Institute of Information Security and Dependability
Dr. Mattias Ulbrich
https://formal.kastel.kit.edu/

Übungsblatt 8

Grundbegriffe der Informatik — Winter 2023/24

Tutor*in: 　　 Tutorium Nr.:

Nach-,Vorname: ,

Matr.nr.:

Ausgabe: 19. Dezember 2023, 14:30 Uhr

Abgabe: 19. Januar 2024, 12:30 Uhr

Bitte beachten Sie die Hinweise auf der letzten Seite.

---

*Von Tutor*in auszufüllen:*

Blatt 8: / 20 　　 Blätter 1 – 8: / 162

Aufgabe 1 - Das schwarze Buch (4 Punkte)

Sei S die Menge aller Studierenden des KIT, die sich gerade mit GBI beschäftigen und sei I eine Interpretation für die Symbole $\mathtt{A}, \mathtt{B}, \mathtt{G} \in Rel_{PL}$, $\mathtt{t} \in Fun_{PL}$ mit

- $I(\mathtt{A}) = \{x \in S \mid x \text{ passt im Tutorium auf}\}$
- $I(\mathtt{B}) = \{x \in S \mid x \text{ war dieses Jahr brav}\}$
- $I(\mathtt{G}) = \{x \in S \mid x \text{ ist glücklich}\}$
- $I(\mathtt{t})\colon S \to S$ so, dass x im Tutorium von $(I(\mathtt{t}))(x)$ ist

Dabei ist jede*r Tutor*in immer im eigenen Tutorium.

a) Formalisieren Sie die folgenden Aussagen in Prädikatenlogik. Verwenden Sie dazu keine Variablen- und Funktionssymbole außer den oben eingeführten.

   i) „Nicht alle Studierende, die sich mit GBI beschäftigen, waren dieses Jahr brav.“ (0.5 Punkte)

   ii) „Brave Studierende passen im Tutorium auf.“ (0.5 Punkte)

   iii) „Alle Tutor*innen sind glücklich.“ (1 Punkt)

   iv) „Ein*e Tutor*in ist nur dann glücklich, wenn alle, die im Tutorium sind, auch aufpassen.“ (1 Punkt)

b) Gegeben sei nun die konkrete Studierendenmenge $S' \subseteq S$:

$$S' = \{\text{Alice}, \text{Bob}, \text{Carlos}, \text{David}, \text{Eve}\}$$

Geben Sie I' so an, dass (S', I') ein Modell für die Konjunktion der vier Formeln aus (a) ist. (1 Punkt)

Lösung 1

a) i) $F_1 = \exists \mathtt{x}(\neg \mathtt{B}(\mathtt{x}))$

   ii) $F_2 = \forall \mathtt{x}(\mathtt{B}(\mathtt{x}) \to \mathtt{A}(\mathtt{x}))$

   iii) $F_3 = \forall \mathtt{x}((\exists \mathtt{y}(\mathtt{t}(\mathtt{y}) \doteq \mathtt{y})) \to \mathtt{G}(\mathtt{x}))$

   iv) $F_4 = \forall \mathtt{x}(\mathtt{G}(\mathtt{x}) \to (\forall \mathtt{y}(\mathtt{t}(\mathtt{y}) \doteq \mathtt{x} \to \mathtt{A}(\mathtt{y}))))$

b) Eine mögliche Lösung ist die folgende:

   - $I'(\mathtt{A}) = S'$

- $I'(\texttt{B}) = \emptyset$
- $I'(\texttt{G}) = \{\text{Alice}\}$
- $I'(\texttt{t})\colon S' \to S', s \mapsto \text{Alice}$

Aufgabe 2 - I'm My Own Grandpa (5+2 Punkte)

Hören Sie das Lied I'm My Own Grandpa in der Version von Ray Stevens an. In dieser Aufgabe wollen wir die in den ersten beiden Strophen beschriebenen Verwandtschaftsbeziehungen formalisieren:

Many many years ago,
When I was twenty-three,
I was married to a widow
Who was pretty as can be.

