# Theoretische Informatik und Logik
# Übungsblatt 4 (SS 2017)
# Lösungen

**Aufgabe 4.1** Für jede der folgende Formeln ist folgendes zu tun: Wenn die Formel gültig oder unerfüllbar ist, so beweisen Sie dies mit dem Tableau-Kalkül. Wenn die Formel hingegen sowohl erfüllbar als auch widerlegbar ist, dann geben Sie ein Modell und ein Gegenbeispiel an.

a) $\forall x \forall y[P(x,y) \wedge \neg \forall x \exists y P(x,y)]$

b) $\exists x \forall y[P(x,y) \supset \exists x \forall y P(x,y)]$

c) $\forall x \exists y[P(x,y) \supset \exists x \forall y P(x,y)]$

*Hinweis:* Achten Sie bei jedem Tableau darauf, dass alle bewerteten Formeln eine eindeutige Nummer tragen und dass alle Regelanwendungen über diese Nummern auf ihre jeweiligen Prämissen verweisen. Außerdem sollen alle $\gamma$- und $\delta$-Formeln jeweils auch als solche markiert werden.

### Lösung

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

| | | |
|---|---|---|
| (1) | $\mathbf{t} : \forall x \forall y[P(x,y) \wedge \neg \forall x \exists y P(x,y)]$ | Annahme, $\gamma$-Formel |
| (2) | $\mathbf{t} : \forall y[P(a,y) \wedge \neg \forall x \exists y P(x,y)]$ | von 1, $\gamma$-Formel |
| (3) | $\mathbf{t} : P(a,a) \wedge \neg \forall x \exists y P(x,y)$ | von 2 |
| (4) | $\mathbf{t} : P(a,a)$ | von 3 |
| (5) | $\mathbf{t} : \neg \forall x \exists y P(x,y)$ | von 3 |
| (6) | $\mathbf{f} : \forall x \exists y P(x,y)$ | von 5, $\delta$-Formel |
| (7) | $\mathbf{f} : \exists y P(b,y)$ | von 6, $\gamma$-Formel |
| (8) | $\mathbf{t} : \forall y[P(b,y) \wedge \neg \forall x \exists y P(x,y)]$ | von 1, $\gamma$-Formel |
| (9) | $\mathbf{t} : P(b,a) \wedge \neg \forall x \exists y P(x,y)$ | von 8 |
| (10) | $\mathbf{t} : P(b,a)$ | von 9 |
| (11) | $\mathbf{t} : \neg \forall x \exists y P(x,y)$ | von 9 |
| (12) | $\mathbf{f} : P(b,a)$ | von 7 |
| | $\times$ | Widerspruch (10/12) |

Beachten Sie, dass die $\gamma$-Regel – nach Verwendung der $\delta$-Regel in Zeile 7 – nochmals auf die Formel in Zeile 1 angewendet werden muss um einen Abschluss zu erhalten.

b) Die Formel ist erfüllbar und widerlegbar.

Ein Modell ist besonders einfach anzugeben, da man nur dafür sorgen muss, dass alle atomaren Formeln unter der entsprechenden Interpretation wahr werden. Z.B. ist die ein-elementige Interpretation $\mathcal{I} = \langle \{0\}, \Phi, \xi \rangle$, mit $\Phi(P)(0,0) = \mathbf{t}$ und beliebigem $\xi$, ein Modell der Formel.

Gegenbeispiel: $\mathcal{I}' = \langle D, \Phi, \xi \rangle$, wobei $D = \omega$, $\Phi(P)(m,n) = \mathbf{t} \iff n = m+1$, $\xi$ beliebig. Unter dieser Interpretation besagt die Formel, dass es eine bestimmte natürliche Zahl $x$ gibt, sodass für alle natürliche Zahlen $y$ folgendes gilt: Wenn $y$ der Nachfolger von $x$ ist, dann gibt es eine Zahl, die jede Zahl zum Nachfolger hat. Diese Aussage ist falsch.

c) 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 |
| | $\times$ | Widerspruch (7/9) |

Beachten Sie, dass die $\gamma$-Regel – nach Verwendung der $\delta$-Regel in Zeile 7 – nochmals auf die Formel in Zeile 2 angewendet werden muss um einen Abschluss zu erhalten.

