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 $(A \wedge (A \to B)) \to B$ dargestellten Modus Ponens.

Lösung zu Aufgabe 1

$$\begin{aligned} & \models (A \wedge (A \to B)) \to B \\ \Leftrightarrow \quad & \models \neg(A \wedge (A \to B)) \vee B \\ \Leftrightarrow \quad & \models (\neg A \vee \neg(A \to B)) \vee B \\ \Leftrightarrow \quad & \models \neg A \vee \neg A \vee \neg B \vee B \\ \Leftrightarrow \quad & \models 1 \end{aligned}$$

Aufgabe 2

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

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

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

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

Lösung zu Aufgabe 2

(a) Wir suchen eine Interpretation, die die Formel wahr macht: Die Implikation wird unter anderem dann wahr, wenn B wahr ist, d. h. wenn $I(B) = W$ gilt. In diesem Fall beeinflusst die Wahl von A die Auswertung der Formel nicht mehr, d. h. z. B. ist $I(A) = F$ und $I(B) = W$ ein Modell der Formel.

(b)

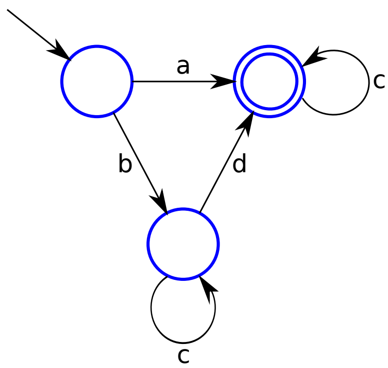
$$
\begin{aligned}
&(\neg A \wedge (A \vee \neg A)) \wedge (\neg(A \leftrightarrow B) \wedge \neg B) \equiv && \text{(tertium non datur)}\\
&(\neg A \wedge \mathbf{1}) \wedge (\neg(A \leftrightarrow B) \wedge \neg B) \equiv && \text{(Biimplikation, De Morgan)}\\
&\neg A \wedge (((A \wedge \neg B) \vee (B \wedge \neg A)) \wedge \neg B) \equiv && \text{(Distrib., Idem.)}\\
&\neg A \wedge ((A \wedge \neg B) \vee (B \wedge \neg A \wedge \neg B)) \equiv &&\\
&\neg A \wedge (A \wedge \neg B) \equiv &&\\
&\mathbf{0} &&
\end{aligned}
$$

(c) (i) Wir zeigen, dass $(A \to B) \to ((B \to C) \to (A \to C))$ eine Tautologie ist.
Fall 1: Ist die Prämisse $(A \to B)$ falsch, dann ist die Formal insgesamt wahr.
Fall 2: Sei also $A \to B$ wahr. Nun gilt es, zu zeigen, dass $(B \to C) \to (A \to C)$ auch wahr ist. Dies ist trivial gegeben, wenn
(Fall 2 a) $B \to C$ falsch ist.
(Fall 2 b) Sei also $B \to C$ wahr. Dann folgt – wegen der Transitivität der Implikation – aus $A \to B$ und $B \to C$, dass auch $A \to C$ wahr ist.

(ii) Interpretationen I mit $I(C) = F$ erfüllen $(A \wedge \neg A \to B) \wedge C$ nicht. Daher ist diese Aussage keine Tautologie.

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:

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

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:

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

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

(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, $P_1 \wedge \neg P_2$ gilt.

Lösung zu Aufgabe 3

(a) Neben den Variablen P_1, P_2, P_3, die wir zur Beschreibung des Startzustandes verwenden, führen wir zwei weitere Mengen von Variablen P'_1, P'_2, P'_3 und P''_1, P''_2, P''_3 ein, die wir zur Beschreibung des zweiten und dritten Zustandes verwenden. Sei $\bar{P}$ Abkürzung für P_1, P_2, P_3, sowie $\bar{P}'$ Abkürzung für P'_1, P'_2, P'_3 und $\bar{P}''$ Abkürzung für P''_1, P''_2, P''_3. Dann beschreibt folgende Formel die Zustände, die nach zwei Schritten aus dem Startzustand mit $\mathrm{val}_I(P_1 \wedge P_2 \wedge P_3) = W$ erreicht werden können:

$$
\begin{array}{rcll}
A & = & P_1 \wedge P_2 \wedge P_3 \wedge & (\quad (f_a(\bar{P}, \bar{P}') \wedge f_c(\bar{P}', \bar{P}'')) \\
 & & & \qquad \vee \\
 & & & \quad\;\; (f_b(\bar{P}, \bar{P}') \wedge (f_c(\bar{P}', \bar{P}'') \vee f_d(\bar{P}', \bar{P}''))) \\
 & & &)
\end{array}
$$

(b) Zu zeigen ist: $A \to (P''_1 \wedge \neg P''_2)$ ist allgemeingültig.

Zunächst berechnen wir die Interpolante C für $A \to (P''_1 \wedge \neg P''_2)$ nach der Konstruktion aus der Vorlesung. Wir wissen zu diesem Zeitpunkt zwar nicht, ob $A \to (P''_1 \wedge \neg P''_2)$ eine Tautologie ist, allerdings gilt $A \to C$ auf jeden Fall, wegen der Konstruktion von C. Wenn wir im Anschluss noch $C \to (P''_1 \wedge \neg P''_2)$ zeigen können, dann haben wir insgesamt die Allgemeingültigkeit von $A \to (P''_1 \wedge \neg P''_2)$ gezeigt.

(i) Konstruktion von C.

Nach Vorlesung kann C über

$$C = \bigvee_{\bar{c} \in \{\mathbf{1}, \mathbf{0}\}^7} A[\bar{c}] \tag{1.1}$$

konstruiert werden, wobei in $A[\bar{c}]$ die Atome $P_1, P_2, P_3, P'_1, P'_2, P'_3, P''_3$, die in A aber nicht in $(P''_1 \wedge \neg P''_2)$ vorkommen durch $c_1, \ldots, c_7$ ersetzt werden.

Die Berechnung von C läßt sich manuell nur handhaben, wenn wir systematische vorgehen und schon während der schrittweisen Berechnung logische Äquivalenz erhaltende Vereinfachungen vornehmen.

Wählen wir für c_1, c_2 oder c_3 den Wert $\mathbf{0}$, so ist $A[\bar{c}] \leftrightarrow \mathbf{0}$ und trägt nichts zu C bei. Diese Beobachtung führt zu

$$C \equiv \bigvee_{\bar{c_0} \in \{\mathbf{1}, \mathbf{0}\}^4} A[1, 1, 1, \bar{c_0}] \tag{1.2}$$

Führen wir die Ersetzungen $P_i \rightsquigarrow 1$ für $1 \leq i \leq 3$ in A aus, so erhalten wir:

$$
\begin{array}{rcl}
A_0 & = & (P'_1 \wedge \neg P'_2 \wedge P'_3 \wedge f_c(\bar{P}', \bar{P}'')) \\
 & & \vee \\
 & & (P'_1 \wedge \neg P'_2 \wedge \neg P'_3 \wedge (f_c(\bar{P}', \bar{P}'') \vee f_d(\bar{P}', \bar{P}'')))
\end{array} \tag{1.3}
$$

Somit kann man (1.2) schreiben als:

$$C \equiv \bigvee_{\bar{c_0} \in \{\mathbf{1}, \mathbf{0}\}^4} A_0[\bar{c_0}] \tag{1.4}$$

Wir sehen, dass für $c_4 = \mathbf{0}$ oder $c_5 = \mathbf{1}$ wiederum $A_0[\bar{c_0}] \leftrightarrow \mathbf{0}$ gilt und somit zur Disjunktion C nichts beiträgt.

$$C \equiv \bigvee_{\bar{c_1} \in \{\mathbf{1}, \mathbf{0}\}^2} A_0[1, 0, \bar{c_1}] \tag{1.5}$$

Führen wir die Ersetzungen $P_1' \rightsquigarrow \mathbf{1}$, $P_2' \rightsquigarrow \mathbf{0}$ in A_0 aus, so erhalten wir:

$$\begin{aligned} A_1 \quad = \quad & (P_3' \wedge P_1'' \wedge \neg P_2'' \wedge P_3'') \\ & \vee \\ & (\neg P_3' \wedge (P_1'' \wedge \neg P_2'' \wedge P_3'') \vee (P_1'' \wedge \neg P_2'' \wedge \neg P_3'')) \end{aligned} \tag{1.6}$$

Somit können wir wieder (1.4) umschreiben zu:

$$C \equiv \bigvee_{\bar{c_1} \in \{\mathbf{1},\mathbf{0}\}^2} A_1[\bar{c_1}] \tag{1.7}$$

Die Formeln sind jetzt klein genug, dass wir das Ergebnis der Ersetzungen $P_3' \rightsquigarrow \mathbf{1}$ und $P_3' \rightsquigarrow \mathbf{0}$ direkt ausrechnen können. Das führt zu

$$C \equiv \bigvee_{d \in \{\mathbf{1},\mathbf{0}\}} (P_1'' \wedge \neg P_2'' \wedge P_3'')[d] \vee \bigvee_{d \in \{\mathbf{1},\mathbf{0}\}} (P_1'' \wedge \neg P_2'' \wedge P_3'') \vee (P_1'' \wedge \neg P_2'' \wedge \neg P_3''))[d] \tag{1.8}$$

wobei die einzige noch verbleibende Ersetzung $P_3'' \rightsquigarrow d$ ist. Die Formel in der zweiten großen Disjunktion lässt sich mit Hilfe des Distributivgesetzes vereinfachen zu

$$\begin{aligned} (P_1'' \wedge \neg P_2'' \wedge P_3'') \vee (P_1'' \wedge \neg P_2'' \wedge \neg P_3'') \quad & \equiv \quad (P_1'' \wedge \neg P_2'') \wedge (P_3'' \vee \neg P_3'') \\ & \equiv \quad (P_1'' \wedge \neg P_2'') \end{aligned}$$

Eingesetzt in (1.8) erhält man

$$C \equiv (\bigvee_{d \in \{\mathbf{1},\mathbf{0}\}} (P_1'' \wedge \neg P_2'' \wedge P_3'')[d]) \vee (P_1'' \wedge \neg P_2'') \tag{1.9}$$

In der zweiten Disjunktion kann die Ersetzung durch d wegfallen, da P_3'' nicht mehr vorkommt.

In der ersten Disjunktion liefert $P_3'' \rightsquigarrow \mathbf{0}$ keinen Beitrag und es bleibt

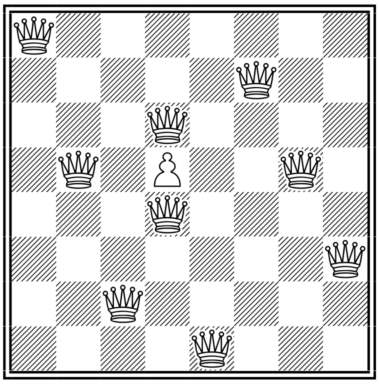
$$\begin{aligned} C \quad & \equiv \quad (P_1'' \wedge \neg P_2'') \vee (P_1'' \wedge \neg P_2'') \\ & \equiv \quad (P_1'' \wedge \neg P_2'') \end{aligned} \tag{1.10}$$

(ii) Wie eingangs schon angedeutet ist $A \to C$ nach Konstruktion eine Tautologie. Wegen (1.10) ist $C \to (P_1'' \wedge \neg P_2'')$ trivialer Weise eine Tautologie. Insgesamt haben wir also gezeigt, dass $A \to (P_1'' \wedge \neg P_2'')$ eine Tautologie ist.

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.



Lösung zu Aufgabe 4

Wir führen für jedes Feld des Schachbretts eine Boolesche Variable $D_{i,j}$ ein, mit der Vorstellung, dass $D_{i,j}$ genau dann den Wert *wahr* hat, wenn auf dem Feld (i, j) eine Dame steht. Zusätzlich führen wir für jedes Feld des Schachbretts eine Boolesche Variable $B_{i,j}$ ein, mit der Vorstellung, dass $B_{i,j}$ genau dann den Wert *wahr* hat, wenn auf dem Feld (i, j) der Bauer steht.

Schreibweise. Im folgenden schreiben wir

$$\bigwedge_{i:b(i)} \phi(i)$$

als Abkürzung für eine endliche Konjunktion der aussagenlogischen Formeln $\phi(i)$, für die gilt, dass

- $1 \leq i \leq 8$,
- die Bedingung $b(i)$ ist erfüllt.

Dabei ist i eine Variable auf der Metaebene, und b ist eine Formel der Metaebene.

Zudem steht $\bigvee_i \phi(i)$ für $\bigvee_{i:true} \phi(i)$; $\bigvee_{i:false}$ steht für *false*; $\bigwedge_{i:false}$ steht für *true*; und Abkürzungen wie $\bigvee_{i,j:b(i,j)} \phi(i, j)$ mit mehreren Variablen sind analog definiert.

Struktur der Formalisierung. Wir formalisieren das Problem als eine aussagenlogische Formel

$$A = A_1 \land A_2 \land A_3 \land A_4$$

Die drei Teilformeln sind jeweils wie folgend.

Genau ein Bauer steht auf dem Brett.

$$A_1 = \bigvee_{x,y} \left(B_{x,y} \land \bigwedge_{i,j:(i,j)\neq(x,y)} \neg B_{i,j} \right)$$

Genau neun Damen stehen auf dem Brett. Sei

$$M = \{(i, j) \mid 1 \leq i, j \leq 8\}$$

die Menge aller Felder des Bretts. Damit kodiert folgende Formel die Tatsache, dass es genau 9 Damen auf dem Brett gibt:

$$A_2 = \bigvee_{S:S\subset M,\#S=9} \left(\bigwedge_{i,j:(i,j)\in S} D_{i,j} \land \bigwedge_{i,j:(i,j)\notin S} \neg D_{i,j} \right)$$

(Wir haben dabei die Schreibweise der endlichen Disjuktion auf eine naheliegende Weise „mißbraucht“.)

