UNIVERSITÄT KARLSRUHE (TH)
Institut für Theoretische Informatik
Prof. Dr. B. Beckert
M. Ulbrich

Formale Systeme, WS 2008/2009

Lösungen zum Übungsblatt 4

Dieses Blatt wurde in der Übung am 12.12.2008 besprochen.

Zu Aufgabe 1

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

(b) Sei G obdA 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:
>
> $$\text{val}_{\mathcal{D},\beta}(\sigma(A) \rightarrow \exists x A) = W$$

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 $\sigma(\varphi) \rightarrow \exists x\ \varphi$ allgemeingültig ist.

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

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

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

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

Zu Aufgabe 2

Es gilt im Allgemeinen **nicht** $G \equiv G_{\text{sko}}$, wie uns Aufgabe 1 zeigte, das Zeichen $\equiv$ ist daher mit Vorsicht zu verwenden.

Es gibt verschiedene unterschiedliche Lösungen für diese Aufgaben, aber man sollte immer versucht sein, Skolemsymbole mit möglichst wenig Argumenten zu erzeugen, weil das nachfolgende Beweise effizienter gestalten lässt (weniger Unifikation notwendig!).

Nimmt man die Aufgabenstellung wörtlich, so muss man eigentlich zuerst Pränexnormalform herstellen und danach erst skolemisieren. In der Praxis ist das aber zumeist ungünstig (insofern ist die Aufgabe schlecht formuliert). Besser ist es, zuerst zu skolemisieren und dann die Quantoren nach außen zu ziehen. Dass letztere Reihenfolge besser ist, zeigt der Vergleich der Teilaufgaben (a) und (c). Mehrere Existenzquantoren werden von außen nach innen eliminiert.

(a)

	$(\forall x p(x) \to \forall x q(x)) \to \forall x(p(x) \to q(x))$	
$\equiv$	$(\forall x p(x) \to \forall y q(y)) \to \forall z(p(z) \to q(z))$	Umbenennen der gebundenen Variablen
$\equiv$	$\neg(\neg\forall x p(x) \vee \forall y q(y)) \vee \forall z(\neg p(z) \vee q(z))$	Implikationen auflösen
$\equiv$	$(\forall x p(x) \wedge \exists y \neg q(y)) \vee \forall z(\neg p(z) \vee q(z))$	Implikationen nach innen schieben
$(\equiv)$	$(\forall x p(x) \wedge \neg q(c)) \vee \forall z(\neg p(z) \vee q(z))$	Skolemisieren
$\equiv$	$\forall x \forall z((p(x) \wedge \neg q(c)) \vee (\neg p(z) \vee q(z))$	Allquantoren nach außen ziehen
$\equiv$	$\forall x \forall z((p(x) \vee \neg p(z) \vee q(z)) \wedge (\neg q(c) \vee \neg p(z) \vee q(z))$	Matrix in KNF überführen

(b)

	$\exists x(\forall y\ p(x,y) \vee \exists z(p(x,z) \wedge \forall x\ p(z,x)))$	
$\equiv$	$\exists x(\forall y\ p(x,y) \vee \exists z(p(x,z) \wedge \forall w\ p(z,w)))$	Umbenennen gebundener Variablen
$(\equiv)$	$\forall y\ p(c,y) \vee (p(c,d) \wedge \forall w\ p(d,w))$	Skolemisieren
$\equiv$	$\forall y \forall w(p(c,y) \vee (p(c,d) \wedge p(d,w)))$	Allquantoren nach außen ziehen
$\equiv$	$\forall y \forall w((p(c,y) \vee p(c,d)) \wedge (p(c,y) \vee p(d,w)))$	Matrix in KNF

(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).

