Diskrete Mathematik

Sebastian Iwanowski
FH Wedel

Kapitel 3: Beweisverfahren

Referenzen zum Nacharbeiten:

Iwanowski/Lang 3
Meinel 3, 6, 7
Beutelspacher 3 (als unterhaltsame Ergänzung: Beutelspacher 1, 2)
Steger 0.3

3. Beweisverfahren

3.1 Kernstrukturen der Mathematik

- **Voraussetzungen: Axiome**

  Axiome sind Forderungen, die nicht bewiesen werden müssen.
  Sie sind implizite (d.h. häufig nicht erwähnte) Voraussetzungen vieler Aussagen.

- **Benennungen: Definitionen**

  Definitionen sind vereinfachende Schreibweisen. Sie sind keine Aussagen oder Axiome, d.h. weder zu fordern noch zu beweisen.

- **Aussagen: Satz, Lemma, Korollar**

  Sätze, Lemmata oder Korollare sind wahre Aussagen.
  Ob es sich bei einem Sachverhalt um eine Aussage handelt (und nicht um eine Definition oder ein Axiom), ist meistens leicht einzusehen.
  Schwieriger ist es zu beweisen, ob es sich um eine wahre Aussage handelt.

- **Beweise**

  Kette von logischen Schlussfolgerungen, um die Wahrheit einer Aussage, ausgehend von einer Behauptung (häufig in Form von Axiomen) zu belegen.

3. Beweisverfahren

3.1 Kernstrukturen der Mathematik

Das Axiomensystem von Peano für die natürlichen Zahlen:

Gegeben sei eine Menge $\mathbb{N}$ und eine Nachfolgerelation $\sigma \subset \mathbb{N} \times \mathbb{N}$

1) $0 \in \mathbb{N}$
2) Die Nachfolgerelation ist eine Funktion.
3) Die Nachfolgerelation ist injektiv.
4) 0 ist nicht Nachfolger einer natürlichen Zahl.
5) Mit einer endlich oft hintereinandergeschalteten Anwendung der Nachfolgerelation auf 0 kann man *jedes* Element von $\mathbb{N}$ erzeugen.

Satz: Das Axiomensystem von Peano ist minimal.

Die Wegnahme eines einzigen Axioms lässt auch andere Strukturen zu, welche alle anderen Axiome erfüllen, aber nicht als Repräsentation von $\mathbb{N}$ gewünscht sind.

3. Beweisverfahren

3.2 Vollständige Induktion

Die vollständige Induktion ist ein systematisches Beweisverfahren, welches in der Informatik häufige Verwendung findet.

Grundprinzip (einfachste Variante):

Zu beweisen ist eine Aussage der Form A(n) für ein beliebiges $n \in \mathbb{N}$

1) **Induktionsverankerung:** Beweise: Es gilt A (0)
2) **Induktionsschluss:** Beweise: Aus A (n) folgt A (n+1)

   Der Beweis soll die Gültigkeit für A (n) nicht zeigen, sondern voraussetzen.
   Zu zeigen ist nur die Gültigkeit von A (n+1).

   Der Induktionsschluss muss für wirklich alle $n \geq 0$ gelten (keine Einschränkungen!)

Beispiele: siehe Übungsaufgaben

Eigene Übung macht den Meister !

3. Beweisverfahren

3.2 Vollständige Induktion

Verallgemeinertes Grundprinzip:

Zu beweisen ist eine Aussage der Form A(n) für ein beliebiges $n \in \mathbb{N}$

1) **Induktionsverankerung:** Beweise: Es gilt A (0)
2) **Induktionsschluss:** Beweise: Aus A (0), ..., A(n) folgt A (n+1)

Anwendungsbeispiele:

1) Primzahlzerlegung (Existenz):

   Jede natürliche Zahl n > 1 kann in ein Produkt $p_1 \cdot p_2 \cdot \ldots \cdot p_k$ zerlegt werden, wobei alle p_i Primzahlen sind. (Beweis durch Induktion über n)

2) Teilbarkeitsnachweis über Quersummenbildung

   Jede natürliche Zahl n ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist. (Beweis durch Induktion über n)