This widow had a grown-up daughter
Who had hair of red.
My father fell in love with her,
And soon they too were wed.

Wir betrachten dazu eine prädikatenlogische Signatur Σ mit den Konstantensymbolen (also nullstelligen Funktionssymbolen) $\mathrm{r}, \mathrm{w}, \mathrm{f}, \mathrm{d}$ und den zweistelligen Relationssymbolen $\mathrm{S}(\cdot,\cdot), \mathrm{C}(\cdot,\cdot)$.

Wir verwenden hier nur Interpretationen (D, I), für die Folgendes gilt:

- $I(\mathrm{r})$ ist der Sänger Ray Stevens.
- $I(\mathrm{w})$ ist die Witwe.
- $I(\mathrm{f})$ ist Rays Vater.
- $I(\mathrm{d})$ ist die Tochter der Witwe.
- $(x, y) \in I(\mathrm{S})$ genau dann wenn x ein Ehepartner von y ist.
- $(x, y) \in I(\mathrm{C})$ genau dann wenn x ein Kind von y ist.

a) Formalisieren Sie die folgenden Aussagen in Prädikatenlogik mit der Signatur Σ. Verwenden Sie dabei nur die Operatoren $\rightarrow, \wedge, \vee, \neg$.

   i) „Die Witwe ist mit Ray verheiratet.“ (0.5 Punkte)

   ii) „Ray ist das Kind seines Vaters.“ (0.5 Punkte)

iii) „Die Tochter der Witwe ist das Kind der Witwe.“ (0.5 Punkte)

iv) „Rays Vater ist mit der Tochter der Witwe verheiratet.“ (0.5 Punkte)

v) „Es gilt für alle x, y, dass wenn x der Ehepartner von y ist, y auch der Ehepartner von x ist (Man sagt auch: ‚Die Ehepartner-Relation ist symmetrisch.‘).“ (0.5 Punkte)

vi) „Ein Kind eines Ehepartners ist auch das Kind des jeweils anderen Ehepartners.“ (0.5 Punkte)

b) Beweisen Sie in natürlicher Sprache, dass aus den Aussagen aus Teilaufgabe (a) folgt, dass Ray sein eigener Großvater ist, also dass

$$\Gamma \vdash \exists x\ (C(r,x) \wedge C(x,r))$$

wobei Γ die Menge der Formeln aus Teilaufgabe (a) ist. (2 Punkte)

c) **Bonusaufgabe:** Beweisen Sie dasselbe im Kalkül des natürlichen Schließens. (2 Punkte)

Lösung 2

a) i) $S(w,r)$

ii) $C(r,f)$

iii) $C(d,w)$

iv) $S(f,d)$

v) $\forall x\ \forall y\ (S(x,y) \rightarrow S(y,x))$

vi) $\forall x\ \forall y\ \forall z\ (S(x,y) \wedge C(z,x) \rightarrow C(z,y))$

b) Da Rays Vater mit der Tochter der Witwe verheiratet und Ray das Kind seines Vaters ist, folgt mit Aussage (vi), dass Ray auch das Kind der Tochter der Witwe ist, also dass $C(r,d)$. Da Ray mit der Witwe verheiratet ist, folgt mit Aussage (vi), dass ihre Tochter auch seine Tochter ist, also dass $C(d,r)$. Insgesamt folgt also, dass $C(r,d) \wedge C(d,r)$, woraus wir direkt die zu beweisende Aussage ableiten können.

