# Theoretische Informatik und Logik
# Übungsblatt 4 (2022W)
# Lösungsvorschlag

*Allgemeine Hinweise:*
Nummerieren Sie alle auftretenden Formeln in Tableau-Beweisen und geben Sie entsprechende Herkunftshinweise bei allen Regelanwendungen an. Außerdem sind $\gamma$- und $\delta$-Formeln jeweils als solche zu markieren. Beachten Sie die Notationsvereinbarungen auf Folie 321.
Programme und Korrektheitsaussagen beziehen sich auf den Datentyp $\mathbb{Z}$.

**Aufgabe 4.1**
Geben Sie zu folgenden Behauptungen jeweils entweder einen Tableau-Beweis oder ein Gegenbeispiel an.

a) $\forall x \exists y [P(x,y) \supset \exists x \forall y P(x,y)]$ ist gültig.

b) Aus $\forall x f(x) = x$, $\forall x g(x) = f(f(a))$ und $\exists x [P(x) \wedge \neg P(g(x))]$ folgt $\forall x [P(f(x)) \supset x \neq a]$.

c) $\neg \forall x [(x \neq a \wedge f(x) = a) \supset \forall y (f(y) \neq x \vee f(y) \neq f(x))]$ ist unerfüllbar.

**Lösung 4.1**

a) Folgendes geschlossene Tableau (=Tableau-Beweis) zeigt die Gültigkeit der Formel:

| | | |
|---|---|---|
| (1) | $\mathbf{f} : \forall x \exists y [P(x,y) \supset \exists x \forall y P(x,y)]$ | Annahme, $\delta$-Formel |
| (2) | $\mathbf{f} : \exists y [P(a,y) \supset \exists x \forall y P(x,y)]$ | von 1, $\gamma$-Formel |
| (3) | $\mathbf{f} : P(a,a) \supset \exists x \forall y P(x,y)$ | von 2 |
| (4) | $\mathbf{t} : P(a,a)$ | von 3 |
| (5) | $\mathbf{f} : \exists x \forall y P(x,y)$ | von 3, $\gamma$-Formel |
| (6) | $\mathbf{f} : \forall y P(a,y)$ | von 5, $\delta$-Formel |
| (7) | $\mathbf{f} : P(a,b)$ | von 6 |
| (8) | $\mathbf{f} : P(a,b) \supset \exists x \forall y P(x,y)$ | von 2 |
| (9) | $\mathbf{t} : P(a,b)$ | von 8 |
| (10) | $\mathbf{f} : \exists x \forall y P(x,y)$ | von 8, $\gamma$-Formel |
| | $\times$ | Widerspruch (7/9) |

Beachten Sie, dass bei Anwendung der $\delta$-Regel auf Zeile (6) eine neue Konstante gewählt werden muss. Die Verwendung von $a$ zur Substitution von $y$ wäre inkorrekt, da man ja nicht annehmen kann, dass die bereits in (2), (3) und (5) vorkommende Konstante $a$ eine Zeuge für die Falschheit von $\forall y P(a,y)$ ist. Die $\gamma$-Regel muss daher – nach Verwendung der $\delta$-Regel in Zeile 7 – nochmals auf die Formel in Zeile 2 angewendet werden, damit man das Tableau schließen kann. Aus demselben Grund bringt es nichts in (3) $P(a,b)$ abzuleiten, da ja dann in (7) wiederum eine neue Konstante statt $b$ eingesetzt werden muss

b) Folgender Tableau-Beweis zeigt, dass die Konsequenzbehauptung stimmt.

| | | |
|---|---|---|
| (1) | $\mathbf{t} : \forall x f(x) = x$ | Annahme, $\gamma$-Formel |
| (2) | $\mathbf{t} : \forall x g(x) = f(f(a))$ | Annahme, $\gamma$-Formel |
| (3) | $\mathbf{t} : \exists x [P(x) \wedge \neg P(g(x))]$ | Annahme, $\delta$-Formel |
| (4) | $\mathbf{f} : \forall x [P(f(x)) \supset x \neq a]$ | Annahme, $\delta$-Formel |
| (5) | $\mathbf{t} : P(b) \wedge \neg P(g(b))$ | von 3 |
| (6) | $\mathbf{f} : P(f(c)) \supset c \neq a$ | von 4 |
| (7) | $\mathbf{t} : P(b)$ | von 5 |
| (8) | $\mathbf{t} : \neg P(g(b))$ | von 5 |
| (9) | $\mathbf{f} : P(g(b))$ | von 8 |
| (10) | $\mathbf{t} : P(f(c))$ | von 6 |
| (11) | $\mathbf{f} : c \neq a$ | von 6 |
| (12) | $\mathbf{t} : c = a$ | von 11 |
| (13) | $\mathbf{t} : f(a) = a$ | von 1 |
| (14) | $\mathbf{t} : g(b) = f(f(a))$ | von 2 |
| (15) | $\mathbf{f} : P(f(f(a)))$ | $S^{=}$: 14→9 |
| (16) | $\mathbf{f} : P(f(a))$ | $S^{=}$: 13→15 |
| (17) | $\mathbf{t} : P(f(a))$ | $S^{=}$: 12→10 |
| | $\times$ | Wid.: 16/17 |

