Lehrstuhl für Sprachen und Beschreibungsstrukturen WS 2008/09
Einführung in die Informatik 2 **Übungsblatt 1**
Prof. Dr. Helmut Seidl, T.M. Gawlitza, S. Pott 14.10.08

Abgabe: 21.10.08 (vor der Vorlesung)

Aufgabe 1.1 (P) Aussagenlogik

Zeigen oder widerlegen Sie (Verwenden Sie dabei für Aufgabe a) eine Wahrheitstabelle, für alle anderen Aufgaben die Äquivalenzregeln der Aussagenlogik):

a) $A \iff B \equiv (A \Rightarrow B) \wedge (B \Rightarrow A)$
b) $A \iff B \equiv (A \wedge B) \vee (\neg A \wedge \neg B)$
c) $(\neg A \wedge (A \Rightarrow B)) \Rightarrow \neg B \equiv \mathbf{true}$
d) $(\neg B \wedge (A \Rightarrow B)) \Rightarrow \neg A \equiv \mathbf{true}$
e) $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$
f) $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C) \equiv \mathbf{true}$
g) $(A \Rightarrow B) \wedge (A \Rightarrow C) \equiv A \Rightarrow (B \wedge C)$

Vereinfachen Sie folgende Aussagen:

a) $(A \wedge \neg B) \vee (A \wedge B)$
b) $(A \Rightarrow B) \vee (B \Rightarrow A)$

Lösungsvorschlag 1.1

a) Beweis über Wertetabelle:

A	B	$A \iff B$	$A \Rightarrow B$	$B \Rightarrow A$	$(A \Rightarrow B) \wedge (B \Rightarrow A)$
1	1	1	1	1	1
0	1	0	1	0	0
1	0	0	0	1	0
0	0	1	1	1	1

b)

$$
\begin{aligned}
(A \wedge B) \vee (\neg A \wedge \neg B) &\equiv (A \vee \neg A) \wedge (A \vee \neg B) \wedge (B \vee \neg A) \wedge (B \vee \neg B) \\
&\equiv \mathbf{true} \wedge (A \vee \neg B) \wedge (B \vee \neg A) \wedge \mathbf{true} \\
&\equiv (B \Rightarrow A) \wedge (A \Rightarrow B) \\
&\equiv (A \iff B)
\end{aligned}
$$

c)

$$
\begin{aligned}
(\neg A \wedge (A \Rightarrow B)) \Rightarrow \neg B &\equiv \neg(\neg A \wedge (\neg A \vee B)) \vee \neg B \\
&\equiv \neg(\neg A) \vee \neg B \qquad \text{(Absorptionsregel)} \\
&\equiv \\
&\equiv A \vee \neg B \\
&\not\equiv \mathbf{true}
\end{aligned}
$$

d)

$$
\begin{aligned}
(\neg B \wedge (A \Rightarrow B)) \Rightarrow \neg A &\equiv \neg(\neg B \wedge (\neg A \vee B)) \vee \neg A \\
&\equiv (B \vee (A \wedge \neg B)) \vee \neg A \\
&\equiv ((B \vee A) \wedge (B \vee \neg B)) \vee \neg A \\
&\equiv ((B \vee A) \wedge \mathbf{true}) \vee \neg A \\
&\equiv B \vee A \vee \neg A \\
&\equiv B \vee \mathbf{true} \\
&\equiv \mathbf{true}
\end{aligned}
$$

e)

$$
\begin{aligned}
A \Rightarrow B &\equiv \neg A \vee B \\
&\equiv \neg(\neg B) \vee (\neg A) \\
&\equiv \neg B \Rightarrow \neg A
\end{aligned}
$$

f)

