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

Formale Systeme, WS 2008/2009

Lösungen zum Übungsblatt 3

Dieses Blatt wurde in der Übung am 28.11.2008 besprochen.

Zu Aufgabe 1

(a) Aus dieser Klauselmenge kann direkt ein System von linearen Ungleichungen aufgestellt werden:

$$\begin{array}{ccccccccl}
a & + & b & + & (1-c) & \geq & 1 & & (1) \\
(1-a) & & & & & \geq & 1 & & (2) \\
a & + & b & + & c & \geq & 1 & & (3) \\
a & + & (1-b) & & & \geq & 1 & & (4) \\
\hline
a & & & & & \leq & 0 & & (2') \iff (2) \\
 & & b & & & \leq & a & & (4') \iff (4) \\
 & & & & c & \leq & a+b & & (1') \iff (1)
\end{array}$$

Äquivalenzumformungen (Umstellungen) ergeben die Gleichungen (2'), (4') und (1'), aus denen ersichtlich wird, dass $0 \geq a \geq b \geq c$ gilt. Eine solche Belegung mit nur nicht-positiven Werten kann aber unmöglich (3) erfüllen. Dieses Gleichungssystem hat also keine Lösung, also ist die Klauselmenge unerfüllbar.

N.B.: Für diesen Beweis haben wir das Gleichungssystem ganz allgemein über $\mathbb{Q}$ betrachtet. Es hat keine Lösungen in den rationalen Zahlen, die Klauselmenge muss (nach Vorlesung) also unit-resolvierbar sein.

(b) Negat der Formel und Umformen in Klauselmenge ergibt:

$$\{\{B, C, \neg D\},\ \{B, D\},\ \{\neg C, \neg D\},\ \{\neg B\}\}$$

Das System von Ungleichungen aufsetzen und Umformungen darauf anwenden ergibt:

$$\begin{array}{cccccccl}
b & + & c & + & (1-d) & \geq & 1 & (1) \\
b & + & d & & & \geq & 1 & (2) \\
 & & (1-c) & + & (1-d) & \geq & 1 & (3) \\
(1-b) & & & & & \geq & 1 & (4)
\end{array}$$

Aus (4) und weil alle Variablen den Wert 0 oder 1 haben, erhält man $b = 0$. Dies eingesetzt in (2) liefert $d = 1$. Damit erhält man aus (1), dass $c = 1$. Diese Werte eingesetzt in (3) führen zum Widerspruch.

Zu Aufgabe 2

Zur Wiederholung eine Kurzfassung des Davis-Putnam-Algorithmus:

```
function DPLL(S)
   if S is a consistent set of literals
      then return true;
   if S contains an empty clause
      then return false;
   for every unit clause l in S
      S := unit-propagate(l, S);
   l := chooseLiteral(S);
   return DPLL(S_{l←1}) OR DPLL(S_{l←0});
```

Die Ausgangsmenge S hat keine Einerklausel, daher muss ein Literal l gewählt werden, über das die Fallunterscheidung stattfinden soll. Geschickterweise wählen wir B, damit bei diesem Schritt dann Einerklauseln entstehen.

- $S_{B\leftarrow\mathbf{1}}$:

$\{\neg B, C\}$,	$\{C\}$	–
$\{\neg A, B, C\}$,	–	–
$\{\neg A, B, \neg C\}$,	–	–
$\{\neg B, \neg C\}$,	$\{\neg C\}$	$\square$
$\{A, B, C\}$,	–	–
$\{A, B, \neg C\}$	–	–

Im zweiten Schritt wurde hier die Einerklausel $\{C\}$ gewählt und wahr gemacht. Es entsteht die leere Klausel, also ist die Menge $S_{B\rightarrow\mathbf{1}}$ unerfüllbar.

