# Formale Grundlagen der Informatik

Herbstsemester 2020

Prof. Dr. Matthias Krause
Dr. Matthias Hamann

**Beweise**

(Stand: 25.08.2020)

Lehrstuhl für Theoretische Informatik
Universität Mannheim

# Beweise

# Motivation

- Das Beweisen von Aussagen spielt eine zentrale Rolle in Mathematik und Informatik (und nicht nur dort!).
- Häufige Frage der Studenten: „Wie kommt man eigentlich auf diesen Beweis?“
- (Unbefriedigende) Antwort: Es gibt kein ‘Patentrezept’. ☹
- Beispiele für offene Beweise: Millenium-Probleme (Preisgeld jeweils eine Million US-Dollar) oder die Goldbachsche Vermutung von 1742 („Jede gerade Zahl, die größer als 2 ist, ist Summe zweier Primzahlen.“).
- **ABER:** Es gibt grundlegende **Beweistechniken**, die zum ‘Handwerkszeug’ eines Mathematikers/Informatikers gehören.
- Danach hilft nur: **üben, üben, üben!**

# Direktes Beweisen

# Direktes Beweisen

Wir wollen beweisen, dass eine Aussage $H^*$ in einem gegebenen Kontext wahr ist. Ein direkter Beweis für $H^*$ in $n$ Schritten ergibt sich durch eine Folge von $n$ Aussagen $H_1, H_2, \ldots, H_n$, für die gilt:

(1) Die Aussage $H_1$ ist im gegebenen Kontext (offensichtlich) wahr,

(2) die Aussagen $H_i \to H_{i+1}$ sind für $i = 1, \ldots, n-1$ im gegebenen Kontext (offensichtlich) wahr,

(3) die Aussage $H_n \to H^*$ ist im gegebenen Kontext (offensichtlich) wahr.

**Theorem 1**

*Aus (1), (2) und (3) ergibt sich, dass $H^*$ wahr ist.*

**Beweis:** Aus der Wahrheit von $H_1$ und $H_1 \to H_2$ ergibt sich die Wahrheit von $H_2$ usw., bis sich aus der Wahrheit von $H_n$ und $H_n \to H^*$ die Wahrheit von $H^*$ ergibt. $\square$

# Direktes Beweisen - Beispiel 1

**Definition 2**

Es bezeichne $s_n$ die Summe der ersten $n$ natürlichen Zahlen größer Null, also $s_n = \sum_{i=1}^{n} i$.

**Beispiel:** $s_1 = 1$, $s_2 = 1 + 2 = 3$, $s_3 = 1 + 2 + 3 = 6$ usw.

**Theorem 3 (Gaußsche Summenformel)**

*Für alle natürlichen Zahlen $n \geq 1$ gilt $s_n = \frac{n(n+1)}{2}$.*

**Beweis:** Es bezeichne $H^*$ die Aussage des Theorems.

Wir definieren Aussagen $H_1, \ldots, H_5$, so dass die Aussage $H_1$, die Aussagen $H_i \rightarrow H_{i+1}$, $i = 1, \ldots, 4$, und die Aussage $H_5 \rightarrow H^*$ im uns bekannten Kontext der Mathematik wahr sind.

Das ergibt einen direkten Beweis der Aussage $H^*$.

# Direktes Beweisen - Beispiel 1 (Fortsetzung)

Die Aussagen $H_1$ bis $H_5$:

- Aussage $H_1$ : $s_n = \sum_{i=1}^{n} i$. ($H_1$ ist wahr gemäß der Definition.)
- Aussage $H_2$ : $2 \cdot s_n = \sum_{i=1}^{n} i + \sum_{i=1}^{n} i$.
- Aussage $H_3$ : $2 \cdot s_n = \sum_{i=1}^{n} i + \sum_{i=1}^{n}(n + 1 - i)$.
- Aussage $H_4$ : $2 \cdot s_n = \sum_{i=1}^{n}(i + n + 1 - i) = \sum_{i=1}^{n}(n + 1)$.
- Aussage $H_5$ : $2 \cdot s_n = n \cdot (n + 1)$.
- Aussage $H^*$ : $s_n = \frac{n \cdot (n+1)}{2}$.