Auf keinem Feld stehen Bauer und Dame zugleich.

$$A_4 = \bigwedge_{i,j} \neg(B_{i,j} \wedge D_{i,j})$$

Es gibt keine Bedrohung zwischen zwei Damen. Wir ordnen die Bedrohungen nach Reihen, Spalten, Haupt- und Nebendiagonalen:

$$A_3 = \mathit{Reihen} \wedge \mathit{Spalten} \wedge \mathit{Diag}^+ \wedge \mathit{Diag}^-$$

Die folgende Formel besagt, dass, falls zwei Damen in der gleichen Reihe stehen, der Bauer dazwischen stehen muss:

$$\mathit{Reihen} = \bigwedge_{i,i',j:\, i<i'} \left((D_{i,j} \wedge D_{i',j}) \to \bigvee_{i'':\, i<i''<i'} B_{i'',j} \right)$$

Das gleiche für Spalten, Haupt- und Nebendiagonalen:

$$\begin{aligned}
\mathit{Spalten} &= \bigwedge_{i,j,j':\, j<j'} \left((D_{i,j} \wedge D_{i,j'}) \to \bigvee_{j'':\, j<j''<j'} B_{i,j''} \right) \\
\mathit{Diag}^+ &= \bigwedge_{i,j,i',j':\, i<i',\, i'-i=j'-j} \left((D_{i,j} \wedge D_{i',j'}) \to \bigvee_{i'',j'':\, i<i''<i',\, i''-i=j''-j} B_{i'',j''} \right) \\
\mathit{Diag}^- &= \bigwedge_{i,j,i',j':\, i<i',\, i'-i=j-j'} \left((D_{i,j} \wedge D_{i',j'}) \to \bigvee_{i'',j'':\, i<i''<i',\, i''-i=j-j''} B_{i'',j''} \right)
\end{aligned}$$

Fazit. Insgesamt hat das 9-Damen-Problem eine Lösung, wenn die aussagenlogische Formel

$$A = A_1 \wedge A_2 \wedge A_3 \wedge A_4$$

erfüllbar ist. Jedes Modell der Formel ergibt eine zulässige Konfiguration der Figuren auf dem Brett.

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?

Lösung zu Aufgabe 5

Die Formalisierung ist die Konjunktion folgender Teile:

Der Benutzer möchte den Mail-Client *mutt* installieren.	$mutt$
Der Mail-Client erfordert einen *smtp daemon*.	$mutt \rightarrow smtp\_daemon$
Ein gültiger *smtp daemon* ist entweder *sendmail*, *postfix* oder *exim*,	$smtp\_daemon \rightarrow$ $(sendmail \lor postfix \lor exim)$
es kann nur einer gleichzeitig installiert werden.	$\neg(sendmail \land postfix)$ $\neg(sendmail \land exim)$ $\neg(postfix \land exim)$
sendmail macht das installierte Legacy-Paket *sendmail-tls* obsolet,	$\neg(sendmail \land sendmail\text{-}tls)$
das aber nicht deinstalliert werden darf.	$sendmail\text{-}tls$

Die Formel hat zwei verschiedene Modelle:

$I(mutt) = W, I(smtp\_daemon) = W, I(sendmail) = F, I(postfix) = W, I(exim) = F, I(sendmail\text{-}tls) = W$

oder

$I(mutt) = W, I(smtp\_daemon) = W, I(sendmail) = F, I(postfix) = F, I(exim) = W, I(sendmail\text{-}tls) = W$

Die als wahr interpretierten Atome geben genau die Pakete an, die installiert sind oder werden müssen, um den Benutzerwunsch zu erfüllen.

Im allgemeinen wählt der in openSuSE implementierter SAT-Solver das Modell, das sich am wenigsten von dem Modell unterscheidet, das den Anfangszustand des Systems beschreibt.

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.

Lösung zu Aufgabe 6

Für jedes Land i gibt es drei AL-Variablen R_i, G_i, B_i. Nun muss für einen gegebenen Graphen formalisiert werden, dass

1. Jedes Land mindestens 1 Farbe hat,
2. jedes Land höchstens 1 Farbe hat und
3. benachbarte Länder nicht dieselbe Farbe haben.

Schreibweise. Im folgenden schreiben wir

$$\bigwedge_{i:b(i)} \phi(i)$$

als Abkürzung für eine endliche Konjunktion der aussagenlogischen Formeln $\phi(i)$, für die gilt, dass die Bedingung $b(i)$ ist erfüllt. Dabei ist i eine Variable auf der Metaebene, und b ist eine Formel der Metaebene. Abkürzungen wie $\bigvee_{i,j:b(i,j)} \phi(i,j)$ mit mehreren Variablen sind analog definiert.

Formalisierung.

$$\begin{aligned} F = \quad & \bigwedge_{i:0\leq i<L} (R_i \vee G_i \vee B_i) \\ \wedge \quad & \bigwedge_{i:0\leq i<L} \neg\big((R_i \wedge G_i) \vee (G_i \wedge B_i) \vee (B_i \wedge R_i)\big) \\ \wedge \quad & \bigwedge_{i,j:0\leq i,j<L, Na(i,j)} \big(\neg(R_i \wedge R_j) \wedge \neg(G_i \wedge G_j) \wedge \neg(B_i \wedge B_j)\big) \end{aligned}$$

Hinweis. Lässt man die zweite Bedingung weg, so erhält man eine bezüglich Erfüllbarkeit äquivalente Formel.

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.

Lösung zu Aufgabe 7

Wir führen für jede Zellenposition (i, j) des Sudoku und jede Zahl k zwischen 1 und 9 eine Boolesche Variable

$$D_{i,j}^k$$

ein, mit der Vorstellung, dass $D_{i,j}^k$ den Wert *wahr* hat, wenn auf dem Feld (i, j) die Zahl k steht.

Wir benutzen kartesische Koordinaten zur Notation von Positionen.

Formalisierung Die folgenden vier Bedingungen haben zur Folge, dass das Sudoku vollständig (u.U. auch mehrfach) gefüllt ist und jede Zeile, Spalte und Region die Zahlen von 0 bis 9 aufweist:

Jede Zahl kommt mindestens einmal pro Zeile vor.

$$D_{1,y}^v \vee D_{2,y}^v \vee D_{3,y}^v \vee D_{4,y}^v \vee D_{5,y}^v \vee D_{6,y}^v \vee D_{7,y}^v \vee D_{8,y}^v \vee D_{9,y}^v$$

jeweils für alle $1 \leq y \leq 9$ und $0 \leq v \leq 9$.

Jede Zahl kommt mindestens einmal pro Spalte vor.

$$D_{x,1}^v \vee D_{x,2}^v \vee D_{x,3}^v \vee D_{x,4}^v \vee D_{x,5}^v \vee D_{x,6}^v \vee D_{x,7}^v \vee D_{x,8}^v \vee D_{x,9}^v$$

jeweils für alle $1 \leq x \leq 9$ und $0 \leq v \leq 9$.

Jede Zahl kommt mindestens einmal pro Region vor. Die Formel

$$D_{1,1}^v \vee D_{1,2}^v \vee D_{1,3}^v \vee D_{2,1}^v \vee D_{2,2}^v \vee D_{2,3}^v \vee D_{3,1}^v \vee D_{3,2}^v \vee D_{3,3}^v$$

für alle $0 \leq v \leq 9$ kodiert, dass die Ziffer v mindestens einmal in der Region links unten vorkommen muss. Analog für alle anderen Regionen.

Auf jeder Zelle steht mindestens eine Zahl.

$$D_{x,y}^0 \vee D_{x,y}^1 \vee D_{x,y}^2 \vee D_{x,y}^3 \vee D_{x,y}^4 \vee D_{x,y}^5 \vee D_{x,y}^6 \vee D_{x,y}^7 \vee D_{x,y}^8 \vee D_{x,y}^9$$

jeweils für alle $1 \leq x \leq 9$ und $1 \leq y \leq 9$.

Die folgende Bedingung legt (zusammen mit den vorigen) die Anzahl der Eintragungen für das Sudoku auf genau 90 fest (neun Zeilen, wobei jede Zeile die Zahlen von 0 bis 9 genau einmal enthält). Außerdem wird sichergestellt, dass jede Zeile genau ein doppelt belegtes Feld enthält – im gesamten Sudoku sind also 9 doppelt belegte Felder zu verteilen.

Jede Zahl kommt *höchstens* einmal in jeder Zeile vor.

$$\neg(D_{x_1,y}^v \wedge D_{x_2,y}^v)$$

für alle $0 \leq v \leq 9$ und $1 \leq x_1, x_2, y \leq 9$ mit $x_1 < x_2$.

Aus den Bedingungen “jede Zahl kommt mindestens einmal pro Spalte bzw. Region vor” folgt, dass jede Spalte und Region mindestens ein doppelt gefülltes Feld enthalten muss. Das Sudoku enthält jeweils 9 Spalten und Regionen und es gibt 9 doppelt belegte Felder, die zu verteilen sind. Daraus folgt, dass jede Spalte und Region genau ein doppelt belegtes Feld aufweist.

Jede Zeile, Spalte und Region hat daher genau 10 Eintragungen. Daraus folgt zusammen mit der Bedingung, dass jede Zahl mindestens einmal pro Zeile/Spalte/Region vorkommen muss, dass keine zwei Eintragungen mit der gleichen Zahl existieren.

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.

Lösung zu Aufgabe 8

Seien $A \equiv P_1 \wedge P_2 \wedge P_3$ und $B \equiv P_1 \vee P_2 \vee P_4$.

Zunächst zeigen wir: $A \to B$ ist eine Tautologie. Für $\mathrm{val}_I(P_1) = F$ ist $\mathrm{val}_I(A) = F$ und damit die Implikation trivialer Weise erfüllt. Für $\mathrm{val}_I(P_1) = W$ ist anderseits $\mathrm{val}_I(B) = W$ und damit die Implikation ebenfalls erfüllt.

Die Argumentation zeigt eigentlich schon: P_1 ist eine Interpolante für $A \to B$, denn

- P_1 ist in A und B enthalten und
- offensichtlich gilt sowohl $A \to P_1$ als auch $P_1 \to B$.

Aus dem selben Grund ist aber auch P_2 eine Interpolante. $P_1 \wedge P_2$ und $P_1 \vee P_2$ sind weitere Interpolanten.

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 $A \to B$.

Lösung zu Aufgabe 9

Seien C_1 und C_2 Interpolanten der Tautologie $A \to B$. Es gilt:

- $A \to C_1$ und
- $A \to C_2$, weil C_i Interpolaten sind, und
- $C_1 \to (C_1 \vee C_2)$, weil es eine AL-Tautologie ist.

Aus den ersten beiden Aussagen folgt bereits $A \to (C_1 \wedge C_2)$ und aus der ersten und dritten schon $A \to (C_1 \vee C_2)$. Die beiden anderen Aussagen folgen ziemlich analog aus:

- $C_1 \to B$,
- $C_2 \to B$ und
- $(C_1 \wedge C_2) \to C_1$.

Aus den ersten beiden folgt $(C_1 \vee C_2) \to B$ und aus dem ersten und dritten $(C_1 \wedge C_2) \to B$.

Offensichtlich kommt jede aussagenlogische Variable in $C_1 \wedge C_2$ und $C_2 \vee C_1$ sowohl in A als auch in B vor.

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.

Lösung zu Aufgabe 10

Offensichtlich kommt jede aussagenlogische Variable in D sowohl in A als auch in B vor.

Wir betrachten eine Interpretation I mit $val_I(A) = W$. Wir zielen darauf $val_I(D) = W$ zu zeigen. Seien, wie gesagt, $Q_1, \ldots, Q_k$ alle Variablen in B, die nicht in A vorkommen. Weiterhin seien $c_1, \ldots, c_k$ Konstanten aus $\{\mathbf{1}, \mathbf{0}\}$ und J die Belegung mit

$$J(Q) = \begin{cases} val_I(c_i) & \text{falls } Q = Q_i \text{ für } 1 \leq i \leq k \\ I(Q) & \text{sonst} \end{cases}$$

Es gilt weiterhin $val_J(A) = W$, da ja nur die Belegung von Aussagenvariablen geändert wurden, die nicht in A vorkommen. Da $A \to B$ eine Tautologie ist gilt auch $val_J(B) = W$. Das läßt sich äquivalent auch schreiben als $val_I(B[c_1, \ldots, c_k]) = W$. Wiederholt man dieses Argument für jedes k-Tupel $(c_1, \ldots, c_k) \in \{\mathbf{1}, \mathbf{0}\}^k$ dann erhält man.

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

Damit ist schon einmal $val_I(A \to D) = W$ gezeigt für beliebiges I.

Gelte jetzt $val_I(D) = W$. Dann gilt für insbesondere für $c_i = \mathbf{1} \Leftrightarrow I(Q_i) = W$, $1 \leq i \leq k$, auch $val_I(B[c_1, \ldots, c_n]) = W$, denn $B[c_1, \ldots, c_n]$ ist ja konjunktiver Bestandteil von D. In diesem Fall gilt aber auch

$$val_I(B) = val_I(B[c_1, \ldots, c_n]) = W.$$

Damit ist auch die Allgemeingültigkeit von $D \to B$ gezeigt.

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) $(p \to q) \land (q \to s)$

(c) $(p \to (\neg p \lor q)) \land \neg(p \to q)$

(d) $(p \land \neg(q \land r)) \lor (\neg p \land \neg((q \land r) \lor \neg q))$

Lösung zu Aufgabe 11

Generelle Vorgehensweise: (1) Biimplikationen und Implikationen auflösen, (2) NNF herstellen, (3) Distributivgesetz anwenden, dabei stets (4) Zwischenergebnisse vereinfachen (Idempotenz, Absorption, tertium non datur, usw.).

Beachten Sie, dass Normalformen im Allgemeinen nicht eindeutig sind. Andere Rechenwege können also zu anderen Ergebnissen führen.

(a) DNF:

$$\begin{aligned}
&p \rightarrow (p \rightarrow q) \equiv \\
&\neg p \vee (\neg p \vee q) \equiv \quad \text{(Idempotenz)} \\
&\neg p \vee q
\end{aligned}$$

Dies ist auch die KNF.

(b) KNF:

$$(p \rightarrow q) \wedge (q \rightarrow s) \equiv (\neg p \vee q) \wedge (\neg q \vee s)$$

DNF:

$$\begin{aligned}
&(p \rightarrow q) \wedge (q \rightarrow s) \equiv \\
&(\neg p \vee q) \wedge (\neg q \vee s) \equiv && \text{(Distr.)} \\
&((\neg p \vee q) \wedge \neg q) \vee ((\neg p \vee q) \wedge s) \equiv && \text{(Distr.)} \\
&(\neg p \wedge \neg q) \vee (q \wedge \neg q) \vee (\neg p \wedge s) \vee (q \wedge s) \equiv \\
&(\neg p \wedge \neg q) \vee \qquad\qquad\quad (\neg p \wedge s) \vee (q \wedge s)
\end{aligned}$$

(c) DNF:

$$\begin{aligned}
&(p \rightarrow (\neg p \vee q)) \wedge \neg(p \rightarrow q) \equiv \\
&(\neg p \vee (\neg p \vee q)) \wedge \neg(\neg p \vee q) \equiv && \text{(Idem.)} \\
&(\neg p \vee q) \wedge \neg(\neg p \vee q) \equiv && \text{(man sieht nun direkt)} \\
&\mathbf{0}
\end{aligned}$$

Als Schreibweise für die DNF würde man an dieser Stelle die leere Disjunktion $\vee$ benutzen. Dies ist auch die KNF. Achtung: Die leere Konjunktion $\wedge$ entspricht dagegen einer allgemeingültigen Formel.

