INFORMATIK I
ZENTRALÜBUNG AM 16.11.2005

MATTHIAS HÖLZL
LMU MÜNCHEN

Inhaltsverzeichnis

1. Beweismethoden

Zum Beweis mathematischer Aussagen stehen verschiedene Beweismethoden zur Verfügung. Zu den am häufigsten verwendeten Methoden gehören:

- Direkter Beweis
- Deduktionskriterium (Implikations-Eliminations-Regel)[1]
- Beweis durch Fallunterscheidung[1]
- Widerspruchsbeweis
- Mathematische Induktion

In den meisten Beweisen werden verschiedene Beweismethoden kombiniert. Zum Beispiel wird in einem Induktionsbeweis die Induktionsaussage häufig durch einen direkten Beweis in Verbindung mit der Induktionsvoraussetzung gezeigt.

1.1. **Direkter Beweis.** Als „direkte Beweise" bezeichnet man Beweise, bei denen man die zu zeigende Behauptung unmittelbar aus Voraussetzungen ableitet, deren Wahrheit bekannt ist. Häufig verwendete Schritte in direkten Beweisen sind z.B. Anwendung von Modus Ponens oder direktes Ausrechnen arithmetischer Gleichungen.

1.1.1. *Modus Ponens.* Die Schlussweise des *Modus Ponens* (oft als *MP* abgekürzt, eigentlich *Modus ponendo ponens*) ist ein Beweis, der nach folgendem Schema abläuft: Aus den *Prämissen* A und $\mathsf{A} \implies \mathsf{B}$ folgt die *Konklusion* B. Anders ausgedrückt: Wenn man weiß, dass eine Aussage A wahr ist, und wenn man weiß, dass aus der Aussage A die Aussage B folgt, dann weiß man auch, dass B wahr ist.

[1] Dieses Beweisverfahren wurde in der Übung nicht besprochen.

Beispiel 1. Wenn wir z.B. wissen, dass die beiden folgenden Aussagen zutreffen (wahr sind):

- Wenn es regnet wird die Straße nass.
- Es regnet.

Dann dürfen wir folgern, dass auch die Aussage "Die Straße wird nass" wahr ist.

Beispiel 2. Das „traditionelle" Beispiel für den Modus Ponens ist folgendes: Alle Menschen sind sterblich (d.h. wenn jemand ein Mensch ist, dann ist diese Person sterblich), Sokrates ist ein Mensch. Also ist Sokrates sterblich.[2]

1.1.2. *Ausrechnen.* Eine weitere Möglichkeit direkte Beweise zu führen ist das Ausrechnen bzw. Umformen arithmetischer Gleichungen.

Beispiel 3. Wir wollen die folgende Behauptung zeigen:

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

Anschaulich kann man das Problem nach dem folgenden Verfahren lösen. Man schreibt die Summe der Zahlen von 1 bis n zweimal hin, einmal von vorne und einmal von hinten beginnend:

$$\begin{array}{ccccccccccc}
0 & + & 1 & + & 2 & + & 3 & + & \cdots & + & n \\
n & + & (n-1) & + & (n-2) & + & (n-3) & + & \cdots & + & 0 \\
\hline
n & + & n & + & n & + & n & + & \cdots & + & n
\end{array}$$

Dann hat man $n+1$ Summanden, die jeweils den Wert n haben, also ergibt sich für die Summe $2\cdot\sum_{i=0}^{n} i$ der Wert $n\cdot(n+1)$. Das ist in der angegebenen Form kein mathematischer Beweis. (Faustregel: Wenn in einem Beweisversuch "$\cdots$" vorkommt ist es kein gültiger Beweis.)

Wir können den anschaulich formulierten Beweisversuch aber in einen gültigen direkten Beweis überführen. Statt der Aussage

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

zeigen wir entsprechend der vorhergehenden Veranschaulichung die äquivalente Aussage

$$2\cdot\sum_{i=0}^{n} i = n(n+1)$$

durch Umformung:

$$2\cdot\sum_{i=0}^{n} i = \sum_{i=0}^{n} i + \sum_{i=0}^{n} i$$

[2] Bei kritischer Betrachtung kann man aber argumentieren, dass dieses Beispiel besser durch eine Kombination mit der Eliminationsregel für den Allquantor formalisiert wird als durch reinen Modus Ponens.

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

Dabei setzen wir voraus, dass die gängigsten Rechenregeln für Produkte und Summen (z.B. $2 \cdot n = n + n$) bereits bewiesen sind.

1.2. **Deduktionskriterium.** Das *Deduktionskriterium* ist gewissermaßen das Gegenstück zum Modus Ponens: Um eine Aussage $A \implies B$ aus Vorausetzungen $V_1, \ldots, V_n$ zu beweisen nimmt man die Aussage A an, und zeigt, dass unter dieser zusätzlichen Voraussetzung die Aussage B gilt. (Man zeigt also: Aus den Voraussetzungen $V_1, \ldots, V_n, A$ folgt die Aussage B.) Dann gilt auch, dass aus $V_1, \ldots, V_n$ die Aussage $A \implies B$ folgt.

