Grundbegriffe der Informatik — Aufgabenblatt 9
Lösungsvorschläge

Matr.nr.:							

Nachname:

Vorname:

Tutorium Nr.: Tutor*in:

Ausgabe: Freitag, 13.01.2023, 14:30 Uhr

Abgabe: Freitag, 20.01.2023, 12:30 Uhr
Online, oder in einem Briefkasten mit der Aufschrift GBI im UG des Info-Gebäudes (50.34)

Lösungen werden nur korrigiert, wenn sie
- handschriftlich erstellt sind (Tablet-Ausdruck erlaubt) und
- mit dieser Seite als Deckblatt
- in der oberen **linken** Ecke zusammengeheftet

rechtzeitig abgegeben werden.

Abgaberegeln für Teilnehmer der Tutorien mit Online-Abgabe:
- handschriftlich erstellt (Scans und lesbare Fotos akzeptiert)
- **rechtzeitig**, mit diesem Deckblatt in **genau einer** PDF-Datei
- in ILIAS unter "Tutorien" im Ordner des richtigen Tutoriums abgeben.

---

*Von Tutor*in auszufüllen:*

erreichte Punkte

Blatt 9:	/ 22
Blätter 7 – 9:	/ 61 (+4)
Blätter 1 – 9:	/ 185 (+4)

Aufgabe 9.1 (1 + 1 + 1,5 + 2,5 = 6 Punkte)

Sei $\mathtt{P}$ ein zweistelliges[1] und $\mathtt{Q}$ ein einstelliges Relationssymbol, $\mathtt{c}$ ein Konstantensymbol sowie $\mathtt{f}$ ein einstelliges Funktionssymbol. Eine geschlossene Formel F heißt *erfüllbar*, wenn sie ein Modell besitzt. In der Vorlesung am Rande erwähnt: $\mathtt{TRUE}$ ist die Formel, die immer wahr ist, und als Abkürzung für $\mathtt{x} \doteq \mathtt{x}$ steht.

a) $(\forall \mathtt{x}\ \mathtt{f(x,\ f(x))}) \rightarrow (\forall \mathtt{x} \exists \mathtt{y}\ \mathtt{f(x,\ y)})$

b) $(\mathtt{Q(c)} \rightarrow \mathtt{TRUE}) \vee (\mathtt{TRUE} \rightarrow \mathtt{Q(c)})$

c) $(\forall \mathtt{x} \forall \mathtt{y}\ (\mathtt{f(x)} \doteq \mathtt{f(y)} \rightarrow \mathtt{x} \doteq \mathtt{y})) \rightarrow \exists \mathtt{x}\ \mathtt{f(x)} \doteq \mathtt{x}$

d) $(\exists \mathtt{x} \forall \mathtt{y}\ \mathtt{P(f(x),\ y)}) \rightarrow (\exists \mathtt{x} \forall \mathtt{y}\ \mathtt{P(x,\ f(y))})$

Geben Sie für jede dieser vier Formeln an, ob sie entweder

(i) keine Formel der Prädikatenlogik erster Stufe *oder*
(ii) allgemeingültig *oder*
(iii) erfüllbar, aber nicht allgemeingültig *oder*
(iv) unerfüllbar (also nicht erfüllbar)

ist. Falls eine Formel F erfüllbar, aber nicht allgemeingültig ist, geben Sie ein Modell für F und ein Modell für $\neg F$ an. Geben Sie auch in den anderen Fällen eine Begründung für Ihre Zuordnung an.