3. Beweisverfahren

3.2 Vollständige Induktion

Induktive Definition für Funktionen $\mathbb{N} \rightarrow \mathbb{N}$:

Die Funktion wird in 2 Schritten definiert:

i. Die Funktion wird für eine konstante natürliche Zahl definiert (in der Regel 0 oder 1).

ii. Es wird eine Regel angegeben, wie man aus dem Funktionswert des Vorgängers den Funktionswert des Nachfolgers konstruiert

Beispiele:

1) Fakultät $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$

   i) $0! = 1$

   ii) $n! = n \cdot (n-1)!$

2) Fibonaccizahlen F_n

   i) $F_0 = 0 \quad F_1 = 1$

   ii) $F_n = F_{n-1} + F_{n-2}$

3. Beweisverfahren

3.2 Vollständige Induktion

Verallgemeinerung: Rekursive Definitionen für beliebige Mengen:

Die Menge wird in 2 Schritten definiert:

i. Einige Elemente werden explizit angegeben (*terminale Elemente*)

ii. Es werden Regeln angegeben, wie man neue Elemente aus alten Elementen erzeugen kann (*Rekursionsregeln*).

Beispiele:

1) Grammatikdefinitionen über endlichen Alphabeten

   i) Einige konkrete Wörter werden direkt definiert (Konstante aus Terminalsymbolen).

   ii) Produktionsregeln geben an,
   wie man aus vorhandenen Wörtern der Grammatik neue Wörter bilden kann.

2) Backus-Naur-Formen für Syntax von Programmiersprachen
   (wird in anderen Vorlesungen näher besprochen)

3. Beweisverfahren

3.2 Vollständige Induktion

Anwendungen in der Geometrie und Graphentheorie

Beispiel: Färbung von Landkarten

Definitionen:

Eine **Landkarte** ist eine Unterteilung eines zweidimensionalen Gebiets in Zellen (den Ländern), die von eindimensionalen Kurven (den Grenzen) begrenzt werden.
Länder können auch ins Unendliche offen sein.

Eine **zulässige Färbung** einer Landkarte ist eine Zuweisung von Farben an jedes Land der Landkarte derart, dass benachbarte Länder (solche mit einer gemeinsamen Grenze, einzelne Grenzpunkte zählen nicht) unterschiedliche Farben haben.

Satz:

Für jede Landkarte, die dadurch entsteht, dass n Geraden (Kreise) beliebig in eine Ebene gezeichnet werden, existiert eine zulässige Färbung mit 2 Farben.

Beweis: Beutelspacher, Kap. 3.3 (für Geraden)

3. Beweisverfahren

3.3 Beweisstrategien

Direkter Beweis

$$(p \rightarrow q) \land p \Rightarrow q$$

Modus ponens

Beweis durch Kontraposition

$$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p$$

Kontraposition

Indirekter Beweis (Widerspruchsbeweis)

$$(\neg p \rightarrow q) \land (\neg p \rightarrow \neg q) \Rightarrow p$$

Indirekter Beweis

$$(\neg p \rightarrow p) \Rightarrow p$$

Widerspruchsbeweis

$$(\neg p \rightarrow \perp) \Rightarrow p$$

Widerspruchsbeweis

3. Beweisverfahren

3.3 Beweisstrategien

Äquivalenzbeweis

$\mathbf{p \leftrightarrow q \Leftrightarrow (p \rightarrow q) \land (q \rightarrow p)}$

Ersetzen der Äquivalenz durch Implikationen

Beweis durch Fallunterscheidung

$\mathbf{((p_1 \lor p_2) \rightarrow p) \land (p_1 \lor p_2) \Rightarrow p}$

Fallunterscheidung für 2 Fälle

analog: Fallunterscheidung für mehr als zwei Fälle

Abzählbeweis (Schubfachprinzip, Taubenschlagverfahren)

Gegeben **f: M** $\rightarrow$ **N,** wobei **M,N** endlich sind

Dann gilt: **|M|** > **|N|** $\Rightarrow$ **f** ist nicht injektiv