**Aufgabe 4.2** Betrachten Sie folgende Formeln (Axiome) zum Datentyp $\mathbb{B}$ aus Aufgabe 3.2. (Wir lassen alle Unterstreichungen weg und schreiben $s \neq t$ für $\neg s = t$.)

A1: $\square \neq \epsilon$
A2: $f(\epsilon, \epsilon) = \square$
A3: $f(\square, \square) \neq \square$
A4: $\forall x \forall y [f(x,y) = \epsilon \supset (x = \epsilon \vee y = \epsilon)]$
A5: $\forall x \forall y [(x = \epsilon \wedge y \neq \epsilon) \supset f(x,y) = \epsilon]$
A6: $\forall x \forall y [(x \neq \epsilon \wedge y = \epsilon) \supset f(x,y) = \epsilon]$
A7: $\forall x ((x = \epsilon \vee x = \square) \vee \exists y \exists z [(y \neq \epsilon \wedge z \neq \epsilon) \wedge x = f(y,z)])$
A8: $\forall x \forall y \forall z [z = f(x,y) \supset (z \neq \epsilon \vee (x \neq \epsilon \vee y \neq \epsilon))]$

a) Zeigen Sie, dass $\mathcal{B} = \{A1, \ldots, A8\}$ keine vollständige Axiomatisierung von $Th(\mathbb{B})$ ist, indem Sie ein Modell von $\mathcal{B}$ angeben, dessen Gegenstandsbereich aus nur 3 Elementen besteht.

b) Zeigen Sie mit dem Tableau-Kalkül, dass $\exists x \exists y \forall z (f(x,z) = y \vee z \neq \epsilon)$ aus A2 logisch folgt.

c) Geben Sie mindestens 3 paarweise nicht logisch äquivalente Formeln aus $Th(\mathbb{B})$ an, die nicht aus $\mathcal{B}$ logisch folgen. Argumentieren Sie (informell) für die Richtigkeit Ihrer Lösung.

**Lösung**

a) Es ist leicht zu überprüfen, dass folgende 3-elementige Interpretation $\mathcal{I} = \langle \{0,1,2\}, \Phi, \xi \rangle$ alle Formeln in $\mathcal{B}$ wahr macht:

- $\Phi(\epsilon) = 0$,
- $\Phi(\square) = 1$,
- die Funktion $\Phi(f)$ ist durch folgende Tafel spezifiziert:

| | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 1 | 0 | 0 |
| 1 | 0 | 2 | 2 |
| 2 | 0 | 2 | 2 |

- $\xi$ ist beliebig, da es keine freien Variablen in $\mathcal{B}$ gibt.

b) Folgendes geschlossenes Tableau zeigt, dass $\exists x \exists y \forall z (f(x,z) = y \vee z \neq \epsilon)$ aus A2 folgt:

| | | |
|---|---|---|
| (1) | $\mathbf{t} : f(\epsilon, \epsilon) = \square$ | Annahme (A2) |
| (2) | $\mathbf{f} : \exists x \exists y \forall z (f(x,z) = y \vee z \neq \epsilon)$ | Annahme, $\gamma$-Formel |
| (3) | $\mathbf{f} : \exists y \forall z (f(\epsilon,z) = y \vee z \neq \epsilon)$ | von 2, $\gamma$-Formel |
| (4) | $\mathbf{f} : \forall z (f(\epsilon,z) = \square \vee z \neq \epsilon)$ | von 3, $\delta$-Formel |
| (5) | $\mathbf{f} : f(\epsilon,a) = \square \vee a \neq \epsilon$ | von 4 |
| (6) | $\mathbf{f} : f(\epsilon,a) = \square$ | von 5 |
| (7) | $\mathbf{f} : a \neq \epsilon$ | von 5 |
| (8) | $\mathbf{t} : a = \epsilon$ | von 7 |
| (9) | $\mathbf{f} : f(\epsilon,\epsilon) = \square$ | $S^{=}$: 8→6 |
| | $\times$ | Widerspruch (1/9) |

c) $F_1$: $\exists x \exists y \exists z \exists u (x \neq y \wedge x \neq z \wedge x \neq u \wedge y \neq z \wedge y \neq u \wedge z \neq u)$
$F_1$ drückt aus, dass es mindestens 4 verschiedene Elemente in der Domäne gibt. Das trifft auf die Menge der binären Bäume zu. Daher gilt $F_1 \in Th(\mathbb{B})$. Anderseits ist die Formel im Modell von $\mathcal{B}$ aus a) falsch und kann daher nicht bereits aus $\mathcal{B}$ logisch folgen.