Lösung 9.1

a) Dies ist keine Formel der der Prädikatenlogik (1. $\mathtt{f}$ ist einstellig, wird aber sowohl mit einem als auch mit zwei Argumenten verwendet. 2. Mit einem Funktionszeichen ($\mathtt{f}$) kann keine atomare Formel gebildet werden, sondern ein Term.)

b) Dies ist eine Tautologie, da die aussagenlogische Struktur $(\mathtt{Q} \rightarrow \mathtt{TRUE}) \vee (\mathtt{TRUE} \rightarrow \mathtt{Q})$ bereits allgemeingültig in Aussagenlogik ist.

c) Diese Formel besagt, dass wenn $I(\mathtt{f})$ eine injektive Funktion ist, sie auch einen Fixpunkt haben muss. Es gibt Funktionen, die das erfüllen, aber es gilt nicht für alle Funktionen.
Modell für F: $D = \{a\}, I(\mathtt{f}) = I_{\{a\}}$. Mit beliebiger Variablenbelegung β beliebig macht sie F wahr ($val_{D,I,\beta} = \mathbf{w}$).
Modell, für $\neg F$, also eine Interpretation, die F nicht zu wahr auswertet: $D' = \{a, b\}, I'(\mathtt{f})(a) = b, I'(\mathtt{f})(b) = a$. Mit beliebiger Variablenbelegung β gilt $val_{D,I,\beta}(F) = \mathbf{f}$.

d) Diese Formel ist allgemeingültig.
Wegen der Semantik der Implikation genügt es zu zeigen, dass jedes Modell von $A = (\exists \mathtt{x} \forall \mathtt{y}\ \mathtt{P(f(x),\ y)})$ auch Modell von $B = (\exists \mathtt{x} \forall \mathtt{y}\ \mathtt{P(x,\ f(y))})$ ist.
Sei also (D, I) ein beliebiges Modell von A.

$$
\begin{aligned}
& val_{D,I,\beta}(A) = \mathbf{w} \\
\iff & \text{Es gibt ein } d \in D, \text{ so dass für alle } e \in D \text{ gilt: } val_{D,I,(\beta^d_x)^e_y}(\mathtt{P(f(x),\ y)}) = \mathbf{w} \\
\iff & \text{Es gibt ein } d \in D, \text{ so dass für alle } e \in D \text{ gilt: } (I(\mathtt{f})(d), e) \in I(\mathtt{P}) \\
\implies & \text{Es gibt ein } d' \in D, \text{ so dass für alle } e \in D \text{ gilt: } (d', e) \in I(\mathtt{P}) \qquad (1)
\end{aligned}
$$

[1] Dies bezieht sich auf den Wert der Stelligkeitsunktion ar. Also $\mathrm{ar}(\mathtt{P}) = 2$ und $\mathrm{ar}(\mathtt{Q}) = \mathrm{ar}(\mathtt{f}) = 1$.

Der letzte Schritt ist nicht unbedingt notwendig, aber genügt, um das Folgende zu zeigen, und macht es lesbarer: Für die Relation $I(\texttt{P}) \in D \times D$ gibt es ein Argument $d' \in D$, das mit allen Elementen $e \in D$ in Relation steht. Und genau dieses Element d' können wir nutzen, um zu zeigen, dass (D, I) auch Modell von B ist. Dazu stellen wir fest:

$$
\begin{aligned}
& val_{D,I,\beta}(B) = \mathbf{w} \\
\iff & \text{Es gibt ein } r \in D, \text{ so dass für alle } s \in D \text{ gilt: } val_{D,I,(\beta^r_x)^s_y}(\texttt{P(x, f(y))}) = \mathbf{w} \\
\iff & \text{Es gibt ein } r \in D, \text{ so dass für alle } s \in D \text{ gilt: } (r, I(\texttt{f})(s)) \in I(\texttt{P}) \qquad (2)
\end{aligned}
$$

Wenn man das betrachtet, stellt man leicht fest, dass (2) eine Folgerung aus (1) ist. Dazu wählt man für r das Element d'. Und für einen beliebigen Wert von s kann man für $e = I(\texttt{f})(s)$ wählen, und (2) ist erfüllt.

