WS 2011/12

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2011WS/ds/uebung/

9. November 2011

ZÜ III

Übersicht:

1. Übungsbetrieb: Fragen, Probleme?
   „Das Versteh' ich nicht!“

2. Thema: Vollständige Induktion
   Nachtrag

3. Vorbereitung auf TA's Blatt 4:

   Aussagenlogische Normalformen (VA 1)
   Grenzwert und Wachstum (VA 2, VA 3)
   Rechnung modulo m (VA 4)
   Beispiel einer Gruppenalgebra

1. Übungsbetrieb

1.1 Fragen, Probleme?

?

1.2 ,,Das Versteh' ich nicht!“

Falsche Lesetechnik? Lesen und hören Sie strukturiert!

Eine Definition wird zunächst syntaktisch funktional analysiert.

Ein inhaltliches Verständnis entsteht in nachfolgenden Schritten.

2. Thema

2.1 Nachtrag vollständige Induktion ZÜ 2

(siehe dort)

3. Vorbereitung auf TA's Blatt 4

3.1 VA 1, Aussagenlogische Normalformen

Eine disjunktive bzw. konjunktive Normalform eines aussagenlogischen Ausdrucks ist im Sinne der Vorlesung eine

Disjunktion von Vollkonjunktionen

bzw. eine

Konjunktion von Volldisjunktionen.

VA 2.1

1. Leiten Sie durch äquivalente Umformung 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 2.1

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:

Anreicherung von Konjunktionen durch Einfügung von Tautologien

$$\neg x \vee x \,.$$

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

Lösung VA 2.2:

Anreicherung von Disjunktionen durch Einfügung von Widersprüchen

$$\neg x \wedge x \,.$$

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

3.2 VA 2, Grenzwert und Wachstum

VA 2.1

Im Folgenden bezeichnet 1 in $o(1)$ die konstante Funktion, die für alle $n \in \mathbb{N}_0$ den Wert 1 besitzt.

2. Man zeige durch Rückführung auf die Definition des Wachstums $o(f(n))$:

$$\frac{1}{n+1} \in o(1)\,.$$

Lösung:

Sei $f(n) = \frac{1}{n+1}$ für alle $n \in \mathbb{N}_0$.

Dann haben wir zu zeigen

$$(\forall c > 0\ \exists n_c \in \mathbb{N}_0\ \forall n \geq n_c)\ \left[\left|\frac{1}{n+1}\right| < c \cdot 1\right].$$

Wir erfüllen

schrittweise den obigen prädikatenlogischen Ausdruck von ,,links nach rechts“ gemäß der Klammerung

$$\forall c > 0\ \left[\exists n_c \in \mathbb{N}_0\ \left[\forall n \geq n_c \left[\left|\frac{1}{n+1}\right| < c \cdot 1\right]\right]\right].$$

Als Erstes nehmen wir ein beliebiges $c > 0$ an.

Für dieses $c > 0$ ist Folgendes nachzuweisen.

$$\exists n_c \in \mathbb{N}_0 \quad \left[\forall n \geq n_c \left[\left| \frac{1}{n+1} \right| < c \cdot 1 \right] \right] .$$

Den Existenzbeweis führen wir wieder konstruktiv.
Wir konstruieren ein geeignetes n_c wie folgt:

$$n_c := \left\lceil \frac{1}{c} \right\rceil + 17.$$

Nun müssen wir zeigen, dass gilt

$$\forall n \geq n_c \left[\left| \frac{1}{n+1} \right| < c \cdot 1 \right] .$$

Wir nehmen ein beliebiges n mit $n \geq n_c$ an und haben zu zeigen:

$$\left| \frac{1}{n+1} \right| < c \cdot 1 .$$

Wegen $n \geq n_c = \lceil \frac{1}{c} \rceil + 17$ gilt $n > \frac{1}{c}$, mithin $\frac{1}{n} < c$.