$F_2$: $f(\square,\square) \neq f(f(\square,\square),\square)$
Diese Formel drückt aus, dass die beiden Bäume, die durch den linken bzw. den rechten Term der Gleichung repräsentiert werden, nicht identisch sind. Dies ist in ($\mathbb{B}$) wahr, aber im Modell von $\mathcal{B}$ aus a) falsch und kann daher nicht bereits aus $\mathcal{B}$ logisch folgen.

$F_3$ $f(\square, f(\square,\square)) \neq f(f(\square,\square),\square)$
Die Begründung ist wie für $F_2$.

Die jeweilige Bedeutung der Formeln macht klar, dass diese nicht logisch äquivalent sind: Man könnte zum jedem Paar $(F_i, F_j)$, wobei $i \neq j$ und $i,j \in \{1,2,3\}$ Interpretationen angeben, in denen $F_i$ wahr und $F_j$ falsch ist. (Da es hier um allgemeine logische Äquivalenz geht, ist es irrelevant, welche anderen Formeln in diesen Interpretationen wahr oder falsch sind.)

**Aufgabe 4.3** (Siehe Folie 409 für die Definition relevanter Eigenschaften von Relationen.)

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

b) Zeigen Sie, dass Serialität in a) notwendig ist. Genauer: Spezifizieren Sie eine Interpretation in der $\Phi(R)$ eine partiell funktionale, aber keine schwach gerichtete Relation ist.

**Lösung**

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 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) Die Vorgängerrelation für natürliche Zahlen ist partiell funktional, aber nicht euklidisch. Etwas formaler: Wir erhalten ein Gegenbeispiel $\mathcal{I} = \langle \omega, \Phi, \xi \rangle$ zur Konsequenzbehauptung $\forall x \exists y[R(x,y) \wedge \forall z(R(x,z) \supset y = z)] \models \forall x \forall y \forall z[(R(x,y) \wedge R(x,z)) \supset R(y,z)]$ indem wir $\Phi(R)(m,n) = \mathbf{t} \Longleftrightarrow n = m + 1$ setzen ($\xi$ beliebig).

**Aufgabe 4.4** Untersuchen Sie folgende Varianten der $\gamma$- bzw. der $\delta$-Regel für PL-Tableaux.

a) Wenn man bei der $\gamma$-Regel verlangt, dass der einzusetzende Term $t$ keine neuen Konstanten (Parameter) enthält: Bleibt der Tableau-Kalkül korrekt? Bleibt er vollständig?

b) Wenn man für die $\delta$-Regel nicht verlangt, dass die einzusetzende Konstante $c$ bisher nicht im Tableau vorkommt: Bleibt der Tableau-Kalkül korrekt? Bleibt er vollständig?

Begründen Sie positive Antworten und geben Sie jeweils ein konkretes Gegenbeispiel bei einer negativen Antwort an. (Gehen Sie davon aus, dass der Tableau-Kalkül, so wie er in der Vorlesung präsentiert wurde, korrekt und vollständig ist.)

**Lösung**

a) Jedes Tableau, in dem die eingeschränkte Variante der $\gamma$-Regel verwendet wird, bleibt ein regelkonformes Tableau auch gemäß der ursprünglichen Regeln. Insbesondere entstehen durch die Variante keine neuen *geschlossenen* Tableaux. Daher bleibt der Kalkül korrekt.

