1 Beweistechniken

Nachfolgend wollen wir die wesentlichen Techniken zum Führen eines mathematischen Beweises wiederholen. Dieser Abschnitt kann dabei keinesfalls das intensive Studium dieser Techniken ersetzen, er soll jedoch eine Hilfestellung bieten, um das entsprechende Wissen aufzufrischen. Wir wollen dabei damit beginnen, uns vor Augen zu führen, was ein Beweis überhaupt ist: Ein Beweis ist eine Folge von Aussagen, von denen jede logisch aus den bisherigen folgt (siehe Ableitungsbegriff der Kalküle). Dabei starten wir mit "Dingen", die wir als gültig (wahr) annehmen (siehe Axiome der Kalküle). Als Konsequenz hat ein Beweis drei Teile, einen Anfang, eine Mitte und ein Ende. Der Anfang enthält dabei jene Dinge, die wir als wahr annehmen wollen, wobei die Definitionen der Objekte über die wir sprechen oder aber über sie bewiesene Aussagen dazu gehören. Die Mitte wird aus jenen Aussagen gebildet, die wir jeweils logisch aus dem zuvor gesagten folgern. Das Ende ist die Aussage, die wir beweisen möchten.

Beispiele:

a) Unter Verwendung der Gruppen-Axiome wollen wir zeigen, dass $a\cdot(b-c) = a\cdot b - a\cdot c\ \forall a,b,c\in\mathbb{R}$ gilt. Dabei sei $0\cdot x = x\cdot 0 = 0\ \forall x\in\mathbb{R}$ gegeben.

Anfang: Wir machen uns klar, was uns die Gruppen-Axiome liefern (Assoziativität, Kommutativität, Distributivität, neutrale Elemente, Inverse). Des Weiteren vergegenwärtigen wir uns die Definition von $a-b := a+(-b)$, d. h. die Subtraktion entspricht der Addition des inversen Elementes. Wir nehmen als gegeben an (da z. B. an anderer Stelle bewiesen) $0\cdot x = x\cdot 0 = 0$.

Mitte:

$$\begin{array}{rcll} a\cdot(b-c) & = & a\cdot(b+(-c)) & \text{Definition}\\ & = & a\cdot b + a\cdot(-c) & \text{Distributivität}\\ a\cdot c + a\cdot(-c) & = & a\cdot(c+(-c)) & \text{Distributivität}\\ & = & a\cdot 0 & \text{Inverses bzgl. } +\\ & = & 0 & \text{gegeben}\\ \rightsquigarrow a\cdot(-c) & = & -(a\cdot c) & \text{additives Inverses (Definition)}\\ \rightsquigarrow a\cdot b + a\cdot(-c) & = & a\cdot b - (a\cdot c) & \end{array}$$

Damit folgt mit dem oben gezeigten $a\cdot(b-c) = a\cdot b + a\cdot(-c)$ nun

Ende:

$$a\cdot(b-c) = a\cdot b - (a\cdot c) = a\cdot b - a\cdot c.$$

□

Man mache sich die Bedeutung der letzen Gleichheit klar!

b) Seien f und g Funktionen mit $A \overset{f}{\mapsto} B \overset{g}{\mapsto} C$. Wir zeigen, dass aus f, g injektiv auch $g\circ f$ injektiv folgt.

Anfang: Definition der Injektivität; Definition $(g\circ f)(x) = g(f(x))$; Annahme f, g injektiv (d. h. $(\forall x, x'\in A)(f(x) = f(x') \rightsquigarrow x = x'$) und

$(\forall x, x' \in B)(g(x) = g(x') \rightsquigarrow x = x')$.