	$(\forall x p(x) \to \forall x q(x)) \to \forall x(p(x) \to q(x))$	
$\equiv$	$(\forall x p(x) \to \forall y q(y)) \to \forall z(p(z) \to q(z))$	Umbenennen der gebundenen Variablen
$\equiv$	$\neg(\neg\forall x p(x) \vee \forall y q(y)) \vee \forall z(\neg p(z) \vee q(z))$	Implikationen auflösen
$\equiv$	$(\forall x p(x) \wedge \exists y \neg q(y)) \vee \forall z(\neg p(z) \vee q(z))$	Implikationen nach innen schieben
$\equiv$	$\forall x \forall z((p(x) \wedge \exists y \neg q(y)) \vee (\neg p(z) \vee q(z))$	Allquantoren nach außen ziehen
$(\equiv)$	$(\forall x p(x) \wedge \neg q(f(x,z))) \vee \forall z(\neg p(z) \vee q(z))$	Skolemisieren
$\equiv$	$\forall x \forall z((p(x) \vee \neg p(z) \vee q(z)) \wedge (\neg q(f(x,z)) \vee \neg p(z) \vee q(z))$	Matrix in KNF überführen

Zu Aufgabe 3

Mit ψ_a, ψ_b, ψ_c werden die Formeln aus der Aufgabenstellung bezeichnet.

(a) in $\mathcal{Z}$: Die Auswertung von ψ_a in $\mathcal{Z}$ ergibt die Bedingung

$$\text{Ist } y \in \mathbb{Z} \text{ gerade, dann ist auch } y+2 \text{ gerade}$$

Dies ist in $\mathbb{Z}$ erfüllt, denn aus $y = 2k$ folgt, dass $y+2 = 2(k+1)$ trivialerweise auch gerade ist.

in $\mathcal{Z}_{\text{Jint}}$: Die Auswertung von ψ_a in $\mathcal{Z}$ ergibt die Bedingung

$$\text{Gibt es für } y \in \mathbb{Z}_{\text{Jint}} \text{ ein } k_1 \in \mathbb{Z}_{\text{Jint}} \text{ mit } y = 2 *_{\mathcal{Z}_{\text{Jint}}} k_1, \text{ so gibt es für } y +_{\mathcal{Z}_{\text{Jint}}} 2 \text{ ein } k_2 \in \mathbb{Z}_{\text{Jint}} \text{ mit } y +_{\mathcal{Z}_{\text{Jint}}} 2 = 2 *_{\mathcal{Z}_{\text{Jint}}} k_2.$$

Nach Definition[1] gilt für die Operationen in $\mathcal{Z}_{\text{Jint}}$:

$$\begin{aligned} 2 *_{\mathcal{Z}_{\text{Jint}}} k_1 +_{\mathcal{Z}_{\text{Jint}}} 2 &= \text{mod}_{\mathcal{Z}_{\text{Jint}}}(2 *_{\mathcal{Z}} k_1) +_{\mathcal{Z}_{\text{Jint}}} 2 \\ &= \text{mod}_{\mathcal{Z}_{\text{Jint}}}(2 *_{\mathcal{Z}} k_1 +_{\mathcal{Z}} 2) \\ &= \text{mod}_{\mathcal{Z}_{\text{Jint}}}(2 *_{\mathcal{Z}} (k_1 +_{\mathcal{Z}} 1)) \\ &= 2 *_{\mathcal{Z}_{\text{Jint}}} \text{mod}_{\mathcal{Z}_{\text{Jint}}}(k_1 +_{\mathcal{Z}} 1) = 2 *_{\mathcal{Z}_{\text{Jint}}} (k_1 +_{\mathcal{Z}_{\text{Jint}}} 1) \end{aligned}$$

Für $k_2 = k_1 +_{\mathcal{Z}_{\text{Jint}}} 1$ gilt also die Behauptung.