c) Folgendes geschlossene Tableau zeigt die Unerfüllbarkeit der Formel:

| | | |
|---|---|---|
| (1) | $\mathbf{t} : \neg\forall x[(x \neq a \wedge f(x) = a) \supset \forall y(f(y) \neq x \vee f(y) \neq f(x))]$ | Annahme |
| (2) | $\mathbf{f} : \forall x[(x \neq a \wedge f(x) = a) \supset \forall y(f(y) \neq x \vee f(y) \neq f(x))]$ | von 1, $\delta$-Formel |
| (3) | $\mathbf{f} : (b \neq a \wedge f(b) = a) \supset \forall y(f(y) \neq b \vee f(y) \neq f(b))$ | von 2 |
| (4) | $\mathbf{t} : b \neq a \wedge f(b) = a$ | von 3 |
| (5) | $\mathbf{f} : \forall y(f(y) \neq b \vee f(y) \neq f(b))$ | von 3, $\delta$-Formel |
| (6) | $\mathbf{f} : f(c) \neq b \vee f(c) \neq f(b)$ | von 5 |
| (7) | $\mathbf{f} : f(c) \neq b$ | von 6 |
| (8) | $\mathbf{f} : f(c) \neq f(b)$ | von 6 |
| (9) | $\mathbf{t} : f(c) = b$ | von 7 |
| (10) | $\mathbf{t} : f(c) = f(b)$ | von 8 |
| (11) | $\mathbf{t} : b \neq a$ | von 4 |
| (12) | $\mathbf{t} : f(b) = a$ | von 4 |
| (13) | $\mathbf{t} : b = f(b)$ | $S^{=}$: 9→10 |
| (14) | $\mathbf{t} : b = a$ | $S^{=}$: 13→12 |
| (15) | $\mathbf{f} : b = a$ | von 11 |
| | $\times$ | Wid. 14/15 |

**Aufgabe 4.2**

a) Zeigen Sie mit dem Tableau-Kalkül: Jede partiell funktionale und serielle Relation ist schwach gerichtet.

b) Zeigen Sie, dass Serialität notwendig für die Gülitgkeit der Konsequenzbehauptung in a) ist. Genauer: Spezifizieren Sie eine Interpretation $\mathcal{I} = \langle D, \Phi, \xi \rangle$, in der $\Phi(R)$ eine partiell funktionale, aber keine schwach gerichtete Relation ist.

**Lösung 4.2**

a) Es gilt $pf, ser \models sger$ zu zeigen, wobei

$pf = \forall x \forall y \forall z[(R(x,y) \wedge R(x,z)) \supset y = z]$ (partielle Funktionalität)
$ser = \forall x \exists y R(x,y)$ (Serialität)
$sger = \forall x \forall y \forall z[(R(x,y) \wedge R(x,z)) \supset \exists u(R(y,u) \wedge R(z,u))]$ (schwache Gerichtetheit).

Ein möglicher Tableau-Beweis dieser Konsequenzbehauptung sieht wie folgt aus:

| | | | |
|---|---|---|---|
| (1) | $\mathbf{t} : \forall x \forall y \forall z[(R(x,y) \wedge R(x,z)) \supset y = z]$ | | $\gamma$-Formel, Annahme |
| (2) | $\mathbf{t} : \forall x \exists y R(x,y)$ | | $\gamma$-Formel, Annahme |
| (3) | $\mathbf{f} : \forall x \forall y \forall z[(R(x,y) \wedge R(x,z)) \supset \exists u(R(y,u) \wedge R(z,u))]$ | | $\delta$-Formel, Annahme |
| (4) | $\mathbf{f} : \forall y \forall z[(R(a,y) \wedge R(a,z)) \supset \exists u(R(y,u) \wedge R(z,u))]$ | | von 3, $\delta$-Formel |
| (5) | $\mathbf{f} : \forall z[(R(a,b) \wedge R(a,z)) \supset \exists u(R(b,u) \wedge R(z,u))]$ | | von 4, $\delta$-Formel |
| (6) | $\mathbf{f} : (R(a,b) \wedge R(a,c)) \supset \exists u(R(b,u) \wedge R(c,u))$ | | von 5 |
| (7) | $\mathbf{t} : R(a,b) \wedge R(a,c)$ | | von 6 |
| (8) | $\mathbf{f} : \exists u(R(b,u) \wedge R(c,u))$ | | von 6, $\gamma$-Formel |
| (9) | $\mathbf{t} : \exists y R(b,y)$ | | von 2, $\delta$-Formel |
| (10) | $\mathbf{t} : R(b,d)$ | | von 9 |
| (11) | $\mathbf{t} : \forall y \forall z[(R(a,y) \wedge R(a,z)) \supset y = z]$ | | von 1, $\gamma$-Formel |
| (12) | $\mathbf{t} : \forall z[(R(a,b) \wedge R(a,z)) \supset b = z]$ | | von 11, $\gamma$-Formel |
| (13) | $\mathbf{t} : (R(a,b) \wedge R(a,c)) \supset b = c$ | | von 12 |
| (14) | $\mathbf{f} : R(a,b) \wedge R(a,c)$ von 13 | (15) $\mathbf{t} : b = c$ | von 13 |
| | $\times$ Wid.: 7/14 | (16) $\mathbf{f} : R(b,d) \wedge R(c,d)$ | von 8 |
| | | (17) $\mathbf{f} : R(b,d)$ von 16 | (18) $\mathbf{f} : R(c,d)$ von 16 |
| | | $\times$ Wid.: 10/17 | (19) $\mathbf{f} : R(b,d)$ $S^{=}$: 15→18 |
| | | | $\times$ Wid.: 10/19 |