(d) DNF:

$$\begin{aligned}
&(p \wedge \neg(q \wedge r)) \vee (\neg p \wedge \neg((q \wedge r) \vee \neg q)) \equiv && \text{(De Morgan)} \\
&(p \wedge (\neg q \vee \neg r)) \vee (\neg p \wedge ((\neg q \vee \neg r) \wedge q) \equiv && \text{(Distr.)} \\
&(p \wedge \neg q) \vee (p \wedge \neg r) \vee (\neg p \wedge \neg q \wedge q) \vee (\neg p \wedge \neg r \wedge q) \equiv \\
&(p \wedge \neg q) \vee (p \wedge \neg r) \vee \qquad\qquad\qquad\quad (\neg p \wedge \neg r \wedge q)
\end{aligned}$$

KNF:

$$\begin{aligned}
&(p \wedge \neg(q \wedge r)) \vee (\neg p \wedge \neg((q \wedge r) \vee \neg q)) \equiv && \text{(De Morgan)} \\
&(p \wedge (\neg q \vee \neg r)) \vee (\neg p \wedge ((\neg q \vee \neg r) \wedge q) \equiv && \text{(Distr.)} \\
&(p \wedge (\neg q \vee \neg r)) \vee (\neg p \wedge \neg q \wedge q) \vee (\neg p \wedge \neg r \wedge q) \equiv \\
&(p \wedge (\neg q \vee \neg r)) \vee \qquad\qquad\qquad (\neg p \wedge \neg r \wedge q) \equiv && \text{(Distr.)} \\
&(p \vee \neg p) \wedge (p \vee \neg r) \wedge (p \vee q) \wedge (\neg q \vee \neg r \vee \neg p) \wedge (\neg q \vee \neg r \vee \neg r) \wedge (\neg q \vee \neg r \vee q) \equiv \\
&\qquad (p \vee \neg r) \wedge (p \vee q) \wedge (\neg q \vee \neg r \vee \neg p) \wedge (\neg q \vee \neg r) \equiv && \text{(Absorp.)} \\
&\qquad (p \vee \neg r) \wedge (p \vee q) \wedge (\neg q \vee \neg r) \equiv && \text{(Transitivität d. Impl.)} \\
&\qquad\qquad (p \vee q) \wedge (\neg q \vee \neg r)
\end{aligned}$$

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}?

Lösung zu Aufgabe 12

(a) Die Anwendung des beschriebenen Verfahrens auf A_4 ergibt folgendes (modulo Assoziativität):

$$A_4 = \underbrace{\underbrace{P_1 \leftrightarrow P_2}_{Q_1} \leftrightarrow P_3}_{Q_2} \leftrightarrow P_4$$

Dies führt zu folgenden Äquivalenzen:

$$\begin{array}{lcl} Q_1 & \leftrightarrow & P_1 \leftrightarrow P_2 \\ Q_2 & \leftrightarrow & Q_1 \leftrightarrow P_3 \\ & & Q_2 \leftrightarrow P_4 \end{array}$$

$Q_i \leftrightarrow (Q_{i-1} \leftrightarrow P_{i+1})$ (mit $Q_0 = P_1$) lässt sich wie folgt als KNF mit 4 Klausel mit je zwei Disjunktionen darstellen. Zunächst bemerken wir das jede Äquivalenz $A \leftrightarrow B$ logisch äquivalent ist zu $(A \wedge B) \vee (\neg A \wedge \neg B)$ und zu $(A \vee \neg B) \wedge (\neg A \vee B)$. Von diesen beiden Äquivalenzen wird in der folgenden äquivalenten Umformungskette Gebrauch gemacht.

$$\begin{array}{lll} & Q_i \leftrightarrow (Q_{i-1} \leftrightarrow P_{i+1}) & \\ \equiv & Q_i \vee \neg(Q_{i-1} \leftrightarrow P_{i+1}) & \wedge \quad \neg Q_i \vee (Q_{i-1} \leftrightarrow P_{i+1}) \\ \equiv & Q_i \vee \neg((Q_{i-1} \wedge P_{i+1}) \vee (\neg Q_{i-1} \wedge \neg P_{i+1})) & \wedge \quad \neg Q_i \vee ((\neg Q_{i-1} \vee P_{i+1}) \wedge (Q_{i-1} \vee \neg P_{i+1})) \\ \equiv & Q_i \vee (\neg(Q_{i-1} \wedge P_{i+1}) \wedge \neg(\neg Q_{i-1} \wedge \neg P_{i+1})) & \wedge \quad \neg Q_i \vee ((\neg Q_{i-1} \vee P_{i+1}) \wedge (Q_{i-1} \vee \neg P_{i+1})) \\ \equiv & Q_i \vee ((\neg Q_{i-1} \vee \neg P_{i+1}) \wedge (Q_{i-1} \vee P_{i+1})) & \wedge \quad (\neg Q_i \vee \neg Q_{i-1} \vee P_{i+1}) \wedge (\neg Q_i \vee Q_{i-1} \vee \neg P_{i+1}) \\ \equiv & (Q_i \vee \neg Q_{i-1} \vee \neg P_{i+1}) \wedge (Q_i \vee Q_{i-1} \vee P_{i+1}) & \wedge \quad (\neg Q_i \vee \neg Q_{i-1} \vee P_{i+1}) \wedge (\neg Q_i \vee Q_{i-1} \vee \neg P_{i+1}) \end{array}$$

Insgesamt ergibt sich also:

$$\begin{array}{lll} A_4 & \equiv & (Q_1 \vee \neg P_1 \vee \neg P_2) \wedge (Q_1 \vee P_1 \vee P_2) \quad \wedge \quad (\neg Q_1 \vee \neg P_1 \vee P_2) \wedge (\neg Q_1 \vee P_1 \vee \neg P_2) \\ & \wedge & (Q_2 \vee \neg Q_1 \vee \neg P_3) \wedge (Q_2 \vee Q_1 \vee P_3) \quad \wedge \quad (\neg Q_2 \vee \neg Q_1 \vee P_3) \wedge (\neg Q_2 \vee Q_1 \vee \neg P_3) \\ & \wedge & (Q_2 \vee \neg P_4) \wedge (\neg Q_2 \vee P_4) \end{array}$$

(b) Die Anwendung des beschriebenen Verfahrens auf A_n ergibt folgendes (modulo Assoziativität):

$$A_n = \underbrace{\underbrace{\underbrace{P_1 \leftrightarrow P_2}_{Q_1} \leftrightarrow P_3}_{Q_2} \leftrightarrow \ldots \leftrightarrow P_{n-1}}_{Q_{n-2}} \leftrightarrow P_n$$

Dies führt zu folgenden Äquivalenzen:

$$\begin{array}{lcl} Q_1 & \leftrightarrow & P_1 \leftrightarrow P_2 \\ Q_2 & \leftrightarrow & Q_1 \leftrightarrow P_3 \\ Q_3 & \leftrightarrow & Q_2 \leftrightarrow P_4 \\ & \vdots & \\ Q_{n-2} & \leftrightarrow & Q_{n-3} \leftrightarrow P_{n-1} \\ & & Q_{n-2} \leftrightarrow P_n \end{array}$$

Für die ersten $n-2$ Äquivalenzen lässt sich die KNF mit je 4 Disjunktionen bilden (siehe oben), für $Q_{n-2} \leftrightarrow P_n$ mit 2 Disjunktionen. Insgesamt sind das also

$$(n-2) \cdot 4 + 2 = 4n - 6$$

Klauseln, nur $O(n)$ viele.

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.

Lösung zu Aufgabe 13

Exemplarisch für A'; A'' analog.

$$\begin{aligned} A &= (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R) \\ &\stackrel{1}{\equiv} (P \wedge \neg Q \wedge R) \vee (\neg P \wedge Q \wedge R) \vee (P \wedge Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \vee (\neg P \wedge Q \wedge \neg R) \vee (P \wedge \neg Q \wedge R) \\ &\stackrel{2}{\equiv} (P \wedge \neg Q) \vee (\neg P \wedge Q) \vee (P \wedge R) \end{aligned}$$

Es wird die *Kommutativität* und *Assoziativität* gebraucht, um die Teilformeln umzustellen oder umzugruppieren.

Zu 1: Die erste Teilformel kann wegen der *Idempotenz* von $\vee$ dupliziert werden und wird am Ende hinzugefügt.

Zu 2: Jeweils zwei Teilformeln lassen sich dann wegen *Distributivität* (a), *Tertium-non-datur* (b) und der Eigenschaft von **1** als *neutralem Element* bezgl. $\wedge$ (c) reduzieren, beispielsweise:

$$\begin{aligned} & (P \wedge \neg Q \wedge R) \vee (P \wedge \neg Q \wedge \neg R) \\ \stackrel{(a)}{\equiv}\ & (P \wedge \neg Q) \wedge (R \vee \neg R) \\ \stackrel{(b)}{\equiv}\ & (P \wedge \neg Q) \wedge \mathbf{1} \\ \stackrel{(c)}{\equiv}\ & P \wedge \neg Q \end{aligned}$$

Man soll sehen, dass die beiden Formeln A' und A'' beide (minimale) DNF für A sind und diese daher (obwohl Normalform) überhaupt nicht eindeutig ist.

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.

Lösung zu Aufgabe 14

Angenommen es gäbe eine erfüllende Interpretation I für $S \setminus \{C\}$. Sei L ein isoliertes Literal in C. Nach Annahme muß es mindestens ein solches geben. Wir setzen:

$$J(P) = \begin{cases} I(P) & \text{falls } P \text{ nicht im Literal } L \text{ vorkommt} \\ W & \text{falls } L = P \\ F & \text{falls } L = \neg P \end{cases}$$

Offensichtlich gilt $J(C) = W$. Aber gilt auch noch $J(D) = W$ für alle anderen Klauseln D in S? Sicher, da $\bar{L}$ in keiner Klausel in S vorkommt, kann schlimmstenfalls der Wechseln von $I(L) = F$ zu

$J(L) = W$ erfolgen. Aus $I(D) = W$ folgt also auch $J(D) = W$.

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.

Lösung zu Aufgabe 15

(1) Ist C eine tautologische Klausel in S, dann ist $S \setminus \{C\}$ erfüllbar, wegen der minimalen Inkonsistenz von S. Es gibt also I mit $I(D) = W$ für alle $D \in S$, $D \neq C$. Da C aber tautologisch ist gilt auch $I(C) = W$, was im Widerspruch zu angekommenen Unerfüllbarkeit von S steht.

(2) Da S unerfüllbar ist gibt es auf jeden Fall eine Klausel $D \in S$ mit $I(D) = F$. Wäre D eine isolierte Klausel, so wäre nach Aufgabe 14 $S \setminus \{D\}$ unerfüllbar, im Widerspruch zur minimalen Unerfüllbarkeit von S. Also gibt es sogar für jedes Literal L in D eine Klausel C, in der $\bar{L}$ vorkommt. Da für alle Literale L in D wegen $I(D) = F$ auch $I(L) = F$ gelten muß gilt $I(\bar{L}) = W$ und damit auch $I(C) = W$.

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?

Lösung zu Aufgabe 16

Offizielle Antwort: Es ist unwahrscheinlich. Gäbe es nämlich eine solche effiziente Transformation, so wäre damit zugleich **P = NP** gezeigt. Das Erfüllbarkeitsproblem für eine beliebige Formel in KNF (SAT) ist NP-vollständig, für eine Formel in DNF ist es aber in linearer Zeit lösbar (einmal durchgehen und schauen, ob eine widerspruchsfreie Konjunktion dabei ist). Nehmen wir also an, man könnte eine beliebige konjunktive Formel in polynomieller Zeit in eine (kurze) disjunktive Normalform überführen, so könnte damit auch man durch polynomielle Reduktion das Erfüllbarkeitsproblem SAT in polynomieller Zeit lösen, es wäre in **NP**-hart und in **P**, woraus **P=NP** folgte.

Aufgabe 17

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

Lösung zu Aufgabe 17

Sei A eine Äquivalenzformel. Es gilt der Zusammenhang $(*)$:

> A ist allgemeingültig $\Leftrightarrow$ Jede Variable in A hat eine gerade Anzahl von Vorkommen und die Konstante $\mathbf{0}$ hat eine gerade Anzahl von Vorkommen.

Außerdem ist $\neg A \equiv A \leftrightarrow \mathbf{0}$. Wenn A unerfüllbar ist, dann ist $\neg A$ allgemeingültig. Diese Zusammenhänge kann man für diese Aufgabe ausnutzen:

A ist erfüllbar.

$\Leftrightarrow$ A ist nicht unerfüllbar.

$\Leftrightarrow$ $\neg A$ ist nicht allgemeingültig.

$\Leftrightarrow$ $A \leftrightarrow \mathbf{0}$ ist nicht allgemeingültig

$\overset{(*)}{\Leftrightarrow}$ Es gilt nicht: Jede Variable in $A \leftrightarrow \mathbf{0}$ hat eine gerade Zahl an Vorkommen und $\mathbf{0}$ hat eine gerade Anzahl an Vorkommen

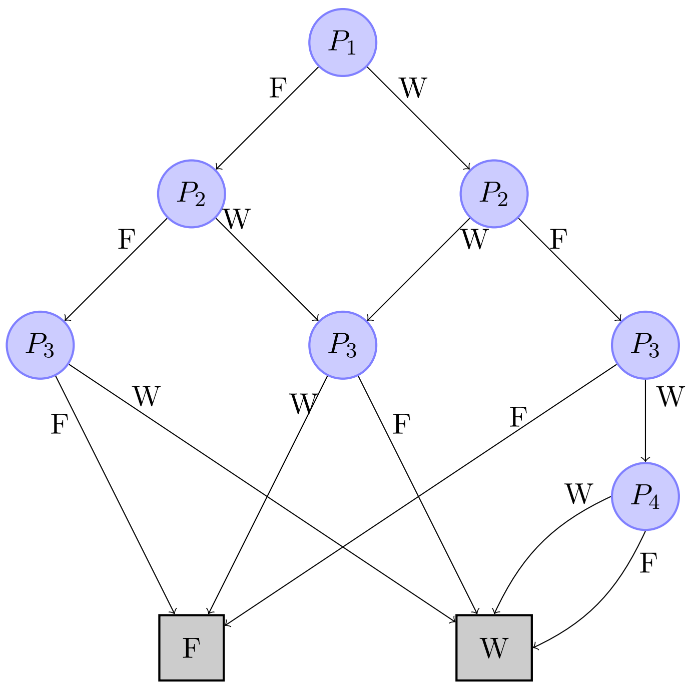
$\Leftrightarrow$ Es gibt eine Variable in $A \leftrightarrow \mathbf{0}$ mit einer ungerade Zahl an Vorkommen oder $\mathbf{0}$ hat eine ungerade Zahl an Vorkommen in $A \leftrightarrow \mathbf{0}$.