Es gibt wenige Beweise, die allein durch das Deduktionskriterium geführt werden können, meist dient das Deduktionskriterium dazu, eine zu beweisende Aussage so umzuformen, dass andere Beweisregeln anwendbar werden. Ein triviales (und etwas sophistisches) Beispiel ist das folgende:

Beispiel 4. Es gilt: $A \wedge B \implies A$. Zum Beweis mittels Deduktionskriterium nehmen wir an, dass $A \wedge B$ gilt. Dann gelten aber sowohl A als auch B, also gilt insbesondere A. Daraus folgt die Behauptung.

1.3. **Beweis durch Fallunterscheidung.** Wenn wir Aussage A, B und C haben, für die die folgenden Eigenschaften gelten: $A \vee B$, $A \implies C$, $B \implies C$, dann gilt auch C.

Beispiel 5. Der Betrag einer reellen Zahl x ist immer nichtnegativ. Denn es gilt: $x < 0 \vee x \geq 0$. Falls $x < 0$ ist, so ist $|x| = -x$ und $-x > 0$. Falls $x \geq 0$ ist, so ist $|x| = x$ also $|x| \geq 0$.

(Bei diesem Beispiel wurden die Rechenregeln für reelle Zahlen als Voraussetzungen angenommen.)

1.4. **Widerspruchsbeweis.** In der klassischen Logik gilt für jede Aussage A, dass entweder A oder $\neg A$ wahr ist, dass also gilt $A \vee \neg A$. Diese Eigenschaft nutzt man beim Widerspruchsbeweis (auch *Reduction ad Absurdum* genannt) aus.

Ein *Widerspruch* ist eine Aussage B, für die gleichzeitig B und $\neg B$ gelten.

Wenn aus Voraussetzungen $V_1, \ldots, V_n$ *ein* Widerspruch $B \wedge \neg B$ folgt, so gilt für jede beliebige Aussage C, dass aus $V_1, \ldots, V_n$ auch die Aussage $C \wedge \neg C$ folgt.[3] Insofern sind Voraussetzungen, die zu Widersprüchen führen uninteressant, da dann jede Aussage sowohl „wahr“ als auch „falsch“ ist.

[3] Der Beweis geht folgendermaßen: Man kann sich leicht überlegen (z.B. mit Wahrheitstafeln), dass gilt $\neg B \implies (\neg B \vee (C \wedge \neg C))$. Da $\neg B$ wahr ist folgt also mittels Modus Ponens, dass $\neg B \vee (C \wedge \neg C)$ gilt; das ist (siehe z.B. Blatt 1) äquivalent zu $B \implies (C \wedge \neg C)$. Da auch B gilt erhält man durch nochmalige Anwendung von Modus Ponens die Aussage $C \wedge \neg C$.

Um A mit einem Widerspruchsbeweis aus Voraussetzungen $V_1, \dots V_n$ zu zeigen geht man folgendermaßen vor: Man nimmt $\neg A$ an und leitet daraus einen Widerspruch her, es gilt also: aus $V_1, \dots, V_n, \neg A$ folgt $B \wedge \neg B$. Somit gilt nach dem gerade Gezeigten auch: aus $V_1, \dots, V_n, \neg A$ folgt A. Nach dem Deduktionskriterium folgt aus $V_1, \dots, V_n$ also $\neg A \implies A$. Da immer gilt $A \implies A$ ergibt sich mit einer Fallunterscheidung, die Aussage: Aus $V_1, \dots, V_n$ folgt A.

Man hat also folgendes Schema:

- Annahme von $\neg A$, Herleitung eines Widerspruchs.
- Daraus folgt A.

Beispiel 6. Zu zeigen: Es gibt keine größte Primzahl.

- Annahme (um einen Widerspruch zu erhalten): Es gibt eine größte Primzahl.
- Seien $p_1, \dots p_n$ alle Primzahlen. Dann gilt für alle i mit $1 \leq i \leq n$: $(p_1 \cdots p_n + 1) \bmod p_i = 1$. Somit ist $p_1 \cdots p_n + 1$ von keiner Primzahl aus $\{p_i \mid 1 \leq i \leq n\}$ teilbar. Somit gibt es eine Primzahl, die größer ist als p_n. Also sind $p_1, \dots p_n$ nicht alle Primzahlen.
- Die Aussage „Es gibt eine größte Primzahl“ führt zu einem Widerspruch, somit kann es keine größte Primzahl geben.

1.5. Induktion.

1.5.1. *Induktionsbeweis (Analysis).* Die einfachste Form der Induktion ist der bekannte „Schluss von n auf $n+1$“. Hier zeigt man, dass die zu beweisende Aussage für die Zahl 0 gilt, und dass man „von n auf $n+1$ schließen kann“. Anschaulich gesprochen zeigt man die Richtigkeit der Aussage „von unten“ her: Die Aussage gilt für 0, deshalb gilt sie für $0+1$, deshalb gilt sie für $0+1+1$, etc. Da man aber jede natürliche Zahl irgendwann durch fortgesetzte Addition von 1 erreicht, ist dadurch die Aussage für alle natürlichen Zahlen bewiesen. Das Induktionsschema ist also:

- Zeige die zu beweisende Aussage für $n = 0$.
- Zeige die Aussage für $n+1$ *unter der Voraussetzung, dass sie für n gilt.*

Beispiel 7.