Mitte:

$$\begin{array}{lll} (g \circ f)(x) = (g \circ f)(x') & \rightsquigarrow & g(f(x)) = f(f(x')) \qquad \text{Definition} \\ & \rightsquigarrow & f(x) = f(x') \qquad g \text{ injektiv} \\ & \rightsquigarrow & x = x' \qquad f \text{ injektiv} \end{array}$$

Ende: Also $g \circ f$ injektiv, wie zu beweisen war. □

Ist man erst einmal geübt im Führen von Beweisen, ist es nicht mehr erforderlich, diese strenge Strukturierung einzuhalten und insbesondere im Anfangs-Teil alle Details zusammenzutragen, die in den Beweis einfließen können. Es hilft jedoch insbesondere dem Ungeübten typische Fehler beim Beweisen zu vermeiden, die da sind:

- falsche Annahmen treffen;
- zu strake Annahmen treffen;
- Definitionen fehlerhaft anwenden oder die Verwendung der falschen Definitionen.

Aber auch

- zu große Schritte machen (so dass eine Aussage nicht offensichtlich aus den vorherigen folgt und man dabei insbesondere unzulässige Schritte unternimmt);
- "Handwaving" (es muss doch irgendwie so sein, wie denn auch sonst?); eine solche Argumentation ist kein Beweis;
- inkorrekte Logik verwenden, insbesondere die Negation einer Aussage falsch zu bestimmen.

Für die Ausgestaltung eines Beweises stehen verschiedenste Techniken zur Verfügung. Welche dabei sinnvoller Weise zur Anwendung kommt hängt insbesondere von der Art der zu beweisenden Aussage ab.

Implikationen und Äquivalenzen: Viele Behauptungen haben die Form

$$A \rightsquigarrow B \quad \text{bzw.} \quad A_1 \wedge A_2 \wedge \cdots \wedge A_k \rightsquigarrow B.$$

Dabei ist A manchmal nicht ausdrücklich angegeben, in diesem Fall liegt A implizit (z. B. Gruppen-Axiome) vor. Um $A \rightsquigarrow B$ zu beweisen, können wir auf folgende Techniken zurückgreifen

- direkter Beweis: Wir zeigen B unter der Annahme A (siehe Beispiel Injektivität);
- indirekter Beweis (auch Beweis durch Kontraposition): Wir zeigen $\neg A$ unter der Annahme $\neg B$ (d. h. wir zeigen $\neg B \rightsquigarrow \neg A$);

- Beweis durch Widerspruch: Wir zeigen einen Widerspruch unter der Annahme $A \wedge \neg B$ (reductio ad absurdum).

Eine Äquivalenz $A \leftrightarrow B$ zeigt man dann, indem man nacheinander die Implikationen $A \rightsquigarrow B$ und $B \rightsquigarrow A$ zeigt. Dieses Vorgehen bedeutet insbesondere, dass man die Gleichheit zweier Mengen $A = B$ über die Teilmengenbeziehungen $A \subseteq B$ und $B \subseteq A$ beweist ($A \subseteq B$ ist nämlich gleichbedeutend mit $x \in A \rightsquigarrow x \in B$).

Vollständige Induktion: Diese Technik eignet sich insbesondere, um Aussagen für alle $n \in \mathbb{N}$ zu beweisen. Das Grundprinzip der vollständigen Induktion ist dabei

- Induktionsanfang (Anker): Die Aussage gilt für $n = 1$ (bzw. für die kleinste natürliche Zahl, für die sie behauptet wurde);
- Induktionsschritt: Zeige, dass wenn die Aussage für ein beliebiges aber festes $n \in \mathbb{N}$ gilt, dass daraus folgt, die Aussage gilt auch für $n + 1$.