$\Leftrightarrow$ Es gibt eine Variable in A mit einer ungeraden Zahl an Vorkommen oder $\mathbf{0}$ hat eine gerade Zahl an Vorkommen in A.

1.4 Shannongraphen

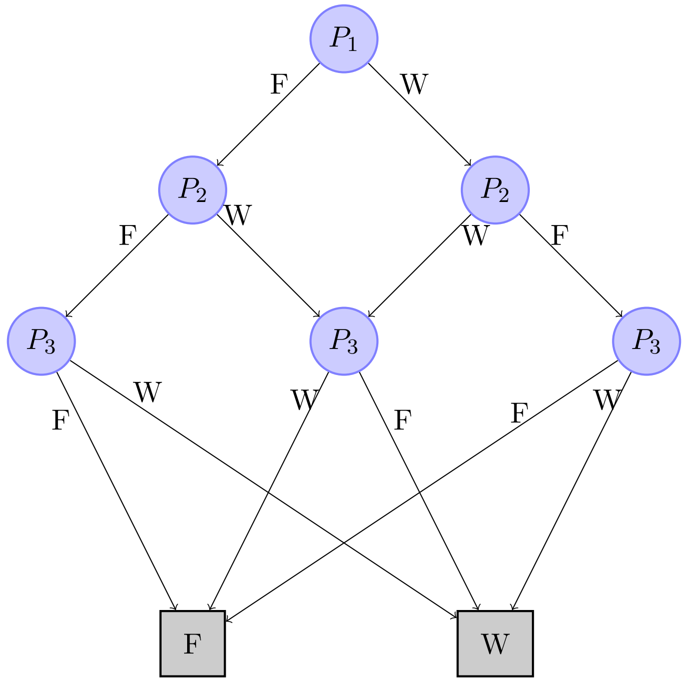
Aufgabe 18

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.

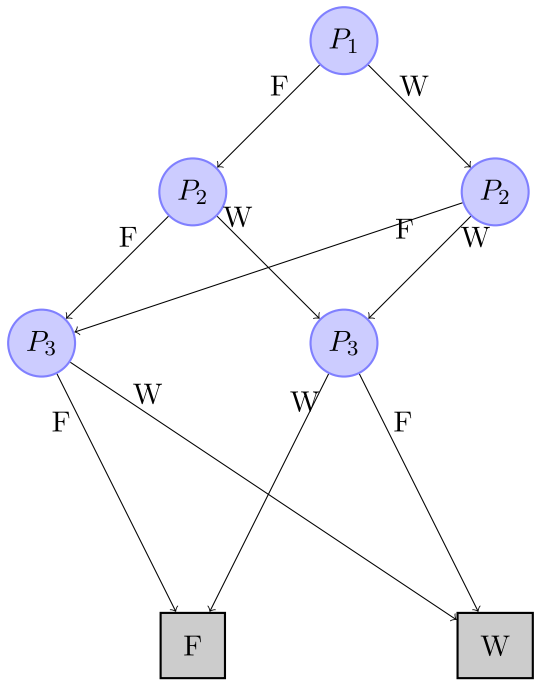


Lösung zu Aufgabe 18

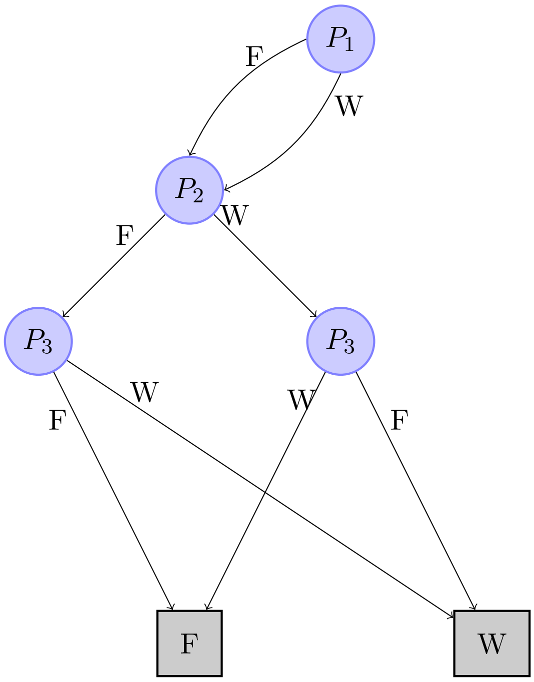
1. Schritt:



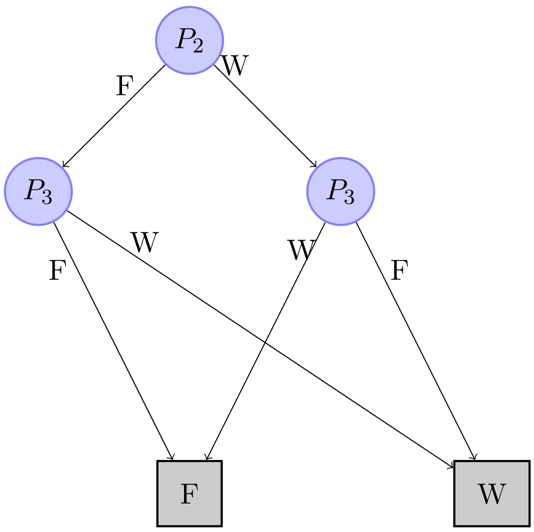
2. Schritt:



3. Schritt:



4. Schritt:



Aufgabe 19

Gegeben sei die Formel

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

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

Erstellen Sie einen reduzierten Shannongraphen (BDD) für F.

Lösung zu Aufgabe 19

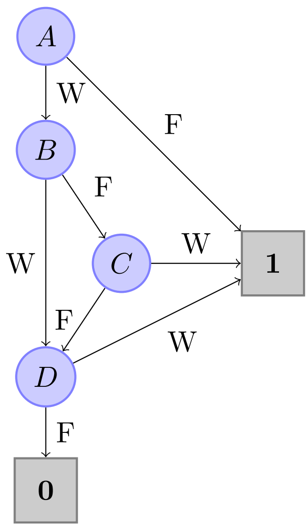


Abbildung 1.1: Shannon-Graph zu Aufgabe 19

Siehe Abbildung 1.1.

Wenn man den Graphen nach Algorithmus erstellt, erhält man zunächst 3 Knoten mit Beschriftung D, deren Untergraphen aber isomorph sind und der Graph daher auf einen mit einem solchen Knoten reduziert werden kann und muss.

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.

Lösung zu Aufgabe 20

Abbildung 1.2 zeigt den gesuchten BDD. Wie man sieht ist die Reihenfolge der Variablen bei BDDs durchaus von Bedeutung!

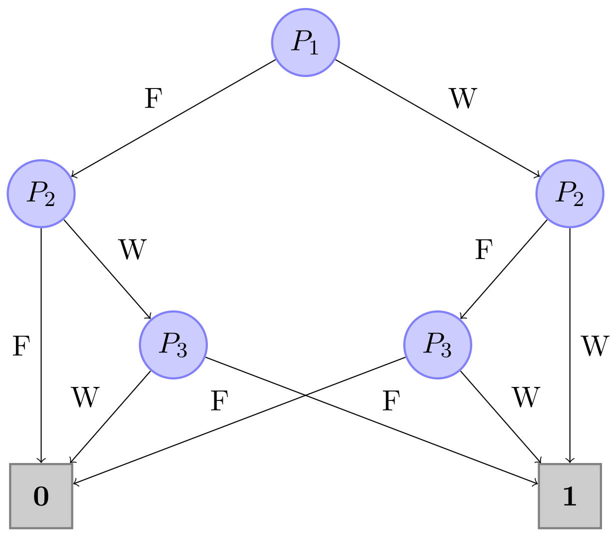


Abbildung 1.2: Shannon-Graph zu Aufgabe 20

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.

Lösung zu Aufgabe 21

Geht man streng nach Schema vor, so beginnt man mit einem vollständigen Entscheidungsbaum (s. Abb. 1) und wendet darauf das Reduktionsverfahren aus der Vorlesung an. Zunächst wird man feststellen, dass die P_4-Unterbäume wegen Isomorphie auf zwei reduziert werden können. Im entstehenden Graphen sind je zwei bei einem P_3-Knoten beginnende Untergraphen isomorph, die beiden P_2 bleiben erhalten. Insgesamt ergibt sich Abbildung 2.

Man kann auch direkt auf diese Darstellung kommen, wenn man von der Aufgabenstellung selbst ausgeht. Es spielt bei der Auswertung des Graphen keine Rolle in welcher Nullen und Einsen aufeinander folgen, einzig die bisherige Parität der Eingabe ist relevant. Z.B. sollten wir uns beim Auswerten von P_4 im selben Knoten befinden, egal, ob $(P_1, P_2, P_3) = (1, 0, 0)$ oder $(0, 1, 0)$ oder $(1, 1, 1)$ war. Einzig die bisherige Parität und die Belegung von P_4 sind entscheidend für die weitere Auswertung. Da es nur 2 Paritätszustände gibt, ist klar, dass es für $i \geq 2$ genau 2 Knoten mit der Beschriftung P_i geben muss. Eine 1 führt dabei zur jeweils anderen „Paritäts-Gruppe", eine 0 erhält die Parität.

Weiterführende Frage: Wie sieht der reduzierte Shannongraph für die allgemeine Funktion f_n aus?

Das oben gessagte gilt auch für allgemeines n: Das Verhalten hängt nicht von der Belegung der vorangegangenen Variablen ab, sondern nur von deren Parität, damit wird es weiter für jede Variable zwei Knoten geben, für jede Parität einen.

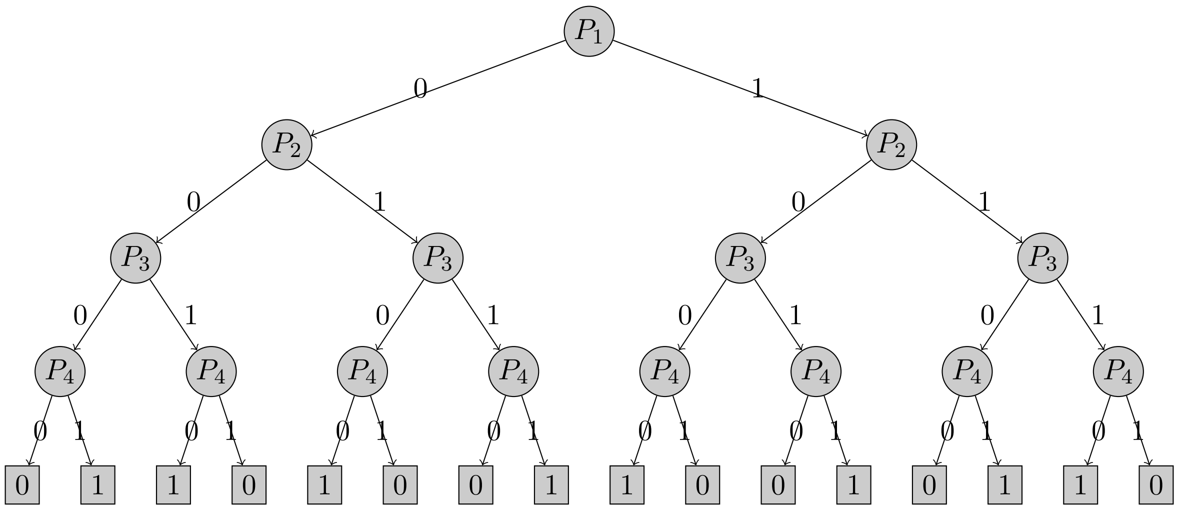


Abbildung 1.3: Ausgangsbaum für Aufgabe 21

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

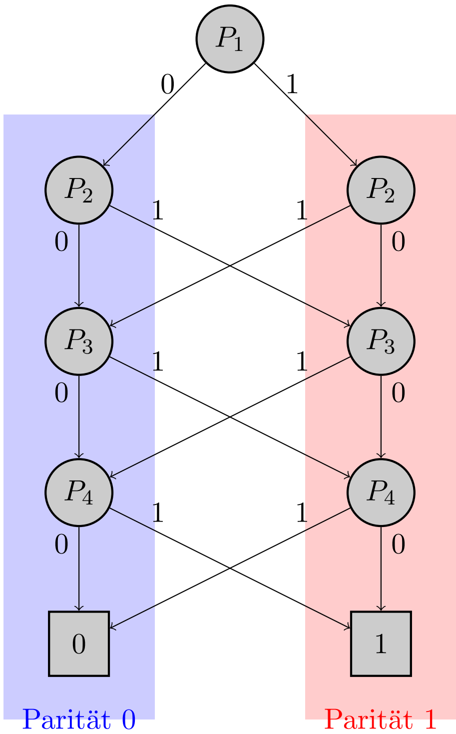


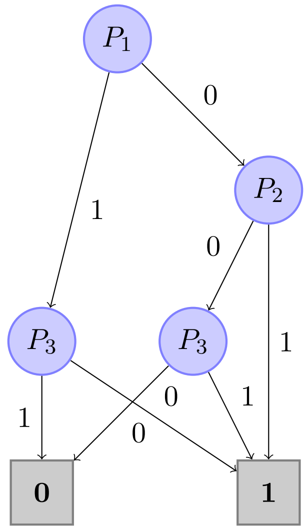
Abbildung 1.4: Shannongraph zu Aufgabe 21

Aufgabe 22

Geben Sie zu folgendem Shannongraphen je eine äquivalente aussagenlogische Formel in

(a) disjunktiver Normalform und

(b) konjunktiver Normalform an.