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

Die Aussage gilt für $n = 0$:

$$\sum_{i=0}^{0} i = 0 = \frac{0 \cdot 1}{2}$$

Wenn die Aussage für eine Zahl n gilt, so gilt sie auch für $n+1$:

$$\begin{aligned}
\sum_{i=0}^{n+1} i &= \sum_{i=0}^{n} i + (n+1) \\
&= \frac{n(n+1)}{2} + n + 1 = \frac{n(n+1) + 2n + 2}{2} \\
&= \frac{n^2 + n + 2n + 2}{2} = \frac{(n+1)(n+2)}{2}
\end{aligned}$$

1.5.2. *Induktionsbeweis (Werteverlauf).* Statt „von unten nach oben“ vorzugehen kann man auch den umgekehrten Weg wählen: Um die Aussage für n zu zeigen nimmt man an, dass man sie für alle kleineren Zahlen $0, \dots, n-1$ bereits bewiesen hat und zeigt die Gültigkeit der Aussage unter dieser Voraussetzung. Der Beweis für jede der Zahlen m aus $0, \dots, n-1$ geht wieder nach dem selben Schema: Wir nehmen an, dass die Aussage für alle kleineren Zahlen $0, \dots, m-1$ bereits bewiesen ist, und zeigen die Aussage unter dieser Voraussetzung für m. Die natürlichen Zahlen haben eine Eigenschaft, die garantiert, dass dieses Beweisverfahren funktioniert: Nach endlich vielen Schritten muss der Beweis für die Zahl 0 geführt werden, da es für jede natürliche Zahl n nur endlich viele natürliche Zahlen gibt, die kleiner als n sind. Und für die Zahl 0 müssen wir zeigen, dass die Aussage für 0 gilt, wobei wir annehmen dürfen, dass sie für alle natürlichen Zahlen, die kleiner sind als 0 gilt. Da es aber keine natürlichen Zahlen gibt, die kleiner sind als 0 heißt das schlicht: Wir müssen die Aussage für die Zahl 0 beweisen. Dann sind wir aber wieder in der gleichen Situation wie vorher: Für den Beweis, dass die Aussage für 1 gilt, haben wir nur angenommen, dass die Aussage für 0 gilt, also folgt aus dem Beweis für 0 der Beweis für 1, usw. Also erhalten wir das folgende Induktionsschema durch Werteverlauf:

Um zu zeigen, dass eine Aussage für alle natürlichen Zahlen n gilt:

- Zeige die Aussage für n *unter der Voraussetzung, dass sie für alle* $n' < n$ *gilt.*

1.5.3. *Induktion für fundierte Mengen (Werteverlauf).* Wir haben bei der Begründung, dass dieses Induktionsschema korrekt ist nur eine wesentliche Eigenschaft der natürlichen Zahlen benutzt, nämlich die, dass jede „absteigende Kette“ natürlicher Zahlen endlich ist; d.h., es gibt keine unendlich lange Kette $n_0, n_1, \dots$ für die gilt $n_i > n_{i+1}$. Daher können wir das Werteverlaufsschema auch auf andere Mengen verallgemeinern, die diese Eigenschaft haben:

Um zu zeigen, dass eine Aussage für alle Elemente einer *fundierten Menge*, d.h. einer Menge auf der es eine fundierte Relation $\prec$ gibt, gilt:

- Zeige die Aussage für n *unter der Voraussetzung, dass sie für alle* $n' \prec n$ *gilt.*

1.5.4. *Induktion für beliebeige Mengen (Abbildung in eine fundierte Menge).* Seien A eine beliebige Menge, M eine Menge mit einer fundierten Relation $\prec$ und $h : A \to M$ eine Funktion. Dann kann man auf der Menge A eine Relation $\prec_A$ folgendermaßen definieren: für alle $x, y \in A$ gilt $x \prec_A y$ genau dann, wenn $h(x) \prec h(y)$ gilt. Man kann sich leicht überlegen, dass die so definierte Relation $\prec_A$ auf A ebenfalls eine fundierte Relation ist. Nach dem Werteverlaufsschema für fundierte Mengen kann man also Induktionsbeweise für A bezüglich der Relation $\prec_A$ führen. Wenn man die Definition der Relation $\prec_A$ nicht angeben will, kann man das Werteverlaufsschema folgendermaßen umformulieren:

Um zu zeigen, dass eine Aussage für alle Elemente einer *beliebigen Menge* A gilt:

- Seien M eine Menge, $\prec$ eine fundierte Relation auf M, $h : A \to M$ eine Funktion, so dass für alle $x \in A$ gilt: Die Aussage gilt für x *unter der Voraussetzung, dass sie für alle* y *mit* $h(y) \prec h(x)$ *gilt.*