Aufgabensammlung für die Vorlesung Formale Systeme

Bernhard Beckert

8. Februar 2017

Aufgabe 0

Melden Sie sich beim ILIAS-Online-Kurs an und machen Sie sich mit den Funktionen der dortigen Foren vertraut. In den Foren können Sie Fragen zur Vorlesung stellen, welche von Ihren Kommilitonen und uns gelesen und beantwortet werden. Bitte beachten Sie, dass die Praxisaufgaben eigenständig bearbeitet werden müssen, und insofern insbesondere keine (Teil-)Lösungen zu den Praxisaufgaben den Foren gepostet werden dürfen.

Kapitel 1

Aussagenlogik

1.1 Einleitende Beispiele

Aufgabe 1

Prüfen Sie die *Allgemeingültigkeit* des als aussagenlogische Formel $(A \wedge (A \rightarrow B)) \rightarrow B$ dargestellten Modus Ponens.

Aufgabe 2

(a) Zeigen Sie, dass folgende Formel erfüllbar ist, indem Sie ein Modell angeben.

$$((A \rightarrow (A \wedge \neg A)) \vee (A \leftrightarrow B)) \rightarrow B$$

(b) Zeigen Sie durch aussagenlogische Umformungen, dass folgende Formel unerfüllbar ist.

$$(\neg A \wedge (A \vee \neg A)) \wedge (\neg(A \leftrightarrow B) \wedge \neg B)$$

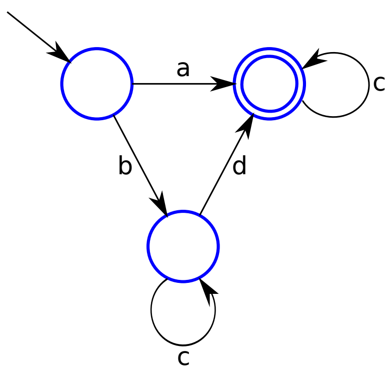
(c) überprüfen Sie, ob folgende Formeln Tautologien sind. Begründen Sie Ihre Antwort.

(i) $(A \rightarrow B) \rightarrow ((B \rightarrow C) \rightarrow (A \rightarrow C))$

(ii) $(A \wedge \neg A \rightarrow B) \wedge C$

Aufgabe 3

Geben sei nebenstehender Automat.



Die Zustände in diesem Automaten sind aussagenlogische Interpretationen über der Signatur $\Sigma = \{P_1, P_2, P_3\}$. Die Zustandsübergänge des Automaten sind mit Aktionen a, b, c und d annotiert, welche beschreiben, wie sich eine Interpretation beim Übergang von einem Zustand in den nächsten ändert. Für unseren Automaten sind die Aktionen folgendermaßen definiert:

$$a : I \mapsto I' \text{ mit } I'(P_1) = I(P_1), I'(P_2) = I(\neg P_2), I'(P_3) = I(P_3)$$
$$b : I \mapsto I' \text{ mit } I'(P_1) = I(P_1), I'(P_2) = I(\neg P_2), I'(P_3) = I(\neg P_3)$$
$$c : I \mapsto I' \text{ mit } I'(P_1) = I(P_1), I'(P_2) = I(P_2), I'(P_3) = I(P_3)$$
$$d : I \mapsto I' \text{ mit } I'(P_1) = I(P_1), I'(P_2) = I(P_2), I'(P_3) = I(\neg P_3)$$

Für jede Aktion definieren wir eine Formel, die den jeweiligen Zustandsübergang beschreibt. Dazu führen wir zu jeder aussagenlogischen Variable P_i eine gestrichene Version P_i' ein, welche den Wert von P_i im Folgezustand beschreibt:

$$\begin{aligned}
f_a(P_1, P_2, P_3, P_1', P_2', P_3') &\equiv \quad P_1' \leftrightarrow P_1 \land P_2' \leftrightarrow \neg P_2 \land P_3' \leftrightarrow P_3 \\
f_b(P_1, P_2, P_3, P_1', P_2', P_3') &\equiv \quad P_1' \leftrightarrow P_1 \land P_2' \leftrightarrow \neg P_2 \land P_3' \leftrightarrow \neg P_3 \\
f_c(P_1, P_2, P_3, P_1', P_2', P_3') &\equiv \quad P_1' \leftrightarrow P_1 \land P_2' \leftrightarrow P_2 \land P_3' \leftrightarrow P_3 \\
f_d(P_1, P_2, P_3, P_1', P_2', P_3') &\equiv \quad P_1' \leftrightarrow P_1 \land P_2' \leftrightarrow P_2 \land P_3' \leftrightarrow \neg P_3
\end{aligned}$$

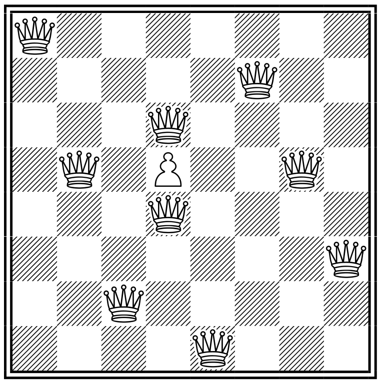
Gelte nun im Startzustand $P_1 \land P_2 \land P_3$.

(a) Geben Sie eine Formel an, die beschreibt, welche Zustände nach zwei Schritten erreicht werden können.

(b) Zeigen Sie, dass in allen Zuständen, die nach zwei Schritten erreicht werden können, $P_1 \land \neg P_2$ gilt.

Aufgabe 4

Eine Abwandlung des sogenannten *8-Damen-Problems* (siehe Skriptum) ist das *9-Damen-Problem*: Es geht darum, neun Damen so auf einem üblichen Schachbrett zu plazieren, dass sie sich gegenseitig nicht bedrohen. Bei 9 Damen ist dies jedoch nur möglich, wenn sich zusätzlich ein Bauer auf dem Brett befindet. Steht der Bauer auf gerader Linie zwischen zwei Damen, so bedrohen sich diese nicht. Eine mögliche Lösung des Problems zeigt die Abb. rechts.



Formalisieren Sie das 9-Damen-Problem als ein Erfüllbarkeitsproblem der Aussagenlogik. Orientieren Sie sich dabei an der Lösung des 8-Damen-Problems aus dem Skriptum.

Aufgabe 5

Die Linux-Distribution openSUSE verwendet für die Paketverwaltung einen SAT-Solver. Das Verfahren ist unter `https://en.opensuse.org/openSUSE:Libzypp_satsolver_basics` beschrieben.

Formalisieren Sie das folgende Szenario mittels Aussagenlogik, benutzen Sie die kursiv gedruckten Begriffe als Variablennamen:

1. Der Benutzer möchte den Mail-Client *mutt* installieren.
2. Der Mail-Client erfordert einen *smtp daemon*.
3. Ein gültiger *smtp daemon* ist entweder *sendmail*, *postfix* oder *exim* (es kann nur einer gleichzeitig installiert werden).
4. *sendmail* macht das installierte Legacy-Paket *sendmail-tls* obsolet, das aber nicht deinstalliert werden darf.

Kann die Paketverwaltung die Wünsche des Benutzers erfüllen?

Aufgabe 6

Gegeben sei eine Landkarte mit L Ländern, die mit den Zahlen von 0 bis $L-1$ bezeichnet werden. Die binäre Relation $Na(i, j)$ trifft auf zwei Länder i und j zu ($0 \leq i, j < L$), wenn sie benachbart sind. Die Landkarte soll nun mit den **drei** Farben *rot*, *grün* und *blau* so eingefärbt werden, dass keine zwei benachbarten Länder dieselbe Farbe erhalten.

Geben Sie – in Abhängigkeit von L und Na – eine aussagenlogische Formel F an, so dass F genau dann erfüllbar ist, wenn eine Färbung der geforderten Art möglich ist.

Hinweis: Die Landkarte muss nicht zwei-dimensional sein, d. h. der durch $Na(i, j)$ gegebene Graph muss nicht planar einbettbar sein.

