Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. Bernhard Beckert
Thorsten Bormer, Dr. Vladimir Klebanov, Dr. Mattias Ulbrich

Formale Systeme, WS 2014/2015

Übungsblatt 6

Dieses Übungsblatt wird in der Übung am 12.12.2014 besprochen.

Aufgabe 1

Zu einer prädikatenlogischen Formel G in Pränexnormalform bezeichne G_{sko} die durch Skolemisierung (genauer: durch wiederholte Anwendung von Lemma 4.61 im Skriptum) aus G konstruierte Formel in Skolem-Normalform.

(a) Geben Sie (ohne Beweis) jeweils eine prädikatenlogische Formel G in Pränexnormalform an, so dass Folgendes gilt:

- (i) $\neg G_{\text{sko}} \wedge G$ ist erfüllbar,
- (ii) $\neg G_{\text{sko}} \wedge G$ ist unerfüllbar,
- (iii) $G \rightarrow G_{\text{sko}}$ ist nicht allgemeingültig.

(b) Zeigen Sie, dass $G_{\text{sko}} \rightarrow G$ für alle prädikatenlogischen Formeln G in Pränexnormalform allgemeingültig ist.

Lösung 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: $G_{i+1} = \forall x_1 \dots \forall x_{l_i}\ \sigma(\varphi_i)$ wobei $\sigma(x) = f_i(x_1, \dots, x_{l_i})$ 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. $\square$

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 $\text{val}_{(I,\beta)}(\forall x\ A) = W$. Dann ist zu zeigen, dass $\text{val}_{(I,\beta)}(\forall x\ B) = W$.

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

Aufgabe 2

Berechnen Sie für die prädikatenlogischen Formeln (a) und (b) zunächst die Pränex-Normalform und dann die Skolem-Normalform.

(a) $(\forall x\ p(x) \to \forall x\ q(x)) \to \forall x(p(x) \to q(x))$

(b) $\exists x(\forall y\ p(x, y) \lor \exists z(p(x, z) \land \forall x\ p(z, x)))$

(c) Geben Sie eine Skolem-Normalform für (a) an, die sich von Ihrer Lösung zu (a) nicht nur durch Umbenennung und Äquivalenzumformung unterscheidet.

Lösung zu Aufgabe 2

Es gilt im Allgemeinen $G \equiv G_{\text{sko}}$ **nicht**, wie uns Aufgabe 1 zeigte.

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!).

(a) Überführen in Pränex-Normalform

$$\begin{array}{lll}
 & (\forall x\ p(x) \to \forall x\ q(x)) \to \forall x(p(x) \to q(x)) & \\
\equiv & (\forall x_1\ p(x_1) \to \forall x_2\ q(x_2)) \to \forall x_3(p(x_3) \to q(x_3)) & \text{Umbenennen der gebundenen Variablen} \\
\equiv & (\forall x_2 \exists x_1(p(x_1) \to q(x_2))) \to \forall x_3(p(x_3) \to q(x_3)) & \text{Innere Quantoren aus der Implikation ziehen} \\
 & & \text{Dabei erweist es sich als sinnvoll, } x_2 \text{ vor } x_1 \text{ zu setzen} \\
\equiv & \exists x_2 \forall x_1 \forall x_3((p(x_1) \to q(x_2)) \to (p(x_3) \to q(x_3))) & \text{Alle Quantoren nach außen} \\
\equiv & \exists x_2 \forall x_1 \forall x_3((p(x_1) \land \neg q(x_2)) \lor \neg p(x_3) \lor q(x_3)) & \text{Matrix in} \dots \\
\equiv & \exists x_2 \forall x_1 \forall x_3((p(x_1) \lor \neg p(x_3) \lor q(x_3)) \land \dots & \\
 & \quad \dots \land (\neg q(x_2) \lor \neg p(x_3) \lor q(x_3)) & \dots \text{KNF überführen}
\end{array}$$

Skolemisieren: für x_2 wird eine Konstante c eingeführt.

$$\forall x_1 \forall x_3((p(x_1) \lor \neg p(x_3) \lor q(x_3)) \land (\neg q(c) \lor \neg p(x_3) \lor q(x_3)))$$