Warum wird so eine Aussage für alle natürlichen Zahlen bewiesen? Hintergrund sind die Peano-Axiome, die die Menge der natürlichen Zahlen wie folgt definieren: 1 ist eine natürliche Zahl; ist n eine natürliche Zahl, dann auch $n+1$. Man mache sich klar, warum so alle $n \in \mathbb{N}$ als natürliche Zahl identifiziert werden und überlege sich dann, warum entsprechend eine vollständige Induktion tatsächlich einen entsprechenden Beweis liefert.
Als Variante existiert die *allgemeine Induktion*, bei der man für den Induktionsschritt annimmt, dass die zu beweisende Aussage für alle n' kleiner gleich einem beliebigen aber festen $n \in \mathbb{N}$ (und ggf. größer einem $k \in \mathbb{N}$) gilt.
Eine vollständige Induktion kann *strukturell* geführt werden. Diese Form eines Beweises ist im Kontext der formalen Sprachen besonders bedeutsam und wird beispielsweise herangezogen, um zu zeigen, dass die von einer Grammatik erzeugte Sprache gleich einer gegebenen ist. Nachfolgendes Beispiel sollen das entsprechende Vorgehen im Detail beleuchten:

Beispiel: Gegeben seien $\mathcal{L} = \{a\} \cdot \{b\}^* \cdot \{c, d\}$ sowie $G = (I, T, P, S)$ mit $I = \{S, B, C\}$, $T = \{a, b, c, d\}$ und

$$P = \left\{ \begin{array}{lcl} S & \rightarrow & aB, \\ B & \rightarrow & bB, \\ B & \rightarrow & C, \\ C & \rightarrow & c, \\ C & \rightarrow & d \end{array} \right\}.$$

Behauptung: G erzeugt *genau* die Sprache $\mathcal{L}$.

Beweis: Wir zeigen zuerst die folgende Hilfsbehauptung. Dazu seien

$$
\begin{aligned}
M_0 &:= \{S\}\,, \\
M_1 &:= \{ab^nB | n \geq 0\}\,, \\
M_2 &:= \{ab^nC | n \geq 0\}\,, \\
M_3 &:= \mathcal{L} = \{ab^nc | n \geq 0\} \cup \{ab^nd | n \geq 0\}\,.
\end{aligned}
$$

Hilfsbehauptung: Für die Menge aller Satzformen $\vartheta(G)$ gilt $\vartheta(G) = M_0 \cup M_1 \cup M_2 \cup M_3 =: M$.

1. $\vartheta(G) \subseteq M$ (1)

   Die Menge aller Satzformen $\vartheta(G)$ ist (rekursiv) aufzählbar, da sie durch Anwenden der Regeln aus P entstehen. Daher können wir über alle $\beta \in \vartheta(G)$ durch eine *strukturelle Induktion* iterieren, in diesem Fall eine Induktion über die Anzahl N der Ableitungsschritte in G.

   Induktionsanfang: Startsymbol [$N = 0$ Schritte] $S \in M_0 \curvearrowright S \in M$. ✓

   Induktionsvoraussetzung: Für eine nicht-leere Teilmenge $T \subseteq \vartheta(G)$, die alle Satzformen umfasse, die sich in höchstens N Schritten ableiten lassen, gelte die [Hilfhilfs-] behauptung (1), d. h. $(\forall \beta \in T)\ (\beta \in M)$.

   Induktionsschritt: Sei $\beta \in T$ beliebig. Nach Induktionsvoraussetzung gilt dann einer der folgenden Fälle:

   (a) $\beta \in M_0 \rightsquigarrow \beta = S$.
   Dann kann nur die Regel $S \to aB$ angewendet werden; $\beta' = aB \in M_1$ [mit $n = 0$]. Das bedeutet in diesem Fall sind auch alle Satzformen mit Ableitungen der Länge $N + 1$ in M.

   (b) $\beta \in M_1 \rightsquigarrow (\exists n \geq 0)\ (\beta = ab^nB)$.
   Hier können 2 Regeln angewendet werden

   - $B \to bB \rightsquigarrow \beta' = ab^nbB = ab^{n+1}B \in M_1$,
   - $B \to C \rightsquigarrow \beta' = ab^nC \in M_2$.

   Beide Ableitungen enden wieder mit Satzformen in M.