b) Es geht um die Konsequenzbehauptung $pf \models sger$.

Man betrachte, z.B., $\mathcal{I} = \langle \{0,1\}, \Phi, \xi \rangle$, mit $\Phi(R)(m,n) = \mathbf{t} \iff m = 0$ und $n = 1$. (Da keine freien Variablen in $pf$ und $sger$ vorkommen, ist $\xi$ beliebig). Die Relation $\Phi(R)$ ist offensichtlich partiell funktional. Aber es müsste auch $\Phi(R)(1,1) = \mathbf{t}$ gelten um schwache Gerichtetheit zu erfüllen.

Ein anderes Beispiel ist die Vorgängerrelation für natürliche Zahlen. Diese ist ebenfalls partiell funktional, aber nicht schwach gerichtet. Formaler: Wir erhalten ein Gegenbeispiel $\mathcal{I} = \langle \omega, \Phi, \xi \rangle$ zur Konsequenzbehauptung $pf \models sger$, indem wir $\Phi(R)(m,n) = \mathbf{t} \iff n = m - 1$ setzen. Da $\Phi(R)$ eine

nacheindeutige Relation ist, ist sie partiell funktional. Aber $\Phi(R)$ ist nicht schwach gerichtet. Um dies zu sehen, betrachte man folgende Variablenbelegung: $\xi'(x) = 1$ und $\xi'(y) = \xi'(z) = 0$. Diese Belegung macht die linke Seite der Implikation $(R(x,y) \wedge R(x,z)) \supset \exists u(R(y,u) \wedge R(z,u))$ wahr. (0 ist der Vorgänger von 1.) Aber die rechte Seite der Implikation ist falsch, da 0 keinen Vorgänger in den natürlichen Zahlen $\omega$ hat. Zusammenfassend gilt, wie verlangt, dass $\mathcal{I}$ ein Modell von $pf$ und ein Gegenbeispiel zu *sger* ist.

**Aufgabe 4.3**

Finden Sie alle Fehler in den folgenden Beweisversuchen. Sie müssen die Fehler nicht korrigieren, sondern nur möglichst klar beschreiben. Betrachten Sie jeden Ableitungsschritt für sich; ignorien Sie also 'Folgefehler'.

a) Folgendes Tableau zeigt, dass $\forall x \exists y(Q(a,y) \supset Q(y,x))$ aus $\forall x(\neg Q(a,x) \wedge \neg Q(x,a))$ logisch folgt.

| | | | | | |
|---|---|---|---|---|---|
| (1) | $\mathbf{t} : \forall x \exists y(Q(a,y) \supset Q(y,x))$ | | | | Annahme, $\gamma$-Formel |
| (2) | $\mathbf{f} : \forall x(\neg Q(a,x) \wedge \neg Q(x,a))$ | | | | Annahme, $\delta$-Formel |
| (3) | $\mathbf{t} : \exists y(Q(a,y) \supset \forall x Q(y,x))$ | | | | von 1, $\delta$-Formel |
| (4) | $\mathbf{f} : \neg Q(a,a)$ | | | | von 2 |
| (5) | $\mathbf{t} : \exists y Q(a,y)$ | von 3 | (7) | $\mathbf{f} : \forall x Q(a,x)$ | von 3, $\delta$-Formel |
| (6) | $\mathbf{t} : Q(a,a)$ | von 4, $\delta$-Formel | (8) | $\mathbf{f} : Q(a,a)$ | von 7 |
| | $\times$ | Wid.: 6/8 | | $\times$ | Wid.: 4/8 |

b) Folgendes Tableau zeigt, dass $\forall x \exists y(x = f(f(y)) \supset \exists z f(a) = f(z))$ erfüllbar ist.