Lösung zu Aufgabe 22

(a) Die natürlichste DNF ist die Disjunktion aller Pfade zur **1**. Die genommenen Kanten eines Pfades werden dabei konjunktiv verknüpft: Bei Kanten-Markierung **1** mit dem Literal des verlassenen Knotens, bei Kanten-Markierung **0** mit der Negation des entsprechenden Literals.

$$(P_1 \wedge \neg P_3) \vee (\neg P_1 \wedge \neg P_2 \wedge P_3) \vee (\neg P_1 \wedge P_2)$$

(b) Wie so oft ist das das Duale: Die Konjunktion aller Pfade zur 0. Die genommenen Kanten eines Pfades werden dabei disjunktiv verknüpft: Bei Kanten-Markierung $\boxed{\mathbf{0}(!)}$ mit dem Literal des verlassenen Knotens, bei Kanten-Markierung $\boxed{\mathbf{1}(!)}$ mit der Negation des entsprechenden Literals.

$$(\neg P_1 \vee \neg P_3) \wedge (P_1 \vee P_2 \vee P_3)$$

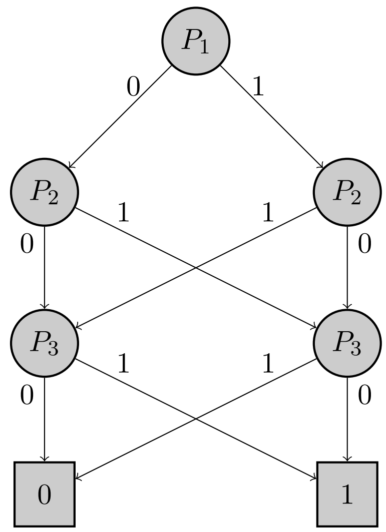
Idee: Während man bei (a) alle möglichen Wege zur **1** aufzählt, stellt man in (b) Bedingungen auf, damit die **0** vermieden wird.

Aufgabe 23

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

(a) disjunktiver Normalform und

(b) konjunktiver Normalform an.



Lösung zu Aufgabe 23

Zu (a): Die natürlichste DNF ist die Disjunktion aller Pfade zur **1**. Die genommenen Kanten eines Pfades werden dabei konjunktiv verknüpft: Bei Kanten-Markierung **1** mit dem Literal des verlassenen Knotens, bei Kanten-Markierung **0** mit der Negation des entsprechenden Literals.

$$(P_1 \wedge \neg P_2 \wedge \neg P_3) \vee (P_1 \wedge P_2 \wedge P_3) \vee (\neg P_1 \wedge P_2 \wedge \neg P_3) \vee (\neg P_1 \wedge \neg P_2 \wedge P_3)$$

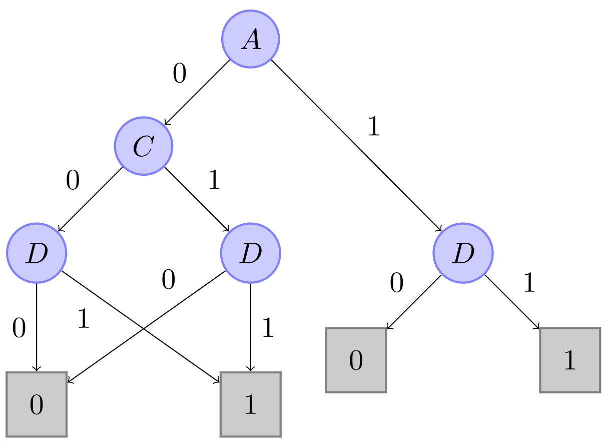
Zu (b): Wie so oft ist das das Duale: Die Konjunktion aller Pfade zur 0. Die genommenen Kanten eines Pfades werden dabei disjunktiv verknüpft: Bei Kanten-Markierung $\boxed{\mathbf{0}(!)}$ mit dem Literal des verlassenen Knotens, bei Kanten-Markierung $\boxed{\mathbf{1}(!)}$ mit der Negation des entsprechenden Literals.

$$(P_1 \vee P_2 \vee P_3) \wedge (P_1 \vee \neg P_2 \vee \neg P_3) \wedge (\neg P_1 \vee \neg P_2 \vee P_3) \wedge (\neg P_1 \vee P_2 \vee \neg P_3)$$

Idee: Während man bei (a) alle möglichen Wege zur 1 aufzählt, stellt man in (b) Bedingungen auf, damit die 0 vermieden wird.

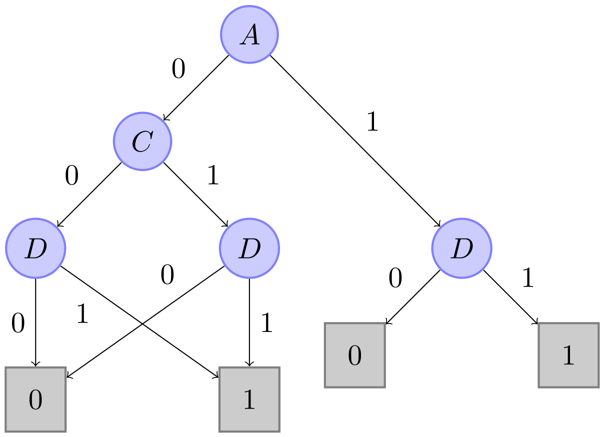
Aufgabe 24

Geben Sie zu dem dargestellten Shannongraphen den reduzierten Shannongraphen an.

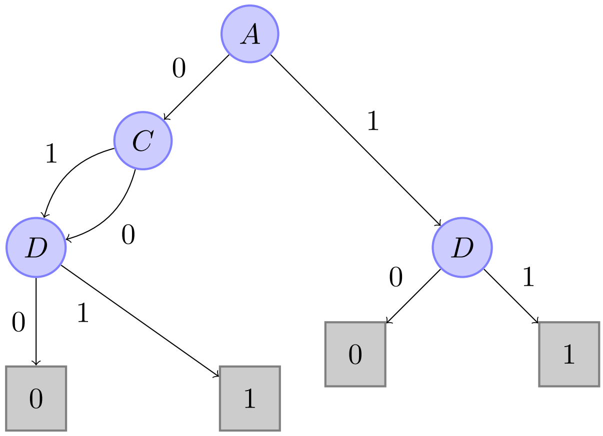


Lösung zu Aufgabe 24

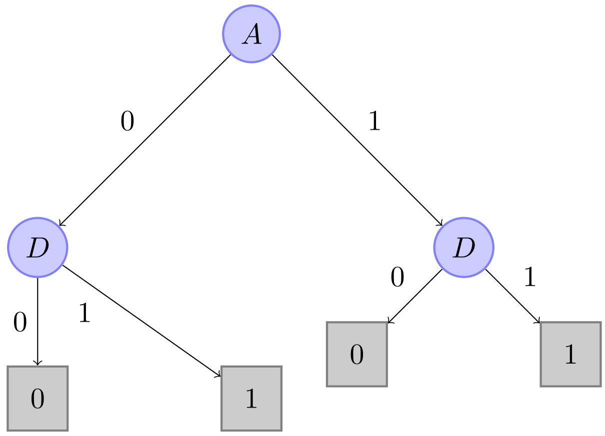
Die notwendigen Reduktionsschritte können Abbildung 1.5 entnommen werden.



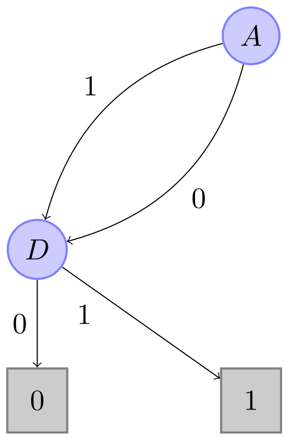
(a) Ausgangsgraph



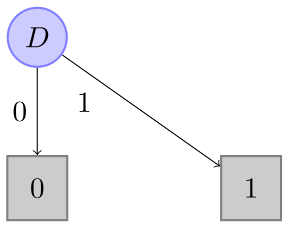
(b) Reduktion isomorpher Teilgraphen



(c) Elimination doppelter Kanten



(d) Reduktion isomorpher Teilgraphen



(e) Elimination doppelter Kanten

Abbildung 1.5: Reduktion des Shannongraphen

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?

Lösung zu Aufgabe 25

(a) Die Formel $A \vee \neg A$ ist Horn und erfüllbar. Implikationsschreibweise:

$$A \rightarrow A$$

Modell: $I(A) = F$.

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

ist nicht Horn (da die erste und dritte Disjunktion mehr als ein positives Literal hat).

Allerdings gehört diese Formel zu der sog. Formelklasse *Renamable Horn*. Das sind solche Formeln, die man in eine Hornformel transformieren kann, indem man für eine, mehrere oder auch alle der aussagenlogischen Variablen X in der Klausel (zugleich) alle positiven Vorkommen von X durch $\neg X$ ersetzt und alle negativen Vorkommen $\neg X$ durch X. Die Erfüllbarkeit der Formel bleibt dabei erhalten (evtl. Modelle der neuen und der alten Formel sind „Spiegelbilder" voneinander). Die Erfüllbarkeit der neuen Hornformel und damit auch die Erfüllbarkeit der alten Formel) kann dann mit dem üblichen Markierungsalgorithmus getestet werden.

Vertauscht man in diesem Beispiel die Polarität der Literale A und C, so erhält man eine Hornformel:

$$(\neg A \vee B) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C) \wedge C \quad .$$

Implikationsschreibweise:

$$\begin{array}{l} A \rightarrow B \\ B \wedge C \rightarrow A \\ A \wedge B \wedge C \rightarrow \mathbf{0} \\ C \end{array}$$

Die umbenannte Formel ist erfüllbar (Modell: $I(A) = F, I(B) = F, I(C) = T$), somit hat auch die ursprüngliche Formel ein Modell (mit entsprechend invertierter Polarität der Literale lautet das Modell: $I(A) = T, I(B) = F, I(C) = F$).

(c) Die Formel $(A \vee B) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee \neg B \vee C) \wedge \neg C$ ist weder Horn noch Renamable Horn. Diese Formel ist jedoch „fast" Horn. In solchen Fällen ist es möglich, eine Fallunterscheidung über die Belegungen der „störenden" Literale vorzunehmen und die Erfüllbarkeit der verbleibenden Hornformeln mit dem Markierungsalgorithmus zu entscheiden.

Das störende Literal ist hier A. Setzen wir zuerst $I(A) = F$, erhalten wir die Formel:

$$\begin{array}{l} B \\ B \rightarrow C \\ C \rightarrow \mathbf{0} \end{array}$$

Diese ist unerfüllbar. Setzen wir nun $I(A) = W$, so erhalten wir die Formel:

$$C \to B$$
$$C \to \mathbf{0}$$

Diese Formel ist erfüllbar und hat als Modell $I(B) = F$, $I(C) = F$. Da wir in der Fallunterscheidung $I(A) = W$ gesetzt haben, lautet das Gesamtmodell also: $I(A) = W, I(B) = F$, $I(C) = F$.

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

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

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

Lösung zu Aufgabe 26

(a) (i) Zunächst Fakten markieren: P_1 und P_3
$(\boxed{P_1} \wedge P_2 \to \boxed{P_3}) \wedge (\boxed{P_1} \wedge \boxed{P_3} \to P_4) \wedge \boxed{P_1} \wedge (P_2 \to P_4) \wedge \boxed{P_3}$
(ii) Wegen $P_1 \wedge P_3 \to P_4$ muss P_4 auch markiert werden:
$(\boxed{P_1} \wedge P_2 \to \boxed{P_3}) \wedge (\boxed{P_1} \wedge \boxed{P_3} \to \boxed{P_4}) \wedge \boxed{P_1} \wedge (P_2 \to \boxed{P_4}) \wedge \boxed{P_3}$
(iii) Keine weitere Markierung möglich und keine Widersprüche $\Longrightarrow$ Erfüllbar

Bei dieser Hornformel ist erkennbar, dass jede Klausel ein positives Literal enthält und somit die konstante Interpretation $I_W \equiv W$, die jede Variable zu W auswertet, die Formel erfüllt.

(b) (i) Zunächst die Fakten markieren: P_5
$\boxed{P_5} \wedge (P_2 \wedge P_4 \to \mathbf{0}) \wedge (\boxed{P_5} \to P_1) \wedge (P_2 \wedge \boxed{P_5} \to P_4) \wedge (P_1 \to P_2)$
(ii) Wegen $P_5 \to P_1$ muss auch P_1 markiert werden.
$\boxed{P_5} \wedge (P_2 \wedge P_4 \to \mathbf{0}) \wedge (\boxed{P_5} \to \boxed{P_1}) \wedge (P_2 \wedge \boxed{P_5} \to P_4) \wedge (\boxed{P_1} \to P_2)$
(iii) Wegen $P_1 \to P_2$ muss auch P_2 markiert werden.
$\boxed{P_5} \wedge (\boxed{P_2} \wedge P_4 \to \mathbf{0}) \wedge (\boxed{P_5} \to \boxed{P_1}) \wedge (\boxed{P_2} \wedge \boxed{P_5} \to P_4) \wedge (\boxed{P_1} \to \boxed{P_2})$
(iv) Wegen $P_2 \wedge P_5 \to P_4$ muss auch P_4 markiert werden.
$\boxed{P_5} \wedge (\boxed{P_2} \wedge \boxed{P_4} \to \mathbf{0}) \wedge (\boxed{P_5} \to \boxed{P_1}) \wedge (\boxed{P_2} \wedge \boxed{P_5} \to \boxed{P_4}) \wedge (\boxed{P_1} \to \boxed{P_2})$
(v) In der Klausel $P_2 \wedge P_4 \to \mathbf{0}$ sind alle Variablen im Rumpf markiert, der Kopf enthält aber $\mathbf{0}$ $\Longrightarrow$ Nicht erfüllbar

(c) Diese Formel enthält keine Fakten $\Longrightarrow$ Erfüllbar, z.B. durch die Belegung $I_F \equiv F$, die jede Variable zu F auswertet.

(d) Die Formel $A \wedge (\neg A \vee B) \wedge (\neg B \vee \neg C \vee D) \wedge \neg E \wedge (\neg A \vee \neg C) \wedge D$ ist erfüllbar. Implikationsschreibweise:

$$A \wedge (A \to B) \wedge (B \wedge C \to D) \wedge (E \to \mathbf{0}) \wedge (A \wedge C \to \mathbf{0}) \wedge D$$

Modell: $I(A) = W$, $I(B) = W$, $I(C) = F$, $I(D) = W$, $I(E) = F$.