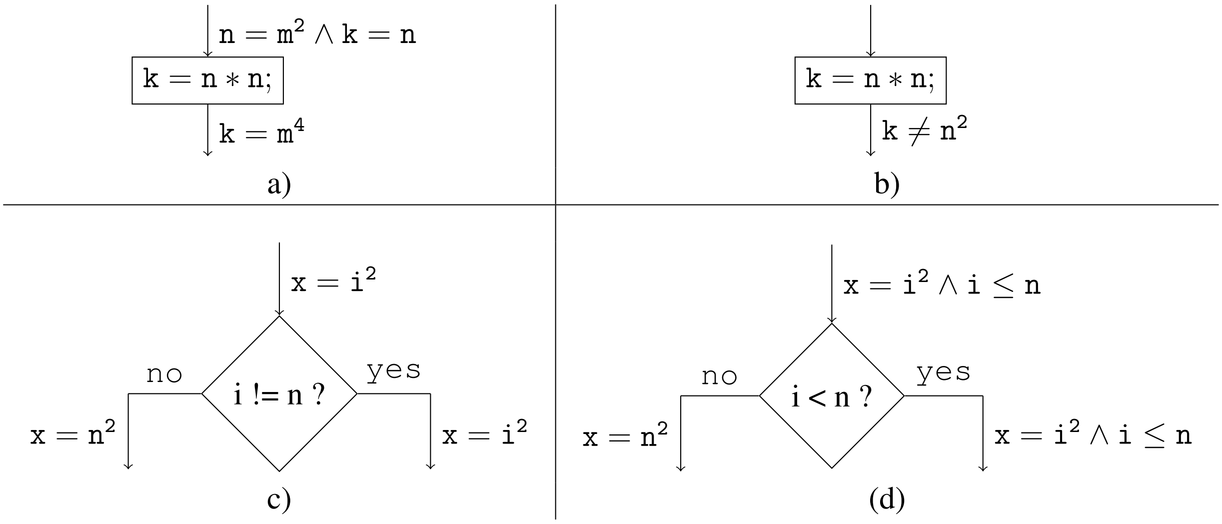
$$
\begin{aligned}
(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C) &\equiv ((\neg A \vee B) \wedge (\neg B \vee C)) \Rightarrow (\neg A \vee C) \\
&\equiv \neg((\neg A \vee B) \wedge (\neg B \vee C)) \vee (\neg A \vee C) \\
&\equiv (A \wedge \neg B) \vee (B \wedge \neg C) \vee \neg A \vee C \\
&\equiv \neg A \vee (A \wedge \neg B) \vee C \vee (B \wedge \neg C) \\
&\equiv ((\neg A \vee A) \wedge (\neg A \vee \neg B)) \vee ((C \vee B) \wedge (C \vee \neg C)) \\
&\equiv (\neg A \vee \neg B) \vee (C \vee B) \\
&\equiv B \vee \neg B \vee C \vee \neg A \\
&\equiv \mathbf{true}
\end{aligned}
$$

g)

$$
\begin{aligned}
(A \Rightarrow B) \wedge (A \Rightarrow C) &\equiv (\neg A \vee B) \wedge (\neg A \vee C) \\
&\equiv \neg A \vee (B \wedge C) \\
&\equiv A \Rightarrow (B \wedge C)
\end{aligned}
$$

Aufgabe 1.2 (P) Verifikation

Überprüfen Sie, ob folgende Zusicherungen lokal konsistent sind beziehungsweise ergänzen Sie fehldende Zusicherungen, so dass lokale Konsistenz hergestellt wird.



