Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. B. Beckert
Dr. Vladimir Klebanov

Formale Systeme, WS 2009/2010

Lösungen zum Übungsblatt 6

Dieses Blatt wurde in der Übung am 11.12.2009 besprochen.

Zu Aufgabe 1

(a) Axiomatisiere p als strikte Halbordnung

- p ist transitiv: $\forall x \forall y \forall z (p(x,y) \wedge p(y,z) \rightarrow p(x,z))$
- p ist irreflexiv: $\forall x \neg p(x,x)$

Also insgesamt: $F = (\forall x \forall y \forall z (p(x,y) \wedge p(y,z) \rightarrow p(x,z))) \wedge (\forall x \neg p(x,x))$

(b) Die Unendlichkeit eines Modells kann erzwungen werden, wenn man im Universum eine unendlich aufsteigende Kette fordern kann.

Dies kann durch

$$U = \forall x \exists y (p(x,y))$$

gemacht werden. Setze also

$$G = U \wedge F \ .$$

Sei (D, I) ein beliebiges Modell von G. Dann ist die Relation $I(p) \subseteq D \times D$ zyklenfrei. Hätte sie einen Zyklus $z_1 \xrightarrow{I(p)} z_2 \xrightarrow{I(p)} \ldots \xrightarrow{I(p)} z_r$, so würde wegen der Transitiviät auch $z_0 \xrightarrow{I(p)} z_0$ gelten und es ein Element geben, das reflexiv bzgl. $I(p)$ ist. Das widerspräche aber der axiomatisierten Irreflexitivität.

Sei (D, I) ein beliebiges Modell und $d_0 \in D$ beliebiges Element. Dann gibt es eine unendliche Kette $(d_0 \xrightarrow{I(p)} d_1 \xrightarrow{I(p)} \ldots)$ mit $d_i \in D$ und $(d_i, d_{i+1}) \in I(p)$. Die Existenz eines Nachfolgers wird durch U sichergestellt.

Da die Folge keinen Zyklus enthalten darf, müssen die d_i paarweise verschieden sein und damit die Menge D unendlich.

Zu Aufgabe 2

Seien mit ϕ_a bis ϕ_e die Formeln aus den Aufgabenteilen bezeichnet.

(a)

	$\exists x(\forall x(\neg f(x) \doteq f(x)))$	$a \doteq a$ ist für jeden Term a immer wahr
$\equiv$	$\exists x(\forall x(\neg \mathbf{1}))$	die gebundene Variable x tritt nicht auf
$\equiv$	$\exists x(\neg \mathbf{1})$	die gebundene Variable x tritt nicht auf
$\equiv$	$\neg \mathbf{1} \equiv \mathbf{0}$	Die Formel ist also unerfüllbar

(b) Sei (D, I) eine beliebige Interpretation und β eine beliebige Variablenbelegung.

$$\begin{array}{ll} & \mathrm{val}_{I,\beta}(\forall x(f(x) \doteq c)) = W \\ \iff & \text{Für alle } d \in D \text{ gilt } \mathrm{val}_{I,\beta_x^d}(f(x) \doteq c) = W \\ \implies & \mathrm{val}_{I,\beta_x^{val_I(f(f(c)))}}(f(x) \doteq c) = W \\ \iff & I(f)(val_{I,\beta}(f(f(c)))) = I(c) \\ \iff & \mathrm{val}_{I,\beta}(f(f(f(c))) \doteq c) = W \end{array}$$

also

$$\begin{array}{ll} & \mathrm{val}_{I,\beta}(\forall x(f(x) \doteq c)) = W \implies \mathrm{val}_{I,\beta}(f(f(f(c))) \doteq c) = W \\ \iff & \mathrm{val}_{I,\beta}(\phi_b) = W \end{array}$$

Also ist ϕ_b allgemeingültig.