Aufgabe 7

Wir betrachten eine Variante von Sudoku. Dabei müssen in das 9×9-Sudoku-Gitter die Zahlen von **0** bis 9 so eingetragen werden, dass

- in jeder der neun Spalten
- in jeder der neun Reihen
- und in jeder der neun Regionen

alle Zahlen einmal vorkommen. Für jede der neun Regionen existiert dazu ein besonderes Feld, in das *zwei* Zahlen eingetragen werden müssen. (Dieses Feld wird dabei für die vorliegende Aufgabe nicht vorgegeben, sondern soll aus dem Modell der erzeugten Formel abgelesen werden können.)

Formalisieren Sie die Regeln dieses Logikrätsels als ein Erfüllbarkeitsproblem der Aussagenlogik. Orientieren Sie sich dabei an der in der Vorlesung vorgestellten Formalisierung für Sudoku.

1.2 Interpolanten

Aufgabe 8

Geben Sie zwei Formeln A und B so an, dass $A \to B$ eine Tautologie ist und dass es mindestens zwei nicht äquivalente Interpolanten für $A \to B$ gibt. Geben Sie für Ihr Beispiel zwei solche Interpolanten an und zeigen Sie, dass diese tatsächlich Interpolanten von $A \to B$ sind.

Aufgabe 9

Zeigen Sie:

Sind C_1 und C_2 Interpolanten für die Implikation $A \to B$, dann sind auch $C_1 \vee C_2$ und $C_1 \wedge C_2$ Interpolanten für $A \to B$.

Aufgabe 10

Sei $A \to B$ eine Tautologie.
Seien $Q_1, \ldots, Q_k$ alle Variablen in B, die nicht in A vorkommen. Sind c_i Konstanten aus $\{\mathbf{1}, \mathbf{0}\}$ dann bezeichne $B[c_1, \ldots, c_k]$, wie im Beweis von Lemma 2.22 aus dem Skriptum, die Formel, die aus B entsteht, wenn man alle Vorkommen von Q_i durch c_i ersetzt. Außerdem sei:

$$D \equiv \bigwedge_{(c_1,\ldots,c_n)\in\{\mathbf{1},\mathbf{0}\}^n} B[c_1, \ldots, c_n]$$

Zeigen Sie, dass D eine Interpolante von $A \to B$ ist.

1.3 Normalformen

Aufgabe 11

Formen Sie die folgenden Formeln in die disjunktive sowie konjunktive Normalform um. Verwenden Sie dafür die in der Vorlesung vorgestellten Äquivalenzen. Kennzeichnen Sie klar die durchgeführten Schritte.

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

(b) $(p \to q) \wedge (q \to s)$

(c) $(p \to (\neg p \vee q)) \wedge \neg(p \to q)$

(d) $(p \wedge \neg(q \wedge r)) \vee (\neg p \wedge \neg((q \wedge r) \vee \neg q))$

Aufgabe 12

Für $n \in \mathbb{N}$ ist die Formel

$$A_n = P_1 \leftrightarrow P_2 \leftrightarrow P_3 \leftrightarrow \ldots \leftrightarrow P_{n-1} \leftrightarrow P_n$$

gegeben. Sei A_n^{kknf} eine zu A_n erfüllbarkeitsäquivalente Formel in kurzer KNF. Dabei sei die kurze KNF mit einer geringfügigen Modifikation des Verfahrens aus der Vorlesung hergestellt worden, bei dem für je eine Äquivalenz zwischen zwei Atomen ein neues Atom Q_i eingeführt wird.

(a) Geben Sie A_4^{kknf} an.

(b) Wie viele Disjunktionen enthält A_n^{kknf}?

Aufgabe 13

Gegeben sei die Formel

$$A = (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R) \ .$$

Zeigen Sie, dass die Normalformen

$$\begin{aligned} A' &= (P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge R) \\ A'' &= (P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (Q \wedge R) \end{aligned}$$

äquivalent zu A sind.

Aufgabe 14

Sei S eine Menge von Klauseln. Für ein Literal L sei $\bar{L}$ das zu L *komplementäre* Literal, d.h.

$$\bar{L} = \begin{cases} \neg A & \text{falls } L = A \\ A & \text{falls } L = \neg A \end{cases}$$

Ein Literal L heißt *isoliert* in S (im Englischen *pure literal in* S), wenn $\bar{L}$ in keiner Klausel in S vorkommt. Eine Klausel C in S heißt *isoliert*, wenn sie ein isoliertes Literal enthält.

Ist S eine unerfüllbare Klauselmenge und C eine isolierte Klausel in S, dann ist auch $S \setminus \{C\}$ unerfüllbar.

Aufgabe 15

Definition. Eine unerfüllbare Klauselmenge S heißt eine *minimal unerfüllbare* Klauselmenge, wenn jede echte Teilemenge $S_0 \subset S$ erfüllbar ist.

Sei S eine minimal unerfüllbare Klauselmenge dann gilt

1. S enthält keine tautologische Klausel, d.h. keine Klausel C, die für eine aussagenlogische Variable P sowohl P selbst als auch $\neg P$ enthält.

2. für jede Interpretation I gibt es Klauseln $C, D \in S$ und ein Literal L, so dass $I(C) = W$, $I(D) = F$, L kommt in C und $\bar{L}$ kommt in D vor.

Aufgabe 16

In der Vorlesung wurde ausgenutzt, dass jede aussagenlogische Formel sich effizient in eine erfüllbarkeitsäquivalente kurze konjunktive Normalform umwandeln lässt.

Kann es eine auch eine kurze *disjunktive* Normalform geben, die effizient (d. h. in polynomieller Zeit) aus einer beliebigen aussagenlogischen Formel berechnet werden kann?

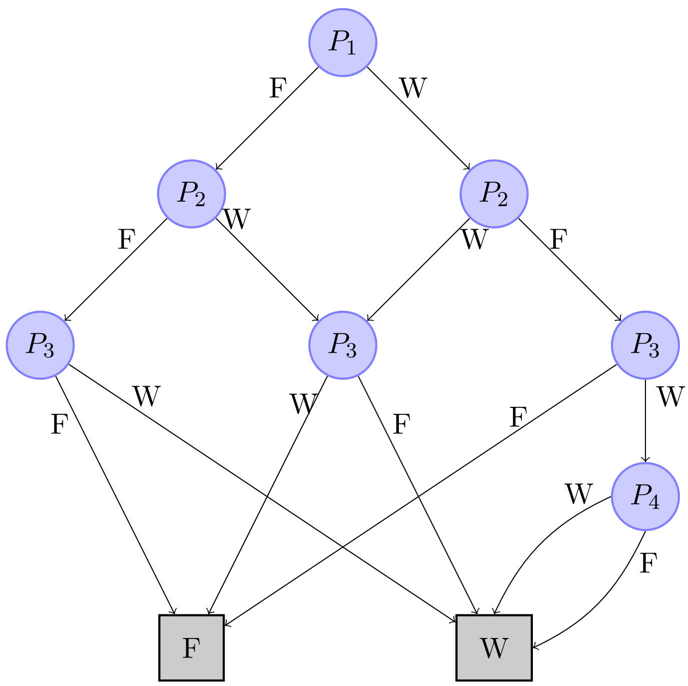
Aufgabe 17

Formulieren Sie ein Kriterium für die *Erfüllbarkeit* einer Äquivalenzformel A. Begründen Sie, dass das Kriterium notwendig und hinreichend ist.

1.4 Shannongraphen

Aufgabe 18

Konstruieren Sie zu dem folgenden Shannongraphen den reduzierten Shannongraphen (mit der gleichen Variablen-Ordnung $P_1 < P_2 < P_3 < P_4$). Verwenden Sie das Verfahren aus der Vorlesung. Geben Sie alle Zwischenschritte an, d. h. geben Sie nach jedem Reduktionsschritt den daraus resultierenden Graphen an.



Aufgabe 19

Gegeben sei die Formel

$$F = (A \wedge (B \vee \neg C)) \to D$$

und die Ordnung $A < B < C < D$ auf den aussagenlogischen Variablen.