| | | |
|---|---|---|
| (1) | $\mathbf{f} : \forall x \exists y(x = f(f(y)) \supset \exists z f(a) = f(z))$ | Annahme |
| (2) | $\mathbf{t} : \forall x \exists y\, x = f(f(y))$ | von 1, $\gamma$-Formel |
| (3) | $\mathbf{f} : \exists z f(a) = f(z)$ | von 1, $\delta$-Formel |
| (4) | $\mathbf{f} : f(a) = f(b)$ | von 3, $\gamma$-Formel |
| (5) | $\mathbf{t} : \exists y\, f(b) = f(y)$ | von 2, $\gamma$-Formel |
| (6) | $\mathbf{t} : f(b) = f(a)$ | von 5, $\delta$-Formel |
| | $\times$ | Wid.: 4/6 |

**Lösung 4.3**

a) Es gibt folgende Fehler:

1. Der Ansatz im Tableau ist falsch. Um einen indirekten Beweis für die Konsequenzbehauptung zu erbringen, muss die Prämisse wahr und die Konklusion falsch gesetzt werden. Die ersten beiden Zeilen müssten lauten:

   | | | |
   |---|---|---|
   | (1) | $\mathbf{t} : \forall x(\neg Q(a,x) \wedge \neg Q(x,a))$ | Annahme, $\gamma$-Formel |
   | (2) | $\mathbf{f} : \forall x \exists y(Q(a,y) \supset Q(y,x))$ | Annahme, $\delta$-Formel |

2. Der Inferenz-Schritt von (1) nach (3) entspricht keiner Regel des Tableau-Kalküls. $\forall x \exists y(Q(a,y) \supset Q(y,x))$ und $\exists y(Q(a,y) \supset \forall x Q(y,x))$ sind zwar logisch äquivalent sind; aber diese semantische Tatsache darf nicht einfach in den (naturgemäß syntaktischen) Kalkül 'importiert' werden.

3. Wie im vorigen Schritt, wurde im Schritt von (2) auf (4) Semantik mit Syntax vermischt: $\neg Q(a,a)$ ist keine Instanz von $\forall x(\neg Q(a,x) \wedge \neg Q(x,a))$. Allenfalls wäre $\neg Q(a,a) \wedge \neg Q(a,a)$ eine Instanz von $\forall x(\neg Q(a,x) \wedge \neg Q(x,a))$.

4. (2) ist eine $\delta$-Formel ist. Das bedeutet: Wir kennen kein bestimmtes Element, dass bezeugen kann, dass die all-quantifizierte Aussage falsch ist. Entsprechend verlangt die $\delta$-Regel, dass ein neuen Parameter, also eine nicht bereits vorkommende Konstante, die quantifizierte Variable ersetzen muss. Hier wurde aber $a$, also eine bereits vorkommende Konstante verwendet.

5. Der Schritt von (3) auf (5) und (7) ist falsch, da (3) keine Implikation, sondern eine existenz-quantifizierte Formel ist. (Außerdem müsste man, falls wirklich die Implikationsregel auf eine als wahr bewertete Formel angewendet wird, die linke Teilformel der Implikation mit '$\mathbf{f}$' und die rechte Teilformel mit '$\mathbf{t}$' bewerten.)

6. Abgesehen von 5.), wurde in (7) die in (3) existenz-quantifizierte Variable $y$ einer $\delta$-Formel durch die bereits vorkommende Konstante $a$ ersetzt.

7. In (5) sollte markiert werden, dass $\mathbf{t} : \exists y Q(a,y)$ eine $\delta$-Formel ist.

8. (6) wird fälschlicherweise als $\delta$-Formel bezeichnet. Es ist aber eine atomare bewertete Formel; also weder vom Typ $\delta$ noch $\gamma$.

9. Unterhalb von Zeile (6): Der vermeintliche Widerspruch zwischen (6) und (8) ist keiner, denn $\mathbf{t} : Q(a,a)$ und $\mathbf{f} : Q(a,a)$ liegen auf unterschiedlichen Ästen des Tableaus und beziehen sich daher auch zwei verschiedene Fälle des Beweises, die natürlich nicht vermischt werden dürfen.
10. In (8) muss bei Anwendung der $\delta$-Regel auf (7) eine neue Konstante, statt dem bereits vorkommenden $a$, für $x$ eingesetzt werden.
11. Unterhalb von Zeile (8): Es besteht zwar ein logischer Widerspruch zwischen (4) und (8), aber es gibt keine Tableau-Regel, die den Abschluss des Astes bereits an dieser Stelle rechtfertigt. Es muss zunächst die Negations-Regel auf (4) angewendet werden um die Zeile '(9) $\mathbf{t} : Q(a,a)$ von 4' zu erhalten, bevor der Ast regelkonform abgeschlossen werden kann.

b) Der Ansatz ist im Prinzip richtig: Wenn man ein geschlossenes Tableau angibt, dass mit der Annahme beginnt, dass $\forall x \exists y (x = f(f(y)) \supset \exists z f(a) = f(z))$ falsch ist, dann ist damit die Gültigkeit dieser Formel gezeigt. Da jede gültige Formel auch erfüllbar ist, wäre die Behauptung tatsächlich bewiesen.

