Theoretische Informatik und Logik
Übungsblatt 4 (2021W)
Lösungsvorschlag

Allgemeine Hinweise: Nummerieren Sie alle auftretenden Formeln in Tableau-Beweisen und geben Sie entsprechende Herkunftshinweise bei allen Regelanwendungen an. Außerdem sind γ- und δ-Formeln jeweils als solche zu markieren. Beachten Sie die Notationsvereinbarungen auf Folie 321.

Aufgabe 4.1

Für jede der folgenden Behauptungen: Finden Sie entweder einen Tableau-Beweis oder geben Sie ein Gegenbeispiel an.

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

b) Aus $\forall x(\exists y Q(x, y) \supset P(f(x)))$ und $\forall x f(g(x)) = x$ folgt $\exists y \exists x \neg Q(y, x) \vee P(c)$.

c) $\forall z \exists x(P(x, f(z)) \supset \forall y P(y, f(z)))$ und $\forall x f(x) = a$ folgt $\exists x P(x, a)$.

Lösung 4.1

a) Die Behauptung ist richtig, wie folgender Tableau-Beweis zeigt:

(1)	$\mathbf{t} : \forall x \neg[\neg P(f(a), x) \supset \neg\exists x \forall y P(y, x)]$	Annahme, γ-Formel
(2)	$\mathbf{t} : \neg[\neg P(f(a), a) \supset \neg\exists x \forall y P(y, x)]$	von 1
(3)	$\mathbf{f} : \neg P(f(a), a) \supset \neg\exists x \forall y P(y, x)$	von 2
(4)	$\mathbf{t} : \neg P(f(a), a)$	von 3
(5)	$\mathbf{f} : \neg\exists x \forall y P(y, x)$	von 3
(6)	$\mathbf{t} : \exists x \forall y P(y, x)$	von 5, δ-Formel
(7)	$\mathbf{t} : \forall y P(y, b)$	von 6, γ-Formel
(8)	$\mathbf{t} : \neg[\neg P(f(a), b) \supset \neg\exists x \forall y P(y, x)]$	von 1
(9)	$\mathbf{f} : \neg P(f(a), b) \supset \neg\exists x \forall y P(y, x)$	von 8
(10)	$\mathbf{t} : \neg P(f(a), b)$	von 9
(11)	$\mathbf{f} : \neg\exists x \forall y P(y, x)$	von 9
(12)	$\mathbf{f} : P(f(a), b)$	von 10
(13)	$\mathbf{t} : P(f(a), b)$	von 7
	$\times$	Widerspruch (12/13)

Beachten Sie, dass die δ-Regel jeweils nach einer neuen Konstante verlangt. Entsprechend muss die γ-Regel — nach Verwendung der δ-Regel in Zeile 7 — nochmals auf die γ-Formel in der Zeile 1 angewendet werden, um ein geschlossenes Tableau zu erhalten.

Beachten Sie auch, dass es keine Tableau-Regel gibt, die es erlauben würde den Ast (und damit, in diesem Fall, das ganze Tableau) bereits mit Verweis auf Zeilen 10 und 13 abzuschließen. Der Kalkül verlangt die explizite Elimination der Negation von Zeile 10 in Zeile 12.

b) Folgendes geschlossene Tableau zeigt die Richtigkeit der Konsequenzbehauptung:

(1)	$\mathbf{t} : \forall x(\exists y Q(x, y) \supset P(f(x)))$				Annahme – γ-Formel
(2)	$\mathbf{t} : \forall x\, f(g(x)) = x$				Annahme – γ-Formel
(3)	$\mathbf{f} : \exists y \exists x \neg Q(y, x) \vee P(c)$				Annahme [keine δ- oder γ-Formel!]
(4)	$\mathbf{t} : \exists y Q(g(c), y) \supset P(f(g(c)))$				von 1 [keine δ- oder γ-Formel!]
(5)	$\mathbf{f} : \exists y \exists x \neg Q(y, x)$				von 3 – γ-Formel
(6)	$\mathbf{f} : P(c)$				von 3
(7)	$\mathbf{f} : \exists x \neg Q(g(c), x)$				von 5 – γ-Formel
(8)	$\mathbf{f} : \neg Q(g(c), a)$				von 7
(9)	$\mathbf{t} : Q(g(c), a)$				von 8
(10)	$\mathbf{f} : \exists y Q(g(c), y)$	von 4 γ-Formel	(11)	$\mathbf{t} : P(f(g(c)))$	von 4
(12)	$\mathbf{f} : Q(g(c), a)$	von 10	(13)	$\mathbf{t} : f(g(c)) = c$	von 2
	$\times$	Wid.: 9/12	(14)	$\mathbf{t} : P(c)$	$S^{=}$: 13→11
				$\times$	Wid.: 6/14