Erstellen Sie einen reduzierten Shannongraphen (BDD) für F.

Aufgabe 20

Geben Sie den reduzierten Shannon Graphen (BDD) an, der äquivalent ist zu der sh-Formel

$$sh(P_3, P_2, P_1)$$

und die Ordnung $P_1 < P_2 < P_3$ auf den aussagenlogischen Variablen respektiert.

Aufgabe 21

Gegeben sei für $n \in \mathbb{N}$ die **Paritätsfunktion**[1] $f_n : \{0,1\}^n \to \{0,1\}$ durch

$$f_n(P_1, P_2, \ldots, P_n) = \begin{cases} 1 & \text{falls die Summe } P_1 + \cdots + P_n \text{ ungerade ist} \\ 0 & \text{sonst} \end{cases}$$

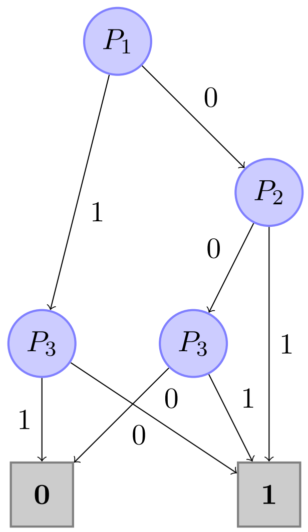
Geben Sie einen reduzierten Shannongraphen für die Funktion f_4 an.

Aufgabe 22

Geben Sie zu folgendem Shannongraphen je eine äquivalente aussagenlogische Formel in

(a) disjunktiver Normalform und

(b) konjunktiver Normalform an.



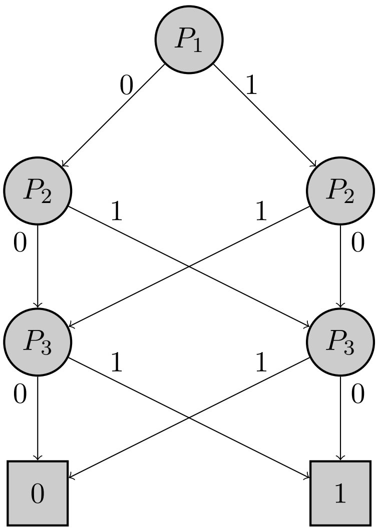
Aufgabe 23

Geben Sie zu dem nebenstehend dargestellten Shannongraphen je eine äquivalente aussagenlogische Formel in

(a) disjunktiver Normalform und

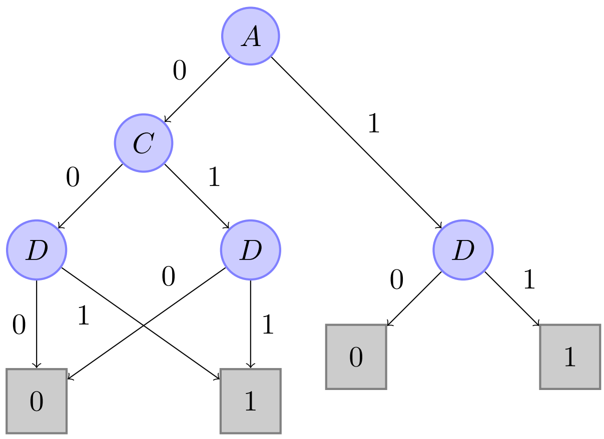
(b) konjunktiver Normalform an.

[1] Streng genommen müsste diese Funktion auf der Menge $\{F, W\}$ operieren, aber die Formulierbarkeit als Summe legt diese etwas andere Schreibweise nahe.



Aufgabe 24

Geben Sie zu dem dargestellten Shannongraphen den reduzierten Shannongraphen an.



1.5 Hornformeln

Aufgabe 25

Gegeben seien folgende Formeln der AL:

(a) $A \vee \neg A$

(b) $(A \vee B) \wedge (\neg A \vee \neg B \vee C) \wedge (A \vee \neg B \vee C) \wedge \neg C$

(c) $(A \vee B) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge \neg C$

Entscheiden Sie, welche der angegebenen Formeln Hornformeln sind. Wie könnte man den Markierungsalgorithmus heranziehen, um die Erfüllbarkeit der nicht-Hornformeln zu entscheiden?

Aufgabe 26

überprüfen Sie folgende Hornformeln auf Erfüllbarkeit. Benutzen Sie dazu den in der Vorlesung vorgestellten Markierungsalgorithmus. Geben Sie im Falle der Erfüllbarkeit ein Modell an. Im Fall von Teilaufgabe (d) bringen Sie die Formel zunächst in die Implikationsschreibweise.

(a) $(P_1 \wedge P_2 \to P_3) \wedge (P_1 \wedge P_3 \to P_4) \wedge P_1 \wedge (P_2 \to P_4) \wedge P_3$

(b) $P_5 \wedge (P_2 \wedge P_4 \rightarrow \mathbf{0}) \wedge (P_5 \rightarrow P_1) \wedge (P_2 \wedge P_5 \rightarrow P_4) \wedge (P_1 \rightarrow P_2)$

(c) $(P_3 \rightarrow \mathbf{0}) \wedge (P_1 \rightarrow P_4) \wedge (P_2 \wedge P_4 \rightarrow P_3) \wedge (P_4 \rightarrow P_5)$

(d) $A \wedge (\neg A \vee B) \wedge (\neg B \vee \neg C \vee D) \wedge \neg E \wedge (\neg A \vee \neg C) \wedge D$

Aufgabe 27

Seien $I, J : \Sigma \rightarrow \{W, F\}$ aussagenlogische Interpretationen, dann wird das **Produkt** $I \times J : \Sigma \rightarrow \{W, F\}$ von I und J definiert durch:

$$(I \times J)(P) = \begin{cases} W & \text{falls } I(P) = J(P) = \text{W} \\ F & \text{sonst} \end{cases} \qquad \text{für alle } P \in \Sigma$$

Zeigen Sie: Eine Disjunktion φ von aussagenlogischen Literalen ist genau dann eine Hornklausel, wenn für alle Interpretationen I, J gilt:

$$\text{val}_I(\varphi) = \text{val}_J(\varphi) = W \implies \text{val}_{I \times J}(\varphi) = W$$

Damit haben Sie im wesentlichen gezeigt, dass die durch Hornklauseln darstellbaren Formeln charakterisiert sind durch die Abgeschlossenheit unter der Produktbildung ihrer Interpretationen.

Hinweis: $I \times J$ heißt Produkt, weil wenn man W mit 1 und F mit 0 identifiziert, gerade der Homomorphismus $\text{val}_{I \times J}(\phi) = \text{val}_I(\phi) \cdot \text{val}_J(\phi)$ *gilt.*

1.6 DPLL

Aufgabe 28

Zeigen Sie mit Hilfe des David-Putnam-Verfahrens, dass die Klauselmenge

$$\begin{array}{llll} \{ & \{\neg B, C\}, & \{\neg A, B, C\}, & \{\neg A, B, \neg C\}, \\ & \{\neg B, \neg C\}, & \{A, B, C\}, & \{A, B, \neg C\} \quad \} \end{array}$$

unerfüllbar ist.

Aufgabe 29

Die (aussagenlogische) Klauselmenge S bestehe aus den folgenden Klauseln:

(1)	$\{ P,\ Q,\ T \}$	(5)	$\{ \neg R,\ \neg S,\ T \}$
(2)	$\{ \neg P \}$	(6)	$\{ \neg R,\ P,\ \neg T \}$
(3)	$\{ \neg Q,\ R \}$	(7)	$\{ R,\ \neg T \}$
(4)	$\{ \neg R,\ S \}$		

Zeigen Sie mit Hilfe des Davis-Putnam-Verfahrens, dass S unerfüllbar ist.

Kapitel 2

Prädikatenlogik

2.1 Syntax

Aufgabe 30

Handelt es sich bei den folgenden Zeichenketten um Terme oder Formeln der Prädikatenlogik erster Stufe? Welche Vorkommen welcher Variablen sind frei, welche gebunden?