   (c) $\beta \in M_2 \rightsquigarrow \exists n \geq 0\ (\beta = ab^nC)$.
   Alle möglichen Regeln sind:

   - $C \to c \rightsquigarrow \beta' = ab^nc \in M_3$,
   - $C \to d \rightsquigarrow \beta' = ab^nd \in M_3$.

   (d) $\beta \in M_3 \rightsquigarrow \exists n \geq 0\ (\beta = ab^nc \vee \beta = ab^nd)$.
   Keine Ableitung mehr möglich.

   Da es keine weiteren Möglichkeiten für $\beta \in M$ gibt, haben wir für jedes β', das sich in $N + 1$ Schritten erzeugen lässt, gezeigt, dass es in M enthalten ist.

Nach dem Induktionsprinzip haben wir damit bewiesen, dass jede in G ableitbare Satzform in einer der 4 Mengen M_0, M_1, M_2 *oder* M_3 liegt.

Aber warum hilft uns das mit unserer [Haupt-] Behauptung $\mathcal{L}(G) = \mathcal{L}$?

Weil erstens M_3 genau der Menge $\mathcal{L}$ entspricht und zweitens M_0, M_1 und M_2 nur Satzformen enthalten, die mindestens ein *Nichtterminal* enthalten, d. h. „unfertige" Satzformen. Da die Menge $\vartheta(G)$ aber abgeschlossen ist bezüglich Ableitungen in G müssen alle diese unfertigen Satzformen bei weiterer Ableitung letztlich in terminalen Zeichenreihen aus $M_3 = \mathcal{L}$ münden. Klar?

2. $\vartheta(G) \supseteq M$ (2)

Dieser zweite Teil der [Hilfs-] Behauptung lässt sich aufteilen: Sei $\alpha \in M_0 \cup M_1 \cup M_2 \cup M_3$ beliebig. Dann gibt es offensichtlich ein j mit $\alpha \in M_j$ und es reicht, für jede Menge einzeln zu zeigen, dass sie in $\vartheta(G)$ enthalten ist.

(a) $\alpha \in M_0 \rightsquigarrow \alpha = S \in \vartheta(G)$, denn jede Ableitung beginnt mit dem Startsymbol S, womit dieses selbst natürlich auch eine ableitbare Satzform ist.

(b) $M_1 \subseteq \vartheta(G)$:
Das zeigt man mittels vollständiger Induktion über den Parameter n aus der Definition von M_1:

Induktionsanfang: $n = 0 \rightsquigarrow \alpha = aB$.
Es ist $S \Rightarrow aB \in \vartheta(G)$. ✓

Induktionsvoraussetzung: Sei $ab^nB \in \vartheta(G)$.

Induktionsschritt: Nach Induktionsvoraussetzung existiert für ab^nB eine Ableitung in G, d. h. $S \stackrel{*}{\Rightarrow} ab^nB$. Mittels der Regel $B \to bB$ lässt sich diese fortsetzen:

$$S \stackrel{*}{\Rightarrow} ab^nB \Rightarrow ab^n\, bB = ab^{n+1}B.$$

Damit haben wir eine Ableitung für $ab^{n+1}B$ gefunden, also ist $ab^{n+1}B \in \vartheta(G)$.

(c) $\alpha \in M_2 \rightsquigarrow \alpha \in \vartheta(G)$:
Nach Definition ist $\alpha = ab^nC$ für ein $n \geq 0$. Wie gerade gezeigt, ist $ab^nB \in \vartheta(G)$ [mit dem gleichen n]; es gibt also eine Ableitung

$$S \stackrel{*}{\Rightarrow} ab^nB$$

die sich mit $B \to C$ fortführen lässt:

$$S \stackrel{*}{\Rightarrow} ab^nB \Rightarrow ab^nC \;\rightsquigarrow\; ab^nC = \alpha \in \vartheta(G).$$

