WS 2013/14

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Esparza)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2013WS/ds/uebung/

6. November 2013

ZÜ IV

Übersicht:

1. Fragen, Anregungen?
2. Thema: Informelles präzises Beweisen
3. Hinweise und Tipps zu HA Blatt 4

1. Fragen, Anregungen?

Ihre Fragen in der letzten ZÜ zum Thema Beweise
haben sich in der heutigen ZÜ bereits niedergeschlagen!

Aktuelle Fragen?

Anregungen?

2. Thema: Informelles präzises Beweisen

Wir haben über mathematische Gegenstände bereits so viel gelernt, dass wir **präzise** mathematische Beweise verstehen und selbst formulieren können.

Da wir dabei nur Bezug nehmen auf die natürliche Sprache und

„gesunden Menschenverstand“,

sind diese Beweise **informell**.

Bemerkung:
Das informelle Verständnis von mathematischen Gegenständen ist eine selbstverständliche Voraussetzung jeglicher Formalisierung von Inhalten.

2.1 Überführung von Aussagen in Beweise

Aussagen können durch Verfahren (Vorgänge) interpretiert und bewiesen werden und umgekehrt.

Eine Aussage der Form

$$A \Rightarrow B \qquad \text{(Implikation)}$$

kann bewiesen werden durch

Annahme:	Es gilt A.	
Dann	wird B bewiesen.	(Inferenz)

Analog:

Beweis einer „prädikatenlogischen" Aussage der Form

> für alle $x \in M$ gilt die Eigenschaft $P(x)$
> (oder a.a. $\forall x \in M : P(x)$).

durch

Annahme:	Sei x ein beliebiges Element aus M. (A.a. sei $x \in M$ beliebig.)
Dann	wird $P(x)$ bewiesen.

2.2 Gleichheit von Mengen

Die Aussage einer Mengengleichheit $M = N$ kann gleichwertig übersetzt werden in die Konjunktion von Implikationen

$$\underbrace{\underbrace{x \in M}_{A} \Rightarrow \underbrace{x \in N}_{B}}_{M \subseteq N} \quad \text{und} \quad \underbrace{\underbrace{x \in N}_{B} \Rightarrow \underbrace{x \in M}_{A}}_{N \subseteq M},$$

die allerdings für alle Objekte x gelten muss.

Bemerkung: die Sprechweise ,,für alle x" drückt lediglich eine Konjunktion über alle mit Objekten instantiierten Aussageformen $x \in M$ bzw. $x \in N$ aus.

2.3 Beispiel Distributivität des Relationenprodukts

Für alle Mengen M und binäre Relationen R, S, T über M, d. h. $R, S, T \subseteq M \times M$, gilt die Distributivität des Relationenprodukts $\circ$ gegenüber der Mengenvereinigung $\cup$ von Relationen, d.h., es gilt

$$R \circ (S \cup T) = (R \circ S) \cup (R \circ T)\,.$$

Bemerkung:

Es wird auch gerne die folgende andere Sprechweise für die Formulierung der Voraussetzungen einer Behauptung gewählt:

„Seien M eine Menge und R, S, T binäre Relationen über M ... “ bedeutet, dass die obige Gleichung für alle M, R, S und T gilt.

Man kann auch sagen
„Seien M eine beliebig gewählte Menge und
R, S, T beliebig gewählte binäre Relationen über M“.

Um obige Distributivität beweisen zu können, braucht in allen Fällen nur $R, S, T \subseteq M \times M$ und sonst nichts bekannt zu sein.

Beweis:

Wir verwandeln nun die obige Behauptung in ein Verfahren zur Berechnung ihres Wahrheitswertes.

Der erste Schritt ist immer die Annahme, dass die Voraussetzungen alle gelten. Dazu dient der Text:

Seien M eine beliebig gewählte Menge und R, S, T beliebig gewählte binäre Relationen über M.

In unserem logischen Denkraum haben wir nun Platzhalter für die angenommenen Objekte M, R, S, T erzeugt.

Wir müssen nun für diese Objekte eine Mengengleichung $U = V$ beweisen, die nichts anderes bedeutet als die Konjunktion von Implikationen:

Für alle $x \in M \times M$ gilt

$$x \in U \Rightarrow x \in V \quad \text{und} \quad x \in V \Rightarrow x \in U\,.$$

Hier sind $U = R \circ (S \cup T)$ und $V = (R \circ S) \cup (R \circ T)$ gesetzt.

Wir beweisen zunächst für alle $x \in M \times M$ die Implikation

$$x \in R \circ (S \cup T) \implies x \in (R \circ S) \cup (R \circ T)$$

wie folgt.

Zweiter Schritt:

Wenn für alle x einer Menge eine Implikation gezeigt werden soll, dann nimmt man einfach ein x an, das die Prämisse der Implikation erfüllt. Also:

Sei $x \in M \times M$, so dass $x \in R \circ (S \cup T)$ gilt.

Da x ein Tupel ist, können wir gleichzeitig $x = (u, v)$ annehmen mit irgenwelchen $u, v \in M$, über die wir natürlich zunächst nichts Näheres wissen.

Allerdings wissen wir, dass $x \in R \circ (S \cup T)$ gilt, d. h.

$$x = (u, v) \in R \circ (S \cup T)\,.$$

Dies bedeutet, dass (u, v) aus den Relationen R und $S \cup T$ hervorgeht, und zwar durch Produktbildung.