(b) Überführen in Pränex-Normalform

$$\begin{array}{lll}
 & \exists x(\forall y\ p(x, y) \lor \exists z(p(x, z) \land \forall x\ p(z, x))) & \\
\equiv & \exists x(\forall y\ p(x, y) \lor \exists z(p(x, z) \land \forall w\ p(z, w))) & \text{Umbenennen gebundener Variablen} \\
\equiv & \exists x \exists z \forall y \forall w(p(x, y) \lor (p(x, z) \land p(z, w))) & \text{Herausziehen der Quantoren} \\
\equiv & \exists x \exists z \forall y \forall w((p(x, y) \lor p(x, z)) \land (p(x, y) \lor p(z, w))) & \text{Matrix in KNF}
\end{array}$$

Skolemisieren: für x wird eine Konstante c eingeführt und für z die Konstante d.

$$\forall y \forall w((p(c,y) \vee p(c,d)) \wedge (p(c,y) \vee p(d,w)))$$

(c) Nach der Umbenennung der Variablen (siehe (a)) können die Quantoren auch in anderer Reihenfolge behandelt werden:

$$\begin{array}{lll} & (\forall x_1\ p(x_1) \to \forall x_2\ q(x_2)) \to \forall x_3(p(x_3) \to q(x_3)) & \\ \equiv & \forall x_3((\forall x_1\ p(x_1) \to \forall x_2\ q(x_2)) \to (p(x_3) \to q(x_3))) & \text{Ziehe } x_3 \text{ zuerst heraus} \\ \equiv & \forall x_3((\exists x_1 \forall x_2(p(x_1) \to q(x_2))) \to (p(x_3) \to q(x_3))) & \text{Innere Quantoren aus der Implikation ziehen} \\ \equiv & \ldots & \text{s.o.} \\ \equiv & \forall x_3 \forall x_1 \exists x_2((p(x_1) \vee \neg p(x_3) \vee q(x_3)) \wedge \ldots & \\ & \quad \ldots \wedge (\neg q(x_2) \vee \neg p(x_3) \vee q(x_3)) & \end{array}$$

Skolemisieren: für x_2 wird eine Funktion f eingeführt, die als Argument die freien Variablen x_3 und x_1 erhält:

$$\forall x_1 \forall x_3((p(x_1) \vee \neg p(x_3) \vee q(x_3)) \wedge (\neg q(f(x_3,x_1)) \vee \neg p(x_3) \vee q(x_3))$$

Diese Lösung ist strukturell (nicht nur durch Umbenennung!) verschieden von der Lösung in (a), weil die Skolemfunktion 2 statt keinem Argument erhält.

Aufgabe 3

Transformieren Sie die folgende Formel schrittweise in Skolemnormalform.

$$\forall v \exists x \Big(\big((\forall z r(z,v)) \to (\forall x p(x,z)) \big) \to q(x) \vee r(v,x) \Big)$$

Bei welchem Schritt geht die die Äquivalenz zur ursprünglichen Formel verloren?

Lösung zu Aufgabe 3

$$\forall v \exists x \Big(\big((\forall z r(z,v)) \to \forall x\ p(x,z) \big) \to (q(x) \vee r(v,x)) \Big)$$

i. **All-Abschluss:**

$$\forall z \forall v \exists x \Big(\big(\forall z(r(z,v)) \to \forall x\ p(x,z) \big) \to (q(x) \vee r(v,x)) \Big)$$

ii. **Bereinigen:**

$$\forall z_1 \forall v \exists x \Big(\big(\forall z(r(z,v)) \to \forall x_1\ p(x_1,z_1) \big) \to (q(x) \vee r(v,x)) \Big)$$

iii. **Pränexnormalform:**

$$\begin{array}{ll} & \forall z_1 \forall v \exists x \Big(\big(\forall z(r(z,v)) \to \forall x_1\ p(x_1,z_1) \big) \to (q(x) \vee r(v,x)) \Big) \\ \equiv & \forall z_1 \forall v \exists x \Big(\neg \big(\neg(\forall z\ r(z,v)) \vee \forall x_1\ p(x_1,z_1) \big) \vee (q(x) \vee r(v,x)) \Big) \\ \equiv & \forall z_1 \forall v \exists x \Big(\big(\forall z(r(z,v)) \wedge \neg \forall x_1\ p(x_1,z_1) \big) \vee (q(x) \vee r(v,x)) \Big) \\ \equiv & \forall z_1 \forall v \exists x \Big(\big(\forall z(r(z,v)) \wedge \exists x_1\ \neg p(x_1,z_1) \big) \vee (q(x) \vee r(v,x)) \Big) \\ \equiv & \forall z_1 \forall v \exists x \forall z \exists x_1 \Big(\big(r(z,v) \wedge \neg p(x_1,z_1) \big) \vee (q(x) \vee r(v,x)) \Big) \end{array}$$