(a) $j(f(x), g(x), h(z), k)$

(b) $\forall y \exists p\, p(y)$

(c) $\forall x \forall z\, (g(f(z), f(y)) \to z)$

(d) $\forall x \exists y\, (p(f(x)) \to q(y, z))$

Die Signatur enthalte dabei folgende Symbole: $F_\Sigma = \{f, g, h, i, j, k\}$, $P_\Sigma = \{p, q, r\}$. Die Stelligkeiten der Symbole können Sie als korrekt verwendet annehmen. Außerdem sei $\mathit{Var} = \{x, y, z\}$.

Aufgabe 31

(a) Betrachten Sie jeweils die folgenden Substitutionen σ und Formeln F. Falls σ für F kollisionsfrei ist, geben Sie $\sigma(F)$ an; andernfalls geben Sie an, wo eine Kollision auftritt.

(i)	$\sigma = \{x/c,\ y/f(c, g(x))\}$	$F = \forall x(p(g(x), f(x, y)) \vee q(x))$
(ii)	$\sigma = \{x/f(g(x), c)\}$	$F = \exists y(p(x, y) \vee \exists z \forall x(f(z, c) \doteq f(c, x)))$
(iii)	$\sigma = \{y/g(x),\ z/g(y)\}$	$F = p(x, y) \to \forall x(q(f(x, z)) \vee \exists y(q(f(x, y))))$

(b) Betrachten Sie jeweils die folgenden Formeln F und G. Geben Sie einen allgemeinsten Unifikator μ sowie das Ergebnis $\mu(F) = \mu(G)$ der Unifikation an, falls sie unifizierbar sind.

(Hierbei sind a, b Konstanten, f, g, h Funktionssymbole und v, x, y, z Variablen.)

(i)	$F = f(x, z, z)$	$G = f(g(a, y), h(v), h(y))$
(ii)	$F = f(g(x, z), z, h(b, x))$	$G = f(g(a, y), h(v, a), y)$
(iii)	$F = g(x, y)$	$G = g(f(y), f(x))$
(iv)	$F = f(g(y), h(y, g(y)))$	$G = f(z, h(g(x), g(g(x))))$

Aufgabe 32

Geben Sie eine Folge

$$(s_1, t_1),\ (s_2, t_2),\ (s_3, t_3),\ \ldots$$

von Termpaaren an, so dass:

- Für alle $n \in \mathbb{N}$ sind s_n und t_n unifizierbar.

- Die Größe der Terme s_n und t_n wächst (höchstens) linear in n.
- Die Größe des Ergebnisses $\sigma_n(s_n)$ bzw. $\sigma_n(t_n)$ der Unifikation (σ_n ist ein allgemeinster Unifikator von s_n und t_n) wächst exponentiell in n.

Hinweis: Betrachten Sie die Terme $g(x_1, x_2)$ und $g(c, f(x_1, x_1))$, und verallgemeinern Sie.

Aufgabe 33

Berechnen Sie für die Substitutionen θ, σ jeweils die Komposition $\sigma \circ \theta$.

(a) $\theta = \{x/a,\ y/x\}$, $\quad\sigma = \{v/f(u),\ u/z\}$

(b) $\theta = \{v/h(x,\ y),\ w/b,\ s/y\}$, $\quad\sigma = \{x/d,\ y/d,\ r/f(v)\}$

(c) $\theta = \{u/g(y,\ x),\ v/y,\ w/y\}$, $\quad\sigma = \{u/d,\ x/b,\ y/f(v)\}$

(d) $\theta = \{x/y,\ y/v\}$, $\quad\sigma = \{x/a,\ y/b,\ v/u\}$

Aufgabe 34

Eine Substitution θ ist allgemeiner als eine Substitution σ, geschrieben $\theta \geqslant \sigma$, wenn es eine Substitution τ gibt, so dass $\tau \circ \theta = \sigma$.

(a) Es seien die folgenden Substitutionen gegeben:

$$\mu_1 = \{x/y,\ r/y,\ u/y,\ v/f(z)\}$$
$$\mu_2 = \{r/x,\ y/x,\ u/x,\ v/f(x),\ z/x\}$$
$$\mu_3 = \{x/a,\ y/a,\ z/b,\ u/a,\ v/f(b),\ r/a\}$$

Prüfen Sie für jedes mögliche Paar (μ_i, μ_j), ob $\mu_i \geqslant \mu_j$, und geben Sie ggf. die entsprechende Substitution τ an.

(b) Zeigen Sie folgende Eigenschaften von $\geqslant$:

(i) Reflexivität: $\theta \geqslant \theta$ für alle θ.

(ii) Transitivität: Falls $\theta \geqslant \sigma$ und $\sigma \geqslant \mu$, dann auch $\theta \geqslant \mu$ für alle θ, σ, μ.

Sie dürfen dabei die Assoziativität der Substitutionskomposition $\circ$ benutzen.

2.2 Semantik

Aufgabe 35

Sei Σ eine prädikatenlogische Signatur mit einem zweistelligen Prädikatensymbol p.

Kommt doppelt vor, wird bald gelöscht.

(a) Geben Sie eine prädikatenlogische Formel F über Σ an, so dass gilt: Eine Interpretation (D, I) ist genau dann Modell von F, wenn die Relation $I(p)$ eine *strikte Halbordnung* (also transitiv und irreflexiv) auf D ist.

(b) Geben Sie eine erfüllbare prädikatenlogische Formel G über Σ an, so dass gilt: Wenn eine Interpretation (D, I) Modell von G ist, dann ist D unendlich.

Aufgabe 36

In der Vorlesung wurden die beiden Interpretationen $\mathcal{Z}$ und $\mathcal{Z}_{\text{Jint}}$ der Signatur, die $+, *$ (Funktionssymbole) und $\leq$ (Prädikatsymbol) enthält, vorgestellt.

Überprüfen Sie, ob die folgenden Formeln in $\mathcal{Z}$ und $\mathcal{Z}_{\text{Jint}}$ erfüllt sind oder nicht. Begründen Sie jeweils kurz.

(a) $\forall y(\exists k_1(2 * k_1 \doteq y) \to \exists k_2(2 * k_2 \doteq y + 2))$

(b) $\forall x(0 \leq x \to x \leq x * 2)$

(c) $\exists x \forall y(x \leq y)$

Aufgabe 37

Geben Sie für jede der folgenden Formeln an, ob sie erfüllbar, allgemeingültig, unerfüllbar oder keine Formel der Prädikatenlogik erster Stufe ist. Begründen Sie Ihre Entscheidungen.

(a) $\phi_a = \exists x \neg(\forall x(f(x) \doteq f(x)))$

(b) $\phi_b = \forall x(f(x) \doteq c) \to f(f(f(c))) \doteq c$

(c) $\phi_c = \forall x(\forall y(p(x) \vee \neg p(y)))$

(d) $\phi_d = \forall x((p(x) \doteq \mathbf{1} \wedge p(x) \doteq q(x)) \to q(x) \doteq \mathbf{1})$

(e) $\phi_e = ((r \to s) \to r) \to (r \to (s \to r))$

Bemerkung: p, q, r, s sind Prädikatssymbole, f, g Funktionssymbole (jeweils mit der richtigen Stelligkeit), c ein Konstantensymbol (nullstelliges Funktionssymbol) und x, y sind Variablen. Eine Formel kann mehr als eine der genannten Eigenschaften haben.

Aufgabe 38

Finden Sie eine Formel φ der Prädikatenlogik erster Stufe mit leeren Vokabular, so dass $M \models \varphi$ genau dann gilt, wenn M genau drei Elemente hat. Die Formel φ enthält also als einziges Relationszeichen das Symbol $\doteq$ für die Gleichheit.

Aufgabe 39

Sei Σ eine prädikatenlogische Signatur mit einem zweistelligen Prädikatensymbol p.

(a) Geben Sie eine prädikatenlogische Formel F über Σ an, so dass gilt: Eine Interpretation (D, I) ist genau dann Modell von F, wenn die Relation $I(p)$ eine *strikte Halbordnung* (also transitiv und irreflexiv) auf D ist.