Man sieht direkt, dass die Aussagen $H_1 \to H_2$, $H_2 \to H_3$, $H_3 \to H_4$, $H_4 \to H_5$, $H_5 \to H^*$ im uns bekannten Kontext der Mathematik wahr sind. $\square$

# Direktes Beweisen - Beispiel 2

**Theorem 4**

*Das Quadrat $u^2$ einer ungeraden ganzen Zahl $u$ ist stets ungerade.*

**Beweis:** Sei $u$ eine ungerade ganze Zahl.

Dann lässt sich $u$ darstellen als $u = 2k + 1$, wobei $k$ eine ganze Zahl ist. Durch Anwendung der ersten binomischen Formel erhält man nun

$$\begin{aligned} u^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= \underbrace{2 \cdot \left(2k^2 + 2k\right)}_{\text{gerade}} + 1. \end{aligned}$$

Folglich ist $u^2$ ungerade. □

# Indirektes Beweisen

Wir wollen beweisen, dass eine Aussage $H^*$ in einem gegebenen Kontext wahr ist. Ein indirekter Beweis für $H^*$ in $n$ Schritten ergibt sich durch eine Folge von $n$ Aussagen $H_1, H_2, \ldots, H_n$, für die gilt:

(1) Die Aussage $\neg H^* \to \neg H_n$ ist im gegebenen Kontext (offensichtlich) wahr,

(2) die Aussagen $\neg H_i \to \neg H_{i-1}$ sind für $i = n, \ldots, 2$ im gegebenen Kontext (offensichtlich) wahr,

(3) die Aussage $H_1$ ist im gegebenen Kontext (offensichtlich) wahr.

**Theorem 5**

*Aus (1), (2) und (3) ergibt sich, dass $H^*$ wahr ist.*

**Beweis:** Aus der (angenommenen) Wahrheit von $\neg H^*$ und (1) und (2) ergibt sich die Wahrheit von $\neg H_1$, was im Widerspruch zu (3) steht. Also muss $\neg H^*$ falsch und damit $H^*$ wahr sein. $\square$

# Indirektes Beweisen - Beispiel 1

Eine reelle Zahl heißt rational, wenn sie als Verhältnis zweier ganzer Zahlen dargestellt werden kann. Zeige:

**Theorem 6**

*Die Zahl $\sqrt{2}$ ist nicht rational.*

**Beweis:** Angenommen $\sqrt{2}$ sei rational.

Dann gilt $\sqrt{2} = \frac{a}{b}$ mit ganzen Zahlen $a$, $b$ und $b \neq 0$. Die Zahlen $a$, $b$ sind dabei *teilerfremd*, d. h., sie besitzen keinen gemeinsamen Teiler.

Man erhält $2 = (\sqrt{2})^2 = (a/b)^2 = a^2/b^2$ bzw. $2b^2 = a^2$.
D. h., $a^2$ wäre eine gerade Zahl, was nur dann möglich ist, wenn $a$ eine gerade Zahl ist (vgl. Folie 5), sprich: $a = 2k$, wobei $k$ eine ganze Zahl ist.

Es müssten dann wegen $2b^2 = a^2 = 4k^2$ bzw. $b^2 = 2k^2$ auch $b^2$ und damit $b$ gerade Zahlen sein. Das ist offensichtlich ein Widerspruch zur Voraussetzung, dass $a$ und $b$ teilerfremd sind. $\square$

# Indirektes Beweisen - Beispiel 2

**Theorem 7**

*Für natürliche Zahlen a und b gilt stets* $\sqrt{ab} \leq \frac{a+b}{2}$.