Allerdings ist der Kalkül nun unvollständig, wie folgendes Beispiel zeigt. Die Formel $F = \exists x(P(x) \supset P(x))$ ist offensichtlich gültig, aber die entsprechende Signatur $\Sigma$ enthält gar keine Konstantensymbole. Daher gibt es *keine geschlossene Terme* über $\Sigma$. Das bedeutet aber, dass auf $\mathbf{f} : \exists x(P(x) \supset P(x))$ die modifizierte $\gamma$-Regel gar nicht anwendbar ist und folglich trotz der Gültigkeit von $F$ kein geschlossenes Tableau für $F$ existiert.

b) Der Kalkül bleibt vollständig, da alle Äste, die in der ursprünglichen Variante des Kalküls geschlossen sind, auch weiterhin geschlossen bleiben. Es gibt also mit der neuen $\delta$-Regel allenfalls zusätzliche Tableau-Beweise.

Folgendes Beispiel zeigt, dass der Kalkül nicht mehr korrekt ist: Die Formel $G = \exists x P(x) \supset P(a)$ ist offensichtlich nicht gültig, da wir beispielsweise über dem Gegenstandsbereich der natürlichen Zahlen $\Phi(P) =$ "ist gerade" und $\Phi(a) = 1$ interpretieren können. Jedes Tableau für $G$ muss wie folgt beginnen:

| | | |
|---|---|---|
| (1) | $\mathbf{f} : \exists x P(x) \supset P(a)$ | Annahme |
| (2) | $\mathbf{t} : \exists x P(x)$ | $\delta$-Formel |
| (3) | $\mathbf{f} : P(a)$ | |

Wenn wir nun bei der Elimination des Existenzquantors in (2) $a$ anstatt eines neuen Parameters für $x$ einsetzen, so erhalten wir in der nächsten Zeile

$$(4) \quad \mathbf{t} : P(a)$$

und folglich ein geschlossenes Tableau im Gegensatz zur Tatsache, dass $G$ nicht gültig ist.

### Aufgabe 4.5

a) Untersuchen Sie, ob die Korrektheitsaussage

$$\{x \geq 0\}\, y \leftarrow y + 1\, \{y > 0\}$$

wahr ist. Verwenden Sie dazu die Definition der Wahrheit von Korrektheitsaussagen, um entweder zu argumentieren, dass die Aussage wahr ist, oder um ein Gegenbeispiel anzugeben.

b) Die Hintereinanderausführung der drei Zuweisungen

$$x \leftarrow x + y, \quad y \leftarrow x - y \quad \text{und} \quad x \leftarrow x - y$$

(in dieser Reihenfolge) bewirkt, dass die Variablen $x$ und $y$ ihre Werte vertauschen. Formulieren Sie eine Korrektheitsaussage und beweisen Sie sie mit Hilfe des Hoare-Kalküls.

c) Verwenden Sie die Regeln des Hoare-Kalküls um zu zeigen, dass die folgende Aussage total korrekt, d.h., wahr hinsichtlich totaler Korrektheit ist.
Verwenden Sie die Formel $y = 2 * x_0 + x \wedge y \geq 2 * x$ als Invariante und den Ausdruck $y - 2 * x$ als Terminationsfunktion.
Argumentieren Sie, warum die auftretenden Formeln gültig sind.

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

### Lösung

a) Die Zuweisung terminiert offensichtlich immer (das Programm enthält ja keine Schleife), die partielle bzw. totale Korrektheit der Aussage ist also gleichbedeutend mit:

> Für alle $I \in ENV$ gilt:
> Wenn $\mathcal{M}(I, x \geq 0) = \mathbf{t}$ gilt, dann gilt auch $\mathcal{M}(I', y > 0) = \mathbf{t}$,
> wobei $I' = \mathcal{M}(I, y \leftarrow y + 1)$.

Diese Aussage ist falsch. Um die All-Aussage zu widerlegen, genügt es, eine konkrete Wertebelegung $I$ anzugeben, die die Vorbedingung erfüllt ($\mathcal{M}(I, x \geq 0) = \mathbf{t}$), bei der aber die Nachbedingung in der Wertebelegung $I'$ nach Ausführung des Programms falsch ist ($\mathcal{M}(I', y > 0) = \mathbf{f}$).