c)

$$\dfrac{\dfrac{*_1 \qquad *_2}{\Gamma \vdash C(d,r) \wedge C(r,d)}\ (\wedge I)}{\Gamma \vdash \exists x\ (C(r,x) \wedge C(x,r))}\ (\exists I)$$

wobei $*_1 =$

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash S(w,r)}\,(\text{Ax}) \qquad \dfrac{}{\Gamma \vdash C(d,w)}\,(\text{Ax})}{\Gamma \vdash S(w,r) \wedge C(d,w)}\,(\wedge\text{I}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \forall x\ \forall y\ \forall z\ (S(x,y) \wedge C(z,x) \to C(z,y))}\,(\text{Ax})}{\Gamma \vdash \forall y\ \forall z\ (S(w,y) \wedge C(z,w) \to C(z,y))}\,(\forall\text{E})}{\Gamma \vdash \forall z\ (S(w,r) \wedge C(z,w) \to C(z,r))}\,(\forall\text{E})}{\Gamma \vdash S(w,r) \wedge C(d,w) \to C(d,r)}\,(\forall\text{E})}{\Gamma \vdash C(d,r)}\,(\to\text{E})$$

und $*_2 =$

$$\dfrac{\dfrac{\dfrac{}{\Gamma \vdash S(f,d)}\,(\text{Ax}) \qquad \dfrac{}{\Gamma \vdash C(r,f)}\,(\text{Ax})}{\Gamma \vdash S(f,d) \wedge C(r,f)}\,(\wedge\text{I}) \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \forall x\ \forall y\ \forall z\ (S(x,y) \wedge C(z,x) \to C(z,y))}\,(\text{Ax})}{\Gamma \vdash \forall y\ \forall z\ (S(f,y) \wedge C(z,f) \to C(z,y))}\,(\forall\text{E})}{\Gamma \vdash \forall z\ (S(f,d) \wedge C(z,f) \to C(z,d))}\,(\forall\text{E})}{\Gamma \vdash S(f,d) \wedge C(r,f) \to C(r,d)}\,(\forall\text{E})}{\Gamma \vdash C(r,d)}\,(\to\text{E})$$

Aufgabe 3 - Hoare-Kalkül (6 Punkte)

Für zwei natürliche Zahlen $a, b \in \mathbb{N}_+$ ist der größte gemeinsame Teiler

$$\text{ggT}(a, b) = \max\{x \in \mathbb{N}_+ \mid x \text{ teilt } a \text{ und } x \text{ teilt } b\}$$

Der folgende Algorithmus berechnet den größten gemeinsamen Teiler für zwei gegebene natürliche Zahlen:

Input: $A \in \mathbb{N}_+, B \in \mathbb{N}_+$
$\{A \geq 1 \wedge B \geq 1\}$

$a \leftarrow A$

$b \leftarrow B$

while $a \neq b$ **do**

    if $a > b$ **then**

        $a \leftarrow a - b$

    else

        $b \leftarrow b - a$

    fi

od

$\{a = \mathrm{ggT}(A, B)\}$

return a

a) Seien $a, b, c \in \mathbb{N}_+$ sodass $a > b$. Zeigen Sie, dass $\mathrm{ggT}(a, b) = \mathrm{ggT}(a - b, b)$ und dass $\mathrm{ggT}(c, c) = c$. (2 Punkte)

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

c) Verwenden Sie den in der Vorlesung vorgestellten Hoare-Kalkül, um die Korrektheit des Algorithmus bezüglich der bereits vorgegebenen Vor- und Nachbedingung zu beweisen. Sie können dazu die farblich hervorgehobenen Zeilen im Algorithmus verwenden. (3 Punkte)

   Hinweis: Sie dürfen Ihre Ergebnisse aus der ersten Teilaufgabe verwenden.