(b) in $\mathcal{Z}$: Die Auswertung von ψ_b in $\mathcal{Z}$ ergibt die Bedingung

$$\text{Für alle } \mathbb{Z} \ni x > 0 \text{ gilt } 2 *_{\mathcal{Z}} x > x$$

Wegen $x > 0$ gilt $2 *_{\mathcal{Z}} x = x + x > x > 0$ in $\mathbb{Z}$, also gilt ψ_b in $\mathcal{Z}$.

in $\mathcal{Z}_{\text{Jint}}$: Die Auswertung von ψ_b in $\mathcal{Z}$ ergibt die Bedingung

$$\text{Für alle } \mathbb{Z}_{\text{Jint}} \ni x > 0 \text{ gilt } 2 *_{\mathcal{Z}_{\text{Jint}}} x > x$$

Für $x = \mathsf{MAXINT}$ gilt $2 *_{\mathcal{Z}_{\text{Jint}}} x = \text{mod}_{\mathcal{Z}_{\text{Jint}}}(2 *_{\mathcal{Z}} (2^{31} - 1)) = \text{mod}_{\mathcal{Z}_{\text{Jint}}}(2^{32} - 2) = -2$.
Also ist $x *_{\mathcal{Z}_{\text{Jint}}} 2 = -2 \not> x$, ψ_b ist also nicht erfüllt in $\mathcal{Z}_{\text{Jint}}$.

(c) in $\mathcal{Z}$: Die Auswertung von ψ_c in $\mathcal{Z}$ ergibt die Bedingung

$$\text{Es gibt ein } x \in \mathbb{Z}, \text{ so dass für alle } y \in \mathbb{Z} \text{ gilt } x \leq y.$$

Zu einem beliebigen $x \in \mathbb{Z}$ ist aber $x - 1$ eine ganze Zahl und echt kleiner als x. Somit ist ψ_c in $\mathcal{Z}$ nicht erfüllt.

in $\mathcal{Z}_{\text{Jint}}$: Die Auswertung von ψ_c in $\mathcal{Z}_{\text{Jint}}$ ergibt die Bedingung

$$\text{Es gibt ein } x \in \mathbb{Z}_{\text{Jint}}, \text{ so dass für alle } y \in \mathbb{Z}_{\text{Jint}} \text{ gilt } x \leq y.$$

$x = \mathsf{MININT}$ ist ein solches minimales Element.

Zu Aufgabe 4

Vorbemerkung: Das Symbol $\models$ ist überladen: $M \models \varphi$ kann bedeuten, dass eine Formel φ logische Konsequenz einer Menge M von Formeln ist; und es kann bedeuten, dass eine Interpretation M Modell einer Formel φ ist (φ ist wahr in M). In dieser Aufgabe ist letztere Bedeutung gemeint.

Wir wollen durch eine Formel φ festlegen, dass die eine Interpretation, die Modell ist, *genau* drei Elemente hat, d.h. *wenigstens* drei und *höchstens* drei Elemente hat.

[1] Dabei ist die Funktion $\text{mod}_{\mathcal{Z}_{\text{Jint}}} : \mathbb{Z} \to \mathbb{Z}_{\text{Jint}}$ gegeben durch $\text{mod}_{\mathcal{Z}_{\text{Jint}}}(x) \equiv x \pmod{2^{32}}$ mit $\mathsf{MININT} \leq \text{mod}_{\mathcal{Z}_{\text{Jint}}}(x) \leq \mathsf{MAXINT}$

Wenigstens 3 Elemente ist äquivalent zu der Aussage: "Es gibt drei Elemente, die paarweise verschieden sind", also:

$$\varphi_{\geq 3} := \exists x_1 \exists x_2 \exists x_3 \ (\neg x_1 \doteq x_2 \wedge \neg x_1 \doteq x_3 \wedge \neg x_2 \doteq x_3)$$

Höchstens 3 Elemente kann man äquivalent umformulieren zu: "Es gibt drei (möglicherweise identische) Elemente, so dass jedes Element gleich einem der drei ist", also:

$$\varphi_{\leq 3} := \exists x_1 \exists x_2 \exists x_3 \forall y \ (y \doteq x_1 \vee y \doteq x_2 \vee y \doteq x_3)$$