Wir wählen eine Wertebelegung $I$ mit $I(x) = 0$ und $I(y) = -1$ und erhalten:

$$\mathcal{M}(I, x \geq 0) = (\mathcal{M}(I, x) \geq \mathcal{M}(I, 0)) = (I(x) \geq 0) = (0 \geq 0) = \mathbf{t}$$
$$\mathcal{M}(I, y \leftarrow y + 1) = I' \text{ wobei } I'(y) = \mathcal{M}(I, y + 1) = (-1 + 1) = 0$$
$$I' \overset{y}{\sim} I$$
$$\mathcal{M}(I', y > 0) = (\mathcal{M}(I', y) > \mathcal{M}(I', 0)) = (I'(y) > 0) = (0 > 0) = \mathbf{f}$$

$I$ erfüllt also die Vorbedingung, $I'$ aber nicht die Nachbedingung, die Korrektheitsaussage ist daher falsch.

b) Die Behauptung in der Angabe ist gleichbedeutend mit der Korrektheitsaussage

$$\{\, P\colon x = x_0 \wedge y = y_0 \,\}$$
$$\texttt{begin begin x} \leftarrow x + y\texttt{; } y \leftarrow x - y \texttt{ end; } x \leftarrow x - y \texttt{ end}$$
$$\{\, Q\colon x = y_0 \wedge y = x_0 \,\}$$

Wir erhalten die folgende Ableitung im Hoare-Kalkül.

$$\dfrac{\dfrac{P \supset Q_3 \quad \dfrac{}{\{Q_3\colon Q_2\left[\begin{smallmatrix} x \\ x+y \end{smallmatrix}\right]\}\, x \leftarrow x + y\, \{Q_2\}}\,(\text{zw})}{\{P\}\, x \leftarrow x + y\, \{Q_2\}}\,(\text{imp}) \qquad \dfrac{}{\{Q_2\colon Q_1\left[\begin{smallmatrix} y \\ x-y \end{smallmatrix}\right]\}\, y \leftarrow x - y\, \{Q_1\}}\,(\text{zw})}{\{P\}\,\texttt{begin } x \leftarrow x + y\texttt{; } y \leftarrow x - y \texttt{ end}\,\{Q_1\}}\,(\text{be}) \qquad \dfrac{}{\{Q_1\colon Q\left[\begin{smallmatrix} x \\ y-x \end{smallmatrix}\right]\}\, x \leftarrow x - y\, \{Q\}}\,(\text{zw})}{\{P\}\,\texttt{begin begin } x \leftarrow x + y\texttt{; } y \leftarrow x - y \texttt{ end; } x \leftarrow x - y \texttt{ end}\,\{Q\}}\,(\text{be})$$

Die Zerlegung der Korrektheitsaussage endet mit drei Instanzen des Zuweisungsaxioms, also von $\{G\left[\begin{smallmatrix} e \\ v \end{smallmatrix}\right]\}\, v \leftarrow e\, \{G\}$, und der Implikation $P \supset Q_3$, deren Gültigkeit wir noch zeigen müssen.

$$\begin{aligned}
&P \supset Q_3 \\
&P \supset Q\left[\begin{smallmatrix} x \\ y-x \end{smallmatrix}\right]\left[\begin{smallmatrix} y \\ x-y \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ x+y \end{smallmatrix}\right] \\
&P \supset (x = y_0 \wedge y = x_0)\left[\begin{smallmatrix} x \\ y-x \end{smallmatrix}\right]\left[\begin{smallmatrix} y \\ x-y \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ x+y \end{smallmatrix}\right] \\
&P \supset ((x - y) = y_0 \wedge y = x_0)\left[\begin{smallmatrix} y \\ x-y \end{smallmatrix}\right]\left[\begin{smallmatrix} x \\ x+y \end{smallmatrix}\right] \\
&P \supset ((x - (x - y)) = y_0 \wedge (x - y) = x_0)\left[\begin{smallmatrix} x \\ x+y \end{smallmatrix}\right] \\
&P \supset (y = y_0 \wedge (x - y) = x_0)\left[\begin{smallmatrix} x \\ x+y \end{smallmatrix}\right] \\
&P \supset (y = y_0 \wedge ((x + y) - y) = x_0) \\
(x = x_0 \wedge y = y_0) &\supset (y = y_0 \wedge x = x_0)
\end{aligned}$$

Diese Implikation ist eine Tautologie und daher gültig. Es liegt somit eine Ableitung der Korrektheitsaussage im Hoare-Kalkül vor, die Aussage ist daher wahr (hinsichtlich partieller und totaler Korrektheit).