(c) Da in ϕ_c die gebundenen Variablen nur in jeweils einem der Operanden der Disjunktion auftreten, gilt nach Satz 4.47:

$$\phi_c \equiv (\forall x\ p(x)) \vee (\forall y\ \neg p(y)) =: \phi'_c$$

Wir zeigen zunächst die Erfüllbarkeit von ϕ'_c. Sei $D = \{d_1\}$ ein einelementiges Universum und $I(p) = \{d_1\}$. Die einzig mögliche Variablenbelegung β ist dann $\beta(v) = d_1$ für alle $v \in Var$ und damit

$$\begin{array}{ll} & d_1 \in I(p) \\ \implies & \mathrm{val}_{I,\beta}(p(x)) = W \\ \implies & \mathrm{val}_{I,\beta}(\forall x\ p(x)) = W \text{ weil das die einzig mögliche Var-Belegung ist} \\ \implies & \mathrm{val}_{I,\beta}(\forall x\ p(x) \vee \forall y\ \neg p(y)) = W \\ \implies & \mathrm{val}_{I,\beta}(\phi'_c) = W \end{array}$$

Damit ist gezeigt, daß ϕ_c in (D, I) erfüllt ist.

Umgekehrt gilt für $D' = \{d_1, d_2\}$, $I'(p) = \{d_1\}$, und β' eine beliebige Var-Belegung, daß

$$\begin{array}{ll} & d_2 \notin I(p) \text{ und } d_1 \in I(p) \\ \implies & \mathrm{val}_{I,\beta}(\forall x\ p(x)) = F \text{ und } \mathrm{val}_{I,\beta}(\forall y\ \neg p(y)) = F \\ \implies & \mathrm{val}_{I,\beta}(\phi'_c) = F \end{array}$$

Damit ist gezeigt, daß ϕ'_c in (D', I') nicht erfüllt ist. ϕ_c ist also erfüllbar, aber nicht allgemeingültig

(d) Dies ist keine prädikatenlogische Formel nach unserer Definition. Links und rechts des Gleichheitszeichens $\doteq$ müssen bei uns Terme und nicht Formeln stehen. Das „Gleichheitszeichen“ für Formeln ist $\leftrightarrow$.

Bemerkung: Die modifizierte Formel $\forall x(((p(x) \leftrightarrow \mathbf{1}) \wedge (p(x) \leftrightarrow q(x))) \rightarrow (q(x) \leftrightarrow \mathbf{1}))$ ist dann allgemeingültig.

(e) Da r und s nullstellige Prädikate – also aussagenlogische Variablen – sind, handelt es sich auch um eine AL-Formel (AL ist in PL enthalten!).

Die Formel

$$(r \rightarrow (s \rightarrow r)) \rightarrow ((r \rightarrow s) \rightarrow r)$$

ist keine Tautologie. Sie ist in Interpretationen I mit $I(r) = F$ falsch. Sie ist aber erfüllbar, denn in Interpretationen I mit $I(r) = W$ ist sie wahr.[1]

[1]In einer früheren Version der Lösung war dies nicht richtig dargestellt, weil die in der Lösung verwendete Formel nicht die gleiche war wie die auf dem Aufgabenblatt.

Dagegen ist die Formel

$$((r \to s) \to r) \to (r \to (s \to r))$$

eine Tautologie, was z.B. mit Hilfe des AL-Sequenzenkalküls nachgewiesen werden kann:

$$\begin{array}{l} \Rightarrow ((r \to s) \to r) \to (r \to (s \to r)) \\ (r \to s) \to r \Rightarrow r \to (s \to r) \\ (r \to s) \to r,\ r \Rightarrow s \to r \\ (r \to s) \to r,\ r,\ s \Rightarrow r \\ \text{Axiom} \end{array}$$

Zu Aufgabe 3

Es gilt im Allgemeinen **nicht** $G \equiv G_{\text{sko}}$, wie uns Aufgabe 4 zeigt. Es gilt lediglich $G \overset{\circ}{\equiv} G_{\text{sko}}$: G hat ein Modell genau dann, wenn G_{sko} ein Modell hat („equisatisfiability"). Das Zeichen $\equiv$ darf nicht bei Skolemisierung verwendet werden.

Es gibt unterschiedliche Lösungen für diese Aufgaben, aber man sollte immer versuchen, Skolemsymbole mit möglichst wenig Argumenten zu erzeugen. Das vereinfacht nachfolgende Beweise (weniger Unifikation notwendig!).