Lösungsvorschlag 1.2

a)

$$\begin{aligned}\mathbf{WP}[\![\mathtt{k = n * n}]\!](\mathtt{k = m^4}) &\equiv k = m^4[n^2/k] \\ &\equiv n^2 = m^4 \\ &\Leftarrow n = m^2 \\ &\Leftarrow n = m^2 \land k = n\end{aligned}$$

b)

$$\begin{aligned}\mathbf{WP}[\![\mathtt{k = n * n}]\!](\mathtt{k \neq n^2}) &\equiv n^2 \neq n^2 \\ &\equiv \mathbf{false}\end{aligned}$$

c)

$$\begin{aligned}\mathbf{WP}[\![\mathtt{i\ != n}]\!](\mathtt{x = n^2, x = i^2}) &\equiv (\mathtt{i = n \land x = n^2}) \lor (\mathtt{i \neq n \land x = i^2}) \\ &\equiv (\mathtt{i = n \land x = i^2}) \lor (\mathtt{i \neq n \land x = i^2}) \\ &\equiv (\mathtt{i = n \lor i \neq n}) \land \mathtt{x = i^2} \\ &\equiv \mathbf{true} \land \mathtt{x = i^2} \\ &\equiv \mathtt{x = i^2}\end{aligned}$$

d)

$$\begin{aligned}&\mathbf{WP}[\![\mathtt{i < n}]\!](\mathtt{x = n^2, x = i^2 \land i \leq n}) \\ &\equiv (\mathtt{i \geq n \land x = n^2}) \lor (\mathtt{i < n \land x = i^2 \land i \leq n}) \\ &\Leftarrow (\mathtt{i \geq n \land x = n^2 \land i \leq n}) \lor (\mathtt{i < n \land x = i^2 \land i \leq n}) \\ &\equiv (\mathtt{i \geq n \land x = i^2 \land i \leq n}) \lor (\mathtt{i < n \land x = i^2 \land i \leq n}) \\ &\equiv (\mathtt{i \geq n \lor i < n}) \land \mathtt{x = i^2 \land i \leq n} \\ &\equiv \mathbf{true} \land \mathtt{x = i^2 \land i \leq n} \\ &\equiv \mathtt{x = i^2 \land i \leq n}\end{aligned}$$

Aufgabe 1.3 (P) Verifikation

Gegeben sei folgendes MiniJava-Programm:

```
int n, i, r;
n = read();
i = 0;
r = 0;
while (i != n) {
        i = i + 1;
        r = r + 2*i*n;
        r = r - n;
}
write(r);
```

a) Erstellen Sie das Kontrollfluß-Diagramm!

b) Beweisen Sie, dass, falls eine Ausgabe erfolgt, $\mathtt{n}^3$ ausgegeben wird!

Zur Schleifen-Invariante: Zum Finden einer geeigneten Schleifen-Invariante gehen wir wie folgt vor: Wir bezeichnen den Wert der Programm-Variablen r nach der k-ten Iteration ($k = 0, 1, 2, \ldots$) einfach mal mit r_k. Insbesondere ist also $r_0 = 0$ (Der Schleifenrumpf wurde 0 mal ausgeführt). Weiterhin sieht man, dass sich der Wert der Programm-Variablen n nicht verändert. Der Wert der Programm-Variablen i ist nach der k-ten Iteration k.

Jetzt drücken wir den Wert r_k der Programm-Variablen r nach der k-ten Iteration mithilfe des Wertes r_{k-1}, k und des Wertes der Programm-Variablen n aus.

Scharfes Hinsehen führt zu folgender Vermutung:

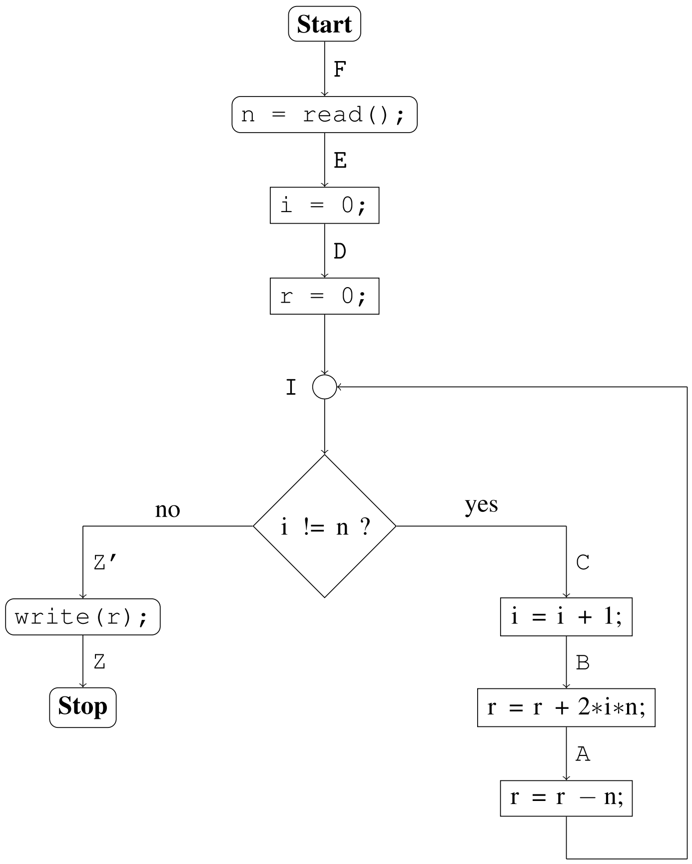
$$r_k = \begin{cases} 0 & \text{falls } k = 0 \\ r_{k-1} + 2 \cdot k \cdot \mathtt{n} - \mathtt{n} & \text{falls } k > 0. \end{cases}$$

Das schreiben wir als Summe in der Form

$$r_k = \sum_{j=1}^{k} ??? = \sum_{j=1}^{\mathtt{i}} ???.$$

Achtung: r_k ist keine Programm-Variable. Der Wert r_k dient nur zur Überlegung. In der Invariante darf r_k nicht vorkommen.

Lösungsvorschlag 1.3



Da wir nachweisen wollen, dass das Programm, sofern eine Ausgabe erfolgt, $\mathtt{n}^3$ ausgibt, setzen wir

$$\mathtt{Z} :\equiv \mathtt{r} = \mathtt{n}^3.$$

Es ergibt sich

$$\mathtt{Z}' :\equiv \mathbf{WP}[\![\mathtt{write(r);}]\!](\mathtt{Z}) \equiv \mathtt{Z} \equiv \mathtt{r} = \mathtt{n}^3.$$

Für die Schleifen-Invariante $\mathtt{I}$ raten wir

$$\mathtt{I} :\equiv \mathtt{r} = \sum_{j=1}^{\mathtt{i}} (2 \cdot \mathtt{j} \cdot \mathtt{n} - \mathtt{n}) = \mathtt{n} \cdot (2 \cdot \sum_{j=1}^{\mathtt{i}} \mathtt{j} - \sum_{j=1}^{\mathtt{i}} 1) = \mathtt{n} \cdot (\mathtt{i} \cdot (\mathtt{i} + 1) - \mathtt{i}) = \mathtt{n} \cdot \mathtt{i}^2.$$

Es ergibt sich

$$\mathbf{WP}[\![\mathtt{r} = \mathtt{r} - \mathtt{n}]\!](\mathtt{I}) \equiv \mathtt{I}[\mathtt{r} - \mathtt{n}/\mathtt{r}] \equiv \mathtt{r} - \mathtt{n} = \mathtt{n} \cdot \mathtt{i}^2 \equiv: \mathtt{A}.$$

Daraus ergibt sich

$$\mathbf{WP}[\![\mathtt{r} = \mathtt{r} + 2 * \mathtt{i} * \mathtt{n}]\!](\mathtt{A}) \equiv \mathtt{A}[\mathtt{r} + 2 * \mathtt{i} * \mathtt{n}/\mathtt{r}] \equiv \mathtt{r} + 2 \cdot \mathtt{i} \cdot \mathtt{n} - \mathtt{n} = \mathtt{n} \cdot \mathtt{i}^2 \equiv: \mathtt{B}.$$