Es folgt

$$\left| \frac{1}{n+1} \right| = \frac{1}{n+1} < \frac{1}{n} < c \cdot 1 .$$

W.z.b.w.

VA 2.2

3. Man zeige: Für reellwertige Funktionen $f : \mathbb{N}_0 \to \mathbb{R}$ gilt

$$\lim_{n\to\infty} f(n) = 0 \quad \Longleftrightarrow \quad f(n) \in o(1)\,.$$

Lösung:

Tatsächlich müssen wir im Wesentlichen nur einige Bezeichnungen ersetzen.

$$\begin{aligned}
\lim_{n\to\infty} f(n) = 0 &\iff (\forall \varepsilon > 0\ \exists n_\varepsilon \in \mathbb{N}_0\ \forall n \geq n_\varepsilon)\ [|f(n) - 0| < \varepsilon] \\
&\iff (\forall c > 0\ \exists n_c \in \mathbb{N}_0\ \forall n \geq n_c)\ [|f(n)| < c \cdot 1] \\
&\iff f(n) \in o(1)\,.
\end{aligned}$$

Bemerkung:
Obiger Beweis ist ein Beispiel für äquivalente Umformung anstelle einer schrittweisen Auflösung der prädikatenlogischen Formel.

3.3 VA 3, Wachstum von Funktionen

1. Man zeige:

$$(\log n^2)^2 \in o(2^{\ln n}) .$$

$\log$ ohne Angabe der Basis bedeutet, dass die Formel für alle zulässigen Basen zu beweisen ist.

Lösung:

Es ist zu zeigen:

$$(\forall c > 0\ \exists n_c \in \mathbb{N}\ \forall n \geq n_c)\ \left[|(\log n^2)^2| < c \cdot 2^{\ln n}\right].$$

Sei b eine beliebige zulässige Basis.

Wir lösen die Formel schrittweise auf.

Sei c eine beliebige reelle Zahl mit $c > 0$.
Nun konstruieren wir ein natürliche Zahl n_c, so dass gilt

$$(\forall n \geq n_c)\,[(\log n^2)^2 < c \cdot 2^{\ln n}]\,.$$

Umformung:

$$(\log_b n^2)^2 = \frac{4}{(\ln b)^2} \cdot (\ln n)^2 < c \cdot 2^{\ln n}\,.$$

Wir bezeichnen $\ln n$ mit x,
d.h. wir setzen $x = \ln n$,
und wir setzen $k = \frac{4}{(\ln b)^2}$.

Nun benutzen wir die Ungleichung $x^3 < 2^x$ für $x \geq 10$.

Die Ungleichung folgt leicht aus $3 \ln x < x \ln 2$ für $x \geq 10$.

Dann gilt für $x \geq 10$ und $\frac{k}{x} \leq c$

$$k \cdot x^2 = \frac{k}{x} \cdot x^3 < c \cdot 2^x \, .$$

Nun setzen wir $x_c = \max\{10, \frac{k}{c}\}$ und $n_c = \lceil e^{x_c} \rceil$

und erhalten für alle $n \geq n_c$ die gewünschte Ungleichung.

3. Sei $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ mit $a_i \in \mathbb{R}$, $a_n \neq 0$.
   Man zeige $f(x) = \mathcal{O}(x^n)$.

Lösung:

Es ist zu zeigen

$$(\exists c > 0\ \exists n_c \in \mathbb{N}\ \forall x \geq n_c)\,[|f(x)| \leq c \cdot x^n]\,.$$

Es gelten für alle $x \geq 1$ die Ungleichungen

$$\begin{aligned} |f(x)| &\leq \left|\sum_{i=0}^{n} a_i \cdot x^i\right| \leq \sum_{i=0}^{n} |a_i| \cdot x^i \\ &\leq x^n \cdot \left(\sum_{i=0}^{n} |a_i| \cdot x^{i-n}\right) \leq x^n \cdot \underbrace{\sum_{i=0}^{n} |a_i|}_{=:c} \end{aligned}$$

Wir können beispielsweise $c = \sum_{i=0}^{n} |a_i|$ und $n_c = 2$ setzen.