Lösung 3

a)
- $\text{ggT}(a, b) = \text{ggT}(a - b, b)$

  Sei k der ggT von a und b.Dann ist k auch ein Teiler von $a - b$, denn:

  Es gibt $n, m \in \mathbb{N}_+$ so, dass $a = kn$ und $b = km$.Da $a > b$, muss $n > m$ gelten, also $n - m > 0$. Damit:

  $$a - b = nk - mk = k(n - m)$$

  Angenommen, $k \neq \text{ggT}(a - b, b) = k'$. Dann gilt $k' > k$ und es gibt n', m' mit $a - b = n'k'$ und $b = m'k'$. Dann:

  $$a = (a - b) + b = (n'k') + m'k' = k'(n' + m')$$

  Also teilt k' nicht nur b, sondern auch a. Außerdem ist $k' > k$, was ein Widerspruch dazu ist, dass k der größte gemeinsame Teiler von a und b ist.
- $\text{ggT}(c, c) = c$ Sei k der ggT von c. Dann muss $k \in \{1, \ldots, c\}$ sein. Da c ein Teiler von sich selbst ist, folgt direkt, dass $k = c$.

b) Sei A der initiale Wert von a und sei B der initiale Wert von b. Eine geeignete Schleifeninvariante ist

$$I = \{\text{ggT}(a, b) = \text{ggT}(A, B) \land a \geq 1 \land b \geq 1\}$$

c)

Input: $A \in \mathbb{N}_+, B \in \mathbb{N}_+$
$\{A \geq 1 \land B \geq 1\}$
$\{\text{ggT}(A, B) = \text{ggT}(A, B) \land A \geq 1 \land B \geq 1\}$
$a \leftarrow A$
$\{\text{ggT}(a, B) = \text{ggT}(A, B) \land a \geq 1 \land B \geq 1\}$
$b \leftarrow B$
$\{\text{ggT}(a, b) = \text{ggT}(A, B) \land a \geq 1 \land b \geq 1\}$
while $a \neq b$ **do**
    $\{\text{ggT}(a, b) = \text{ggT}(A, B) \land a \geq 1 \land b \geq 1 \land a \neq b\}$
    if $a > b$ **then**

$\{\mathrm{ggT}(a,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1 \wedge a \neq b \wedge a > b\}$
$\{\mathrm{ggT}(a-b,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1 \wedge a > b\}$
$a \leftarrow a - b$
$\{\mathrm{ggT}(a,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1\}$
else
$\{\mathrm{ggT}(a,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1 \wedge a \neq b \wedge a \leq b\}$
$\{\mathrm{ggT}(a,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1 \wedge a < b\}$
$\{\mathrm{ggT}(a,b-a) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1 \wedge a < b\}$
$b \leftarrow b - a$
$\{\mathrm{ggT}(a,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1\}$
fi
$\{\mathrm{ggT}(a,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1\}$
od
$\{\mathrm{ggT}(a,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1 \wedge \neg(a \neq b)\}$
$\{\mathrm{ggT}(a,b) = \mathrm{ggT}(A,B) \wedge a \geq 1 \wedge b \geq 1 \wedge a = b\}$
$\{a = \mathrm{ggT}(A,B)\}$
return a

Aufgabe 4 - Prädikatenlogik (5 Punkte)

Es sei folgende prädikatenlogische Formel gegeben:

$$F = (\exists x\,(R(x) \rightarrow Q(x,x))) \rightarrow ((\forall x\, R(x)) \rightarrow \exists x\, Q(x,x))$$

a) Geben Sie ein Modell (D, I) von F an. (1 Punkt)

b) Ist F allgemeingültig? Begründen Sie ihre Antwort. (3 Punkte)

c) Ist F zu der folgenden Formel G äquivalent? Begründen Sie. (1 Punkt)

$$G = (\exists x\,(R(x) \rightarrow Q(x,x))) \rightarrow ((\forall x\, R(x)) \rightarrow \forall x\, Q(x,x))$$