iv. **Skolemisieren:**

$$\begin{aligned} & \forall z_1 \forall v \exists x \forall z \exists x_1 \Big(\big(r(z,v) \wedge \neg p(x_1, z_1)\big) \vee \big(q(x) \vee r(v,x)\big) \Big) \\ \overset{\circ}{\equiv} \quad & \forall z_1 \forall v \forall z \Big(\big(r(z,v) \wedge \neg p(g(z_1,v,z), z_1)\big) \vee \big(q(f(z_1,v)) \vee r(v, f(z_1,v))\big) \Big) \end{aligned}$$

Dieser Schritt ist keine Äquivalenzumformung. Die zweite Formel ist nur erfüllbarkeitsäquivalent ($\overset{\circ}{\equiv}$) zur ersten.

v. **Matrix in KNF:**

$$\begin{aligned} & \forall z_1 \forall v \forall z \Big(\big(r(z,v) \wedge \neg p(g(z_1,v,z), z_1)\big) \vee \big(q(f(z_1,v)) \vee r(v, f(z_1,v))\big) \Big) \\ \equiv \quad & \forall z_1 \forall v \forall z \Big(\big(r(z,v) \vee q(f(z_1,v)) \vee r(v, f(z_1,v))\big) \wedge \big(\neg p(g(z_1,v,z), z_1) \vee q(f(z_1,v)) \vee r(v, f(z_1,v))\big) \end{aligned}$$

Aufgabe 4

Für eine Formel in Skolemnormalform muss die Matrix in konjunktiver Normalform sein. Wie kann man das in der Vorlesung vorgestellte Prinzip der erfüllbarkeitsäquivalenten kurzen KNF für die Aussagenlogik auf die Prädikatenlogik übertragen?

Lösung zu Aufgabe 4

Zur Erinnerung das Vorgehen im aussagenlogischen Fall: Eine binäre Teilformel $A \circ B$ in einer Formel F, wobei A, B Literale sind und $\circ \in \{\wedge, \vee, \rightarrow, \leftrightarrow\}$, wird durch ein neues Symbol X ersetzt und das neue Symbol definiert durch $X \leftrightarrow A \circ B$. Die Definition kann leicht in CNF gewandelt werden und konjunktiv zum Ergebnis verknüpft werden. Dieses Verfahren wird iterativ wiederholt, bis die ganze Formel in CNF vorliegt.

Man könnte versucht sein, dieses Verfahren direkt auf die PL zu übertragen und neue aussagenlogische Variablen (also nullstellige Prädikate) als Abkürzungen für Teilformeln einzuführen. Dies wird aber der veränderten Situation nicht gerecht, da in PL die Auswertung von Teilformeln von den auftretenden logischen Variablen abhängen kann, ein nullstelliges Prädikat aber einen davon unabhängigen Wert hat.

Folgendes Beispiel einer Formel in Skolemnormalform verdeutlicht, dass es nicht genügt, kKNF der AL zu erstellen:

$$\forall x \Big(\big((p(x) \vee p(x)) \vee \neg p(x)\big) \wedge \big(p(c) \wedge \neg p(d)\big) \Big) \tag{1}$$

Diese Formel hat ein Model (z.B. $M = (D, I)$ mit $D = \{o_1, o_2\}, I(c) = o_1, I(d) = o_2, I(p) = \{o_1\}$). Wenn man naiv das Verfahren der AL darauf anwenden würde, so käme dabei als Ergebnis heraus (für neue nullstellige Prädikatensymbole A, B, C):

$$\forall x \big(B \wedge C \wedge (A \leftrightarrow (p(x) \vee p(x))) \wedge (B \leftrightarrow (A \vee \neg p(x))) \wedge (C \leftrightarrow (p(c) \wedge \neg p(d)))\big) \tag{2}$$

Diese naive-falsche kKNF (2) von (1) hat kein Modell [1]. Die Formeln (1) und (2) sind nicht erfüllbarkeitsäquivalent.