3.4 VA 4, Rechnen modulo m

Ganze Zahlen $a, b \in \mathbb{Z}$ nennt man

kongruent modulo m, mit $m \in \mathbb{N}$, i. Z. $a \equiv b \pmod{m}$,

falls sich a und b um ein ganzzahliges Vielfaches von m unterscheiden, d. h.,

falls es ein $k \in \mathbb{Z}$ gibt, so dass gilt

$$a = b + k \cdot m \,.$$

Diesen Zusammenhang kann man der Definition der Operation $\mathrm{mod} : \mathbb{Z} \times \mathbb{N} \to \mathbb{Z}$ zugrunde legen:

$$b = a \bmod m \iff a \equiv b \pmod{m} \text{ und } 0 \leq b < m \,.$$

Teil 1:

Zeigen Sie für alle $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}$:

$$a \equiv a \bmod m \pmod m, \tag{1}$$

$$(a+b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m, \tag{2}$$

$$(a \cdot b) \bmod m = [(a \bmod m) \cdot (b \bmod m)] \bmod m. \tag{3}$$

1. Zu beweisen ist: $a \equiv a \bmod m \pmod m$

Lösung:

Die Kongruenz modulo m ist definiert durch

$$x \equiv y \pmod m \quad :\Longleftrightarrow \quad (\exists k \in \mathbb{Z})\,[\,x = y + k{\cdot}m\,]\,.$$

Nach Definition von $(a \bmod b)$ gilt für ein bestimmtes $k \in \mathbb{Z}$

$$a \bmod b = a + k{\cdot}b\,, \quad \text{d. h.} \quad a = a \bmod b + k'{\cdot}b\,,$$

mithin

$$a \equiv a \bmod b \pmod b\,.$$

2. Zu beweisen ist:
$$(a+b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m\,.$$

Lösung:

Wir setzen linke Seite bzw. rechte Seite der Gleichung

$$\begin{aligned} x &:= (a+b) \bmod m\,, \\ y &:= [(a \bmod m) + (b \bmod m)] \bmod m\,. \end{aligned}$$

und zeigen $x = y$.

Es gilt $0 \leq x, y < m$ und

$$\begin{aligned} x &= a + b + k_x \cdot m\,, \\ y &= (a \bmod m) + (b \bmod m) + k_y \cdot m\,, \\ (a \bmod m) &= a + k_a \cdot m\,, \\ (b \bmod m) &= b + k_b \cdot m \end{aligned}$$

für gewisse $k_a, k_b, k_x, k_y \in \mathbb{Z}$ und es folgt

$$\begin{aligned} y &= a + k_a \cdot m + b + k_b \cdot m + k_y \cdot m \\ &= x - k_x \cdot m + k_a \cdot m + k_b \cdot m + k_y \cdot m \\ &= x + (k_a + k_b + k_y - k_x) \cdot m \\ &= x + k \cdot m\,. \end{aligned}$$

Wegen $0 \leq x, y < m$ folgt $x = y$.

Analog verläuft der Beweis der Gleichung 3:

$$(a \cdot b) \bmod m = [(a \bmod m) \cdot (b \bmod m)] \bmod m \,.$$

Teil 2:

In enger Beziehung zur mod-Operation steht die ganzzahlige Division $a \operatorname{div} m$ zweier Zahlen $a \in \mathbb{Z}, m \in \mathbb{N}$.

Es gilt

$$a = (a \operatorname{div} m) \cdot m + (a \bmod m)\,.$$

Berechnen Sie:

(i) $5 \operatorname{div} 4$, (ii) $(-5) \operatorname{div} 4$, (iii) $(-x) \operatorname{div} 1$.

(i) 5 div 4:

Seien $a = 5$ und $m = 4$.

