

WS 2012/13

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2012WS/ds/uebung/>

31. Oktober 2012

ZÜ II

Übersicht:

1. **Übungsbetrieb:** Anmeldung zu Gruppen, Fragen
2. **Themen:** Überführung von Aussagen in Beweise
Prädikatenlogik und Normalformen
Beweisarten
3. **Vorbereitung:** auf TA Blatt 3:

1. Übungsbetrieb

1.1 Stand der Anmeldungen

Bioinformatiker bitte in Übungsgruppen anmelden!

1.2 Fragen

Fragen zum Übungsbetrieb?

2. Themen

2.1 Thema: Überführung von Aussagen in Beweise

Der aussagenlogische Ausdruck

$$A \Rightarrow B$$

Implikation

kann bewiesen werden durch

Annahme: Es gilt A .

Dann wird B bewiesen.

Inferenz

Analog: Beweis eines prädikatenlogischen Ausdrucks $\forall x P(x)$.

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

2.2 Thema: Prädikatenlogik und Normalformen

Wiederholung Aussagenlogik:

Aussage

Wahrheitswert

Junktor, Aussagenverbindung, Aussagenfunktion

Aussagenlogischer Ausdruck, Formel, Strukturbaum

Aussagenvariable

Aussagenkalkül

Wahrheitsfunktion, Belegung

Formale Semantik der Aussagenlogik

Wiederholung Prädikatenlogik:

Aussageform (mit freien Variablen für Individuen)

Spezialisierung und Quantifizierung von Variablen

Quantifizierte Variablenvorkommen

Prädikat, Prädikatsymbol, Prädikatvariable

Stelligkeit von Prädikaten

Prädikatenlogische Formel, Prädikatenkalkül

Attribute: Eigenschaft, Relation,

Formale Semantik einer Formel, Interpretation

Weitere Begriffe:

Logische Äquivalenz

Tautologie

Widerspruch

Normalformen:

Aussagenlogische Formel: Disjunktive Normalform

Aussagenlogische Formel: Konjunktive Normalform

Prädikatenlogische Formel: Pränexe Normalform

Bemerkung: Für alle Formeln lassen sich entsprechende, logisch äquivalente Normalformen herleiten.

3. Vorbereitung auf TA Blatt 3

3.1 VA 1, Erfüllbarkeit

- 1 Geben Sie eine aussagenlogische Formel F an, so dass F und $\neg F$ erfüllbar ist!

Antwort:

Sei $F = (x \equiv y)$.

Dann ist die Formel F unter der Belegung $x \mapsto 1, y \mapsto 1$ wahr, denn es gilt $(1 \equiv 1) = 1$ (siehe Tabelle in der Vorlesung).

Also ist F erfüllbar.

Die Formel $\neg F$ ist unter der Belegung $x \mapsto 1, y \mapsto 0$ wahr, denn es gilt $(1 \equiv 0) = 0$ und deshalb $\neg(1 \equiv 0) = 1$.

Also ist $\neg F$ erfüllbar.

2 Geben Sie eine nicht erfüllbare Formel an!

Antwort:

$$F = \text{false} .$$

oder

$$F = x \wedge \neg x .$$

3.2 VA 2, Aussagenlogische Normalformen

VA 2.1

- 1 Leiten Sie eine disjunktive Normalform im Sinne der Vorlesung für die folgende Formel F_1 her:

$$F_1 := \neg p \vee (p \wedge q \wedge r).$$

VA 2.2

- 2 Leiten Sie durch äquivalente Umformung eine konjunktive Normalform im Sinne der Vorlesung für die folgende Formel F_2 her:

$$F_2 := (\neg p \vee q) \wedge (\neg p \vee r).$$

Lösung VA 2.1:

F_1 ist nicht in disjunktiver Normalform im Sinne der Vorlesung, denn die erste Konjunktion ist unvollständig. Wir leiten eine Normalform nach der Vorlesungsmethode her. Dazu wird zunächst die Wahrheitstabelle für F_1 erstellt.

p	q	r	$p \Rightarrow (q \Rightarrow r)$	$(p \Rightarrow q) \Rightarrow r$	F
0	0	0	1	0	1
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	1	1	1
1	0	0	1	1	0
1	0	1	1	1	0
1	1	0	0	0	0
1	1	1	1	1	1

Wir lesen die disjunktive Normalform wie folgt ab.

$$\begin{aligned}
 F_1 \equiv & (\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \\
 & \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge r).
 \end{aligned}$$

Wir können das Ergebnis auch durch Anreicherung von Konjunktionen, d.h. hier durch Einfügung von Tautologien $\neg x \vee x$ erreichen wie folgt:

Lösung VA 2.1, Lösung durch Anreicherung:

$$\begin{aligned} F_1 &= \neg p \vee (p \wedge q \wedge r) \\ &\equiv (\neg p \wedge (\neg q \vee q)) \vee (p \wedge q \wedge r) \\ &\equiv (\neg p \wedge \neg q) \vee (\neg p \wedge q) \vee (p \wedge q \wedge r) \\ &\equiv (\neg p \wedge \neg q \wedge (\neg r \vee r)) \vee (\neg p \wedge q \wedge (\neg r \vee r)) \vee (p \wedge q \wedge r) \\ &\equiv (\neg p \wedge \neg q \wedge \neg r) \vee (\neg p \wedge \neg q \wedge r) \\ &\quad \vee (\neg p \wedge q \wedge \neg r) \vee (\neg p \wedge q \wedge r) \vee (p \wedge q \wedge r). \end{aligned}$$

Lösung VA 2.2:

Anreicherung von Disjunktionen durch Einfügung von Widersprüchen

$$\neg x \wedge x.$$

$$\begin{aligned} F_2 &= (\neg p \vee q) \wedge (\neg p \vee r) \\ &\equiv (\neg p \vee q \vee (\neg r \wedge r)) \wedge (\neg p \vee r \vee (\neg q \wedge q)) \\ &\equiv (\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \\ &\quad \wedge (\neg p \vee r \vee \neg q) \wedge (\neg p \vee r \vee q) \\ &\equiv (\neg p \vee q \vee \neg r) \wedge (\neg p \vee q \vee r) \wedge (\neg p \vee r \vee \neg q). \end{aligned}$$

3.3 VA 3, Prädikatenlogik

Wir betrachten prädikatenlogische Formeln mit Prädikaten über dem Universum \mathbb{R} .

- 1 Wir nehmen an, dass für einstellige Prädikate P und Q die folgende Aussage gilt:

$$(\exists x)[P(x)] \wedge (\forall x)[P(x) \Rightarrow Q(x)]$$

Man zeige, dass dann $(\exists x)[Q(x)]$ folgt.

Lösung:

Wir lösen die Formeln schrittweise auf und fügen anschließend die zu beweisende Formel zusammen.

Nach Voraussetzung gilt die Aussage

$$(\exists x)[P(x)].$$

Deshalb können wir von einem $a \in \mathbb{R}$ mit Eigenschaft $P(a)$ als ein bereits bestimmtes Element ausgehen. Von diesem a ist allerdings nur bekannt, dass $P(a)$ gilt.

Sei also $a \in \mathbb{R}$ mit der Eigenschaft $P(a)$.

Da die Aussage

$$(\forall x)[P(x) \Rightarrow Q(x)]$$

ebenfalls gilt, bedeutet dies für das bestimmte a , dass die Aussage

$$[P(a) \Rightarrow Q(a)]$$

gilt.

Es gelten also die beiden Aussagen $P(a)$ und $[P(a) \Rightarrow Q(a)]$.

Daraus können wir mit Modus ponens folgern, dass

$$Q(a)$$

gilt.

Da wir nun sozusagen ein Element a konstruiert haben, für das $Q(a)$ gilt, haben wir bewiesen, dass die Aussage

$$(\exists x)[Q(x)]$$

gilt.

W.z.b.w.

- ② Wir nehmen an, dass für ein 3-stelliges Prädikat P die folgende Aussage F gilt:

$$(\forall x \exists y \forall z) [P(x, y, z)].$$

Man leite eine pränex prädikatenlogische Formel her, die zu

$$\neg F$$

äquivalent ist.

Lösung:

Wenn *nicht* für alle $x \in \mathbb{R}$
die Eigenschaft $Q(x)$ gilt,
dann ist dies gleichbedeutend damit, dass

für mindestens ein $x \in \mathbb{R}$
die Eigenschaft $Q(x)$ *nicht* gilt.

Für alle Formeln $(\forall x)[Q(x)]$ gilt also

$$\neg(\forall x)[Q(x)] \equiv (\exists x)[\neg Q(x)].$$

Achtung: die Formel $\neg(\forall x)[Q(x)]$ ist nicht in pränexer Form.

Wir wenden diese Umformungsregel (nach DeMorgan) nun auf $\neg F$ an wie folgt.

$$\begin{aligned}\neg F &\equiv \neg(\forall x) [\exists y [\forall z [P(x, y, z)]]] \\ &\equiv \exists x [\neg(\exists y) [\forall z [P(x, y, z)]]] \\ &\equiv \exists x [\forall y [\neg(\forall z) [P(x, y, z)]]] \\ &\equiv \exists x [\forall y [\exists z [\neg P(x, y, z)]]] \\ &\equiv (\exists x \forall y \exists z) [\neg P(x, y, z)].\end{aligned}$$

3.4 VA 4, Beweisarten

① *Direkter Beweis:*

Geben Sie für die folgende Aussage einen direkten Beweis an.