Aufgabe 9.2 (1 + 1 + 1 + 2 = 5 Punkte)
In dieser Aufgabe wollen wir den folgenden Satz

Wenn jeder arme Mensch einen reichen Vater hat, dann gibt es einen reichen Menschen, der einen reichen Großvater hat. $(*)$

untersuchen. Dazu wollen wir ihn in Prädikatenlogik formalisieren.

a) Geben Sie eine Signatur (d.h. die Mengen $Var_{PL}, Const_{PL}, Fun_{PL}$ und Rel_{PL}) an, die für die Formalisierung von $(*)$ geeignet ist, d.h. die dort auftrenden Konzepte als geeignete Symbole bereitstellt.

b) Geben Sie eine prädikatenlogische Formel B über der Signatur aus a) an, die die Aussage trifft, dass jeder Mensch entweder reich oder arm ist.

c) Geben Sie eine prädikatenlogische Formel C über der Signatur von a) an, die die Aussage $(*)$ ausdrückt (unter der Annahme, dass Formel B gelte).

d) Ist diese Formel C

- unerfüllbar,
- erfüllbar aber nicht allgemeingültig *oder*
- allgemeingültig?

(wieder unter der Annahme, dass Formel B gelte). Begründen Sie Ihre Entscheidung!

Lösung 9.2
Hinweis: In der Vorlesung haben wir immer Bezeichner verwendet, die nur genau einen Buchstaben lang sind. Der Lesbarkeit halber benutzen wir hier einmal längere Bezeichner.

a) $Var_{PL} = \{\texttt{x}\}, Const_{PL} = \emptyset, Fun_{PL} = \{\texttt{vater}\}, Rel_{PL} = \{\texttt{Reich}, \texttt{Arm}\}$ mit $\text{ar}(\texttt{vater}) = 1$ und $\text{ar}(\texttt{Reich}) = 1, \text{ar}(\texttt{Arm}) = 1$.

b) $\forall \texttt{x}\,((\texttt{Reich(x)} \rightarrow \neg\,\texttt{Arm(x)}) \wedge (\neg\,\texttt{Arm(x)} \rightarrow \texttt{Reich(x)}))$

c) $\forall \texttt{x}\,(\texttt{Arm(x)} \rightarrow \texttt{Reich(vater(x))}) \rightarrow \exists \texttt{x}\,(\texttt{Reich(x)} \wedge \texttt{Reich(vater(vater(x)))})$

d) Die Aussage ist allgemeingültig.

Wir müssen die Aussage für beliebige Interpretationen (D, I, β) zeigen. Nehmen wir also einen beliebigen Menschen $m \in D$ heraus.
Es gelte also die Prämisse

$$val_{D,I,\beta}(\forall x\,(\texttt{Arm(x)} \rightarrow \texttt{Reich(vater(x))})) = \mathbf{w}\ . \tag{3}$$

Wir untersuchen nun die beiden Fälle $m \in I(\texttt{arm})$ und $m \in I(\texttt{reich})$, von denen nach b) genauer einer gelten muss.

Fall 1, $m \in I(\texttt{reich})$**:** Wir machen eine weitere Fallunterscheidung über m's Großvater:

- **Fall 1.1,** $I(\texttt{Vater})(I(\texttt{Vater})(m)) \in I(\texttt{reich})$**:** Das ist der einfache Fall: m ist ein Zeuge für den gesuchten Existenzquantor, d.h., wenn man diesen Wert an die Variable x zuweist (β^m_x), wird die quantifizierte Aussage wahr. m ist reich und hat einen einen reichen Grovater.
- **Fall 1.2,** $I(\texttt{Vater})(I(\texttt{Vater})(m)) \in I(\texttt{arm})$**:** Hier können wir zwei Beobachtungen machen: 1) Nach der Prämisse (3) muss dann m's Urgroßvater reich sein. 2) Wenn m's Vater arm wäre, dann müsste der Großvater nach (3) reich sein. Also gilt $I(\texttt{Vater})(m) \in I(\texttt{reich})$. Nun ist m's Vater ein reicher Mensch, dessen Großvater (m's Urgroßvater) auch reich ist.