In der Praxis ist es zumeist ungünstig, zuerst die Pränexnormalform herstellen und danach erst zu skolemisieren. Besser ist es, zuerst zu skolemisieren und dann die Quantoren nach außen zu ziehen. Daß die letztere Reihenfolge besser ist, zeigt auch der Vergleich der Teilaufgaben (a) und (c). Mehrere Existenzquantoren werden übrigens von außen nach innen eliminiert.

(a)

$$\begin{array}{lll} & (\forall x p(x) \to \forall x q(x)) \to \forall x(p(x) \to q(x)) & \\ \equiv & (\forall x p(x) \to \forall y q(y)) \to \forall z(p(z) \to q(z)) & \text{Umbenennen der gebundenen Variablen} \\ \equiv & \neg(\neg\forall x p(x) \lor \forall y q(y)) \lor \forall z(\neg p(z) \lor q(z)) & \text{Implikationen auflösen} \\ \equiv & (\forall x p(x) \land \exists y \neg q(y)) \lor \forall z(\neg p(z) \lor q(z)) & \text{Negationen nach innen schieben} \\ \overset{\circ}{\equiv} & (\forall x p(x) \land \neg q(c)) \lor \forall z(\neg p(z) \lor q(z)) & \text{Skolemisieren} \\ \equiv & \forall x \forall z((p(x) \land \neg q(c)) \lor (\neg p(z) \lor q(z)) & \text{Allquantoren nach außen ziehen} \\ \equiv & \forall x \forall z((p(x) \lor \neg p(z) \lor q(z)) \land (\neg q(c) \lor \neg p(z) \lor q(z)) & \text{Matrix in KNF überführen} \end{array}$$

(b)

$$\begin{array}{lll} & \exists x(\forall y\ p(x,y) \lor \exists z(p(x,z) \land \forall x\ p(z,x))) & \\ \equiv & \exists x(\forall y\ p(x,y) \lor \exists z(p(x,z) \land \forall w\ p(z,w))) & \text{Umbenennen gebundener Variablen} \\ \overset{\circ}{\equiv} & \forall y\ p(c,y) \lor (p(c,d) \land \forall w\ p(d,w)) & \text{Skolemisieren} \\ \equiv & \forall y \forall w(p(c,y) \lor (p(c,d) \land p(d,w))) & \text{Allquantoren nach außen ziehen} \\ \equiv & \forall y \forall w((p(c,y) \lor p(c,d)) \land (p(c,y) \lor p(d,w))) & \text{Matrix in KNF} \end{array}$$

(c) Vor der Skolemisierung können auch erst die Allquantoren nach außen gezogen werden. Dadurch wird bei der Skolemisierung ein Skolem-Term $f(x,z)$ statt einer Konstanten eingeführt. Diese Lösung ist strukturell (nicht nur durch Umbenennung!) verschieden von der Lösung in (a).

$$\begin{array}{lll} & (\forall x p(x) \to \forall x q(x)) \to \forall x(p(x) \to q(x)) & \\ \equiv & (\forall x p(x) \to \forall y q(y)) \to \forall z(p(z) \to q(z)) & \text{Umbenennen der gebundenen Variablen} \\ \equiv & \neg(\neg\forall x p(x) \lor \forall y q(y)) \lor \forall z(\neg p(z) \lor q(z)) & \text{Implikationen auflösen} \\ \equiv & (\forall x p(x) \land \exists y \neg q(y)) \lor \forall z(\neg p(z) \lor q(z)) & \text{Implikationen nach innen schieben} \\ \equiv & \forall x \forall z((p(x) \land \exists y \neg q(y)) \lor (\neg p(z) \lor q(z)) & \text{Allquantoren nach außen ziehen} \\ \overset{\circ}{\equiv} & (\forall x p(x) \land \neg q(f(x,z))) \lor \forall z(\neg p(z) \lor q(z)) & \text{Skolemisieren} \\ \equiv & \forall x \forall z((p(x) \lor \neg p(z) \lor q(z)) \land (\neg q(f(x,z)) \lor \neg p(z) \lor q(z)) & \text{Matrix in KNF überführen} \end{array}$$