Aufgabe 27

Seien $I, J : \Sigma \to \{W, F\}$ aussagenlogische Interpretationen, dann wird das **Produkt** $I \times J : \Sigma \to \{W, F\}$ 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.*

Lösung zu Aufgabe 27

- **φ Hornklausel $\implies$ Jedes Produkt erfüllender Interpretationen erfüllt φ**

  Sei φ eine Hornklausel. Diese ist (oBdA) entweder von der Form $\varphi = \neg P_1 \vee \ldots \vee \neg P_n \vee Q$ oder von der Form $\varphi = \neg P_1 \vee \ldots \vee \neg P_n$, jeweils für AL-Variablen P_i und ein $n \in \mathbb{N}$.

  Seien ferner $I, J : \Sigma \to \{W, F\}$ zwei Interpretationen mit $\text{val}_I(\varphi) = \text{val}_J(\varphi) = W$. So ist zu zeigen, dass $\text{val}_{I\times J}(\varphi) = W$.

  Enthält φ kein positives Literal, so gibt es wegen $\text{val}_I(\varphi) = W$ ein $i \in \mathbb{N}$ mit $1 \leq i \leq n$ mit $I(P_i) = F$. Damit gilt nach Def. auch $(I \times J)(P_i) = F$ und damit auch $\text{val}_{I\times J}(\varphi) = W$.

  Enthält φ aber ein positives Literal Q, so ist entweder $I(P_i) = F$ oder $J(P_i) = F$ für ein geeignetes i wie im voranstehenden Fall, oder es ist ist $I(P_k) = J(P_k) = W$ für alle an φ beteiligten negativen Literale P_k. Dann muss aber $I(Q) = J(Q) = W$ gelten, damit I und J erfüllende Interpretationen sind. Damit gilt aber auch $(I \times J)(Q) = W$ und $\text{val}_{I\times J}(\varphi) = W$.

- **φ keine Hornklausel $\implies$ Es gibt ein Produkt erfüllender Interpretationen, das φ nicht erfüllt**

  Eine Nicht-Hornklausel enthält mindest zwei positive Literale. Sei also $\psi = P_1 \vee P_2 \vee R$ eine Klausel, in der die beiden verschiedenen AL-Variablen P_1 und P_2 als positive Literale auftreten. Der Rest der Disjunktion ist in R zusammengefasst (und enthalte nicht mehr P_1 und P_2).

  Sei I eine Belegung mit $I(P_1) = W, I(P_2) = F$ und
  sei J eine Belegung mit $J(P_1) = F, J(P_2) = W$. Dann ist offensichtlich $val_I(\psi) = val_J(\psi) = W$ erfüllt, aber für das Produkt gilt: $(I \times J)(P_1) = (I \times J)(P_2) = F$. Wenn nun I und J so gewählt sind, dass sie R nicht zu W auswerten (das geht!), so gilt: $\text{val}_{I\times J}(\psi) = F$.

  Für Klauseln mit (mind.) zwei positiven Literalen gilt die Aussage also nicht! $\square$

1.6 DPLL

Aufgabe 28

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

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

unerfüllbar ist.

Lösung zu Aufgabe 28

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.

- Fall S_B: Im zweiten Schritt wird hier die Einerklausel $\{C\}$ gewählt und wahr gemacht:

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

  Es entsteht die leere Klausel, also ist die Menge S_B unerfüllbar.

- Fall $S_{\neg B}$: 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.

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

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.

Lösung zu Aufgabe 29

Wähle die Einerklausel $\{\neg P\}$.

Ergebnis der Vereinfachung von S mit $\{\neg P\}$ ist die Menge S', bestehend aus:

$\{ Q, T \}$ $\{ \neg Q, R \}$ $\{ \neg R, S \}$
$\{ \neg R, \neg S, T \}$ $\{ \neg R, \neg T \}$ $\{ R, \neg T \}$

Die Menge S' enthält keine Einerklauseln. Wir widerlegen $S' \cup \{Q\}$ und $S' \cup \{\neg Q\}$.

Zur Widerlegung von $S' \cup \{Q\}$:
Ergebnis der Vereinfachung von $S' \cup \{Q\}$ mit $\{Q\}$ ist:

$\{ R \}$ $\{ \neg R, S \}$ $\{ \neg R, \neg S, T \}$ $\{ \neg R, \neg T \}$ $\{ R, \neg T \}$

Ergebnis der Vereinfachung dieser Klauselmenge mit $\{R\}$ ist:

$\{ S \}$ $\{ \neg S, T \}$ $\{ \neg T \}$

Ergebnis der Vereinfachung dieser Klauselmenge mit $\{S\}$ ist:

$\{ T \}$ $\{ \neg T \}$

Ergebnis der Vereinfachung dieser Klauselmenge mit $\{T\}$ ist:

$\square$

Damit ist, da nun die leere Klausel enthalten ist, die Klauselmenge $S' \cup \{Q\}$ widerlegt.

Zur Widerlegung von $S' \cup \{\neg Q\}$:
Ergebnis der Vereinfachung von $S' \cup \{\neg Q\}$ mit $\{\neg Q\}$ ist:

$\{ T \}$ $\{ \neg R, S \}$ $\{ \neg R, \neg S, T \}$ $\{ \neg R, \neg T \}$ $\{ R, \neg T \}$

Ergebnis der Vereinfachung dieser Klauselmenge mit $\{T\}$ ist:

$\{ \neg R, S \}$ $\{ \neg R \}$ $\{ R \}$

Ergebnis der Vereinfachung dieser Klauselmenge mit $\{R\}$ ist:

$\{ S \}$ $\square$

Damit ist, da nun die leere Klausel enthalten ist, auch die Klauselmenge $S' \cup \{\neg Q\}$ widerlegt.

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 $\mathit{Var} = \{x, y, z\}$.

Lösung zu Aufgabe 30

(a) $j(f(x), g(x), h(z), k)$ ist ein wohlgeformter Term.

(b) $\forall y \exists p\, p(y)$ ist weder Term noch Formel. In PL1 ist es nicht möglich, über Prädikatensymbole zu quantifizieren ($\exists p$).

(c) $\forall x \forall z\, (g(f(z), f(y)) \to z)$ ist weder Term noch Formel. Implikation zwischen Termen ist nicht wohlgeformt.

(d) $\forall x \exists y\, (p(f(\underset{\substack{\uparrow \\ \text{gebunden}}}{x})) \to q(\overset{\substack{\text{gebunden} \\ \downarrow}}{y}, \underset{\substack{\uparrow \\ \text{frei}}}{z}))$ ist eine Formel. Die Variablenvorkommen sind entsprechend markiert.

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.

$$\begin{array}{rlll} \text{(i)} & \sigma = \{x/c,\ y/f(c, g(x))\} & & F = \forall x(p(g(x), f(x, y)) \lor q(x)) \\ \text{(ii)} & \sigma = \{x/f(g(x), c)\} & & F = \exists y(p(x, y) \lor \exists z \forall x(f(z, c) \doteq f(c, x))) \\ \text{(iii)} & \sigma = \{y/g(x),\ z/g(y)\} & & F = p(x, y) \to \forall x(q(f(x, z)) \lor \exists y(q(f(x, y)))) \end{array}$$

(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)	$F = f(g(y), h(y, g(y)))$	$G = f(z, h(g(x), g(g(x))))$

<u>Lösung zu Aufgabe 31</u>

(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.

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

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

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

(b) (i) unifizierbar. Robinson ergibt:

$\mu_0 = id$	$\mu_0(F) = f(\boxed{x}, z, z)$	$\mu_0(G) = f(\boxed{g(a, y)}, h(v), h(y))$
$\mu_1 = \{x/g(a, y)\}$	$\mu_1(F) = f(g(a, y), \boxed{z}, z)$	$\mu_1(G) = f(g(a, y), \boxed{h(v)}, h(y))$
$\mu_2 = \{x/g(a, y), z/h(v)\}$	$\mu_2(F) = f(g(a, y), h(v), h(\boxed{v}))$	$\mu_2(G) = f(g(a, y), h(v), h(\boxed{y}))$
$\mu_3 = \{x/g(a, y), z/h(y), v/y\}$	$\mu_3(F) = \mu_3(G) = f(g(a, y), h(y), h(y))$	

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

(ii) unifizierbar. Robinson ergibt:

$\mu_0 = id$	$\mu_0(F) = f(g(\boxed{x}, z), z, h(b, x))$ $\mu_0(G) = f(g(\boxed{a}, y), h(v, a), y)$
$\mu_1 = \{x/a\}$	$\mu_1(F) = f(g(a, \boxed{z}), z, h(b, a))$ $\mu_1(G) = f(g(a, \boxed{y}), h(v, a), y)$
$\mu_2 = \{x/a, z/y\}$	$\mu_2(F) = f(g(a, y), \boxed{y}, h(b, a))$ $\mu_2(G) = f(g(a, y), \boxed{h(v, a)}, y)$
$\mu_3 = \{x/a, z/h(v, a), y/h(v, a)\}$	$\mu_3(F) = f(g(a, h(v, a)), h(v, a), h(\boxed{b}, a))$ $\mu_3(G) = f(g(a, h(v, a)), h(v, a), h(\boxed{v}, a))$
$\mu_4 = \{x/a, z/h(b, a), y/h(b, a), v/b\}$	$\mu_4(F) = \mu_4(G) = f(g(a, h(b, a)), h(b, a), h(b, a))$

(iii) Im ersten Schritt des Robinsonalgorithmus erhält man:

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

Nun aber muss der Algorithmus abbrechen, weil $D(\{\mu_1(F), \mu_1(G)\}) = \{y, f(f(y))\}$ und die sind nicht unifizierbar, weil y eine Variable ist und in $f(f(y))$ auftritt.

(iv) unifizierbar. Der Robinsonalgorithmus mit Zwischenergebnissen:

$$\begin{array}{lll} \mu_0 = id & \mu_0(F) = f(\boxed{g(y)}, h(y, g(y))) & \mu_0(G) = f(\boxed{z}, h(g(x), g(g(x)))) \\ \mu_1 = \{z/g(y)\} & \mu_1(F) = f(g(y), h(\boxed{y}, g(y))) & \mu_1(G) = f(g(y), h(\boxed{g(x)}, g(g(x)))) \\ \mu_2 = \{z/g(g(x)), y/g(x)\} & \multicolumn{2}{c}{\mu_2(F) = \mu_2(G) = f(g(g(x)), h(g(x), g(g(x))))} \end{array}$$

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.

Lösung zu Aufgabe 32

$$\begin{array}{rcl} s_n & := & g(x_1, x_2, \ldots, x_{n-1}, x_n) \\ t_n & := & g(c, f(x_1, x_1), f(x_2, x_2), \ldots, f(x_{n-1}, x_{n-1})) \end{array}$$

Die Länge $|s_n|$ von s_n ist $n+1$ und $|t_n|$ ist $3n-1$, also linear in n (Klammern und Kommata nicht gezählt). Der allgemeinste Unifikator instantiiert x_1 mit c und x_{i+1} mit $f(x_i, x_i)$ $(1 \leq i < n)$. Darum gilt

$$\begin{array}{rcll} |\sigma(x_1)| & = & 1 & \\ |\sigma(x_i + 1)| & = & 1 + 2 \cdot |\sigma(x_i)| & \text{für } 1 \leq i < n \end{array}$$

und also

$$|\sigma(x_i)| = 2^i - 1 \qquad \text{für } 1 \leq i \leq n$$

Schließlich

$$\begin{array}{rcl} |\sigma(s_n)| = |\sigma(t_n)| & = & 1 + \sum_{i=1}^{n} (2^i - 1) \\ & = & 2^{n+1} - n + 1 \end{array}$$

Die Länge von $\sigma_n(s_n) = \sigma(t_n)$ ist also exponentiell in n.

Aufgabe 33

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

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

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

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

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

Lösung zu Aufgabe 33

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

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

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

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

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.

Lösung zu Aufgabe 34

(a) Es ist klar, dass für $i = 1, 2, 3$ gilt $\mu_i \geqslant \mu_i$ (siehe auch nächste Teilaufgabe). Für alle anderen Paare:

- $\mu_1 \geqslant \mu_2$ mit Substitution $\{y/x, z/x\}$
- $\mu_1 \geqslant \mu_3$ mit Substitution $\{y/a, z/b\}$
- $\mu_2 \not\geqslant \mu_3$, da die Substitution x/a und x/b gleichzeitig substituieren müßte
- $\mu_2 \not\geqslant \mu_1$, da die Substitution x/y und x/z gleichzeitig substituieren müßte
- $\mu_3 \not\geqslant \mu_1$, da die Substitution x/a und x/y gleichzeitig substituieren müßte
- $\mu_3 \not\geqslant \mu_2$, da die Substitution r/a und r/x gleichzeitig substituieren müßte

(b) (i) Reflexivität: Es ist klar, dass $id \circ \theta = \theta$, also $\theta \geqslant \theta$ für alle θ.

(ii) Transitivität: $\theta \geqslant \sigma$ und $\sigma \geqslant \mu$ bedeutet die Existenz von σ_1, σ_2 so, dass $\sigma_1 \circ \theta = \sigma$ und $\sigma_2 \circ \sigma = \mu$. Nun gilt $(\sigma_2 \circ \sigma_1) \circ \theta = \sigma_2 \circ (\sigma_1 \circ \theta) = \sigma_2 \circ \sigma = \mu$. Die erste Gleichheit ergibt sich aus der Assoziativität, die anderen beiden aus der o.g. Existenzaussage. Damit haben wir bewiesen, dass eine Substitution existiert (nämlich $\sigma_2 \circ \sigma_1$), mit der $\theta \geqslant \mu$ für alle θ, σ, μ.

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.

Lösung zu Aufgabe 35

(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.

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

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

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

Lösung zu Aufgabe 36

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

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

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

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

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

Sei 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 $\mathsf{MININT} \leq \text{mod}_{\mathcal{Z}_{\text{Jint}}}(x) \leq \mathsf{MAXINT}$ die Normalisierungsfunktion für Java-Integer. Nach Definition gilt für die Operationen in $\mathcal{Z}_{\text{Jint}}$:

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

Für $k_2 := k_1 \overset{J}{+} 1$ gilt also die Behauptung.