Fall 2, $m \in I(\texttt{arm})$**:** Nach (3) ist $I(\texttt{Vater})(m) \in I(\texttt{reich})$. Der Rest des Arguments folgt analog wie in Fall 1, wenn man m's Vater $I(\texttt{Vater})(m)$ statt m betrachtet.

Aufgabe 9.3 (1 + 3 + 1 = 5 Punkte)

a) Gegeben sind die beiden Formeln

$$F_1 = \texttt{P(x, f(x))} \qquad \text{und} \qquad F_2 = \texttt{P(f(y), f(f(a)))}\ .$$

Geben Sie eine Substitution σ an, so dass $\sigma(F_1) = \sigma(F_2)$ gilt, d.h., dass nach die Resultate nach der Anwendung der Substitution auf beiden Formeln die (syntaktisch) selbe Formel liefern. Eine solche Substitution nennt man *Unifikator* von F_1 und F_2.

b) Gegeben ist die Formel $G = \exists x\ \texttt{P(x, y)}$. Für eine Formel F bezeichne $M(F)$ die Menge aller Modelle von F.
Geben Sie zwei Subsitutionen σ^+ und σ^- an, so dass

$$M(\sigma^-(G)) \not\subseteq M(G) \quad \text{und} \quad M(G) \subsetneq M(\sigma^+(G)) \tag{4}$$

gilt. (Beachten Sie, dass wir hier nach *echten* Teilmengen suchen!)
Hinweis: Sie dürfen annehmen, dass die Signatur weitere Funktions- und Konstantensymbole enthält.
Nachtrag: Eine der beiden Substitutionen (nennen wir sie $\sigma^?$) hat einen Nachteil: Wir beobachten, dass das Ergebnis $\sigma^?(G)$ keine logische Folgerung von G mehr ist wegen (4). Da man möchte, dass das Einsetzen von Termen für freie Variablen die Gültigkeit einer Aussage nicht zerstört, muss man die Menge der hier zugelassenen Substitutionen einschränken.

c) Betrachten Sie für diese Teilaufgabe die folgende prädikatenlogische Formel:

$$H = \forall y\,(\texttt{R(x, y)} \wedge \texttt{R(y, x)} \rightarrow \texttt{x} \doteq \texttt{y}) \wedge (\texttt{f(x, y)} \doteq \texttt{x} \rightarrow \texttt{f(y, x)} \doteq \texttt{y})$$

Geben Sie den Wahrheitswert $val_{D,I,\beta}(H)$ für die Formel H bezgl. der folgenden Interpretation und Variablenbelegung an:

$$\begin{aligned} D &= \mathbb{Z}, \\ I(\texttt{R}) &= \leq, \\ I(\texttt{f}) &: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (x,y) \mapsto x \\ \beta(\texttt{x}) &= 15 \\ \text{und } \beta(\texttt{y}) &= 4. \end{aligned}$$

Lösung 9.3

a) Mit $S = \{\texttt{x}/\texttt{f(a)}, \texttt{y}/\texttt{a}\}$ erhalten wir

$$\begin{aligned} \sigma_S(F_1) &= \texttt{P(f(a), f(f(a)))} \\ \sigma_S(F_2) &= \texttt{P(f(a), f(f(a)))} \end{aligned}$$

b) Wir betrachten die Substitutionen

$$\begin{aligned} \sigma^- &= \sigma_{S^-}, \quad \text{mit } S^- = \{\texttt{y}/\texttt{x}\} \\ \sigma^+ &= \sigma_{S^+}, \quad \text{mit } S^+ = \{\texttt{y}/\texttt{c}\} \end{aligned}$$