(b) Geben Sie eine erfüllbare prädikatenlogische Formel G über Σ an, so dass gilt: Wenn eine Interpretation (D, I) Modell von G ist, dann ist D unendlich.

Aufgabe 40

Gegeben sei die Signatur $\Sigma = (F_\Sigma, P_\Sigma, \alpha_\Sigma)$ mit

- $F_\Sigma = \{b, f\}$,
- $P_\Sigma = \{p\}$ und
- $\alpha_\Sigma(b) = 0, \alpha_\Sigma(f) = 1, \alpha_\Sigma(p) = 1$.

(a) Wieviele verschiedene Herbrand-Interpretationen über Σ gibt es?

(b) Wieviele verschiedene Herbrand-Modelle besitzt die Formel

$$p(f(f(b))) \wedge \forall x(p(x) \to p(f(x))) \ ? \tag{2.1}$$

Zählen Sie sie auf.

(c) Jedes Herbrand-Modell über Σ der Formel (2.1) ist auch Modell der Formel

$$\forall x(p(f(f(x)))) \ . \tag{2.2}$$

Geben Sie eine (Nicht-Herbrand-)Interpretation an, die Modell von (2.1) aber nicht von (2.2) ist.

Aufgabe 41

Gegeben sei die Struktur $I = \langle U, A \rangle$ folgendermaßen:

$$\begin{aligned}
&U = \mathbb{R},\\
&p^I = \{z \mid z \geq 0\},\\
&q^I = \{(x,y) \mid x = y\},\\
&f^I(z) = z^2,\\
&g^I(x,y) = x + y,\\
&x^I = \sqrt{2},\\
&y^I = -1
\end{aligned}$$

Bestimmen Sie den Wert folgender Terme und Formeln:

1. $I(g(f(x), f(y)))$
2. $I(\forall x \ p(f(x)))$
3. $I(\exists z \ \forall x \ \forall y \ q(g(x,y), z))$
4. $I(\forall y \ (q(f(x), y) \rightarrow p(g(x,y))))$

Aufgabe 42

Zeigen Sie mit Hilfe des Kompaktheitssatzes, dass es keine prädikatenlogische Formel geben kann, die genau die zusammenhängenden, gerichteten Graphen charakterisiert. Ein Graph ist zusammenhängend, wenn es für je zwei verschiedene Knoten des Graphen einen Pfad zwischen diesen Knoten gibt.

Sei dazu eine prädikatenlogische Signatur $\Sigma = (\emptyset, \{kante\}, kante \mapsto 2)$ gegeben. Weiterhin sei die Domäne D festgelegt als die Menge der Knoten. Die Interpretation des Prädikatsymbols $kante(u, v)$ ist wahr gdw. im Graph eine gerichtete Kante zwischen u und v verläuft.

Zeigen Sie, dass es keine Formel F gibt, so dass für jede Interpretation (D, I) über Σ gilt:

(D, I) ist Modell von $F \Leftrightarrow$ der durch (D, I) beschriebene Graph: $(D, I(kante))$ ist zusammenhängend.

2.3 Formalisierung

Aufgabe 43

Tante Agathe wurde in ihrem Haus tot aufgefunden. Nach bisherigen Ermittlungen gilt Folgendes als sicher:

1. Im Haus lebten nur Agathe, ihr Butler und Onkel Charles.
2. Agathe wurde von einem Hausbewohner getötet.
3. Wer jemanden tötet, hasst sein Opfer.
4. Charles hasst niemanden, den Agathe hasste.

5. Der Täter ist niemals reicher als das Opfer.
6. Der Butler hasst alle, die nicht reicher als Agathe sind oder die Agathe hasste.
7. Kein Bewohner des Hauses hasst(e) alle Hausbewohner.

Gegeben ist ferner die prädikatenlogische Signatur $\Sigma_{Agathe} = (F, P, \alpha)$ mit

- $P = \{\text{kills}, \text{hates}, \text{richer}\}$
- $F = \{a, b, c\}$
- $\alpha(a) = \alpha(b) = \alpha(c) = 0, \qquad \alpha(\text{kills}) = \alpha(\text{hates}) = \alpha(\text{richer}) = 2$

Formalisieren Sie die Aussagen 1-7 in Prädikatenlogik mit dem Vokabular aus Σ_{Agathe}.

Aufgabe 44

In dieser Aufgabe sollen Aussagen über Verwandtschaftsbeziehungen in Prädikatenlogik formalisiert werden. Die Signatur $\Sigma_{\text{Verwandtschaft}}$ enthalte die zweistelligen Prädikate *mutter* und *vater*. Formeln werden in Interpretationen ausgewertet, in denen das Universum eine Menge von Personen ist. Dabei bedeutet die Aussage $I(\mathit{mutter})(a, b)$ (bzw. $I(\mathit{vater})(a, b)$), dass a die Mutter (der Vater) von b ist. Formalisieren Sie in der Signatur $\Sigma_{\text{Verwandtschaft}}$:

(a) „Jede Person hat genau eine Mutter.“

(b) „Niemand kann ein Elternteil seiner eigenen Eltern sein.“

(c) „Dagobert ist der Onkel von Donald.“
Seien dazu *Donald* und *Dagobert* zwei Konstantensymbole in $\Sigma_{\text{Verwandtschaft}}$.

Aufgabe 45

Formalisieren Sie die folgenden Aussagen in Prädikatenlogik:

(a) Wenn jeder arme Mensch einen reichen Vater hat, dann gibt es einen reichen Menschen, der einen reichen Großvater hat.

(b) In einer Bar gibt es stets eine Person P, so dass, falls P etwas trinkt, alle anwesenden Personen etwas trinken.

(c) Jeder Barbier rasiert alle Personen, außer denen, die sich selbst rasieren.

Aufgabe 46

Seien p und q Prädikate über den natürlichen Zahlen. Die Semantik von p und q sei gegeben durch:

- $p(x, y)$ gilt genau dann, wenn x die Zahl y teilt und
- $q(x, y)$ gilt genau dann, wenn $x \leq y$ ist.

Für alle Interpretationen I, deren Universum die natürlichen Zahlen sind und für die gilt, dass

$$p^I = \{(x, y) \mid x \text{ teilt } y\} \text{ und}$$
$$q^I = \{(x, y) \mid x \leq y\}$$

ist, muss z.B. für die im Aufgabenteil (a) gebildete Formel F gelten, dass F^I genau dann wahr ist, wenn y^I eine Primzahl ist.

Formalisieren Sie mit Hilfe der Prädikatenlogik:

(a) y ist eine Primzahl.

(b) y ist eine gerade Zahl.

(c) ggt ist der größte gemeinsame Teiler der beiden Zahlen x und y.

(d) kgV ist das kleinste gemeinsame Vielfache der beiden Zahlen x und y.

(e) x und y sind teilerfremde Zahlen.

(f) zwischen zwei verschiedenen natürlichen Zahlen liegt stets eine natürliche Zahl

2.4 Normalformen

Aufgabe 47

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) $G \to G_{\text{sko}}$ ist nicht allgemeingültig.

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

Aufgabe 48

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) $\exists x(\forall y\ p(x,y) \vee \exists z(p(x,z) \wedge \forall x\ p(z,x)))$

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

Aufgabe 49

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?

Aufgabe 50

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?

Kapitel 3

Kalküle

3.1 Hilbertkalkül

Aufgabe 51

(a) Zeigen Sie mit Hilfe des Hilbertkalküls aus der Vorlesung die Aussage

$$\models \neg A \to (A \to B) \ . \tag{3.1}$$

Verwenden Sie dabei das in der Vorlesung vorgestellte Deduktionstheorem.

(b) Zeigen Sie mit Hilfe des Hilbertkalküls aus der Vorlesung die Aussage

$$\models (\neg A \to A) \to A \ .$$

Sie können in der Ableitung die Aussage (3.1) aus (a) als Axiom verwenden.

Hinweis: Diese Teilaufgabe ist kniffliger als (a). Es empfiehlt sich bei der Ableitung mit Gleichung (3.1) zu beginnen, worin B durch einen geeigneten Term ersetzt wurde.