Kompakter lässt sich der Korrektheitsbeweis mit Annotationen schreiben. Wir beginnen mit dem ursprünglichen Programm und fügen schrittweise Bedingungen hinzu, die die zulässigen Wertebelegungen an der jeweiligen Stelle beschreiben. Die Bedingungen ergeben sich aus den Regeln des Hoare-Kalküls. Wir rücken die `begin`- und `end`-Anweisungen ein, die der Syntax wegen notwendig sind, aber nichts zur Lesbarkeit des Programms beitragen. Der Index der Formelbezeichnungen richtet sich nach der Reihenfolge, in der die Annotationen hinzugefügt wurden.

$\{\, P\colon x = x_0 \wedge y = y_0 \,\}$
zw↑ $\{\, Q_3\colon x + y - (x + y - y) = y_0 \wedge x + y - y = x_0 \,\}$
`begin begin`
x $\leftarrow x + y$;
zw↑ $\{\, Q_2\colon x - (x - y) = y_0 \wedge x - y = x_0 \,\}$
y $\leftarrow x - y$
`end;`
zw↑ $\{\, Q_1\colon x - y = y_0 \wedge y = x_0 \,\}$
x $\leftarrow x - y$
`end`
$\{\, Q\colon x = y_0 \wedge y = x_0 \,\}$

Zuletzt muss noch, der Implikationsregel folgend, gezeigt werden, dass die Formel $P \supset Q_3$ gültig ist; Nachweis siehe oben.

c) 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.

$\{\, P\colon x = x_0 \wedge x \geq 0 \,\}$
zw↑ $\{\, F_5\colon Inv\binom{3x}{y} \,\}$
`begin`
y $\leftarrow 3 * x$;
wh $\{\, F_1\colon Inv \,\}$
`while` $2 * x \neq y$ `do`
`begin`
wh $\{\, F_2\colon Inv \wedge 2 * x \neq y \wedge t = t_0 \,\}$
zw↑ $\{\, F_7\colon Inv\binom{y+1}{y}\binom{x+1}{x} \wedge 0 \leq t\binom{y+1}{y}\binom{x+1}{x} < t_0 \,\}$
x $\leftarrow x + 1$;
zw↑ $\{\, F_6\colon Inv\binom{y+1}{y} \wedge 0 \leq t\binom{y+1}{y} < t_0 \,\}$
y $\leftarrow y + 1$
wh $\{\, F_3\colon Inv \wedge 0 \leq t < t_0 \,\}$
`end`
`end`
wh $\{\, F_4\colon Inv \wedge \neg 2 * x \neq y \,\}$
$\{\, Q\colon x = 2 * x_0 \,\}$

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

$\boldsymbol{P \supset F_5}$ $\quad x = x_0 \wedge x \geq 0 \supset Inv\binom{3x}{y}$
$x = x_0 \wedge x \geq 0 \supset 3x = 2x_0 + x \wedge 3x \geq 2x$
$x = x_0 \wedge x \geq 0 \supset x = x_0 \wedge x \geq 0$

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

$\boldsymbol{F_4 \supset Q}$ $\quad Inv \wedge \neg 2x \neq y \supset x = 2x_0$
$y = 2x_0 + x \wedge y \geq 2x \wedge 2x = y \supset x = 2x_0$

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.