Daraus ergibt sich

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{i} = \mathtt{i} + 1]\!](\mathtt{B}) &\equiv \mathtt{B}[\mathtt{i} + 1/\mathtt{i}] \\
&\equiv \mathtt{r} + 2 \cdot (\mathtt{i} + 1) \cdot \mathtt{n} - \mathtt{n} = \mathtt{n} \cdot (\mathtt{i} + 1)^2 \\
&\equiv \mathtt{r} + 2 \cdot \mathtt{n} \cdot \mathtt{i} + \mathtt{n} = \mathtt{n} \cdot \mathtt{i}^2 + 2 \cdot \mathtt{n} \cdot \mathtt{i} + \mathtt{n} \\
&\equiv \mathtt{r} = \mathtt{n} \cdot \mathtt{i}^2 \\
&\equiv \mathtt{I} \\
&\equiv: \mathtt{C}.
\end{aligned}$$

Das $C \equiv I$ gilt ist ein gutes Zeichen. Es bleibt die lokale Konsistenz an der Verzweigung zu überprüfen. Dies bedeutet, es muss überprüft werden, ob folgende Aussage gilt:

$$\mathtt{I} \implies \mathbf{WP}[\![\mathtt{i!=n}]\!](\mathtt{Z}', \mathtt{C}). \tag{1}$$

Los geht's:

$$\begin{aligned}
\mathbf{WP}[\![\mathtt{i!=n}]\!](\mathtt{Z}', \mathtt{C}) &\equiv \mathbf{WP}[\![\mathtt{i!=n}]\!](\mathtt{Z}', \mathtt{I}) \\
&\equiv (\mathtt{i} = \mathtt{n} \wedge \mathtt{Z}') \vee (\mathtt{i} \neq \mathtt{n} \wedge \mathtt{I}) \\
&\equiv (\mathtt{i} = \mathtt{n} \wedge \mathtt{r} = \mathtt{n}^3) \vee (\mathtt{i} \neq \mathtt{n} \wedge \mathtt{I}) \\
&\equiv (\mathtt{i} = \mathtt{n} \wedge \mathtt{r} = \mathtt{n} \cdot \mathtt{n}^2) \vee (\mathtt{i} \neq \mathtt{n} \wedge \mathtt{I}) \\
&\equiv (\mathtt{i} = \mathtt{n} \wedge \mathtt{r} = \mathtt{n} \cdot \mathtt{i}^2) \vee (\mathtt{i} \neq \mathtt{n} \wedge \mathtt{I}) \\
&\equiv (\mathtt{i} = \mathtt{n} \wedge \mathtt{I}) \vee (\mathtt{i} \neq \mathtt{n} \wedge \mathtt{I}) \\
&\equiv (\mathtt{i} = \mathtt{n} \vee \mathtt{i} \neq \mathtt{n}) \wedge \mathtt{I} && \text{(Distributivgesetz)} \\
&\equiv \mathbf{true} \wedge \mathtt{I} && \text{(Komplementärgesetz)} \\
&\equiv \mathtt{I} && \text{(Neutralitätsgesetz).}
\end{aligned}$$

Damit ist (**??**) gezeigt. Damit folgt:

$$\mathbf{WP}[\![\mathtt{r = 0;}]\!](\mathtt{I}) \equiv \mathtt{I}[0/\mathtt{r}] \equiv 0 = \mathtt{n} \cdot \mathtt{i}^2 \equiv: \mathtt{D}.$$

Daraus folgt:

$$\mathbf{WP}[\![\mathtt{i = 0;}]\!](\mathtt{D}) \equiv \mathtt{D}[0/\mathtt{i}] \equiv 0 = \mathtt{n} \cdot 0^2 \equiv 0 = 0 \equiv \mathbf{true} \equiv: \mathtt{E}.$$

Daraus folgt schließlich:

$$\mathbf{WP}[\![\mathtt{n = read();}]\!](\mathtt{E}) \equiv \forall \mathtt{n}.\mathbf{true} \equiv \mathbf{true} \equiv: \mathtt{F}.$$