Aufgabe 52

Angenommen, für Hilbertkalküle R_1 und R_2 gilt[1]

(a) für R_1: $(\phi \to \psi) \vdash_{R_1} \neg(\psi \to \neg\phi)$ (für alle Formeln ϕ und ψ)

(b) für R_2: $M \vdash_{R_2} (\phi \wedge \neg\phi)$

Kann R_1 korrekt sein? Kann R_1 vollständig sein? Wie verhält es sich bezüglich Korrektheit und Vollständigkeit mit R_2 in Abhängigkeit der Formelmenge M?

3.2 Resolutionskalkül für Aussagenlogik

Aufgabe 53

Zeigen Sie mithilfe des Resolutionskalküls

(a) die Unerfüllbarkeit der Klauselmenge

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

(b) die Allgemeingültigkeit der Formel

$$\neg A \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge \neg D) \vee (D \wedge B) \vee (\neg B \wedge C) \ ,$$

(c) die Allgemeingültigkeit der Formel

$$(A \to (B \to C)) \to ((A \to B) \to (A \to C)) \ .$$

[1] R_1 und R_2 sind hier Kalküle mit anderen Regeln und/oder Axiomen als der aus der Vorlesung.

Aufgabe 54

Bei der Wahl eines guten Passworts sei folgendes zu beachten:

(1) Das Passwort muss sicher sein, und man muss es sich merken können. (2) Passwörter beinhalten Zahlen oder Sonderzeichen oder beides. (3) Ist das Passwort kurz und enthält keine Sonderzeichen, dann ist es nicht sicher. (4) Ein Passwort mit Sonderzeichen kann man sich nicht merken. (5) Ein Passwort mit Zahlen muss kurz sein, damit man es sich merken kann.

(a) Formalisieren Sie die Anforderungen an ein Passwort in Aussagenlogik. Verwenden Sie dazu die folgenden aussagenlogischen Variablen mit der angegebenen Bedeutung.

Das Passwort...

Si ist sicher

M kann man sich merken

Z enthält Zahlen

So enthält Sonderzeichen

K ist kurz

(b) Zeigen Sie mit Hilfe des Resolutionskalküls, dass ein solches Passwort nicht existieren kann.

Aufgabe 55

Widerlegen Sie die Vollständigkeit einer Variante des Resolutionskalküls, bei der jede Klausel nur einmal zur Resolution verwendet werden darf.

Hinweis: Suchen Sie ein Gegenbeispiel (nicht ganz einfach!).

Aufgabe 56

Bei der Wahl eines guten Passworts sei folgendes zu beachten:

(1) Das Passwort muss sicher sein, und man muss es sich merken können. (2) Passwörter beinhalten Zahlen oder Sonderzeichen oder beides. (3) Ist das Passwort kurz und enthält keine Sonderzeichen, dann ist es nicht sicher. (4) Ein Passwort mit Sonderzeichen kann man sich nicht merken. (5) Ein Passwort mit Zahlen muss kurz sein, damit man es sich merken kann.

(a) Formalisieren Sie die Anforderungen an ein Passwort in Aussagenlogik. Verwenden Sie dazu die folgenden aussagenlogischen Variablen mit der angegebenen Bedeutung.

Das Passwort...

Si ist sicher

M kann man sich merken

Z enthält Zahlen

So enthält Sonderzeichen

K ist kurz

(b) Zeigen Sie mit Hilfe des Resolutionskalküls, dass ein solches Passwort nicht existieren kann.

Aufgabe 57

Man könnte versucht sein, zur Verkürzung von Beweisen im Resolutionskalkül zwei Resolutionsanwendungen in einer neuen Regel zusammenzufassen:

$$\frac{C_1 \cup \{P, Q\}, \quad C_2 \cup \{\neg P, \neg Q\}}{C_1 \cup C_2}$$

Zeigen Sie, dass diese Regel nicht korrekt ist.

Aufgabe 58

Wir nennen einen Resolutionsschritt

$$\frac{C_1 \cup \{P\}, C_2 \cup \{\neg P\}}{C_1 \cup C_2}$$

einen *negativen Resolutionschritt* wenn die Klausel $C_2 \cup \{\neg P\}$ nur negative Literale enthält.

Beweisen oder widerlegen Sie die Vollständigkeit einer Variante des Resolutionskalküls, bei der nur negative Resolutionsschritte erlaubt sind.

Aufgabe 59

Die lineare Resolution ist eine Variante der Resolution: Bei der Resolventenbildung muss eine der Elternklauseln entweder die Startklausel (eine zu Beginn frei gewählte Klausel) oder die Resolvente aus dem vorangegangenen Resolutionsschritt sein. Die jeweils andere Elternklausel kann frei gewählt werden.

Es gilt: Für jede unerfüllbare Klauselmenge gibt es eine Ableitung der leeren Klausel durch lineare Resolution, aber nicht jede angefangene Ableitung mit linearer Resolution kann zu einem Beweis geschlossen werden. Es kann also Sackgassen in der Beweissuche geben (lineare Resolution ist *nicht beweiskonfluent*). Insbesondere spielt die Wahl der Startklausel dabei eine Rolle; die Wahl einer ungünstigen Startklausel kann in die Sackgasse führen.

(a) Geben Sie für die Klauselmenge

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

eine Ableitung der leeren Klausel $\square$ mittels linearer Resolution an.

(b) Geben Sie für die Klauselmenge aus (a) einen angefangenen linearen Resolutionsbeweis an, der nicht zur leeren Klausel $\square$ führen kann, also eine Sackgasse darstellt.

3.3 Resolutionskalkül für Prädikatenlogik

Aufgabe 60

Zeigen Sie die Unerfüllbarkeit der folgenden Klauselmenge mittels des Resolutionskalküls:

$$\begin{array}{llll} \{ & \{p(x_1, f(x_1))\}, & \{\neg p(x_2, x_3), \neg p(x_3, x_4), p(x_2, x_4)\}, & \{p(g(d), x_8)\}, \\ & \{\neg p(c, c), \neg p(d, g(x_7))\}, & \{p(x_5, x_6), \neg p(x_6, x_5)\} & \} \end{array}$$

Darin sind p ein zweistelliges Prädikatensymbol, $x_1, \ldots, x_8$ Variablen, f, g einstellige Funktionssymbole und c, d Symbole für konstante Funktionen.

Geben Sie für alle Resolutionsschritte den verwendeten Unifikator an.

Aufgabe 61

Zeigen Sie die Unerfüllbarkeit der folgenden Klauselmenge mittels des Resolutionskalküls *in vier Resolutionsschritten*:

$$\{\{p(a)\}, \quad \{\neg p(x), p(f(x))\}, \quad \{\neg p(f(f(f(f(a)))))\}\}$$

Geben Sie für alle Resolutionsschritte den verwendeten Unifikator an.

Aufgabe 62

Es sei eine prädikatenlogische Signatur gegeben, die die einstelligen Prädikatensymbole p, q und r enthält und das einstellige Funktionssymbol f. Zeigen Sie mit Hilfe des prädikatenlogischen Resolutionskalküls, dass die Formel

$$\big((\forall x\ p(x)) \to (\forall x\ q(x))\big) \land \big(\forall x(q(x) \to r(x))\big) \to \big(\exists x(p(x) \to r(f(x)))\big)$$

allgemeingültig ist.

Aufgabe 63

Betrachten wir – nur für diese Übungsaufgabe – die folgende geänderte Version der Definition von $Res(M)$ aus Definition 5.17 im Skript:

$$Res'(M) = \ \{B \mid \text{ es gibt Klauseln } C_1, C_2 \text{ aus } M, \text{ so dass } B \text{ eine Resolvente von } C_1, C_2 \text{ ist.}\}$$

Gegenüber der offiziellen Definition ist die Variantenbildung, d.h. die Umbennung der Variablen in C_1, C_2, weggefallen. Wie wird dadurch Korrektheit und Vollständigkeit des Kalküls beeinflußt? Geben Sie ein Beispiel an, das dies belegt.