Anmerkung: Um einen kompakten Tableau-Beweis zu erhalten wurde in Zeile 4 — mit Blick auf die Zeilen 2 und 3 — der Term $g(c)$ für die Anwendung der γ-Regel auf 1 gewählt.

c) Die Konsequenzbehauptung ist falsch wie, z.B., folgendes ein-elementige Gegenbeispiel $\mathcal{I} = \langle\{0\}, \Phi, \xi\rangle$ zeigt:
$\Phi(P)(0,0) = \mathbf{f}$; $\Phi(a) = 0$; $\Phi(f)(0) = 0$; ξ ist irrelevant.
Es ist leicht zu sehen, dass die beiden Prämissen $\forall z \exists x(P(x, f(z)) \supset \forall y P(y, f(z)))$ und $\forall x f(x) = a$ unter $\mathcal{I}$ wahr sind, während die Konklusion $\exists x P(x, a)$ falsch ist.

Aufgabe 4.2

Sind folgende Konsequenzbehauptungen richtig? Im positiven Fall ist ein Tableau-Beweis anzugeben, im negativen Fall ein vollständig spezifiziertes Gegenbeispiel. (Siehe Folie 409 für entsprechende PL-Formeln.)

a) Jede serielle und transitive Relation ist schwach gerichtet.

b) Jede symmetrische Relation ist schwach gerichtet.

Lösung 4.2

a) Die Aussage ist falsch, wie folgendes Gegenbeispiel $\mathcal{I} = \langle\{0, 1, 2\}, \Phi, \xi\rangle$ zeigt:
$\Phi(R)(m, n) = \mathbf{t} \iff m = 0$ oder $m = n$; ξ ist irrelevant.
Es ist leicht zu sehen, dass folgende Formeln unter $\mathcal{I}$ wahr sind:
$\forall x \exists y R(x, y)$ (Serialität)
$\forall x \forall y \forall z[R(x, y) \wedge R(y, z) \supset R(x, z)]$ (Transitivität)
Hingegen ist folgende Formel falsch unter der Interpretation $\mathcal{I}$:
$\forall x \forall y \forall z[(R(x, y) \wedge R(x, z)) \supset \exists u(R(y, u) \wedge R(z, u))]$ (Schwache Gerichtetheit)
Für letztere Behauptung beobachten wir, dass $\Phi(R)(0, 1)$ und $\Phi(R)(0, 2)$ gilt, aber kein n existiert, sodass sowohl $\Phi(R)(1, n)$ als auch $\Phi(R)(2, n)$ wahr wären.
Damit ist gezeigt, dass $\mathcal{I}$ ein Gegenbeispiel zur Behauptung ist, dass jede serielle und transitive Relation schwach gerichtet ist.

b) Folgendes Tableau beweist die Behauptung:

(1)	$\mathbf{t} : \forall x \forall y[(R(x, y) \supset R(y, x)]$	symmetrisch (γ-Formel)
(2)	$\mathbf{f} : \forall x \forall y \forall z[(R(x, y) \wedge R(x, z)) \supset \exists u(R(y, u) \wedge R(z, u))]$	schwache gerichtet (δ-F.)
(3)	$\mathbf{f} : \forall y \forall z[(R(a, y) \wedge R(a, z)) \supset \exists u(R(y, u) \wedge R(z, u))]$	von 2 (δ-Formel)
(4)	$\mathbf{f} : \forall z[(R(a, b) \wedge R(a, z)) \supset \exists u(R(b, u) \wedge R(z, u))]$	von 3 (δ-Formel)
(5)	$\mathbf{f} : (R(a, b) \wedge R(a, c)) \supset \exists u(R(b, u) \wedge R(c, u))]$	von 4
(6)	$\mathbf{t} : R(a, b) \wedge R(a, c)$	von 5
(7)	$\mathbf{f} : \exists u(R(b, u) \wedge R(c, u))$	von 5 (γ-Formel)
(8)	$\mathbf{t} : R(a, b)$	von 6
(9)	$\mathbf{t} : R(a, c)$	von 6
(10)	$\mathbf{f} : R(b, a) \wedge R(c, a)$	von 7
(11)	$\mathbf{t} : \forall y[(R(a, y) \supset R(y, a)]$	von 1 (γ-Formel)
(12)	$\mathbf{t} : R(a, b) \supset R(b, a)$	von 11
(13)	$\mathbf{t} : R(a, c) \supset R(c, a)$	von 11
(14)	$\mathbf{f} : R(a, b)$ v. 12 $\times$ (8/14) | (15) $\mathbf{t} : R(b, a)$	von 12
	(16) $\mathbf{f} : R(a, c)$ von 13 $\times$ (9/16) | (17) $\mathbf{t} : R(c, a)$	von 13
	(18) $\mathbf{f} : R(b, a)$ v. 10 $\times$(15/18) | (19) $\mathbf{t} : R(c, a)$ $\times$(17/19)	von 10

Aufgabe 4.3

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: $\forall x \forall y f(x, y) \neq \bullet$
A2: $\forall x \forall y \forall z g(x, y, z) \neq \bullet$
A3: $\forall x \forall y \forall u \forall v \forall w f(x, y) \neq g(u, v, w)$
A4: $\forall x[x = \bullet \vee (\exists y \exists z f(y, z) = x \vee \exists u \exists v \exists w g(u, v, w) = x)]$

a) Zeigen Sie, dass $\mathcal{B} = \{A1, A2, A3, A4\}$ keine vollständige Axiomatisierung der Theorie $Th(\mathbb{B})$ ist, indem Sie ein Modell von $\mathcal{B}$ angeben, dessen Gegenstandsbereich aus nur endlich vielen Elementen besteht (während es natürlich unendlich viele verschiedene 2-3-Bäume gibt).

b) Geben Sie eine Formel F über der Signatur $\Sigma_{\mathbb{B}}$ an, die nicht logisch aus $\mathcal{B}$ folgt, obwohl sie über dem Datentyp $\mathbb{B}$ gültig ist. Begründen Sie Ihre Behauptung durch Angabe eines Gegenbeispiels zur Konsequenzbehauptung $\mathcal{B} \models F$.

c) Zeigen Sie mit dem Tableau-Kalkül, dass $\forall x \forall y \exists z (f(x, y) \neq f(y, x) \wedge x = f(z, z) \supset y \neq f(z, z))$ logisch gültig ist (und daher keine spezifischen Annahmen aus $Th(\mathbb{B})$ für den Beweis benötigt).

Lösung 4.3

a) $\mathcal{B} = \{A1, A2, A3, A4\}$ hat folgendes 3-elementige Model $\mathcal{I} = \langle \{0, 1, 2\}, \Phi, \xi \rangle$:
$\Phi(\bullet) = 0$; $\Phi(f)(u, v) = 1$ und $\Phi(g)(u, v, w) = 2$ für alle $u, v, w \in \{0, 1, 2\}$; ξ ist irrelevant.
Die Formeln $A1, A2, A3$ und $A4$ sind alle wahr unter der Interpretation $\mathcal{I}$. Wie bereits in der Aufgabenstellung erwähnt, hat das intendierte Model von $Th(\mathbb{B})$ — also das Modell, dass dem Datentyp $\mathbb{B}$ entspricht — sämtliche (unendlich viele) 2-3-Bäume als Gegenstandsbereich. In diesem intendierten Model sind die Formeln $A1, A2, A3$ und $A4$ ebenfalls wahr. Allerdings zeigt $\mathcal{I}$, dass nicht alle Formeln in $Th(\mathbb{B})$ bereits aus $\mathcal{B}$ logisch folgen. Mit anderen Worten: $\mathcal{B}$ ist keine vollständige Axiomatisierung von $Th(\mathbb{B})$.