(d) $\alpha \in M_3 \rightsquigarrow \alpha \in \vartheta(G)$:
Analog zu eben heißt $\alpha \in M_3$: $(\exists n \geq 0)\ (\alpha = ab^nc \vee \alpha = ab^nd)$.
Wir verwenden wieder bereits Gezeigtes, nämlich dass es eine Ableitung

$$S \stackrel{*}{\Rightarrow} ab^nC$$

gibt, die wir nun auf zwei Arten vollenden können

$$S \stackrel{*}{\Rightarrow} ab^nC \Rightarrow ab^nc \qquad \text{mittels } C \to c,$$
$$S \stackrel{*}{\Rightarrow} ab^nC \Rightarrow ab^nd \qquad \text{mittels } C \to d.$$

Für alle möglichen $\alpha \in M_3$ haben wir also eine Ableitung in G gefunden.

Da $M_3 = \mathcal{L}$ haben wir somit insbesondere für alle $w \in \mathcal{L}$ eine Ableitung gefunden, d. h. alle Wörter von $\mathcal{L}$ lassen sich in G erzeugen.

Zusammen mit dem Resultat aus (1) ergibt sich die Behauptung. □

Es bedarf einiger Übung, entsprechende Beweise selbständig führen zu können. In den Aufgaben zu Kapitel 2 wird dazu zahlreich Gelegenheit geboten.

Existenzquantoren: Die Existenz eines Objektes mit einer entsprechenden Eigenschaft zeigt man oft konstruktiv, d. h. durch die Benennung eines Weges, wie man zu dem behaupteten Objekt gelangt. Beispiele finden sich in diesem Buch viele, wie etwa die Konstruktion eines äquivalenten DEA zu gegebenem NEA oder die der Simulation von `If` $x = 0$ durch `Loop`. Auch ein indirekter Beweis ist möglich, indem man die Annahme $\neg(\exists x : E(x)) \equiv \forall x : \neg E(x)$ zu einem Widerspruch führt. Hier kann dann ein einfaches Gegenbeispiel genügen. Möchte man zeigen, dass es genau eine $x \in D$ mit einer speziellen Eigenschaft E gibt, so zeigt man

1. $\exists x_0 \in D : E(x_0)$ (mindestens ein Element);
2. $\forall x \in D \setminus \{x_0\} : \neg E(x)$ (kein weiteres), oder
   $(\forall x \in D)(\forall y \in D) : (E(x) \wedge E(y) \rightsquigarrow x = y)$.

Eine Varinate sind Aussagen, für die die Nicht-Existenz $(\neg(\exists x : E(x)))$ eines Objektes mit Eigenschaft E bewiesen werden soll. Hier kann man die Annahme der Existenz zu einem Widerspruch führen.

Allquantoren: Hier geht es darum, Eigenschaften für alle Objekte eine bestimmten Art zu beweisen. Für viele solche Eigenschaft eignen sich Induktionsbeweise. Oft bietet sich aber auch ein indirekter Beweis ein. Will man Aussage mit Allquantoren direkt beweisen, so ist meist eine Fallunterscheidung (z. B. positive und negative Zahlen) hilfreich. Hier ist auf die Vollständigkeit der Unterscheidung zu achten oder diese sogar u. U. zu beweisen (nämlich dann, wenn ihre Vollständigkeit nicht offensichtlich ist).
Zuletzt sei angemerkt, dass Abhängigkeiten von Quantoren bestehen können. So können Existenzaussagen für alle x einer bestimmten Art A wie etwa in

$$(\forall x \in A)(\exists y \in B) : E(x, y)$$

getroffen werden. Dabei ist das y als dem jeweiligen x zugeordnet zu betrachten (gebunden). Dies kann man sich in einem Beweis zu Nutze machen, indem man

beispielsweise zu jedem $x \in A$ ein entsprechendes $y \in B$ konstruktiv angibt, etwa durch die Angabe einer Funktion f, welche y aus x berechnet. Für dieses f ist dann $\forall x \in A : E(x, f(x))$ zu zeigen.