3.4 Tableaukalkül für die Aussagenlogik

Aufgabe 64

Zeigen Sie oder widerlegen Sie mithilfe des Tableaukalküls für die Aussagenlogik die Allgemeingültigkeit folgender Formeln. Falls eine der Formeln nicht allgemeingültig ist, geben Sie eine erfüllende Belegung ihres Negats als Gegenbeispiel an.

(a) $((A \to B) \to C) \to (B \to C)$

(b) $(B \to C) \to ((A \to B) \to C)$

Aufgabe 65

(a) Geben Sie für den sh-Operator korrekte und vollständige Regeln für den aussagenlogischen Tableaukalkül an.

(b) Zeigen Sie die Korrektheit und Vollständigkeit Ihrer Regeln aus Teilaufgabe (a).

3.5 Tableaukalkül für die Predikatenlogik

Aufgabe 66

Das folgende Rätsel stammt aus dem Buch "To Mock a Mockingbird – and Other Logic Puzzles" von Raymond Smullyan.

Der Verein der Barbiere unterliegt folgenden Regeln:

1. Wenn ein Mitglied A ein Mitglied B rasiert – dabei spielt es keine Rolle, ob A ungleich B ist – dann rasieren alle Mitglieder auch A.
2. Vier der Mitglieder sind: Guido, Lorenzo, Petrucio und Cesare.
3. Guido rasiert Cesare.

Zeigen sie, dass aus diesen Regeln folgt:

4. Petrucio rasiert Lorenzo.

(a) Formalisieren Sie 1.–4. in Prädikatenlogik. Die Domäne sei die Menge aller Personen.

Verwenden Sie dazu

- das einstellige Prädikatsymbol $m(\cdot)$ mit der Bedeutung $I(m(X)) = W$ gdw. X Mitglied des Clubs ist.
- das zweistellige Prädikatsymbol $r(\cdot, \cdot)$ mit der Bedeutung $I(r(X, Y)) = W$ gdw. Person X Person Y rasiert.
- die Konstanten g, l, p, c für die Bezeichnung der Barbiere Guido, Lorenzo, Petrucio und Cesare.

(b) Zeigen sie mit Hilfe des Tableaukalküls der Prädikatenlogik, dass aus den Formeln zu 1.–3. die Aussage 4. folgt.

Aufgabe 67

Zeigen Sie mit Hilfe des prädikatenlogischen Tableaukalküls, dass die Formel

$$\forall y \forall x \forall z \big((p(x, z) \to p(y, z)) \to q(x, y) \big) \wedge \neg \exists y \forall x (q(x, x) \vee r(y))$$

unerfüllbar ist.

Aufgabe 68

In der Vorlesung ist folgender Satz als Beispiel für ein Ableitbarkeitsproblem vorgestellt worden und mithilfe des Resolutionskalküls bewiesen worden:

Jede transitive (1), symmetrische (2) und endlose (3) binäre Relation ist reflexiv (4).

Formalisiert als Folgerung in Prädikatenlogik lautet die Aussage folgendermaßen:

$$\begin{aligned}
\{ \quad & \forall x \forall y \forall z \big(r(x, y) \wedge r(y, z) \to r(x, z) \big) \;, && (3.1)\\
& \forall x \forall y \big(r(x, y) \to r(y, x) \big) \;, && (3.2)\\
& \forall x \exists y \big(r(x, y) \big) \; \} && (3.3)\\
\models \quad & \forall x \big(r(x, x) \big) && (3.4)
\end{aligned}$$

Zeigen Sie mit Hilfe des prädikatenlogischen Tableaukalküls, dass die oben stehende Aussage gilt.

Aufgabe 69

In der Abschlussregel des Tableaukalküls (Definition 5.4 im Skriptum) wird gefordert, dass eine schließende Substitution immer auf das gesamte Tableau angewandt werden muss, und nicht etwa nur auf den Pfad, der gerade geschlossen wird.

Geben Sie eine geschlossene[2], *nicht* allgemeingültige PL1-Formel φ und ein zugehöriges Tableau für 0φ an, das (fälschlicherweise) geschlossen[2] werden könnte, wenn die Abschlusssubstitution nur auf jeweils einen Pfad angewendet werden müsste.

Aufgabe 70

Vervollständigen Sie das folgende Tableau, bis es geschlossen ist. Notieren Sie dabei:

[2]Beachten Sie: Das Wort „geschlossen“ hat hier zwei unterschiedliche Bedeutungen. Eine Formel ist geschlossen, wenn sie keine freien Variablen enthält. Ein Tableau ist geschlossen, wenn jeder seiner Äste einen Widerspruch $1\psi, 0\psi$ enthält.

- bei jeder Erweiterung, durch welche Regelanwendung eine Formel auf dem Tableau entstanden ist,
- bei Abschlüssen die beiden Partner,
- die schließende Substitution.

$$
\begin{array}{c}
1\, \neg p(a,b) \rightarrow \exists x\, (p(b,x) \vee q(a,x)) \;{\scriptstyle 1} \\
| \\
0\, \exists y\, \exists x\, (p(x,y) \vee \exists z\, q(x,z)) \;{\scriptstyle 2}
\end{array}
$$

3.6 Sequenzenkalkül

Aufgabe 71

Gegeben sei die Formel

$$F \quad = \quad ((\neg B \wedge \neg A) \vee C) \rightarrow ((\neg A \rightarrow B) \rightarrow C)$$

Zeigen Sie mithilfe des Sequenzenkalküls, dass F allgemeingültig ist.

Kapitel 4

Java Modeling Language

Aufgabe 72

Zur Implementierung einer Personendatenbank wird folgende Java-Klasse verwendet:

```
class Person {
   int age;
   boolean isFemale;
   Person father;
   Person mother;
   Person[] children;

   void celebrateBirthday() {
      age ++;
   }

   void becomeParentTo(Person child) {
      children = addToArray(child);
      if(isFemale) {
         child.mother = this;
      } else {
         child.father = this;
      }
   }

   Person[] addToArray(Person child) {
      Person[] result = new Person[children.length + 1];
      System.arraycopy(children, 0, result, 0, children.length);
      result[children.length] = child;
      return result;
   }
}
```

(a) Formulieren Sie für die Methode `celebrateBirthday()` einen Methoden-Vertrag in JML, der folgendes besagt: *Die Methode darf in jedem Zustand aufgerufen werden. Nach Ausführung der Methode ist der Wert des Feldes* `age` *um genau 1 erhöht, alle anderen Speicherstellen sind unberührt geblieben.*

(b) Beschreiben Sie das Verhalten der Methode `becomeParentTo(Person)` möglichst präzise mit einem JML-Vertrag.

(c) Vervollständigen Sie folgenden Methodenvertrag für die Methode `addToArray(Person)`:

```
/*@ public normal_behaviour
  @  ensures \result.length == ...
  @  ensures (\forall int i; 0 <= i && ...
  @  assignable \nothing;
  @*/
```

Aufgabe 73

(a) Schreiben Sie eine Java-Methode, die die folgende Spezifikation erfüllt: Gegeben ein Array a von ganzzahligen Werten $a_1, \ldots, a_n$ soll die Methode Index i_0 des ersten Auftretens der Zahl 0 liefern, also den Index i_o ausgeben, so dass

(i) $a_{i_0} = 0$ und

(ii) $a_k \neq 0$ für alle $0 \leq k < i_0$.

Falls keiner der Werte $a_1, \ldots, a_n$ gleich 0 ist, so soll die Methode -1 zurückliefern.

(b) Schreiben Sie einen JML-Methodenvertrag, der diese Spezifikation wiedergibt.

Aufgabe 74

Für eine Anwendung im Bankenbereich wird die folgende Klasse zur Modellierung von Geldbeträgen verwendet:

```
class Betrag {
   int euros;
   int cents;

   Betrag(int euros, int cents) {
      this.euros = euros;
      this.cents = cents;
   }

   Betrag add(Betrag b) { ... }
}
```

Es ist das Ziel, die Benutzung dieser Klasse auf *normalisierter Beträge* einzuschränken. Ein Betrag heißt normalisiert, wenn er nicht-negativ ist und der Cent-Anteil im Betrag weniger als einen Euro ausmachen. Die Einschränkung in der Verwendung der Klasse soll mittels Annotatationen in JML formal umgesetzt werden.