b) Es gibt unendlich viele verschiedene Formeln F, die nicht aus $\mathcal{B}$ folgen, aber in $Th(\mathbb{B})$ liegen, also über dem Datentyp $\mathbb{B}$ gültig sind. Für ein konkretes Beispiel können wir die Lösung der Teilaufgabe a) nützen und $F = \exists x \exists y \exists z \exists u (x \neq y \wedge x \neq z \wedge x \neq u \wedge y \neq z \wedge y \neq u \wedge z \neq u)$ setzen.
Die Interpretation $\mathcal{I}$ aus a) ist ein Gegenbeispiel zur Konsequenzbehauptung $A1, A2, A3, A4 \models F$.
Andere mögliche Wahlen für F sind beispielsweise $\exists x \exists y f(x, y) \neq f(y, x)$, $f(\bullet, f(\bullet, \bullet)) \neq f(\bullet, \bullet)$, oder $\forall x \exists y\, g(x, x, y) \neq g(y, x, x)$. Auch diese Formeln sind jeweils gültig in $\mathbb{B}$, aber falsch unter $\mathcal{I}$.

c) Folgendes geschlossenes Tableau zeigt die Gültigkeit von $\forall x \forall y \exists z (f(x, y) \neq f(y, x) \wedge x = f(z, z) \supset y \neq f(z, z))$. (Beachten Sie, dass in der Formel von folgender Klammereinsparungsregel Gebrauch gemacht wird: Konjunktion bindet stärker als Implikation.)

(1)	$\mathbf{f} : \forall x \forall y \exists z (f(x, y) \neq f(y, x) \wedge x = f(z, z) \supset y \neq f(z, z))$	Annahme, δ-Formel
(2)	$\mathbf{f} : \forall y \exists z (f(a, y) \neq f(y, a) \wedge a = f(z, z) \supset y \neq f(z, z))$	von 1, δ-Formel
(3)	$\mathbf{f} : \exists z (f(a, b) \neq f(b, a) \wedge a = f(z, z) \supset b \neq f(z, z))$	von 2, γ-Formel
(4)	$\mathbf{f} : f(a, b) \neq f(b, a) \wedge a = f(c, c) \supset b \neq f(c, c)$	von 3
(5)	$\mathbf{t} : f(a, b) \neq f(b, a) \wedge a = f(c, c)$	von 4
(6)	$\mathbf{f} : b \neq f(c, c)$	von 4
(7)	$\mathbf{t} : f(a, b) \neq f(b, a)$	von 5
(8)	$\mathbf{t} : a = f(c, c)$	von 5
(9)	$\mathbf{t} : b = f(c, c)$	von 6
(10)	$\mathbf{f} : f(a, b) = f(b, a)$	von 7
(11)	$\mathbf{f} : f(f(c, c), b) = f(b, a)$	$S^{=}$: 8→10
(12)	$\mathbf{f} : f(f(c, c), b) = f(b, f(c, c))$	$S^{=}$: 8→11
(13)	$\mathbf{f} : f(f(c, c), f(c, c)) = f(b, f(c, c))$	$S^{=}$: 9→12
(14)	$\mathbf{f} : f(f(c, c), f(c, c)) = f(f(c, c), f(c, c))$ $\times$ $(AB^{=})$	$S^{=}$: 9→13

Anmerkungen:
Bei der Anwendung der γ-Regel auf 3, könnte man in Zeile 4 auch einen anderen geschlossenen Term aus Σ^{par}, anstatt des neuen Konstantensymbols c, wählen (z.B. die bereits verwendeten Konstanten a oder b.) Das würde aber nichts an der Struktur des Beweises ändern.

Beachten Sie, dass Anwendungen der Gleichheitsregeln (Substitutionsregeln für Gleichheitsatome) jeweils nur *ein* Vorkommen eines Terms durch einen anderen ersetzen. Es gibt in unserem Tableau-Kalkül keine Regel mit der man, z.B., beide Vorkommen von a in 10 simultan durch $f(c, c)$ ersetzen könnte. Außerdem können die Gleichheitsregeln nur auf Atomformeln angewendet werden und nicht, z.B., bereits auf die negierte Formel in Zeile 7.