Lösung 4

a) Ein mögliches Modell ist (D, I), wobei $D = \mathbb{R}$ und

- $I(\mathtt{R}) = \mathbb{N}$
- $I(\mathtt{Q}) = \{(x, y) \in \mathbb{R}^2 \mid xy \in \mathbb{N}\}$

b) Ja, denn: Sei $F_1 = \exists\mathtt{x}(\mathtt{R(x)} \rightarrow \mathtt{Q(x,x)})$ und sei $F_2 = (\forall\mathtt{x}\,\mathtt{R(x)}) \rightarrow \exists\mathtt{x}\,\mathtt{Q(x,x)}$. Dann ist $F = F_1 \rightarrow F_2$ und für ein Modell (D, I) von F muss für jede beliebige Variablenbelegung β muss nach Definition von $\rightarrow$ entweder $val_{D,I,\beta}(F_1) = \mathbf{f}$ oder $val_{D,I,\beta}(F_2) = \mathbf{w}$ gelten.

Sei also (D, I) eine beliebige passende Interpretation und sei β eine beliebige passende Variablenbelegung. Wir zeigen, dass $val_{D,I,\beta}(F) = \mathbf{w}$:

- Fall 1: $val_{D,I,\beta}(F_1) = \mathbf{f}$

  Dann gilt $val_{D,I,\beta}(F) = \mathbf{w}$, wie oben beschrieben.

- Fall 2: $val_{D,I,\beta}(F_1) = \mathbf{w}$

  Dann gibt es ein $d \in D$ so, dass $val_{D,I,\beta_{\mathtt{x}}^d}(\mathtt{R(x)} \rightarrow \mathtt{Q(x,x)}) = \mathbf{w}$, also entweder $val_{D,I,\beta_{\mathtt{x}}^d}(\mathtt{R(x)}) = \mathbf{f}$ oder $val_{D,I,\beta_{\mathtt{x}}^d}(\mathtt{Q(x,x)}) = \mathbf{w}$.

  Falls $val_{D,I,\beta_{\mathtt{x}}^d}(\mathtt{R(x)}) = \mathbf{f}$, so gilt $val_{D,I,\beta}(\forall\mathtt{x}\,\mathtt{R(x)}) = \mathbf{f}$ und damit $val_{D,I,\beta}(F_2) = \mathbf{w}$.

  Falls $val_{D,I,\beta_{\mathtt{x}}^d}(\mathtt{Q(x,x)}) = \mathbf{w}$, so auch $val_{D,I,\beta}(\exists\mathtt{x}\,\mathtt{Q(x,x)}) = \mathbf{w}$ und also $val_{D,I,\beta}(F_2) = \mathbf{w}$.

  Damit folgt direkt $val_{D,I,\beta}(F) = \mathbf{w}$ in beiden Fällen.

c) Nein, denn G ist nicht allgemeingültig. Betrachten wir die Interpretation (D, I) mit $D = \mathbb{N}_0$ und

- $I(\mathtt{R}) = \mathbb{N}_0$
- $I(\mathtt{Q}) = \{(0, 0)\}$

zusammen mit einer beliebigen Variablenbelegung β mit $\beta(\mathtt{x}) \in \mathbb{N}_+$, dass $val_{D,I,\beta}(G) = \mathbf{f}$.

Das GBI-Team wünscht Ihnen fröhliche und erholsame Feiertage!

Bitte beachten Sie die folgenden Hinweise:

- Lösungen **müssen** handschriftlich erstellt werden
- Ihre Abgabe sollte die erste Seite dieser Datei als Deckblatt haben
- Ihre Abgabe muss **rechtzeitig** erfolgen

Außerdem, wenn Sie Ihre Ausarbeitung über die Abgabekästen im Keller des Informatik-Gebäudes abgeben:

- Ihre Abgabe muss in der oberen **linken** Ecke zusammengeheftet werden
- Tablet-Ausdrucke sind zulässig

Wenn Sie Ihre Ausarbeitung online über ILIAS abgeben, dann achten Sie darauf:

- Ihre Abgabe muss **genau eine** PDF-Datei sein
- Scans und lesbare Fotos sind zulässig
- Abgabe erfolgt unter „Tutorien“ im Ordner **Ihres** Tutoriums