Es gibt aber folgende Fehler und Mängel im Beweisversuch:

1. Die bewertete Formel (1) ist eine $\delta$-Formel, die als solche bezeichnet werden sollte.
2. Der Schritt von (1) nach (2) und (3) ist inkorrekt. Auf (1) müsste die $\delta$-Regel angewendet werden und nicht die Implikationsregel.
3. In Zeile (3) steht keine $\delta$-Formel, sondern eine $\gamma$-Formel.
4. Die Formel in Zeile (4) ist keine $\gamma$-Formel. (Sie ist auch keine $\delta$-Formel. Aber man kann (4) tatsächlich regelkonform durch Anwendung der $\gamma$-Regel auf die $\gamma$-Formel (3) ableiten.)
5. In Zeile (5) wurde die rechte Seite der Gleichung in Zeile (2), also $f(f(y))$ fälschlicherweise durch $f(y)$ ersetzt.
6. Die bewertete Formel in Zeile (5) ist keine $\gamma$-Formel, sondern eine $\delta$-Formel. (Die Substitution der Variablen $x$ durch den Term $f(b)$ entspricht einer korrekten Anwendung der $\gamma$-Regel auf die $\gamma$-Formel in (2).)
7. (6) ist keine $\delta$-Formel. (Außerdem kann man Folgendes anmerken: Wenn man korrekterweise die $\delta$-Regel, anstatt der $\gamma$-Regel auf (5) anwendet, dann müsste in (6) eine neue Konstante zur Substitution von $y$ verwendet werden und nicht die bereits vorkommende Konstante $a$. Aber das ist ein Folgefehler.)
8. Unterhalb von Zeile (6): Es besteht zwar ein logischer Widerspruch zwischen den Zeilen (4) und (6), aber es gibt keine Tableau-Regel, die den Abschluss des Astes bereits an dieser Stelle erlaubt (siehe Folie 455). Es muss zunächst noch eine der Gleichheitsregeln auf Zeile (4), unter Verwendung der als wahr bewerteten Gleichung $f(b) = f(a)$ in Zeile (6), angewendet werden. Das ergibt entweder die Zeile '(7) $\mathbf{f} : f(a) = f(a)$ $S^{=}$: 6→4' oder die Zeile '(7) $\mathbf{f} : f(b) = f(b)$ $S^{=}$: 6→4' (je nachdem welche der Gleichheitsregeln man anwendet). In beiden Fällen kann man die Abschlussregel für Gleichheit $AB^{=}$ danach anwenden, um den Ast zu schließen.

**Aufgabe 4.4**

Sind die folgenden Korrektheitsaussagen wahr oder falsch hinsichtlich partieller bzw. totaler Korrektheit? Argumentieren Sie mit Hilfe der Definition der Semantik von Korrektheitsaussagen. Es ist keine Ableitung im Hoare-Kalkül notwendig, sondern nur jeweils ein informeller Beweis bzw. ein Gegenbeispiel.

a) $\{x = x\}\ x \leftarrow 3x\ \{x = 3x\}$

b) $\{x < 0\}$ `if` $x > y$ `then` $x \leftarrow x - y$ `else` $x \leftarrow y - x$ $\{x + y < x\}$

c) $\{y = z\}$ `begin` $x \leftarrow y + 1;\ x \leftarrow 3x$ `end` $\{x = 3z + 3\}$

d) $\{y \leq x\}$ `while` $x \geq 0$ `do` $x \leftarrow x - y$ $\{x < 0\}$

e) $\{y \leq x\}$ `while` $x \geq 0$ `do` $x \leftarrow x - y$ $\{x < 0 \wedge y < 0\}$

**Lösung 4.4**

a) Die Korrektheitsaussage ist nicht wahr (weder hinsichtlich partieller noch totaler Korrektheit).

Gegenbeispiel: Variablenbelegung (Umgebung) $I$ mit $I(x) = 1$. Es gilt:

- Die Variablenbelegung erfüllt die Vorbedingung: $\mathcal{M}(I, x = x) = [I(x) = I(x)] = [1 = 1] = \mathbf{t}$.
- Berechnung des Ergebnisses: $\mathcal{M}(I, x \leftarrow 3x) = I'$, wobei $I'(x) = 3 \cdot I(x) = 3 \cdot 1 = 3$ und $I' \overset{x}{\sim} I$.
- Das Ergebnis $I'$ erfüllt die Nachbedingung nicht: $\mathcal{M}(I', x = 3x) = [I'(x) = 3 \cdot I'(x)] = [3 = 9] = \mathbf{f}$.

b) Die Korrektheitsaussage ist weder partiell noch total korrekt.