Aufgabe 4.4

Sind die folgenden Korrektheitsaussagen wahr oder falsch hinsichtlich partieller bzw. totaler Korrektheit? Argumentieren Sie informell mit Hilfe der Definition der Semantik von Korrektheitsaussagen. Es ist keine Ableitung im Hoare-Kalkül notwendig.

a) $\{x = x\}\ x \leftarrow 2x\ \{x = 2x\}$

b) $\{y = z\}$ `begin` $x \leftarrow 2y;\ x \leftarrow 2x$ `end` $\{x = 4z\}$

c) $\{x = 0\}$ `if` $x > y$ `then` $x \leftarrow x - y$ `else` $x \leftarrow y - x\ \{x > 0\}$

d) $\{x = y\}$ `while` $y > 0$ `do` $y \leftarrow x\ \{x \leq 0\}$

e) $\{x = y\}$ `while` $y > 0$ `do` $y \leftarrow x\ \{x < 0\}$

Lösung 4.4

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

Gegenbeispiel: Eine Wertebelegung I mit $I(x) = 1$. Es gilt:

- Die Wertebelegung erfüllt die Vorbedingung: $\mathcal{M}(I, x = x) = (I(x) = I(x)) = (1 = 1) = \text{true}$
- Berechnung des Ergebnisses: $\mathcal{M}(I, x \leftarrow 2x) = I'$, wobei $I'(x) = 2 \cdot 1 = 2$ und $I' \overset{x}{\sim} I$
- Das Ergebnis I' erfüllt die Nachbedingung nicht: $\mathcal{M}(I', x = 2x) = (I'(x) = 2 \cdot I'(x)) = (2 = 4) = \text{false}$

b) 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 $x \leftarrow 2y$ in I auszuwerten ist. Wir erhalten $I' = \mathcal{M}(I, x \leftarrow 2y)$, wobei $I'(x) = 2I(y)$, $I'(y) = I(y)$ und $I'(z) = I(z)$.

  Im nächsten Schritt muss die zweite Anweisung in der Wertebelegung I' ausgewertet werden. Wir erhalten $I'' = \mathcal{M}(I', x \leftarrow 2x)$, wobei $I''(x) = 2 \cdot I'(x) = 4I(y)$, $I''(y) = I'(y) = I(y)$ und $I''(z) = I'(z) = I(z)$.
- Die Auswertung der Nachbedingung $x = 4z$ in I'' ergibt:

$$\mathcal{M}(I'', x = 4z) = (I''(x) = 4I''(z)) = (4I(y) = 4I(z))$$

  Da wegen der Vorbedingung $I(y) = I(z)$ gilt, evaluiert $4I(y) = 4I(z)$ 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.[1]

$$\dfrac{\dfrac{(1)}{y = z \supset x = 4z[^{2x}_{x}][^{2y}_{x}]}{\{y = z\}\, x \leftarrow 2y\, \{x = 4z[^{2x}_{x}]\}} \quad \dfrac{(2)}{x = 4z[^{2x}_{x}] \supset x = 4z[^{2x}_{x}]}{\{x = 4z[^{2x}_{x}]\}\, x \leftarrow 2x\, \{x = 4z\}}}{\{y = z\}\, \texttt{begin}\ x \leftarrow 2y;\ x \leftarrow 2x\ \texttt{end}\, \{x = 4z\}}$$

[1] Die Umkehrung gilt übrigens nicht: Im Allgemeinen folgt aus der Tatsache, dass wir keine Ableitung der Korrektheitsaussage im Hoare-Kalkül finden können, nicht, dass die Aussage falsch ist. Um zu zeigen, dass sie das ist, müssen wir ein Gegenbeispiel angeben.

Formel (2) ist eine Tautologie der Form $A \supset A$. Für Formel (1) erhalten wir:

$$y = z \supset x = 4z\tbinom{2x}{x}\tbinom{2y}{x}$$
$$y = z \supset 2x = 4z\tbinom{2y}{x}$$
$$y = z \supset 2(2y) = 4z$$

Diese Formel ist gültig in $\mathbb{Z}$. Die Korrektheitsaussage der Angabe lässt sich also aus zwei gültigen Formeln durch zweimalige Anwendung der Regel (zw) und einmalige Anwendung von (be) ableiten. Aus der Korrektheit des Hoare-Kalküls folgt, dass die Korrektheitsaussage wahr ist.

c) Die Korrektheitsaussage ist weder partiell noch total korrekt.