**Beweis:** Angenommen es gäbe natürliche Zahlen $a$, $b$ mit $\sqrt{ab} > \frac{a+b}{2}$.

Wir formen um:

$$\begin{aligned} \sqrt{ab} &> \frac{a+b}{2} \\ \Rightarrow \quad ab &> \frac{(a+b)^2}{4} \qquad \text{(da } a, b \geq 0\text{)} \\ \Rightarrow 4ab &> a^2 + 2ab + b^2 \\ \Rightarrow \quad 0 &> a^2 - 2ab + b^2 \\ \Rightarrow \quad 0 &> (a-b)^2. \end{aligned}$$

Widerspruch zur Annahme, dass es sich bei $a$ und $b$ um natürliche Zahlen handelt, da das Quadrat einer ganzen Zahl stets nichtnegativ ist. □

# Beweisen durch vollständige Induktion

# Beweisen durch vollständige Induktion

... dienen dem Beweis von Sätzen der folgenden Art:

**Theorem 8**

*Sei $P$ Prädikat über den natürlichen Zahlen. Dann ist für alle $n \geq n_0$ die Aussage $P(n)$ wahr.*

**Beweisstruktur:**

- **Induktionsanfang:** Zeige, dass $P(n_0)$ wahr ist.
- **Induktionsschritt:** Zeige, dass für alle $n \geq n_0$ die Aussage $P(n) \rightarrow P(n+1)$ wahr ist.

Damit ist $P(n)$ für alle $n \geq n_0$ wahr, da die Aussagen

$$P(n_0), P(n_0) \rightarrow P(n_0+1), \ldots, P(n-1) \rightarrow P(n)$$

wahr sind. (siehe Folie direktes Beweisen) $\square$

## Beweisen durch vollständige Induktion - Beispiel 1

**Theorem 9 (Gaußsche Summenformel)**

*Für jede natürliche Zahl $n \geq 1$ gilt:* $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

**(IA)** $(n = 1)$**:** $\sum_{i=1}^{1} i = 1 = \frac{1 \cdot (1+1)}{2}$

**(IV):** Die Behauptung gelte für ein beliebiges $n \in \mathbb{N}$, $n \geq 1$.

**(IS)** $(n \rightsquigarrow n+1)$**:**

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= \left(\sum_{i=1}^{n} i\right) + (n+1) \\
&\overset{\text{(IV)}}{=} \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+2)(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2} = \frac{(n+1)((n+1)+1)}{2} \qquad \square
\end{aligned}$$

# Beweisen durch vollständige Induktion - Beispiel 2

**Theorem 10**

*Für jede natürliche Zahl $n \geq 1$ gilt: Die Summe $\sum_{i=1}^{n}(2i-1)$ der ersten $n$ ungeraden natürlichen Zahlen beträgt $n^2$.*

**(IA)** $(n = 1)$**:** $\sum_{i=1}^{1}(2i-1) = 2 \cdot 1 - 1 = 1 = 1^2$

**(IV):** Die Behauptung gelte für ein beliebiges $n \in \mathbb{N}$, $n \geq 1$.

**(IS)** $(n \rightsquigarrow n+1)$**:**

$$\begin{aligned}
\sum_{i=1}^{n+1}(2i-1) &= \left(\sum_{i=1}^{n}(2i-1)\right) + (2 \cdot (n+1) - 1) \\
&\overset{\text{(IV)}}{=} n^2 + (2n + 2 - 1) \\
&= n^2 + 2n + 1 \\
&= (n+1)^2 \quad \square
\end{aligned}$$

# Beweisen durch vollständige Induktion - Beispiel 3

**Theorem 11**

*Für jede natürliche Zahl $n \geq 5$ gilt: $2^n > n^2$.*

**(IA) ($n = 5$):** $2^5 = 32 > 25 = 5^2$

**(IV):** Die Behauptung gelte für ein beliebiges $n \in \mathbb{N}$, $n \geq 5$.

**(IS) ($n \rightsquigarrow n + 1$):**

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &\overset{\text{(IV)}}{>} 2 \cdot n^2 = n^2 + n^2 = n^2 + n \cdot n \\ &> n^2 + 3n = n^2 + 2n + n \\ &> n^2 + 2n + 1 = (n+1)^2 \quad \square \end{aligned}$$