(a) Geben Sie eine JML-Klasseninvariante für die Klasse `Betrag` an, die besagt, dass das Betrag-Objekt normalisiert ist.

(b) Geben Sie einen Vertrag für die Method `add` an, der besagt, dass der Betrag, der als Eregebnis zurückgeliefert wird, der Summe des Arguments und des Aufrufempfängers entspricht.

Die Methode darf ein neues Ergebnisobjekt erstellen, darf aber keine existierenden Speicherstellen abändern.

(c) In einem ersten Versuch wird die Methode `add` nun folgendermaßen implementiert:

```
Betrag add(Betrag b) {
   int e = euros + b.euros;
   int c = cents + b.cents;
   return new Betrag(e, c);
}
```

Warum verstößt diese Implementierung gegen die JML-Spezifikation und wie kann das repariert werden?

Kapitel 5

Reduktionssysteme

Aufgabe 75

Gegeben sei die Relation $\succ = \{(a,b),(b,d),(c,b),(d,a),(d,e)\}$.

(a) Bestimmen Sie

(i) $\rightarrow$ (die reflexive, transitive Hülle von $\succ$),

(ii) $\stackrel{+}{\rightarrow}$ (die transitive Hülle von $\succ$) und

(iii) $\leftrightarrow$ (die reflexive, transitive, symmetrische Hülle von $\succ$).

(b) Zeigen Sie, dass $\succ$ lokal konfluent sowie konfluent ist.

(c) Erweitern Sie die Relation $\succ$ um ein Tupel, so dass sie zwar lokal konfluent bleibt, aber nicht mehr konfluent ist.

Aufgabe 76

Seien $N := \mathbb{N} \setminus \{1,0\}$ und $N' := \mathbb{N} \setminus \{0\}$ Teilmengen der natürlichen Zahlen. Die Relation $\succ \subseteq \mathbb{N} \times \mathbb{N}$ ist definiert als

$$a \succ b \quad :\Longleftrightarrow \quad b \text{ teilt } a \text{ und } a \neq b \qquad (a, b \in \mathbb{N}).$$

Betrachten Sie nun die Reduktionssysteme $(N, \succ)$ und $(N', \succ)$:

(a)	Ist $(N, \succ)$ lokal konfluent?	Ist $(N', \succ)$ lokal konfluent?
(b)	Ist $(N, \succ)$ konfluent?	Ist $(N', \succ)$ konfluent?
(c)	Ist $(N, \succ)$ noethersch?	Ist $(N', \succ)$ noethersch?
(d)	Besitzt $(N, \succ)$ irreduzible Elemente? Wenn ja, welche?	Besitzt $(N, \succ)$ irreduzible Elemente? Wenn ja, welche?

Begründen Sie Ihre Antworten kurz.

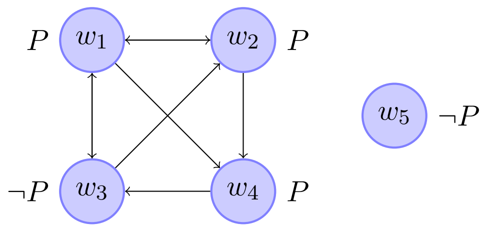
Bemerkung: Mit $\succ$ ist jeweils die Einschränkung auf $N \times N$ bzw. $N' \times N'$ gemeint.

Kapitel 6

Modeallogik

Aufgabe 77

Gegeben sei die modallogische Signatur, die nur das Atom P beinhaltet, sowie folgende Kripke-Struktur $\mathcal{K} = (W, R, I)$ über dieser Signatur:



(D.h., dass $W = \{w_1, w_2, w_3, w_4, w_5\}$,

$R = \{(w_1, w_2), (w_1, w_3), (w_1, w_4), (w_2, w_1), (w_2, w_4), (w_3, w_1), (w_3, w_2), (w_4, w_3)\}$,

und für die Interpretation I gilt: $I(P, w_1) = I(P, w_2) = I(P, w_4) = W$, $I(P, w_3) = I(P, w_5) = F$.)

(a) Geben Sie für jede Welt $x \in W$ eine Formel ϕ_x an, so dass für jede Welt $y \in W, x \neq y$ gilt: $val_x(\phi_x) \neq val_y(\phi_x)$.

(b) Die sogenannte *Extension* von ϕ (in der Struktur $\mathcal{K}$) ist $[\![\phi]\!] := \{w \in W \mid val_w(\phi) = W\}$.

Bestimmen Sie für die Struktur $\mathcal{K}$: $[\![\Box P]\!]$, $[\![\Diamond\Box P]\!]$, $[\![\Diamond\Diamond P]\!]$ und $[\![\Box\Box P]\!]$.

Aufgabe 78

Wir betrachten die Klasse $\mathbf{T}$ der Kripke-Strukturen $\mathcal{K} = (W, R, I)$ mit reflexiver Übergangsrelation R, und eine modallogische Signatur, die das Atom P enthält. Geben Sie eine konkrete $\mathbf{T}$-Struktur $\mathcal{K}$ an, so daß $\mathcal{K} \models P \to \Box\Diamond P$, jedoch $\mathcal{K} \not\models \Diamond P \to \Box\Diamond P$.

Aufgabe 79

Überprüfen Sie, ob die folgenden Formeln mit den Atomen A und B in allen Kripke-Strukturen, bei denen der Kripke-Rahmen eine strikte Totalordnung[1] ist, allgemeingültig sind. Geben Sie für die nicht allgemeingültigen Formeln Gegenbeispiele an.

(a) $\Box A \to \Diamond A$

(b) $\Diamond A \to \Diamond\Diamond A$

(c) $\Diamond A \land \Diamond B \to \Diamond((A \land \Diamond B) \lor (\Diamond A \land B) \lor (A \land B))$

Hinweis: Für alle $W \subseteq \mathbb{Z}$ ist beispielsweise $(W, <)$ eine strikte Totalordnung.

Aufgabe 80

Modallogische Formeln können auf prädikatenlogische Formeln abgebildet werden, indem man jeder modallogischen Variablen p ein einstelliges Prädikat $p(\cdot)$ zuordnet und außerdem die Zugänglichkeitsrelation der Kripkestruktur als zweistelliges Prädikat $r(\cdot,\cdot)$ darstellt.

Geben Sie eine rekursive Definition dieser Abbildung, die modallogische Formeln φ auf prädikatenlogische Formeln φ' abbildet.

Geben Sie auch an, wie jeder Kripkestruktur $\mathcal{K}$ eine prädikatenlogische Interpretation $\mathcal{K}' = (D_{\mathcal{K}'}, I_{\mathcal{K}'})$ zuzuordnen ist, so dass – wie beabsichtigt – gilt:

$$\mathcal{K} \models \varphi \qquad \text{gdw.} \qquad \mathcal{K}' \models \varphi' \ .$$

[1] d.h., eine transitive Relation R, bei der zwischen je zwei Elementen a, b immer genau eine der Beziehungen $R(a,b)$, $a = b$ oder $R(b,a)$ besteht.

Kapitel 7

Lineare Temporale Logik

Aufgabe 81

Überprüfen Sie, ob folgende LTL-Formeln in allen ω-Strukturen gelten. Begründen Sie Ihre Antwort.

(a) $(A \vee B)\,\mathbf{U}\,C \;\leftrightarrow\; (A\,\mathbf{U}\,C) \vee (B\,\mathbf{U}\,C)$

(b) $A\,\mathbf{V}\,(B \wedge C) \;\rightarrow\; (A\,\mathbf{V}\,B) \wedge (A\,\mathbf{V}\,C)$

(c) $(A\,\mathbf{V}\,B) \wedge (A\,\mathbf{V}\,C) \;\rightarrow\; A\,\mathbf{V}\,(B \wedge C)$