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

- Die Wertebelegung I erfüllt die Vorbedingung: $\mathcal{M}(I, x = 0) = (I(x) = 0) = (0 = 0) = \text{true}$
- Berechnung des Ergebnisses:

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

- Das Ergebnis erfüllt nicht die Nachbedingung:

$$\mathcal{M}(I', x > 0) = (I'(x) > 0) = (0 > 0) = \text{false}$$

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 $I(x) = I(y)$ gilt. Wir unterscheiden zwei Fälle.

$I(y) > 0$: Die Schleife wird ausgeführt. Da x denselben Wert wie y besitzt, ändert sich $I(y)$ durch die Zuweisung $y \leftarrow x$ nicht. Somit terminiert die Schleife nicht.

$I(y) \leq 0$: Die Schleifenbedingung ist nicht erfüllt, daher wird die Schleife nicht ausgeführt und das Programm endet mit dem Ergebnis I. Da $I(x) = I(y)$ und $I(y) \leq 0$ gilt, erhalten wir $\mathcal{M}(I, x \leq 0) = \text{true}$, die Nachbedingung ist erfüllt.

Somit 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 $I(x) = I(y) = 1$. 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 Wertebelegung I mit $I(x) = I(y) = 0$. Sie erfüllt die Vorbedingung $x = y$. Da die Schleifenbedigung $y > 0$ nicht zutrifft, terminiert das Programm mit der unveränderten Wertebelegung. I erfüllt aber offenbar nicht die Nachbedingung $x < 0$.

Aufgabe 4.5

Zeigen Sie mit Hilfe des Hoare-Kalküls, dass die folgende Korrektheitsaussage wahr hinsichtlich totaler Korrektheit („total korrekt“) ist. Verwenden Sie die Formel $\boldsymbol{b = 2^{a+1} \wedge 0 < b \leq 2n}$ als Invariante und den Ausdruck $\boldsymbol{n - b}$ als Variante. Welche Funktion berechnet das Programm, wenn man a als das Ergebnis des Programms betrachtet?

$\{n \geq 1\}$
```
begin
  begin
    a ← 0;
    b ← 2
  end;
```

```
  while b ≤ n do
    begin
      a ← a + 1;
      b ← b + b
    end
end
```
$\{2^a \le n < 2^{a+1}\}$

Lösung 4.5

Wir beginnen damit, das Programm entsprechend der Regeln des Hoare-Kalküls zu annotieren. Wir nummerieren die Formeln in der Reihenfolge des Hinzufügens. Die vorgeschlagene Reihenfolge ist nur eine von mehreren Möglichkeiten. *Inv* steht für die Invariante $b = 2^{a+1} \wedge 0 < b \le 2n$ und t für die Variante $n - b$.

$\{Pre\colon n \ge 1\}$
$\{F_6\colon Inv[^2_b][^0_a]\}$
```
begin
  begin
    a ← 0;
```
$\{F_5\colon Inv[^2_b]\}$
```
    b ← 2
  end;
```
$\{F_1\colon Inv\}$
```
  while b ≤ n do
```
$\{F_2\colon Inv \wedge b \le n \wedge t = t_0\}$
```
    begin
```
$\{F_8\colon (Inv \wedge (b \le n \supset 0 \le t < t_0))[^{b+b}_{b}][^{a+1}_{a}]\}$
```
      a ← a + 1;
```
$\{F_7\colon (Inv \wedge (b \le n \supset 0 \le t < t_0))[^{b+b}_{b}]\}$
```
      b ← b + b
    end
```
$\{F_3\colon Inv \wedge (b \le n \supset 0 \le t < t_0)\}$
```
end
```
$\{F_4\colon Inv \wedge b > n\}$
$\{Post\colon 2^a \le n < 2^{a+1}\}$

Wir müssen nun noch die Gültigkeit der Formeln $Pre \supset F_6$, $F_4 \supset Post$ und $F_2 \supset F_8$ argumentieren.

$Pre \supset F_6$:

$$\begin{aligned} & n \ge 1 \supset Inv[^2_b][^0_a] \\ & n \ge 1 \supset (b = 2^{a+1} \wedge 0 < b \le 2n)[^2_b][^0_a] \\ & n \ge 1 \supset (2 = 2^{a+1} \wedge 0 < 2 \le 2n)[^0_a] \\ & n \ge 1 \supset 2 = 2^{0+1} \wedge 0 < 2 \le 2n \end{aligned}$$

Diese Implikation ist gültig, da die Teilformeln $2 = 2^1$ und $0 < 2$ immer wahr sind und $2 \le 2n$ für $n \ge 1$ (Prämisse) gilt.