Dieses Beispiel zeigt, dass nullstelligen Prädikate nicht als Platzhalter für Teilformeln stehen können. Sie erlauben es nicht, in Abhängigkeit von den logischen Variablen unterschiedlich auszuwerten.

Stattdessen muss man folgendermaßen vorgehen:

[1] Angenommen es gebe ein Modell $M = (D, I)$, dann gilt: $I \models \forall x(B \wedge C)$. Da x in B und C nicht auftritt, sind $I(B) = I(C) = W$. Das bedeutet aber auch, dass $I \models p(c)$ und $I \models \neg p(d)$. Wenn nun $I \models A$ gelten würde, so würde auch folgen, dass $I \models \forall x(p(x) \vee p(x))$, was im Widerspruch steht zu $I \models \neg p(d)$, also ist $I(A) = F$. Dann ist aber $I \models \forall x(B \leftrightarrow (A \vee \neg p(x)))$ dasselbe wie $I \models \forall x \neg p(x)$. Das steht aber im Widerspruch zu $I \models p(c)$. Alle Fälle führen also zu einem Widerspruch: es kann kein Modell von (2) geben.

Sei F seine PL1-Formel in Skolemnormalform. Die kurze KNF wird schrittweise gebildet, indem eine binäre Teilformel $A \circ B$ in F ersetzt wird. Die Teilformnen A und B seien wieder Literale, nur können nun in diesen logische Variablen $\bar{x}$ auftreten, wir schreiben daher jetzt $A[\bar{x}] \circ B[\bar{x}]$. Es wird wieder ein neues Prädikatensymbol X verwendet, das anstelle von $A[\bar{x}] \circ B[\bar{x}]$ eingesetzt wird. Dieses muss nun jedoch die auftretenden Variablen als Argument bekommen: $X(\bar{x})$. Als Definition wird $X(\bar{x}) \leftrightarrow (A \circ B)$ in CNF gewandelt und zur Lösung hinzugenommen. Dieses Verfahren wird iterativ wiederholt, bis die ganze Formel in CNF als F_{kknf} vorliegt. Dieser Teil ist wie in der Aussagenlogik.

Es bleibt zu zeigen, dass F und F_{kknf} erfüllbarkeitsäquivalent sind, wobei es genügt, dies für eine Ersetzung (X für $A[x] \circ B[\bar{x}]$) zu betrachten. Sei F_X die Formel, die aus F hervorgeht, indem $A[\bar{x}] \circ B[\bar{x}]$ durch $X(\bar{x})$ ersetzt wurde. Wenn $M = (D, I)$ ein Modell von F_{kknf} ist, so gilt insbesondere, dass $I \models F_X$ und $I \models \forall \bar{x}. X(\bar{x}) \leftrightarrow A[\bar{x}] \circ B[\bar{x}]$, für jede Variablenbelegung β ist $\mathrm{val}_{I,\beta}(X(\bar{x})) = \mathrm{val}_{I,\beta}(A[\bar{x}] \circ B[\bar{x}])$, daher gilt auch $\mathrm{val}_{I,\beta}(F) = \mathrm{val}_{I,\beta}(F_X)$.

Sei umgekehrt $M = (D, I)$ Modell von F. Es kann leicht zu einem Modell von F_{kknf} erweitert werden, wenn man $I(X) := \{\bar{d} \mid I, \beta^{\bar{d}}_{\bar{x}} \models A[\bar{x}] \circ B[\bar{x}]\}$ setzt. Diese Definition sorgt dafür, dass die Definition $\forall \bar{x}. X(\bar{x}) \leftrightarrow A[\bar{x}] \circ B[\bar{x}]$ von X erfüllt wird. Wie oben kann man dann schließen, dass für jede Variablenbelegung β gilt, dass $\mathrm{val}_{I,\beta}(X(\bar{x})) = \mathrm{val}_{I,\beta}(A[\bar{x}] \circ B[\bar{x}])$, und damit wieder $\mathrm{val}_{I,\beta}(F) = \mathrm{val}_{I,\beta}(F_X)$.