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

$$\text{Für alle } x \in \mathbb{Z} \text{ mit } x > 0 \text{ gilt } 2 \overset{\mathbb{Z}}{*} x > x\ .$$

Wegen der der Verträglichkeit von $\overset{\mathbb{Z}}{*}$ mit der Addition in $\mathbb{Z}$ folgt aus $x > 0$, dass $x \overset{\mathbb{Z}}{+} x > x \overset{\mathbb{Z}}{+} 0$. Damit gilt ψ_b in $\mathcal{Z}$.

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

$$\text{Für alle } \mathbb{Z}_{\text{Jint}} \ni x > 0 \text{ gilt } x \overset{J}{+} x > x$$

Für $x = \mathsf{MAXINT}$ gilt $x \overset{J}{+} x = \text{mod}_{\mathcal{Z}_{\text{Jint}}}((2^{31}-1) \overset{\mathbb{Z}}{+} (2^{31}-1)) = \text{mod}_{\mathcal{Z}_{\text{Jint}}}(2^{32}-2) = -2$. Also ist $x \overset{J}{+} x = -2 \not> x$, 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 das minimale Element, das dies erfüllt.

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.

Lösung zu Aufgabe 37

(a)

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

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

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

also

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

Also ist ϕ_b *allgemeingültig*. Jede allgmeingültige Formel ist aber auch insbesondere *erfüllbar*.

(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

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

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

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

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!). Diese Formel lässt sich also mit den Mitteln, die wir in der AL verwendet haben, untersuchen, z.B. einer Wertetabelle.

Man kann auch eine geschickte Fallunterscheidung machen. Wenn $I(r) = W$ gewählt wird, so kann man die rechte Seite zu $\mathbf{1}$ vereinfachen. Die Formel ϕ_e ist also wahr, wenn r wahr ist. Wenn man $I(r) = F$ wählt, so stellt man fest, dass die linke Seite zu $\mathbf{0}$ vereinfacht werden kann. Die Formel ϕ_e ist also auch wahr, wenn r falsch ist.

Dies zeigt, dass die Formel aussagenlogisch allgemeingültig ist, also eine **Tautologie** ist. (Damit ist sie auch erfüllbar.)

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.

Lösung zu Aufgabe 38

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.

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):

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

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.

Lösung zu Aufgabe 39

(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 für eine strikte Halbordnung p 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 $z_1 \xrightarrow{I(p)} z_2 \xrightarrow{I(p)} \ldots \xrightarrow{I(p)} z_r \xrightarrow{I(p)} z_1$, so würde wegen der Transitiviät auch $z_1 \xrightarrow{I(p)} z_1$ 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.

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

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

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.

Lösung zu Aufgabe 40

Das Herbrand-Universum ist $D_H = \{\underbrace{f(f(\ldots f(}_{n}b)\ldots)) \mid n \in \mathbb{N}\}$

(a) Unendlich[1] viele. Für $I(p)$ kann jede beliebige Teilmenge der (unendlich großen) Menge D_H gewählt werden. $I(f)$ ist nicht veränderbar.

(b) 3, nämlich (D, I_0), (D, I_1) und (D, I_2) mit

$$\begin{array}{llllll} I_0(p) = \{ & b, & f(b), & f(f(b)), & f(f(f(b))), \ldots\} = D_H \\ I_1(p) = \{ & & f(b), & f(f(b)), & f(f(f(b))), \ldots\} = D_H \setminus \{b\} \\ I_2(p) = \{ & & & f(f(b)), & f(f(f(b))), \ldots\} = D_H \setminus \{b, f(b)\} \end{array}$$

(c) Um das gewünschte Resultat zu erzielen, muss man ein Universum wählen, in dem nicht jedes Element durch f und b dargestellt werden kann.

Sei also $D = D_H \cup \{c\}$. Es gibt keinen Grundterm t, für den $\mathrm{val}(t) = c$ in Herbrand-Interpretationen gelten kann. Ist nun $I(p) = D_H$ (also ohne c) und $I(f)(c) = c$ und I identisch zu I_H, wo letzteres definiert ist, so gilt offensichtlich (1), da diese Formel keine Bedingungen an c stellt. (2) gilt jedoch nicht, da $\mathrm{val}_{I,\beta}(p(f(f(x)))) = F$ für $\beta(x) = c$ ist.

Alternative Lösung: Wähle (D, I) mit $D = \mathbb{Z}$, $I(f) : x \mapsto x + 1$, $I(b) = 0$, und $I(p) = \{x \in \mathbb{Z} \mid x \geq 0\}$. Auch dann ist (1) erfüllt, nicht aber (2).

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. $I(\forall y \ (q(f(x), y) \to p(g(x, y))))$

[1] sogar überabzählbar unendlich

Lösung zu Aufgabe 41

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

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

In der Aufgabenstellung wurde die Notation x^I, sowie y^I analog zur Angabe der Interpretation der Funktions- und Prädikatsymbole verwendet. Da x und y Variablen sind, wäre jedoch die Angabe einer Variablenbelegung β stattdessen die formal korrekte Vorgehensweise (also: $\beta(x) = \sqrt{2}$, sowie $\beta(y) = -1$).

Der Übersichtlichkeit wegen ist im Folgenden die nicht ganz korrekte, informelle Schreibweise der Variablenbelegung als x^I etc. beibehalten.

Bestimmen Sie den Wert folgender Terme und Formeln:

1. $I(g(f(x), f(y)))$

   Lösung:

$$\begin{aligned}
I(g(f(x), f(y))) &= g^I(I(f(x)), I(f(y)))\\
&= f^I(I(x)) + f^I(I(y))\\
&= (x^I)^2 + (y^I)^2\\
&= (\sqrt{2})^2 + (-1)^2\\
&= 2 + 1\\
&= 3
\end{aligned}$$

2. $I(\forall x\ p(f(x)))$

   Lösung:
   Betrachten wir zunächst $I(p(f(x)))$:

$$I(p(f(x))) = p^I(f^I(x^I))$$

   $p^I(f^I(x^I))$ hat genau denn den Wert true, wenn $(x^I)^2 \geq 0$ ist. Da dies für jede Belegung von x mit Elementen aus U gilt, gilt auch $I_{x/d}(p(f(x))) = true$ für alle $d \in U$. Daraus folgt $I(\forall x\ p(f(x))) = true$

3. $I(\exists z \forall x \forall y\ q(g(x,y), z))$

   Lösung:
   Wir betrachten $I(q(g(x,y), z))$:

$$I(q(g(x,y), z)) = q^I(g^I(x^I, y^I))$$

   $q^I(g^I(x^I, y^I), z^I))$ ist genau dann wahr, wenn $x^I + y^I = z^I$ ist. Es gibt jedoch kein $z \in \mathbb{R}$, so dass für alle $x, y \in \mathbb{R}$ gilt: $x + y = z$
   Daraus folgt $I(\exists z\ \forall x\ \forall y\ q(g(x,y), z)) = false$

4. $I(\forall y(q(f(x),y) \to p(g(x,y))))$

Lösung:
In $\forall y\ (q(f(x),y) \to p(g(x,y)))$ kommt x frei vor und y gebunden. Daher ist $x^I = \sqrt{2}$. Außerdem ist:

$$I(q(f(x),y) \to p(g(x,y))) = q^I(f^I(x^I,y^I) \to p^I(g^I(x^I,y^I))$$

und $q^I(f^I(x^I,y^I) \to p^I(g^I(x^I,y^I))$ ist genau dann wahr, wenn

$$((x^I)^2 = y) \to ((x^I + y^I) \geq 0)$$
$$((\sqrt{2})^2 = y) \to ((\sqrt{2} + y^I) \geq 0)$$

ist. Betrachten wir nun den Wahrheitswert von

$$\forall y(((\sqrt{2})^2 = y) \to ((\sqrt{2} + y) \geq 0)))$$

Die Prämisse $((\sqrt{2})^2 = y)$ ist genau dann wahr, wenn y den Wert 2 hat. Für $y = 2$ ist jedoch auch die Konklusion $\sqrt{2} + 2 \geq 0$ wahr. Daraus folgt:

$$I(\forall y\ (q(f(x),y) \to p(g(x,y)))) = \mathit{true}$$

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 $\Sigma = (\emptyset, \{\mathit{kante}\}, \mathit{kante} \mapsto 2)$ gegeben. Weiterhin sei die Domäne D festgelegt als die Menge der Knoten. Die Interpretation des Prädikatsymbols $\mathit{kante}(u,v)$ 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: $(D,I(\mathit{kante}))$ ist zusammenhängend.

Lösung zu Aufgabe 42

In folgendem Widerspruchsbeweis benutzen wir den Endlichkeitssatz als Spezialfall des Kompaktheitssatzes, um zu zeigen, dass es keine Formel F wie in der Aufgabe gefordert geben kann.

Angenommen, es gäbe eine Formel F, die genau in denen Interpretationen (D,I) zu W auswertet, in denen der durch (D,I) beschriebene Graph: $(D,I(\mathit{kante}))$ zusammenhängend ist.

Seien $a,b \in \Sigma$. Die Aussage:

“es existiert kein Pfad zwischen a und b der Länge n $(n \in \mathbb{N}, n > 0)$”

wird formalisiert durch die Formel:

$$A_n := \neg(a \doteq b) \wedge \neg\exists x_1 \cdots \exists x_{n-1}((\mathit{kante}(a,x_1) \wedge \ldots \wedge \mathit{kante}(x_{n-1},b)) \vee (\mathit{kante}(b,x_{n-1}) \wedge \ldots \wedge \mathit{kante}(x_1,a)))\ .$$

Betrachten wir nun die Formelmenge

$$F \cup \{A_n \mid n \in \mathbb{N}, n > 0\}\ .$$

Jede endliche Teilmenge E dieser Menge hat ein Modell. Sei nämlich A_m die Formel mit dem größten in E vorkommenden Index. Dann ist

$$a^I = a_0$$
$$b^I = a_{m+1}$$
$$\mathit{kante}^I = \{(a_0,a_1), \cdots, (a_m,a_{m+1})\}$$

ein Modell von E.

Nach dem Endlichkeitssatz müsste es also ein Modell von $F \cup \{A_n \mid n \in \mathbb{N}, n > 0\}$ geben. Dies führt zum Widerspruch: F sagt aus, dass der Graph zusammenhängend sein muss und die Formelmenge $\{A_n \mid n \in \mathbb{N}, n > 0\}$ beschreibt, dass es zwischen a^I und b^I keinen Pfad irgendeiner Länge gibt, der Graph also nicht zusammenhängend sein kann.

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}.

Lösung zu Aufgabe 43

1. $\forall x(x \doteq a \vee x \doteq b \vee x \doteq c)$
2. $\exists x(\text{kills}(x, a))$
   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. $\neg\exists x \forall y(\text{hates}(x, y))$

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 $\Sigma_{\text{Verwandtschaft}}$.

Lösung zu Aufgabe 44

(a) $\forall x \exists y(\mathit{mutter}(y,x)) \;\wedge\; \forall x \forall y \forall z(\mathit{mutter}(x,z) \wedge \mathit{mutter}(y,z) \to x \doteq y)$

Das erste Konjunkt besagt, dass jede Person x (mindestens) eine Mutter y hat. Das zweite sagt aus, dass jede Person *höchstens* eine Mutter hat: Wenn es zwei Mütter x und y von z gibt, so müssen diese gleich sein.

(b) $\forall x \forall y\big((\mathit{mutter}(x,y) \vee \mathit{vater}(x,y)) \to (\neg \mathit{mutter}(y,x) \wedge \neg \mathit{vater}(y,x))\big)$

Wenn x Mutter oder Vater von y ist, so kann y weder Mutter von x von Vater von x sein.

(c)
$$\begin{aligned}\exists x \exists y\, (\;& (\mathit{vater}(x,\mathit{Donald}) \vee \mathit{mutter}(x,\mathit{Donald})) \\ \wedge\;& (\mathit{vater}(y,x) \vee \mathit{mutter}(y,x)) \\ \wedge\;& (\mathit{vater}(y,\mathit{Dagobert}) \vee \mathit{mutter}(y,\mathit{Dagobert}))\;)\end{aligned}$$

Dagobert und Donald sind Onkel und Neffe, wenn es zwei Personen x und y gibt, so dass x Elternteil von Donald ist und y Elternteil von sowohl Dagobert als auch von x.

Die Formel unter den Quantoren wird wahr, wenn für x und y die die Verwandtschaft vermittelnden Personen (Elternteil und Großelternteil) gewählt werden.

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.

Lösung zu Aufgabe 45

(a) Die Signatur besteht hier aus den einstelligen Funktionssymbolen *vater*, *mutter* sowie dem einstelligen Prädikatsymbol *reich* mit der ihres Namens entsprechenden Bedeutung. Die Bedeutung von *arm* ist in diesem Kontext als Negation des Prädikats *reich* definiert. Damit ergibt sich als Formalisierung der obigen Aussage:

$$\forall x\, (\neg reich(x) \to reich(vater(x))) \to \exists x\, (reich(x) \wedge (reich(vater(vater(x))) \vee reich(vater(mutter(x)))))$$

(b) Diese Aussage ist auch als Trinker-Paradoxon bekannt und wird durch folgende allgemeingültige Formel beschrieben:

$$\exists x\ (trinkt(x) \rightarrow \forall y\ trinkt(y))$$

(c) Die wörtliche Übersetzung liefert hier die erfüllbare Formel:

$$\forall x\ (barbier(x) \rightarrow \forall y\ \neg rasiert(y,y) \leftrightarrow rasiert(x,y))$$

In der Literatur ist eine andere Version dieser Aussage als Barbier-Paradoxon bekannt und lautet als Rätsel etwa wie folgt:

> Der Barbier zeichnet sich dadurch aus, dass er genau diejenigen rasiert, die sich nicht selbst rasieren. Rasiert der Barbier sich selbst?

Diese Formulierung fordert, im Gegensatz zur Aufgabenstellung, die Existenz eines solchen Barbiers, so dass sich nun als Formalisierung des Rätsels die unerfüllbare Formel

$$\forall y\ \neg rasiert(y,y) \leftrightarrow rasiert(b,y)$$

ergibt. Dabei ist b eine Konstante, die den Barbier bezeichnet.

Eine alternative Formalisierung ist auch:

$$\exists z\ barbier(z) \wedge \forall x\ (barbier(x) \rightarrow \forall y\ \neg rasiert(y,y) \leftrightarrow rasiert(x,y))$$

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

Lösung zu 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.

Die Notation y^I ist hier für Variablenbelegungen verwendet worden. Formal korrekt müsste die Aufgabenstellung also lauten:

> ... ist, muss z.B. für die im Aufgabenteil (a) gebildete Formel F gelten, dass $val_{I,\beta}(F) = W$ gdw. $\beta(y)$ eine Primzahl ist.