Gegenbeispiel: $I(x) = -1$, $I(y) = 0$. Es gilt:

- Die Variablenbelegung $I$ erfüllt die Vorbedingung: $\mathcal{M}(I, x < 0) = [I(x) < 0] = [-1 < 0] = \mathbf{t}$
- Berechnung des Ergebnisses:

$$\begin{aligned}
&\mathcal{M}(I, \texttt{if } x > y \texttt{ then } x \leftarrow x - y \texttt{ else } x \leftarrow y - x) \\
&\quad [\,\mathcal{M}(I, x > y) = [I(x) > I(y)] = [-1 > 0] = \mathbf{f}\,] \\
&= \mathcal{M}(I, x \leftarrow y - x) \\
&= I' \\
&\quad [\,I'(x) = \mathcal{M}(I, y - x) = I(y) - I(x) = 0 - (-1) = 1,\ I'(y) = I(y) = 0\,]
\end{aligned}$$

- Das Ergebnis erfüllt nicht die Nachbedingung:

$$\mathcal{M}(I', x + y < x) = [I'(x) + I'(y) < I'(x)] = [1 + 0 < 1] = \mathbf{f}$$

c) Die Korrektheitsaussage ist partiell und total korrekt.

Argumentation mittels der Semantik von Korrektheitsaussagen:

- Wir betrachten alle Wertebelegungen $I$, die die Vorbedingung erfüllen, für die also $\mathcal{M}(I, y = z) = [I(y) = I(z)]$ wahr ist.
- Die AL-Semantik von `begin-end`-Anweisungen legt fest, dass zuerst die Anweisung $x \leftarrow y + 1$ in $I$ auszuwerten ist. Wir erhalten $I' = \mathcal{M}(I, x \leftarrow y + 1)$, wobei $I'(x) = I(y) + 1$, $I'(y) = I(y)$ und $I'(z) = I(z)$.

  Im nächsten Schritt muss die zweite Anweisung in der Variablenbelegung $I'$ ausgewertet werden. Wir erhalten $I'' = \mathcal{M}(I', x \leftarrow 3x)$, wobei $I''(x) = 3 \cdot I'(x) = 3 \cdot (I(y) + 1) = 3 \cdot I(y) + 3$, $I''(y) = I'(y) = I(y)$ und $I''(z) = I'(z) = I(z)$.
- Die Auswertung der Nachbedingung $x = 3z + 3$ in $I''$ ergibt:

$$\mathcal{M}(I'', x = 3z + 3) = [I''(x) = 3 \cdot I''(z) + 3] = [3 \cdot I(y) + 3 = 3 \cdot I(z) + 3]$$

  Da wegen der Vorbedingung $I(y) = I(z)$ gilt, evaluiert $3 \cdot I(y) + 3 = 3 \cdot I(z) + 3$ zu wahr.

Argumentation mit Hilfe des Hoare-Kalküls: Um zu zeigen, dass eine Korrektheitsaussage wahr ist, können wir auch eine Ableitung der Aussage im Hoare-Kalkül angeben. Tatsächlich ist genau das sein Zweck: Der Hoare-Kalkül vereinfacht Korrektheitsbeweise, da wir nicht mehr auf die Semantikfunktionen zurückgreifen müssen.

$$\dfrac{\dfrac{(zw'')}{\{y = z\}\, x \leftarrow y + 1\, \{y = z \wedge x = y + 1\}} \qquad \dfrac{\dfrac{(2)}{y = z \wedge x = y + 1 \supset (x = 3z + 3[^{3x}_{x}])} \quad (zw)}{\{y = z \wedge x = y + 1\}\, x \leftarrow 3x\, \{x = 3z + 3\}}}{\{y = z\}\, \texttt{begin } x \leftarrow y + 1;\ x \leftarrow 3x \texttt{ end}\, \{x = 3z + 3\}}$$

Die Interpolante $y = z \wedge x = y + 1$ erhält man hier aus dem Axiom $(zw'')$, das zur Zuweisung $x \to y + 1$ und der Vorbedingung $y = z$ passt, weil $x$ weder in $y = z$ noch in $y + 1$ vorkommt.[1]

Nach Durchführung der Substitution lautet die Formel (2) $y = z \wedge x = y + 1 \supset 3x = 3z + 3$. Diese Formel ist gültig in $\mathbb{Z}$.

Die Korrektheitsaussage der Angabe lässt sich somit durch Anwendung der Regel (be) und der Implikationsregel (im rechten Ast) aus den Axiomen $(zw)$ und $(zw'')$ und der gültigen Formel (2) ableiten. Aus der Korrektheit des Hoare-Kalküls folgt, dass die Aussage bezüglich partieller Korrektheit wahr ist. Da Programme ohne `while`-Schleife immer terminieren, gilt auch totale Korrektheit.

d) Die Korrektheitsaussage ist partiell, aber nicht total korrekt.