Das arithmetische Mittel $b = \frac{1}{n} \sum_{i=1}^n a_i$ von n Zahlen a_i , $1 \leq i \leq n$ bleibt unverändert, falls die Folge der a_i mit beliebig vielen b' s erweitert wird, d. h.

$$b = \frac{1}{n} \sum_{i=1}^n a_i = \frac{1}{n+m} \left(\sum_{i=1}^n a_i + m \cdot b \right).$$

Bemerkung:

Auch leeren Summen wird ein Wert zugewiesen, und zwar das jeweilige „neutrale“ Element der Operation, d. h. hier 0 für die leere Summe.

Eine leere Summe liegt z. B. immer dann vor, wenn der Laufindex i bei i_0 beginnt, aber $n < i_0$ gilt, d. h. wir setzen $i_0 \leq i \leq n$ voraus.

Lösung:

Intuitiv ist klar, dass die Hinzunahme des Wertes des arithmetischen Mittels zu den Werten, über die das Mittel gebildet wird, das Mittel selbst nicht verändert.

Die entsprechende Rechnung ist wie folgt.

$$\begin{aligned}\frac{1}{n+m} \left(\sum_{i=1}^n a_i + m \cdot b \right) &= \frac{1}{n+m} \left(\sum_{i=1}^n a_i + m \cdot \frac{1}{n} \sum_{i=1}^n a_i \right) \\ &= \frac{1}{n+m} \left(1 + \frac{m}{n} \right) \sum_{i=1}^n a_i \\ &= \frac{1}{n+m} \left(\frac{n+m}{n} \right) \sum_{i=1}^n a_i \\ &= \frac{1}{n} \sum_{i=1}^n a_i.\end{aligned}$$

② *Indirekter Beweis:*

Es seien $m, n, k \in \mathbb{N}$ natürliche Zahlen mit $m > n \cdot k$.

Zeigen Sie:

Verteilt man m Hamster auf n Käfige, so befinden sich in mindestens einem Käfig $k + 1$ oder mehr Hamster.

Führen Sie einen **indirekten Beweis**, indem Sie annehmen, in allen Käfigen würden sich nach einer Verteilung weniger als $k + 1$ Hamster befinden.

Lösung:

Die Voraussetzung $m > n \cdot k$ bezeichnen wir als Aussage A .

Wir bezeichnen die Anzahl der in Käfig i ($1 \leq i \leq n$) befindlichen Hamster als h_i .

Zu zeigen ist dann die Aussage B mit

$$B = (\exists i, 1 \leq i \leq n) [h_i \geq k + 1].$$

Insgesamt haben wir also die Implikation $A \Rightarrow B$ zu zeigen.

Indirekter Beweis:

Wir zeigen die Kontraposition von $A \Rightarrow B$, d. h.

$$\neg B \Rightarrow \neg A$$

Annahme: Es gelte $\neg B$, d. h., für alle i gelte $h_i < k + 1$.

Wegen $h_i \leq k$ schätzen wir die Gesamtzahl m aller Hamster in den Käfigen ab mit

$$m = \sum_{i=1}^n h_i \leq \sum_{i=1}^n k = n \cdot k.$$

Damit ist die Negation der Voraussetzung $m > n \cdot k$ **gezeigt**, mithin Aussage $\neg A$.

③ *Schubfachprinzip:*

Lassen sich obige Aussagen auch mit dem „Schubfachprinzip“ beweisen?

Antwort:

Das Schubfachprinzip beweist eine Existenzaussage ohne Konstruktion eines bestimmten Elements, wie z.B.:

Es gibt einen Käfig, in dem mehr als k Hamster sitzen.

Die Teilaufgabe 2 kann sehr gut mit dem Schubfachprinzip bewiesen werden.

Dazu definiert man eine Abbildung f , die die Menge der m Hamster in die Menge der n Käfige abbildet.

Aussagen der Art, dass ein Beweis mit einer bestimmten Struktur nicht existiert, sind im Allgemeinen falsch.

Trotzdem bietet sich für den erstgenannten direkten Beweis keine Anwendung des Schubfachprinzips an, weil er auf keine derartige Existenzaussage abzielt.

Teilaufgabe 1 ist für die Anwendung des Prinzips **nicht geeignet**.