Zu Aufgabe 4

(a) (i) $G = \exists x(p(x))$, denn $G_{\text{sko}} = p(c)$ und $\neg p(c) \wedge \exists x(p(x))$ ist erfüllbar.
Ein Modell ist $\mathcal{D} = (\{a, b\}, I(p) = \{a\}, I(c) = b)$

(ii) Z.B. $G = p = G_{\text{sko}}$ (mit p 0-stelliges Prädikat). Für jede variablenfreie Formel G gilt $G = G_{\text{sko}}$, also insbondere auch $\neg G_{\text{sko}} \wedge G = \neg G \wedge G \equiv \mathbf{0}$.

(iii) $G = \exists x(p(x))$, denn $G_{sko} = p(c)$ und $G/G_{sko} \equiv \exists x(p(x))/p(c)$. Die Interpretation $\mathcal{D} = (\{a, b\}, I(p) = \{a\}, I(c) = b)$ ist z. B. kein Modell von $G \to G_{\text{sko}}$.

(b) Sei G o.b.d.A. in Pränexnormalform und die gebundenen Variablen verschieden. Lemma 4.36 im Skript besagt:

> Sei Σ eine Signatur, $\mathcal{D}$ eine Interpretation für Σ, β eine Belegung und σ eine für A kollisionsfreie Substitution mit $\sigma(y) = y$ für alle Variablen $y \neq x$, dann gilt:
>
> $$\mathrm{val}_{\mathcal{D},\beta}(\sigma(A) \to \exists x A) = W$$

Sei n die Anzahl der Existenzquantoren in G. Die Formel G_{sko} wird durch n Skolemisierungsschritte aus G gewonnen. Seinen $G_0, \ldots, G_n$ die Zwischenschritte mit $G_0 = G$ und $G_n = G_{sko}$.

Betrachten wir nun den allgmeinen Schritt $G_i \rightsquigarrow G_{i+1}$ für $0 \leq i < n$.

Jedes G_i ist von der Form $G_i = \forall x_1 \ldots \forall x_{l_i} \exists x\ \varphi_i$ mit $l_i \geq 0$ voranstehenden Allquantoren für ein geeignetes φ_i.

Für G_{i+1} gilt nach der Skolemisierung von x: $G_{i+1} = \forall x_1 \ldots \forall x_{l_i}\ \sigma(\varphi_i)$ wobei $\sigma(x) = f_i(x_1, \ldots, x_{l_i})$ für eine neue Skolemfunktion f_i ist. σ entspricht auf den Variablen verschieden von x der Identität und ist wegen der Annahme über die Variablen kollisionsfrei.

Damit sind die Voraussetzungen von Lemma 4.36 erfüllt und es gilt, daß $\sigma(\varphi) \to \exists x\ \varphi$ allgemeingültig ist.

Wegen (mehrfacher Anwendung) des Lemmas unten gilt auch $(G_i)_{\text{sko}} = G_{i+1} \to G_i$ ist allgemeingültig. Mit der Transitivität von $\to$ folgt: $G_n \to G_0$ ist allgemeingültig. □

Lemma: Wenn $A \to B$ allgemeingültig ist, dann ist auch $\forall x\ A \to \forall x\ B$ allgemeingültig.

Beweis: Sei (D, I) eine Interpretation und β eine Variablenbelegung, $A \to B$ allgemeingültig und gelte $\mathrm{val}_{(I,\beta)}(\forall x\ A) = W$. Dann ist zu zeigen, daß $\mathrm{val}_{(I,\beta)}(\forall x\ B) = W$.

Es gilt, daß $\mathrm{val}_{(I,\beta_x^d)}(A) = W$ für alle $d \in D$ und wegen der Allgemeingültigkeit von $A \to B$ damit auch $\mathrm{val}_{(I,\beta_x^d)}(B) = W$ für alle d. Das wiederum impliziert $\mathrm{val}_{(I,\beta)}(\forall x\ B) = W$. □