- $S_{B\leftarrow\mathbf{0}}$:

		$S_{B\leftarrow\mathbf{0},A\leftarrow\mathbf{1}}$	$S_{B\leftarrow\mathbf{0},A\leftarrow\mathbf{0}}$
$\{\neg B, C\}$,	–	–	–
$\{\neg A, B, C\}$,	$\{\neg A, C\}$	$\{C\}$	–
$\{\neg A, B, \neg C\}$,	$\{\neg A, \neg C\}$	$\{\neg C\}$	–
$\{\neg B, \neg C\}$,	–	–	–
$\{A, B, C\}$,	$\{A, C\}$	–	$\{C\}$
$\{A, B, \neg C\}$	$\{A, \neg C\}$	–	$\{\neg C\}$

Hier gibt es für den zweiten Schritt keine Einerklauseln zum Wählen, so dass erneut eine Verzweigung (z.B. nach A) stattfinden muss. Danach entstehen dann komplementäre Einerklauseln, die wie oben aufgelöst werden.

Zu Aufgabe 3

(a) Benutze die Signatur $\Sigma = \{H, G, M, Z, D\}$ mit offensichtlicher Bedeutung.

(1) $H \vee G$

(2) $(G \wedge \neg M) \rightarrow Z$

(3) $\neg(Z \wedge D)$

(4) $M \rightarrow \neg D$

(5) $\neg(H \wedge D)$

(6) $Z \rightarrow (\neg G \wedge M)$

(7) $\neg Z \rightarrow D$

(b) Diese Aufgabe ist bereits so angelegt, dass die Umformung in KNF leicht erfolgen kann. Hier wird (für (c)) bereits die korrespondierende Klauselmenge angegeben:

[1]	$\{H, G\}$
[2]	$\{\neg G, M, Z\}$
[3]	$\{\neg Z, \neg D\}$
[4]	$\{\neg M, \neg D\}$
[5]	$\{\neg D, \neg H\}$
[6a]	$\{\neg Z, \neg G\}$
[6b]	$\{\neg Z, M\}$
[7]	$\{Z, D\}$

(c) Diese Klauselmenge S enthält keine Einerklausel, also muss eine Verzweigung stattfinden: $S_{H\leftarrow\mathbf{0}}$ und $S_{H\leftarrow\mathbf{1}}$ (andere wären auch wählbar)

(i) $S_{H\leftarrow\mathbf{0}}$:

$H \leftarrow \mathbf{0}$	$G \leftarrow \mathbf{1}$	$Z \leftarrow \mathbf{0}$	$D \leftarrow \mathbf{1}$	$M \leftarrow \mathbf{1}$
$\{G\}$	–	–	–	–
$\{\neg G, M, Z\}$	$\{M, Z\}$	$\{M\}$	$\{M\}$	–
$\{\neg Z, \neg D\}$	$\{\neg Z, \neg D\}$	–	–	–
$\{\neg M, \neg D\}$	$\{\neg M, \neg D\}$	$\{\neg M, \neg D\}$	$\{\neg M\}$	$\square$
–	–	–	–	–
$\{\neg Z, \neg G\}$	$\{\neg Z\}$	–	–	–
$\{\neg Z, M\}$	$\{\neg Z, M\}$	–	–	–
$\{Z, D\}$	$\{Z, D\}$	$\{D\}$	–	–

(ii) $S_{H\leftarrow\mathbf{1}}$:

$H \leftarrow \mathbf{1}$	$D \leftarrow \mathbf{0}$	$Z \leftarrow \mathbf{1}$	$G \leftarrow \mathbf{0}$	$M \leftarrow \mathbf{1}$
–	–	–	–	–
$\{\neg G, M, Z\}$	$\{\neg G, M, Z\}$	–	–	–
$\{\neg Z, \neg D\}$	–	–	–	–
$\{\neg D\}$	–	–	–	–
$\{\neg Z, \neg G\}$	$\{\neg Z, \neg G\}$	$\{\neg G\}$	–	–
$\{\neg Z, M\}$	$\{\neg Z, M\}$	$\{M\}$	$\{M\}$	–
$\{Z, D\}$	$\{Z\}$	–	–	–

Das Verfahren erreicht nun eine Situation, in der keine Klausel mehr zur Verfügung steht (N.B. Das ist sehr verschieden davon, dass die *leere Klausel* abgeleitet würde). Das bedeutet, dass jede Belegung die Wahlen des aktuellen Pfades beinhaltet eine erfüllende Belegung ist. In diesem Fall ist also die Belegung I mit

$$I(H) = W,\ I(D) = F,\ I(Z) = W,\ I(G) = F,\ I(M) = W$$

eine erfüllende Belegung. Das Davies-Putnam-Verfahren kann mit der Ausgabe "erfüllbar" terminieren.