Wir analysieren das Verhalten des Programms für alle Wertebelegungen $I$, die die Vorbedingung erfüllen, für die also $I(y) \leq I(x)$ gilt. Wir unterscheiden zwei Fälle.

$I(x) \geq 0$: Die Schleife wird ausgeführt. Wenn $y$ positiv ist, dann wird $x$ in jedem Schleifendurchlauf kleiner. Daher terminiert das Programm für $I(y) > 0$, da die Schleifenbedingung irgendwann nicht mehr erfüllt ist. Es gilt dann $x < 0$ und somit die Nachbedingung. Andererseits terminiert das Programm nicht, wenn $I(y) \leq 0$ gilt.

[1] Es gibt eine alternative Ableitung mit der Interpolante $3x = 3z + 3$ und der Verwendung der Implikationsregel im linken, statt im rechten Ast.

$I(x) < 0$: Die Schleifenbedingung ist nicht erfüllt, daher wird die Schleife nicht ausgeführt und das Programm endet mit dem Ergebnis $I$. Die Nachbedingung ist offensichtlich erfüllt.

Zusammenfassend gilt: Wenn die Vorbedingung erfüllt ist und das Programm terminiert, dann ist auch die Nachbedingung erfüllt. Somit ist die Korrektheitsaussage partiell korrekt.

Andererseits gibt es Wertebelegungen $I$, die die Vorbedingung erfüllen, für die das Programm aber nicht terminiert. Ein konkretes Beispiel dafür ist $I(x) = I(y) = 0$. Daher ist die Korrektheitsaussage nicht total korrekt.

e) Die Korrektheitsaussage ist nicht partiell und daher auch nicht total korrekt.

Als Gegenbeispiel zur partiellen Korrektheit betrachten wir eine Umgebung $I$ mit $I(x) = I(y) = 1$. Die Schleifenbedingung $x \geq 0$ trifft zu und wir erhalten nach dem ersten Schleifendurchlauf die Umgebung $I'$, für die gilt $I'(x) = I(x) - I(y) = 1 - 1 = 0$, $I'(y) = I(y) = 1$. Auch in $I'$ ist die Schleifenbedingung erfüllt. Nach dem nächsten Schleifendurchlauf erhalten wir $I''$ mit $I''(x) = I'(x) - I'(y) = 0 - 1 = -1$ und $I''(y) = I'(y) = I(y) = 1$. Da nun die Schleifenbedingung $x \geq 0$ nicht mehr zutrifft, terminiert das Programm mit der Variablenbelegung $I''$. In dieser Umgebung ist die Nachbedingung $x < 0 \wedge y < 0$ nicht erfüllt: $I''(y)[= 1] < 0$ ist falsch.

**Aufgabe 4.5**

Verwenden Sie die Regeln des Hoare-Kalküls um zu zeigen, dass die folgende Aussage wahr hinsichtlich totaler Korrektheit im Datentyp $\mathbb{Z}$ ist. (D.h., das Programm ist total korrekt bezüglich der angegebenen Vor- und Nachbedingung.)

$\{\, x = x_0 \wedge x \geq 0 \,\}$
```
begin
y ← 3 * x;
while 2 * x ≠ y do
  begin
  x ← x + 1;
  y ← y + 1
  end
end
```
$\{\, x = 2x_0 \,\}$

Verwenden Sie die Formel $y = 2x_0 + x \wedge y \geq 2x$ als Invariante und den Ausdruck $y - 2x$ als Terminationsfunktion. Der Korrektheitsbeweis soll in linearer Schreibweise, also durch Ergänzung entsprechender Annotationen im Programm, erfolgen. Argumentieren Sie, warum die auftretenden Formeln gültig sind.

**Lösung 4.5**

Wir beginnen damit, dass wir das Programm entsprechend den Regeln des Hoare-Kalküls mit Formeln annotieren. Die Formeln sind in jener Reihenfolge nummeriert, in der sie hinzugefügt wurden. Diese Reihenfolge ist nicht vollkommen eindeutig; etwa hätten die Formeln $F_6$ und $F_7$ vor Formel $F_5$ hinzugefügt werden können.

```
      { P: x = x0 ∧ x ≥ 0 }
zw↑   { F5: Inv[3x/y] }
      begin
      y ←3*x ;
wh    { F1: Inv }
      while 2 * x ≠ y do
        begin
wh      { F2: Inv ∧ 2 * x ≠ y ∧ t = t0 }
zw↑     { F7: Inv[y+1/y][x+1/x] ∧ 0 ≤ t[y+1/y][x+1/x] < t0 }
        x ←x+1;
zw↑     { F6: Inv[y+1/y] ∧ 0 ≤ t[y+1/y] < t0 }
        y ←y+1
wh      { F3: Inv ∧ 0 ≤ t < t0 }
        end
      end
wh    { F4: Inv ∧ ¬2 * x ≠ y }
      { Q: x = 2 * x0 }
```

Gemäß Implikationsregel muss noch die Gültigkeit der Formeln $P \supset F_5$, $F_2 \supset F_7$ und $F_4 \supset Q$ gezeigt werden.