Die Konjunktion $\varphi_{\geq 3} \wedge \varphi_{\leq 3}$ ist eine mögliche Lösung. Da die quantifizierten Variablen x_1, x_2, x_3 in beiden Formeln notwendigerweise dieselben drei Objekte beschreiben, können sie auch in eine Quantifizierung zusammengefasst werden (was ja i.A. nicht geht):

$$\exists x_1 \exists x_2 \exists x_3 \ \big(\neg x_1 \doteq x_2 \wedge \neg x_1 \doteq x_3 \wedge \neg x_2 \doteq x_3 \wedge \forall y (y \doteq x_1 \vee y \doteq x_2 \vee y \doteq x_3)\big)$$

Zu Aufgabe 5

Zur Wiederholung die Definition unserer Folgerbarkeit:

$M \models_\Sigma A \quad :\Leftrightarrow \quad$ Jedes Modell von M ist auch Modell von A.

Etwas freier formuliert kann man sagen:
$M \models A$ heißt Für beliebiges I gilt: (wenn für alle β: $\mathrm{val}(M) = W$) dann (für alle β: $\mathrm{val}(A) = W$)
$M \models^\circ A$ heißt Für beliebiges I gilt: für jedes β gilt: (wenn $\mathrm{val}(M) = W$ dann $\mathrm{val}(A) = W$)

(a) Es gelte $A \models^\circ B$ und für eine Interpretation (D, I) gelte für alle Variablenbelegungen β dass $\mathrm{val}_{I,\beta}(A) = W$. Dann ist zu zeigen, dass auch $\mathrm{val}_{I,\beta}(B) = W$ für alle β.

Sei also $b : Var \to D$ eine Belegung. Nach Voraussetzung ist $\mathrm{val}_{I,b}(A) = W$. Wegen der lokalen Folgerbarkeit $A \models^\circ B$ muss für diese b auch $\mathrm{val}_{I,b}(B) = W$ gelten. Da b eine beliebige Belegung ist, gilt die Aussage auch für alle Belegungen β. □

(b) Wähle $A = p(x)$ und $B = \forall x(p(x))$.

Es gilt $A \models B$, weil aus der Gültigkeit von $\mathrm{val}_{I,\beta}(p(x)) = W$ für alle Belegungen β natürlich gilt, dass $I(p) = D$ und damit $\mathrm{val}_I(\forall x(p(x))) = W$ auch gilt.

Andererseits gilt $A \not\models^\circ B$, wie folgendes Gegenbeispiel beweist: Sei $D = \{d_1, d_2\}, I(p) = \{d_1\}, \beta(x) := d_2$ festgelegt. Dann gilt $\mathrm{val}_{I,\beta}(p(x)) = W$, aber $\mathrm{val}_{I,\beta}(\forall x(p(x))) = F$. Das widerspricht aber der lokalen Folgerbarkeit. □

(c) Dies folgt unmittelbar aus den Definitionen

$A \models^\circ B \iff$ Für beliebige I, β gilt: Aus $\mathrm{val}_{I,\beta}(A) = W$ folgt $\mathrm{val}_{I,\beta}(B) = W$
$\models^\circ A \to B \iff$ Für beliebige I, β gilt: $\mathrm{val}_{I,\beta}(A \to B) = W$
$\models A \to B \iff$ Für beliebige I, β gilt: $\mathrm{val}_{I,\beta}(A \to B) = W$

Nebenbemerkungen: Der Beweis zu (*c*) ist kurz, aber die Aussage ist nicht unwichtig! Während das **Deduktionstheorem** in der Aussagenlogik ($A \models B \iff \models A \to B$) noch gilt, gilt es der ursprünglichen Folgerbarkeit in der PL nicht mehr (siehe (b)). Die Einführung der lokalen Folgerbarkeit überträgt aber diese Eigenschaft in die PL.

In der klassischen PL wird diese Problematik weitgehend ignoriert, weil sie nur dann auftritt, wenn freie Variablen vorkommen. Das kann bei der Formalisierung vermieden werden. Bei der Betrachtung von algorithmischen Beweiskonzepten müssen solche Situationen aber in Betracht gezogen werden, weil Beweisstrategien häufig Quantoren entfernen oder Subformeln betrachten.