Dann gilt

$$(5 \operatorname{div} 4) \cdot 4 \;=\; 5 - (5 \bmod 4) \;=\; 5 - 1 \;=\; 4\,.$$

Es folgt $5 \operatorname{div} 4 = 1$.

(ii) (-5) div 4:

Seien $a = -5$ und $m = 4$.

Dann gilt

$$\begin{aligned} ((-5) \operatorname{div} 4) \cdot 4 &= -5 - ((-5) \bmod 4) \\ &= (-5 - ((-5 + 8) \bmod 4)) \\ &= (-5 - 3) = -8\,. \end{aligned}$$

Es folgt $(-5) \operatorname{div} 4 = -2$.

(iii) $(-x)$ div 1:

Seien $a = -x$ und $m = 1$.

Dann gilt

$$((-x) \operatorname{div} 1) \cdot 1 \;=\; -x - ((-x) \bmod 1) \;=\; -x - 0 \;=\; -x\,.$$

Es folgt $(-x) \operatorname{div} 1 = -x\,.$

3.5 VA 5, Beispiel einer Gruppenalgebra

Seien $S = \mathbb{R} \setminus \{-1\}$ und für alle $x, y \in S$

$$x \circ y = x + y + xy\,.$$

Zeigen Sie, dass die Algebra $A = \langle S, \circ \rangle$ bezüglich des binären Operators $\circ$ eine Gruppe bildet.

Lösung:

1. Zunächst ist zu prüfen, ob durch die Gleichung $x \circ y = x + y + x \cdot y$ tatsächlich eine Abbildung von $S \times S$ in S definiert ist.

   Seien $x, y \in \mathbb{R} \setminus \{-1\}$. Es gilt offenbar $x \circ y \in \mathbb{R}$.

   Wir zeigen, dass $-1 = x + y + x \cdot y$ einen Widerspruch ergibt und deswegen $x, y \in \mathbb{R} \setminus \{-1\}$ gelten muss.

$$\begin{aligned} -1 = x + y + x \cdot y \quad &\Rightarrow \quad -1 - y = x(1 + y) \\ &\Rightarrow \quad x = \frac{-1 - y}{1 + y} \\ &\Rightarrow \quad x = -1\,. \end{aligned}$$

2. Wir zeigen die Assoziativität von $\circ$.

$$
\begin{aligned}
x \circ (y \circ z) &= x + (y \circ z) + x \cdot (y \circ z) \\
&= x + (y + z + y \cdot z) + x \cdot (y + z + y \cdot z) \\
&= x + y + z + y \cdot z + x \cdot y + x \cdot z + x \cdot y \cdot z \\
&= (x + y + x \cdot y) + z + (x + y + x \cdot y) \cdot z \\
&= (x \circ y) + z + x \circ y) \cdot z \\
&= (x \circ y) \circ z \,.
\end{aligned}
$$

3. $x = 0$ ist das Einselement bezüglich $(x \circ y)$.

$$0 \circ y = 0 + y + 0 \cdot y = y\,.$$

Das linke Einselement ist offensichtlich auch rechtes Einselement, d. h. Einselement.

4. Wir zeigen, dass zu einem Element $x \in S$ das Inverse gegeben ist durch $x^{-1} = -\frac{x}{1+x}$.

   Es gilt

$$\begin{aligned} x \circ y = 0 \quad &\Leftrightarrow \quad x + y + x \cdot y = 0 \\ &\Leftrightarrow \quad y = -\frac{x}{1+x}\,. \end{aligned}$$

   Die Existenz eines linken Inversen ist damit bewiesen.

Bemerkung:

Allein schon aus der offensichtlichen Kommutativität folgt hier, dass jedes linke Inverse auch rechtes Inverses ist. Es sei aber bemerkt, dass die Beziehung zwischen linken und rechten Inversen auch ohne Kommutativität ganz allgemein in Gruppen untersucht werden kann.

Es genügt, allein die Existenz der linken Inversen nachzuweisen.

Folgerung:

Damit ist der Nachweis erbracht, dass G eine Gruppe ist.