$\boldsymbol{P} \supset \boldsymbol{F_5}$ $\quad x = x_0 \wedge x \geq 0 \supset \mathit{Inv}[^{3x}_{y}]$

$$x = x_0 \wedge x \geq 0 \supset 3x = 2x_0 + x \wedge 3x \geq 2x$$
$$x = x_0 \wedge x \geq 0 \supset x = x_0 \wedge x \geq 0$$

Diese Formel ist offensichtlich gültig. Da die Vereinfachungsschritte von der zweiten zur dritten Zeile Äquivalenzumformungen sind, ist auch die ursprüngliche Formel gültig.

$\boldsymbol{F_4} \supset \boldsymbol{Q}$

$$\mathit{Inv} \wedge \neg 2x \neq y \supset x = 2x_0$$
$$y = 2x_0 + x \wedge y \geq 2x \wedge 2x = y \supset x = 2x_0$$

Aus $y = 2x_0 + x$ und $2x = y$ erhalten wir $2x = 2x_0 + x$ und daraus wiederum die Konklusion $x = 2x_0$, die Formel ist also gültig.

$\boldsymbol{F_2} \supset \boldsymbol{F_7}$ Die Implikation

$$\mathit{Inv} \wedge 2x \neq y \wedge t = t_0 \supset \mathit{Inv}[^{y+1}_{y}][^{x+1}_{x}] \wedge 0 \leq t[^{y+1}_{y}][^{x+1}_{x}] < t_0$$

ist gleichwertig zu den beiden folgenden, von denen die erste der partiellen Korrektheit der Schleife entspricht und die zweite ihrer Termination.

| | |
|---|---|
| $\mathit{Inv} \wedge 2x \neq y \supset \mathit{Inv}[^{y+1}_{y}][^{x+1}_{x}]$ | partielle Korrektheit |
| $\mathit{Inv} \wedge 2x \neq y \supset 0 \leq t[^{y+1}_{y}][^{x+1}_{x}] < t$ | Termination |

$\boldsymbol{F_2} \supset \boldsymbol{F_7}$ (partielle Korrektheit) Unter Verwendung von $\mathit{Inv} = (y = 2x_0 + x \wedge y \geq 2x)$ erhalten wir:

$$\mathit{Inv} \wedge 2x \neq y \supset (y = 2x_0 + x \wedge y \geq 2x)[^{y+1}_{y}][^{x+1}_{x}]$$
$$\mathit{Inv} \wedge 2x \neq y \supset (y + 1 = 2x_0 + (x{+}1) \wedge (y{+}1) \geq 2(x{+}1))$$
$$\mathit{Inv} \wedge 2x \neq y \supset (y = 2x_0 + x \wedge y \geq 2x + 1)$$
$$(y = 2x_0 + x \wedge y \geq 2x \wedge 2x \neq y) \supset (y = 2x_0 + x \wedge y > 2x)$$

Offenbar gilt die Gleichung $y = 2x_0 + x$, da sie auch unter den Annahmen auftritt. Die rechte Seite $y > 2x$ der Implikation folgt aus den beiden Konjunkten $y \geq 2x$ und $2x \neq y$ auf der linken Seite. Daher ist die Implikation eine gültige Formel.

$\boldsymbol{F_2} \supset \boldsymbol{F_7}$ (Termination) Unter Verwendung von $\mathit{Inv} = (y = 2x_0 + x \wedge y \geq 2x)$ und $t = y - 2x$ erhalten wir:

$$\mathit{Inv} \wedge 2x \neq y \supset 0 \leq t[^{y+1}_{y}][^{x+1}_{x}] < t$$
$$\mathit{Inv} \wedge 2x \neq y \supset 0 \leq y + 1 - 2(x + 1) < t$$
$$y = 2x_0 + x \wedge y \geq 2x \wedge 2x \neq y \supset 0 \leq t - 1 \wedge t - 1 < t$$

$t - 1 < t$ gilt in den ganzen Zahlen immer. Die erste Ungleichung, $0 \leq t - 1$, ist gleichbedeutend mit $t > 0$ bzw. $y > 2x$. Sie folgt aus $y \geq 2x$ und $2x \neq y$. Daher ist auch diese Implikation gültig.

Da alle Implikationen im Datentyp $\mathbb{Z}$ gültig sind, ist das Program bezüglich der Vorbedingung $x = x_0 \wedge x \geq 0$ und der Nachbediingung $x = 2 * x_0$ nicht nur partiell, sondern auch total korrekt. Mit anderen Worten: Die Korrektheitsaussage ist wahr hinsichtlich totaler Korrektheit.