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

$$Inv \wedge 2x \neq y \wedge t = t_0 \supset Inv\left[\begin{smallmatrix} y+1 \\ y \end{smallmatrix}\right]\left[\begin{smallmatrix} x+1 \\ x \end{smallmatrix}\right] \wedge 0 \leq t\left[\begin{smallmatrix} y+1 \\ y \end{smallmatrix}\right]\left[\begin{smallmatrix} x+1 \\ x \end{smallmatrix}\right] < t_0$$

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

| | |
|---|---|
| $Inv \wedge 2x \neq y \supset Inv\left[\begin{smallmatrix} y+1 \\ y \end{smallmatrix}\right]\left[\begin{smallmatrix} x+1 \\ x \end{smallmatrix}\right]$ | partielle Korrektheit |
| $Inv \wedge 2x \neq y \supset 0 \leq t\left[\begin{smallmatrix} y+1 \\ y \end{smallmatrix}\right]\left[\begin{smallmatrix} x+1 \\ x \end{smallmatrix}\right] < t$ | Termination |

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

$$\begin{aligned} Inv \wedge 2x \neq y &\supset (y = 2x_0 + x \wedge y \geq 2x)\left[\begin{smallmatrix} y+1 \\ y \end{smallmatrix}\right]\left[\begin{smallmatrix} x+1 \\ x \end{smallmatrix}\right] \\ Inv \wedge 2x \neq y &\supset (y+1 = 2x_0 + (x{+}1) \wedge (y{+}1) \geq 2(x{+}1)) \\ Inv \wedge 2x \neq y &\supset (y = 2x_0 + x \wedge y \geq 2x + 1) \\ (y = 2x_0 + x \wedge y \geq 2x \wedge 2x \neq y) &\supset (y = 2x_0 + x \wedge y > 2x) \end{aligned}$$

Offenbar gilt die Gleichung $y = 2x_0 + x$, da sie auch unter den Annahmen auftritt. Die Konklusion $y > 2x$ folgt aus den beiden Prämissen $y \geq 2x \wedge 2x \neq y$. Daher ist die Implikation eine gültige Formel.

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

$$\begin{aligned} Inv \wedge 2x \neq y &\supset 0 \leq t\left[\begin{smallmatrix} y+1 \\ y \end{smallmatrix}\right]\left[\begin{smallmatrix} x+1 \\ x \end{smallmatrix}\right] < t \\ Inv \wedge 2x \neq y &\supset 0 \leq y + 1 - 2(x+1) < t \\ y = 2x_0 + x \wedge y \geq 2x \wedge 2x \neq y &\supset 0 \leq t - 1 \wedge t - 1 < t \end{aligned}$$

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

Da alle Implikationen gültig sind, ist die Korrektheitsaussage wahr hinsichtlich totaler Korrektheit (sie ist „total korrekt“).

Alternativ kann der Korrektheitsbeweis auch als Ableitung im Hoare-Kalkül geschrieben werden. Die Abkürzungen $P$, $Q$, $F_1, \ldots, F_7$ haben dabei dieselbe Bedeutung wie im annotierten Programm weiter oben.

$$\dfrac{\dfrac{P \supset F_5 \quad \{F_5\}\, y \leftarrow 3x\, \{F_1\}}{\{P\}\, y \leftarrow 3x\, \{F_1\}}\,(\text{zw}) \quad \dfrac{\dfrac{F_2 \supset F_7 \quad \{F_7\}\, x \leftarrow x+1\, \{F_6\}}{\{F_2\}\, x \leftarrow x+1\, \{F_6\}}\,(\text{imp}) \quad \{F_6\}\, y \leftarrow y+1\, \{F_3\}}{\{F_2\}\,\texttt{begin}\ x \leftarrow x+1;\ y \leftarrow y+1\ \texttt{end}\,\{F_3\}}\,(\text{zw})}{\{F_1\}\,\texttt{while}\ 2x \neq y\ \texttt{do}\ \cdots\,\{F_4\}}\,(\text{be}) \quad \dfrac{\{F_1\}\,\texttt{while}\ 2x \neq y\ \texttt{do}\ \cdots\,\{F_4\} \quad F_4 \supset Q}{\{F_1\}\,\texttt{while}\ 2x \neq y\ \texttt{do}\ \cdots\,\{Q\}}\,(\text{imp})}{\{P\}\,\texttt{begin}\ y \leftarrow 3x;\ \texttt{while}\ 2x \neq y\ \texttt{do begin}\ x \leftarrow x+1;\ y \leftarrow y+1\ \texttt{end}\,\{Q\}}\,(\text{wh})\,(\text{be})$$