Begründung (nicht gefordert):
Sei $G^+ = \sigma_{S^+}(G) = \texttt{∃x P(x, c)}$
Falls (D, I) Modell von G ist, dann gilt $val_{D,I,\beta}(\texttt{∃x P(x, y)}) = \mathbf{w}$, $\forall\beta$. Insbesondere gilt also $val_{D,I,\beta_1}(\texttt{∃x P(x, y)}) = \mathbf{w}$ mit $\beta_1(\texttt{y}) = I(\texttt{c})$. Damit gilt $M(G) \subseteq M(G^+)$.
Um zu zeigen, dass $M(G)$ eine *echte* Teilmenge von $M(G^+)$ ist, geben wir $(D^+, I^+) \in M(G^+)$ an mit $(D^+, I^+) \notin M(G)$. Wähle dazu (D^+, I^+) mit $D^+ = \mathbb{N}_0$ und $I(\texttt{R}) = <$, $I(\texttt{c}) = 5$ ein Modell von G^+, aber kein Modell von G. Es gilt zum Beispiel $\text{val}_{D^+,I^+,\beta_2}(G) = \mathbf{f}$ für $\beta_2(\texttt{y}) = 0$, da keine nicht-negative natürliche Zahl echt kleiner als 0 existiert.

Sei $G^- = \sigma_{S^-}(G) = \texttt{∃x P(x, x)}$
Wir zeigen, dass $M(G^-)$ keine Teilmenge von $M(G)$ ist, indem wir $(D, I) \in M(G^-)$ aber $(D, I) \notin M(G)$ und $(D', I') \in M(G)$ aber $(D', I') \notin M(G^-)$ angeben.
$D = \{0, 1\}, I(\texttt{R}) = \{(0, 0)\}$ ist Modell von G^-, da es $0 \in D$ gibt mit $(0, 0) \in I(\texttt{R})$, für $\beta(\texttt{y}) = 1$ gibt es aber kein solches Element und daher ist (D, I) nicht Modell von G.
$D' = \mathbb{N}_0, I'(\texttt{R}) = >$ ist Modell von G, da es für beliebige natürliche Zahlen immer eine gibt, die noch größer ist. (D', I') ist aber kein Modell von G^-, da keine natürliche Zahl echt größer als sich selbst sein kann.

c) $val_{(D,I,\beta)}(H) = \mathbf{w}$.

Aufgabe 9.4 (1 + 2 + 3 = 6 Punkte)

Für natürliche Zahlen $a, b \in \mathbb{N}_0$ ist die Potenz a^b definiert als das b-fache Produkt von a mit sich selbst:

$$a^b = \underbrace{a \cdot a \cdot \ldots \cdot a}_{b \text{ times}} = \prod_{i=1}^{b} a \, .$$

Eine naheliegende Implementierung dieser Operation arbeitet nach diesem Prinzip und benötigt damit $b - 1$ Multiplikationsoperationen für die Berechnung von a^b. Bei einigen Anwendungen (z. B. in der Kryptographie) müssen große Zahlen a und b (mit hunderten Dezimalstellen) schnell potenziert werden. In solch einem Kontext ergibt es Sinn, sich Gedanken zu machen, wie man Multiplikationen einsparen kann.

Ziel dieser Aufgabe ist es, die Korrektheit von Algorithmus 1 zu beweisen, der bei großen Zahlen deutlich weniger Multiplikationen benötigt.

Die Schleife im Programm implementiert im Wesentlichen die folgende induktive Eigenschaft von Potenzen mit ganzzahligem Exponenten:

$$a^b = \begin{cases} 1 & , b = 0 \\ (a^{\frac{b}{2}})^2 & , b \text{ gerade} \\ (a^{\frac{b-1}{2}})^2 \cdot a & , b \text{ ungerade} \end{cases}$$

$a : \mathbb{N}_0$ **Input:** $b : \mathbb{N}_0$
Output: $r : \mathbb{N}_0$
$\{\texttt{TRUE}\}$
$\{$ $\}$
$x \leftarrow a$;
$n \leftarrow b$;
$r \leftarrow 1$;
$\{$ $\}$
while $n \geq 1$ **do**
  $\{$ $\}$
  if n **mod** $2 = 0$ **then**
    $\{$ $\}$
    $\{$ $\}$
    $x \leftarrow x \cdot x$;
    $n \leftarrow n$ **div** 2 ;
    $\{$ $\}$
  else
    $\{$ $\}$
    $\{$ $\}$
    $r \leftarrow x \cdot r$;
    $x \leftarrow x \cdot x$;
    $n \leftarrow (n - 1)$ **div** 2 ;
    $\{$ $\}$
  end
  $\{$ $\}$
end
$\{$ $\}$
$\{$ $\}$
$\{a^b = r\}$