$F_4 \supset Post$:

$$\begin{aligned} Inv \wedge b > n &\supset 2^a \le n < 2^{a+1} \\ b = 2^{a+1} \wedge 0 < b \le 2n \wedge b > n &\supset 2^a \le n < 2^{a+1} \\ b = 2^{a+1} \wedge 0 < 2^{a+1} \le 2n \wedge 2^{a+1} > n &\supset 2^a \le n < 2^{a+1} \\ b = 2^{a+1} \wedge 0 < 2^a \le n \wedge 2^{a+1} > n &\supset 2^a \le n < 2^{a+1} \\ b = 2^{a+1} \wedge 0 < 2^a \le n < 2^{a+1} &\supset 2^a \le n < 2^{a+1} \end{aligned}$$

Die Implikation in der letzten Zeile ist eine Tautologie der Form $A \wedge B \supset B$.

$F_2 \supset F_8$: Wir teilen den Beweis dieser Implikation in jenen für die partielle Korrektheit und jenen für die Termination.

Partielle Korrektheit:

$$
\begin{aligned}
& Inv \wedge b \leq n \supset Inv[{}^{b+b}_{b}][{}^{a+1}_{a}] \\
& b = 2^{a+1} \wedge 0 < b \leq 2n \wedge b \leq n \supset (b = 2^{a+1} \wedge 0 < b \leq 2n)[{}^{b+b}_{b}][{}^{a+1}_{a}] \\
& b = 2^{a+1} \wedge 0 < b \leq 2n \wedge b \leq n \supset (b + b = 2^{a+1} \wedge 0 < b + b \leq 2n)[{}^{a+1}_{a}] \\
& b = 2^{a+1} \wedge 0 < b \leq 2n \wedge b \leq n \supset b + b = 2^{a+1+1} \wedge 0 < 2b \leq 2n \\
& b = 2^{a+1} \wedge 0 < b \leq 2n \wedge b \leq n \supset b = 2^{a+1} \wedge 0 < b \leq n
\end{aligned}
$$

Die Implikation in der letzten Zeile ist eine Tautologie der Form $A \wedge B \supset A$.

Termination:

$$
\begin{aligned}
& Inv \wedge b \leq n \wedge n - b = t_0 \supset (b \leq n \supset 0 \leq n - b < t_0)[{}^{b+b}_{b}][{}^{a+1}_{a}] \\
& Inv \wedge b \leq n \wedge n - b = t_0 \supset (2b \leq n \supset 0 \leq n - 2b < t_0) \\
& \quad Inv \wedge b \leq n \wedge 2b \leq n \supset 0 \leq n - 2b < n - b
\end{aligned}
$$

Die Konklusion $0 \leq n - 2b$ folgt aus der Prämisse $2b \leq n$. Die Konklusion $n - 2b < n - b$ lässt sich zur Bedingung $b > 0$ vereinfachen, die Teil der Invariante auf der linken Seite ist.

Welche Funktion berechnet das Programm? Zur Beantwortung dieser Frage reicht es, die Nachbedingung so umzuformen, dass wir das Ergebnis a als Funktion der anderen Variablen erhalten.

$2^a \leq n < 2^{a+1}$	Anwenden des 2er Logarithmus
$\mathrm{ld}(2^a) \leq \mathrm{ld}(n) < \mathrm{ld}(2^{a+1})$	
$a \cdot \mathrm{ld}(2) \leq \mathrm{ld}(n) < (a+1) \cdot \mathrm{ld}(2)$	
$a \cdot 1 \leq \mathrm{ld}(n) < (a+1) \cdot 1$	
$a \leq \mathrm{ld}(n) < a + 1$	Definition der Floor-Funktion
$a = \lfloor \mathrm{ld}(n) \rfloor$	

Das Programm berechnet also den ganzzahligen Teil des Zweier-Logarithmus der Eingabe n.

Anmerkung: Durch das Anwenden des Logarithmus auf die Ungleichungskette bleiben die Ungleichheiten erhalten, da der Logarithmus eine monotone Funktion ist.