Zu Aufgabe 4

(a) (i) Nicht kollisionsfrei, da

- x kommt in $\sigma(y)$ vor.
- y kommt im Wirkungsbereich des Quantors $\forall x$ vor.

(ii) Kollisionsfrei, das zweite Auftreten von x (dort gebundene Variable!) wird nicht ersetzt.

$$\sigma(F) = \exists y(p(y, f(g(x), c)) \vee \forall x \exists z(f(z, c) \doteq f(c, x)))$$

(iii) Kollisionsfrei (das zweite Vorkommen von y wird nicht ersetzt)

$$\sigma(F) = p(x, g(x)) \rightarrow \forall x(r(f(x, g(y))) \vee \exists y(r(f(x, y))))$$

(b) (i) unifizierbar. Robinson ergibt:

$\mu_0 = id$	$\mu(F) = q(f(f(\boxed{x}, y), x))$	$\mu_0(G) = q(f(f(\boxed{g(c)}, z), g(z)))$
$\mu_1 = \{x/g(c)\}$	$\mu_1(F) = q(f(f(g(c), \boxed{y}), g(c)))$	$\mu_1(G) = q(f(f(g(c), \boxed{z}), g(z)))$
$\mu_2 = \{x/g(c), y/z\}$	$\mu_2(F) = q(f(f(g(c), z), g(\boxed{c})))$	$\mu_1(G) = q(f(f(g(c), z), g(\boxed{z})))$
$\mu_3 = \{x/g(c), y/c, z/c\}$	$\mu_3(F) = \mu_3(G) = q(f(f(g(c), c), g(c)))$	

Man muss beachten, dass man weitere Ersetzungen nicht einfach zur Menge hinzunehmen kann, sondern auch auf die darin enthaltenen Terme anwenden muss.
Beispielsweise: $\mu_3 = \{x/\boldsymbol{z}, y/g(c)\} \circ \{z/\boldsymbol{c}\} = \{x/\boldsymbol{c}, y/g(c), z/c\}$

(ii) Im ersten Schritt des Robinsonalgorithmus erhält man:

$$\begin{aligned} \mu_1 &= \{x/f(y)\} \\ \mu_1(F) &= p(f(y), y) \\ \mu_1(G) &= p(f(y), f(f(y)) \end{aligned}$$

Nun aber muss der Algorithmus abbrechen, weil $D(\{\mu(F), \mu(G)\}) = \{y, f(f(y))\}$ und die sind nicht unifizierbar, weil y eine Variable ist und in $f(f(y))$ auftritt.

(iii) unifizierbar. Der Robinsonalgorithmus mit Zwischenergebnissen:

$\mu_0 = id$	$\mu_0(F) = p(\boxed{x}, f(y, x))$	$\mu_0(G) = p(\boxed{f(y, c)}, f(g(z), f(g(z), c)))$
$\mu_1 = \{x/f(y, c)\}$	$\mu_1(F) = p(f(y, c), f(\boxed{y}, x))$	$\mu_2(G) = p(f(y, c), f(\boxed{g(z)}, f(g(z), c)))$
$\mu_2 = \{x/f(g(z), c), y/g(z)\}$	$\mu_2(F) = \mu_2(G) = p(f(g(z), c), f(g(z), f(g(z), c)))$	

Zu Aufgabe 5

(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 $z_1 \xrightarrow{I(p)} z_2 \xrightarrow{I(p)} \dots \xrightarrow{I(p)} z_r$, 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 $(d_0 \xrightarrow{I(p)} d_1 \xrightarrow{I(p)} \dots)$ 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 6

(a) $x \doteq \texttt{if}\ \phi\ \texttt{then}\ t_1\ \texttt{else}\ t_2 \ \equiv\ (\phi \rightarrow x \doteq t_1) \wedge (\neg\phi \rightarrow x \doteq t_2) \equiv (\phi \wedge x \doteq t_1) \vee (\neg\phi \wedge x \doteq t_2)$