Es muss folglich ein Element $w \in M$ existieren, so dass sowohl $(u, w) \in R$ gilt als auch $(w, v) \in (S \cup T)$.

Wir können also annehmen:

Sei $w \in M$, so dass $(u, w) \in R$ und $(w, v) \in (S \cup T)$ gilt.

Wir haben nun alle Informationen beisammen, die wir aus den Prämissen ableiten können.

Was aber müssen wir nun zeigen?

Zu zeigen ist:

$$x \in (R \circ S) \cup (R \circ T)\,. \qquad (*)$$

Natürlich können wir für den Beweis nun alles benützen, was wir an Informationen haben.

Also $x = (u, v)$ und $(u, w) \in R$ und $(w, v) \in (S \cup T)$.

Da wir nicht wissen, ob $(w, v) \in S$ oder $(w, v) \in T$ gilt, müssen wir prüfen, ob in beiden Fällen die Aussage $(*)$ ableitbar ist.

Wir müssen eine Fallunterscheidung machen!

Fallunterscheidung

Fall 1: $(w, v) \in S$.

Wir haben $(u, w) \in R$ und $(w, v) \in S$, d.h. definitionsgemäß $(u, v) \in R \circ S$.

Daraus folgt wegen Mengeninklusion $(R \circ S) \subseteq (R \circ S) \cup (R \circ T)$, dass $(u, v) \in (R \circ S) \cup (R \circ T)$ gilt, d.h.

$$x \in (R \circ S) \cup (R \circ T)\,.$$

Fall 2: $(w, v) \in T$.

Analog folgt

$$x \in (R \circ S) \cup (R \circ T)\,.$$

W.z.b.w.

Nun bleibt der Beweis der umgekehrten Implikation.

Für alle $x \in M \times M$ gilt

$$x \in (R \circ S) \cup (R \circ T) \implies x \in R \circ (S \cup T)$$

Den Beweis dieser Umkehrung wollen wir dem Leser überlassen.
Er ist weitgehend analog dem schon vorgestellten Beweis.

Im Folgenden wollen wir im Vorgriff auf prädikatenlogische Identitäten einen sehr kurz erscheinenden Beweis darstellen, der äquivalente Umformungen von Ausdrücken benutzt.

Vorausblick auf kompakten Äquivalenzbeweis.
Dabei lesen wir zunächst das Zeichen $\exists w$ ganz informell als ,,es existiert w" in der natürlichen Wortbedeutung:

$$
\begin{aligned}
&(u,v) \in R \circ (S \cup T) \\
&\quad \Leftrightarrow \quad \exists w \; ((u,w) \in R \;\wedge\; (w,v) \in (S \cup T) \,) \\
&\quad \Leftrightarrow \quad \exists w \; ((u,w) \in R \;\wedge\; ((w,v) \in S \vee (w,v) \in T) \,) \\
&\quad \Leftrightarrow \quad \exists w \; ((u,w) \in R \wedge (w,v) \in S) \;\vee\; ((u,w) \in R \wedge (w,v) \in T) \,) \\
&\quad \Leftrightarrow \quad \exists w \; ((u,w) \in R \wedge (w,v) \in S) \quad \vee \\
&\qquad\qquad\quad \exists w \; ((u,w) \in R \wedge (w,v) \in T)) \\
&\quad \Leftrightarrow \quad (u,v) \in R \circ S \;\vee\; (u,v) \in R \circ T \\
&\quad \Leftrightarrow \quad (u,v) \in (R \circ S \cup R \circ T)\,. \\
&(u,v) \in (R \circ S \cup R \circ T)\,.
\end{aligned}
$$

Bemerkungen:

Der ursprüngliche Beweis der Gleichung erscheint sehr aufwendig aber elementar.

Der äquivalenzbasierte Beweis ist wesentlich kürzer.

Man lernt daraus, dass der mathematische Formalismus auf engstem Raum eine große Informationsmenge darstellen kann.

Allerdings ersetzt der eine Beweis nicht den anderen, wenn es um das Verständnis der Inhalte geht.

3. Hinweise und Tipps zu HA Blatt 4

Die folgenden Hinweise und Tipps zu Hausaufgaben der DS-Übungsblätter von Prof. Esparza sind für die Bearbeitung nicht notwendig, möglicherweise aber hilfreich.

Man sollte zunächst versuchen, die Hausaufgaben ohne Hilfestellung zu lösen.

ad HA 4.3:

Sei $F \rightarrow H$ allgemeingültig.
Nehmen Sie an, dass in Formel F eine Variable x vorkommt, die aber **nicht** in der Formel H vorkommt.

Ersetzen Sie in der Formel F die Variable x durch den Ausdruck **true** bzw. **false** und bezeichnen Sie die erhaltene Formel mit F_t bzw. F_f.

Nun ist klar, dass $F \rightarrow F_t \vee F_f$ allgemeingültig ist. (Beweis?)

Warum ist nun $F_t \vee F_f \rightarrow H$ ebenfalls allgemeingültig?

Erschließen Sie sich alle Fragen der Aufgabe durch iterierte Argumentation und beantworten sind dann die Fragen gemäß Aufgabenstellung.