Algorithmus 1: Ein Algorithmus zur Berechnung von natürlichen Potenzen reeller Zahlen.

a) Berechnen Sie 3^{21} und 2^{12} Schrittweise. Stellen Sie dafür eine Tabelle auf, in der Sie die Variablenbelegung von x, n, und r nach jedem Schleifendurchlauf angeben.

b) Geben Sie eine Schleifeninvariante I für die Schleife in Algorithmus 1 an, mit der sich die Korrektheit des Algorithmus beweisen lässt.

c) Verwenden Sie den in der Vorlesung vorgestellten Hoare-Kalkül, um die Korrektheit des Algorithmus bzgl. der abgedruckten Vorbedingung *true* und Nachbedingung $r = a^b$ zu beweisen. Sie können dazu die leeren geschweiften Klammern in Algorithmus 1 verwenden.

Lösung 9.4

a) Für die Berechnung von 3^{21} gilt vor dem ersten Schleifendurchlauf $x = 3, n = 21, r = 1$. Die geforderte Tabelle für die Variablenbelegungen nach den Schleifendurchläufen lautet:

Durchlauf	x	n	r
1	9	10	3
2	81	5	3
3	6561	2	243
4	43046721	1	243
5	1853020188851841	0	10460353203

Für die Berechnung von 2^{12} gilt vor dem ersten Schleifendurchlauf $x = 2, n = 12, r = 1$. Die geforderte Tabelle für die Variablenbelegungen nach den Schleifendurchläufen lautet:

Durchlauf	x	n	r
1	4	6	1
2	16	3	1
3	256	1	16
4	65536	0	4096

b) Die Invariante wird durch $a^b = x^n \cdot r$ beschrieben.

c) Die Bedingungen lassen sich wie folgt festlegen:

$a : \mathbb{N}_0$ **Input:** $b : \mathbb{N}_0$
Output: $r : \mathbb{N}_0$
$\{\texttt{TRUE}\}$
$\{a^b = a^b \cdot 1\}$
$x \leftarrow a$;
$n \leftarrow b$;
$r \leftarrow 1$;
$\{a^b = x^n \cdot r\}$
while $n \geq 1$ **do**
  $\{a^b = x^n \cdot r \wedge n \geq 1\}$
  if n **mod** $2 = 0$ **then**
    $\{a^b = x^n \cdot r \wedge (n \textbf{ mod } 2 = 0)\}$
    $\{a^b = (x \cdot x)^{(n \textbf{ div } 2)} \cdot r\}$
    $x \leftarrow x \cdot x$;
    $n \leftarrow n$ **div** 2 ;
    $\{a^b = x^n \cdot r\}$
  else
    $\{a^b = x^n \cdot r \wedge \neg(n \textbf{ mod } 2 = 0)\}$
    $\{a^b = (x \cdot x)^{((n-1) \textbf{ div } 2)} \cdot (x \cdot r)\}$
    $r \leftarrow x \cdot r$;
    $x \leftarrow x \cdot x$;
    $n \leftarrow (n - 1)$ **div** 2 ;
    $\{a^b = x^n \cdot r\}$
  end
  $\{a^b = x^n \cdot r\}$
end
$\{a^b = x^n \cdot r \wedge \neg(n \geq 1)\}$
$\{a^b = x^n \cdot r \wedge n = 0\}$
$\{a^b = r\}$

Algorithmus 2: Ein Algorithmus zur Berechnung von natürlichen Potenzen reeller Zahlen.