(b) Sei (D,I) eine beliebige PL-Interpretation.
$\mathrm{val}_{I,\beta}(\exists x.(x \doteq c \ \wedge \ p(f(x)))) = W$
gdw. es gibt ein $d \in D$ mit $\mathrm{val}_{I,\beta_x^d}(x \doteq c \ \wedge \ p(f(x))) = W$
gdw. es gibt ein $d \in D$ mit $\mathrm{val}_{I,\beta_x^d}(x) = \mathrm{val}_{I,\beta_x^d}(c)$ und $\mathrm{val}_{I,\beta_x^d}(f(x)) \in I(p)$
gdw. es gibt ein $d \in D$ mit $d = I(c)$ und $I(f)(d) \in I(p)$
gdw. $I(f)(I(c)) \in I(p)$
gdw. $val_{I,\beta}(p(f(c))) = W$.

(c) Für die Eliminierung aller bedingten Terme in einer Formel $\sigma \in For$, verfahre folgendermaßen:

Solange es einen bedingten Term gibt, vollziehe diese beiden Schritte:

(i) wähle einen bedingten Term $\vartheta = \texttt{if}\ \phi\ \texttt{then}\ t_1\ \texttt{else}\ t_2$ aus, der in einer **atomaren**[1] Unterformel α von σ auftritt.

(ii) Ersetze α durch die Formel $\exists x((\phi \rightarrow x \doteq t_1) \wedge (\neg\phi \rightarrow x \doteq t_2) \wedge \alpha[\vartheta \leftarrow x])$, wobei in $\alpha[\vartheta \leftarrow x]$ alle Vorkommen von ϑ durch die Variable x ersetzt worden sind.

[1]Zur Erinnerung: Das heißt eine Formel der Form $p(t_1, t_2, ..., t_n)$ oder $t_1 \doteq t_2$ für Terme t_i

oder (ii') Ersetze α durch die Formel $((\phi \to \alpha[\vartheta \leftarrow t_1]) \wedge (\neg\phi \to \alpha[\vartheta \leftarrow t_2]))$.

Natürlich gibt es weitere Variationen. (ii) hat gegenüber (ii') den Vorteil, dass pro Ersetzung nur eine Variante von α eingeführt wird statt zwei. Somit wächst die Formel in (ii) linear, während sie in (ii') exponentiell wächst.

Zu Aufgabe 7

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.

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

also

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

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

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

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

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

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 z.B. mit dem AL-Sequenzenkalkül untersucht werden kann:

$$
\begin{array}{l}
\;\blacktriangleright ((r \rightarrow s) \rightarrow r) \rightarrow (r \rightarrow (s \rightarrow r)) \\
(r \rightarrow s) \rightarrow r \blacktriangleright r \rightarrow (s \rightarrow r) \\
(r \rightarrow s) \rightarrow r,\ r \blacktriangleright s \rightarrow r \\
(r \rightarrow s) \rightarrow r,\ r,\ s \blacktriangleright r \\
\text{Axiom}
\end{array}
$$

Dieser Beweis zeigt, dass die Formel aussagenlogisch allgemeingültig ist, also eine **Tautologie** ist.

Zu Aufgabe 8

1. $\forall x(x \doteq a \vee x \doteq b \vee x \doteq c)$

2. $\exists x(\text{kills}(x, a))$
   Man kann argumentieren: Eigentlich gehört aber die Aussage 1. (Stichwort Hausbewohner) noch mit in die Kodierung, so dass die (in Kombination mit (1) äquivalente) Formel $\exists x(\text{kills}(x, a) \wedge (x \doteq a \vee x \doteq b \vee x \doteq c) \equiv \text{kills}(a, a) \vee \text{kills}(b, a) \vee \text{kills}(c, a)$ noch exakter formalisiert.

3. $\forall x \forall y(\text{kills}(x, y) \rightarrow \text{hates}(x, y))$

4. $\forall x(\text{hates}(a, x) \rightarrow \neg\,\text{hates}(c, x))$

5. $\forall x \forall y(\text{kills}(x, y) \rightarrow \neg\,\text{richer}(x, y))$

6. $\forall x((\neg\,\text{richer}(x, a) \vee \text{hates}(a, x)) \rightarrow \text{hates}(b, x))$

7. $\neg \exists x \forall y(\text{hates}(x, y))$