigma^*$
- (2) Falls $w \in \Sigma^*$ und $a \in \Sigma$ so $wa \in \Sigma^*$.
- (3) Für jede Menge A mit Eigenschaften (1) und (2) gilt: $\Sigma^* \subseteq A$.

Induktive Definitionen: Beispiele

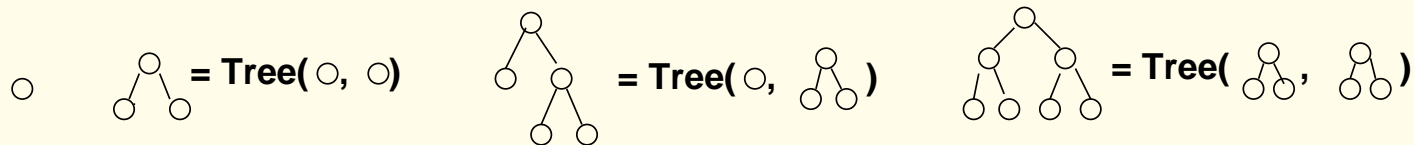
(3) Bin : die Menge aller (vollständigen) binären Bäume

Basismenge: ○ Baum mit nur einem Knoten.

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



Beispiele:



Induktive Definitionen: Beispiele

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

Basismenge: \circ Baum mit nur einem Knoten.

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

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 $\text{Tree}(B_1, B_2) \in A$.

Das bedeutet, dass:

- (1) $\circ \in \text{Bin}$
- (2) Falls $B_1, B_2 \in \text{Bin}$ so $\text{Tree}(B_1, B_2) \in \text{Bin}$.
- (3) Für jede Menge A mit Eigenschaften (1) und (2) gilt: $\text{Bin} \subseteq A$.

Induktive Definitionen: Beispiele

(4) Menge aller aussagenlogischen Formeln

Basismenge: \perp (falsch), \top (wahr), P_0, P_1, P_2, \dots 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 Operationssymbolen ("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: $M \subseteq A$.