Des Weiteren wurden in der Aufgabenstellung keine Angaben über zu verwendende Konstanten aus den natürlichen Zahlen gemacht. Eine Lösungsmöglichkeit besteht darin, diese Konstanten zu definieren und deren Interpretation festzulegen, also:

$$1^I = 1, \text{ sowie } 2^I = 2$$

Die hier vorgestellte Lösung formalisiert die Eigenschaften der benötigten Elemente aus der Menge der natürlichen Zahlen – so etwa für die Zahl 1:

$$y \doteq 1 \equiv \forall z \ (q(y, z)) \ .$$

Die Konstante 2 lässt sich formalisieren als:

$$y \doteq 2 \equiv \overbrace{\forall z \ (q(y, z) \lor \underbrace{\forall v \ (q(z, v)))}_{z \doteq 1}}^{y \doteq 1 \lor y \doteq 2} \land \underbrace{\neg\forall w \ (q(y, w))}_{y \neq 1}$$

Formalisieren Sie mit Hilfe der Prädikatenlogik:

1. y ist eine Primzahl
   Lösung:
   $\forall x(p(x, y) \to \forall z \ (q(x, z)) \lor (x \doteq y)) \land \neg\forall z \ (q(y, z))$
2. y ist eine gerade Zahl
   Lösung:
   $\forall x \forall z \ (\overbrace{(q(x, z) \lor \forall v \ (q(z, v))) \land \neg\forall w \ (q(x, w))}^{x \doteq 2} \to p(x, y))$
3. ggt ist der größte gemeinsame Teiler der beiden Zahlen x und y
   Lösung:
   $p(ggt, x) \land p(ggt, y) \land \forall z(p(z, y) \land p(z, x) \to q(z, ggt))$
   Hierbei sind x, y und ggt freie Variablen.
4. kgV ist das kleinste gemeinsame Vielfache der beiden Zahlen x und y
   Lösung:
   $p(x, kgV) \land p(y, kgV) \land \forall z(p(y, z) \land p(x, z) \to q(kgV, z))$
   Mit den freien Variablen x, y und kgV.
5. x und y sind teilerfremde Zahlen
   Lösung:
   $\neg\exists z(p(z, x) \land p(z, y) \land \neg(\forall z \ (q(y, z))))$
6. zwischen zwei verschiedenen natürlichen Zahlen liegt stets eine natürliche Zahl
   Lösung:
   $\forall x \forall y \ (\neg(x \doteq y) \to \exists z \ (\neg(x \doteq z) \land \neg(y \doteq z) \land ((q(x, z) \land q(z, y)) \lor ((q(y, z) \land q(z, x))))))$

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.

Lösung zu Aufgabe 47

(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 $G \to G_{sko} \equiv \exists x(p(x)) \to p(c)$. 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 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:
>
> $$\text{val}_{\mathcal{D},\beta}(\sigma(A) \to \exists x A) = W$$

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. $\square$

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

(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 48

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

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

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.

$$\forall y \forall w((p(c,y) \lor p(c,d)) \land (p(c,y) \lor p(d,w)))$$

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

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

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

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

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

Aufgabe 49

Transformieren Sie die folgende Formel schrittweise in Skolemnormalform.

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

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

Lösung zu Aufgabe 49

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

i. **All-Abschluss:**

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

ii. **Bereinigen:**

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

iii. **Pränexnormalform:**

$$\begin{aligned}
& \forall z_1 \forall v \exists x \Big(\big(\forall z (r(z, v)) \to \forall x_1\ p(x_1, z_1) \big) \to (q(x) \lor r(v, x)) \Big) \\
\equiv\ & \forall z_1 \forall v \exists x \Big(\neg \big(\neg (\forall z\ r(z, v)) \lor \forall x_1\ p(x_1, z_1) \big) \lor (q(x) \lor r(v, x)) \Big) \\
\equiv\ & \forall z_1 \forall v \exists x \Big(\big(\forall z (r(z, v)) \land \neg \forall x_1\ p(x_1, z_1) \big) \lor (q(x) \lor r(v, x)) \Big) \\
\equiv\ & \forall z_1 \forall v \exists x \Big(\big(\forall z (r(z, v)) \land \exists x_1\ \neg p(x_1, z_1) \big) \lor (q(x) \lor r(v, x)) \Big) \\
\equiv\ & \forall z_1 \forall v \exists x \forall z \exists x_1 \Big(\big(r(z, v) \land \neg p(x_1, z_1) \big) \lor (q(x) \lor r(v, x)) \Big)
\end{aligned}$$

iv. **Skolemisieren:**

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

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

v. **Matrix in KNF:**

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

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?

Lösung zu Aufgabe 50

Zur Erinnerung das Vorgehen im aussagenlogischen Fall: Eine binäre Teilformel $A \circ B$ in einer Formel F, wobei A, B Literale sind und $\circ \in \{\land, \lor, \to, \leftrightarrow\}$, 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:

$$\forall x\Big(\big((p(x) \vee p(x)) \vee \neg p(x)\big) \wedge \big(p(c) \wedge \neg p(d)\big)\Big) \tag{2.3}$$

Diese Formel hat ein Modell (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):

$$\forall x\big(B \wedge C \wedge (A \leftrightarrow (p(x) \vee p(x))) \wedge (B \leftrightarrow (A \vee \neg p(x))) \wedge (C \leftrightarrow (p(c) \wedge \neg p(d)))\big) \tag{2.4}$$

Diese naive-falsche kKNF (2.4) von (2.3) hat kein Modell [2]. Die Formeln (2.3) und (2.4) 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:

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 $\mathrm{val}_{I,\beta}(F) = \mathrm{val}_{I,\beta}(F_X)$.

[2] 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 (2.4) geben.

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.

Lösung zu Aufgabe 51

Wir präsentieren hier die einzelnen Ableitungen im Kalkül, wobei

(Ax1)	für das Abschwächungsaxiom,
(Ax2)	für das Verteilungsaxiom,
(Ax3)	für das Kontrapositionsaxiom,
(MP n, m)	für Modus Ponens mit den beiden beteiligten Formeln (n) und (m),
(DT n)	für das Deduktionstheorem mit der Ausgangsformel (n)

notiert wird.

(a) Die Ableitung im Hilbertkalkül ist:

$$\begin{array}{rll}
 & \vdash & \neg A \to (\neg B \to \neg A) & (1) & \text{(Ax1)} \\
\{\neg A\} & \vdash & \neg B \to \neg A & (2) & \text{(DT 1)} \\
 & \vdash & (\neg B \to \neg A) \to (A \to B) & (3) & \text{(Ax3)} \\
\{\neg A\} & \vdash & A \to B & (4) & \text{(MP 2,3)} \\
 & \vdash & \neg A \to (A \to B) & (5) & \text{(DT 4)}
\end{array}$$

Aus der Korrektheit des Hilbertkalküls folgt die Behauptung.

(b) Die geschickte Instanziierung von B ist $\neg(\neg A \to A)$.

$$\begin{array}{rll}
 & \vdash \neg A \to (A \to \neg(\neg A \to A)) & (6)\ \text{Aus (5)} \\
 & \vdash \big[\neg A \to (A \to \neg(\neg A \to A))\big] \to \big[(\neg A \to A) \to (\neg A \to \neg(\neg A \to A))\big] & (7)\ \text{(Ax2)} \\
 & \vdash (\neg A \to A) \to (\neg A \to \neg(\neg A \to A)) & (8)\ \text{(MP 6,7)} \\
\{\neg A \to A\} & \vdash \neg A \to \neg(\neg A \to A) & (9)\ \text{(DT 8)} \\
 & \vdash \big[\neg A \to \neg(\neg A \to A)\big] \to \big[(\neg A \to A) \to A\big] & (10)\ \text{(Ax3)} \\
\{\neg A \to A\} & \vdash (\neg A \to A) \to A & (11)\ \text{(MP 9,10)} \\
\{\neg A \to A\} & \vdash A & (11)\ \text{DT(10)} \\
 & \vdash (\neg A \to A) \to A & (12)\ \text{DT(11)}
\end{array}$$

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: $M \vdash_{R_2} (\phi \land \neg\phi)$

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?

Lösung zu Aufgabe 52

(a) R_1 ist nicht korrekt.

$$(\phi \to \psi) \models \neg(\psi \to \neg\phi)$$

gilt nicht bzw. $(\phi \to \psi) \to \neg(\psi \to \neg\phi)$ ist nicht allgemeingültig.

R_1 kann vollständig sein. Denn dass etwas nicht allgemeingültiges ableitbar ist, widerspricht der Vollständigkeit des Kalküls keinesfalls. Ein Beispiel eines solchen inkorrekten, aber vollständigen Kalküls wäre der in der Vorlesung vorgestellte Kalkül **H**0 mit der zusätzlichen Regel

$$\frac{\phi \to \psi}{\neg(\psi \to \neg\phi)}$$

(b) R_2 kann korrekt sein.

Dass

$$M \vdash_{R_2} (\phi \land \neg\phi)$$

gelten soll, ist kein Widerspruch zur Korrektheit von R_2, da genau dann, wenn M unerfüllbar ist (also z.B. mit $M \equiv \{\neg(A \to A)\}$)

$$M \models (\phi \land \neg\phi)$$

gilt, bzw. $M \to (\phi \land \neg\phi)$ allgemeingültig ist.

R_2 kann vollständig sein. Auch hier widerspricht die Annahme, dass etwas ableitbar sein soll, nicht der Vollständigkeit des Kalküls.

Anmerkung: Die Frage war nur, ob der Kalkül korrekt bzw. vollständig sein *kann*. Daraus folgt aber nicht, dass der Kalkül auch tatsächlich korrekt (im Falle von R_2) und vollständig (im Falle von R_1 oder R_2) ist. Der Standard-Hilbertkalkül H0 aus der Vorlesung hat diese Eigenschaften. Aber da wir in dieser Aufgabe gerade nicht voraussetzen, dass $R_1 = H0$ oder $R_2 = H0$, wissen wir nicht genug über R_1 und R_2, um mit Bestimmtheit zu sagen, dass R_2 korrekt bzw. R_1 oder R_2 vollständig ist.

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

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

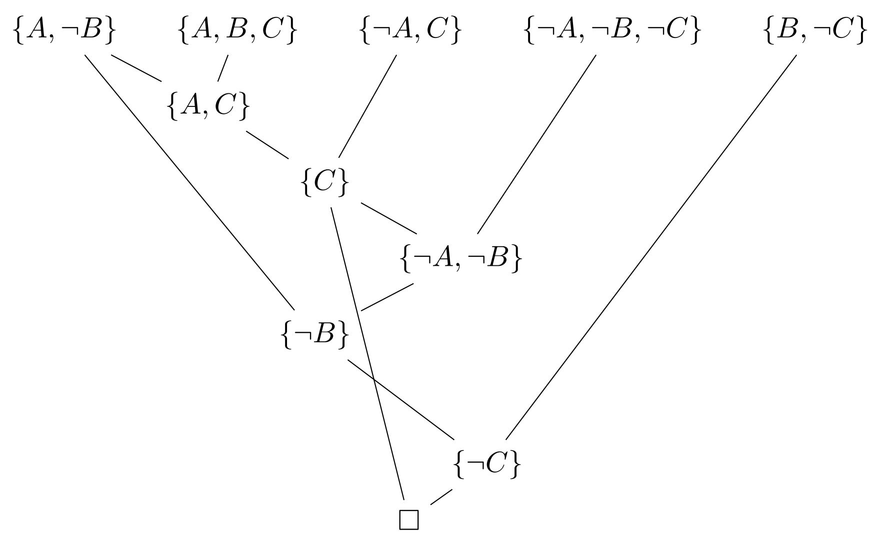
$$\neg A \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge \neg D) \vee (D \wedge B) \vee (\neg B \wedge C) \ ,$$

(c) die Allgemeingültigkeit der Formel

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

Lösung zu Aufgabe 53

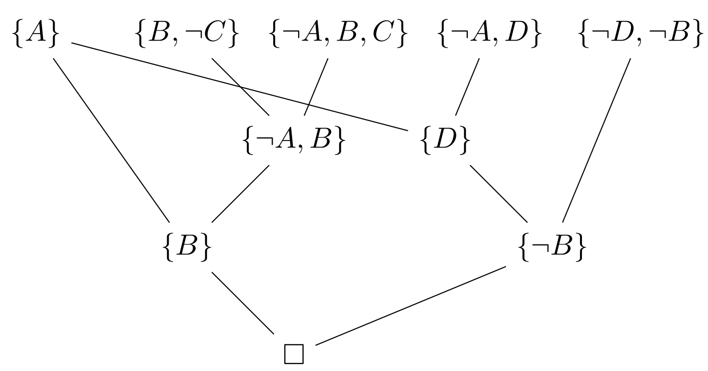
(a) 1. Schritt: Resolution



(b) 1. Schritt: Formel negieren

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

2. Schritt: Klauselschreibweise und Resolution



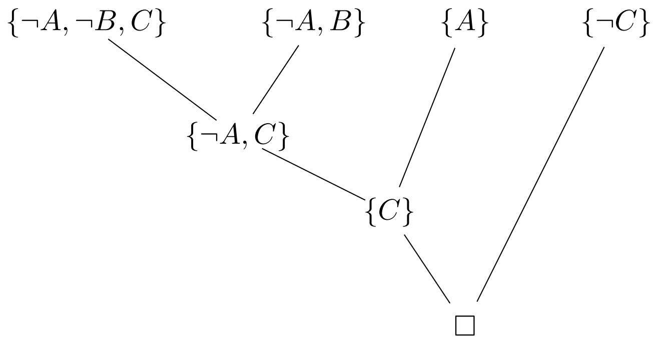
(c) 1. Schritt: Formel negieren

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

2. Schritt: In KNF transformieren

$$\begin{aligned}
&\neg((A \to (B \to C)) \to ((A \to B) \to (A \to C))) \equiv \\
&(A \to (B \to C)) \land \neg((A \to B) \to (A \to C)) \equiv \\
&(A \to (B \to C)) \land ((A \to B) \land \neg(A \to C)) \equiv \\
&(\neg A \lor (B \to C)) \land ((\neg A \lor B) \land (A \land \neg C)) \equiv \\
&(\neg A \lor \neg B \lor C) \land (\neg A \lor B) \land A \land \neg C
\end{aligned}$$

3. Schritt: Klauselschreibweise und Resolution



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

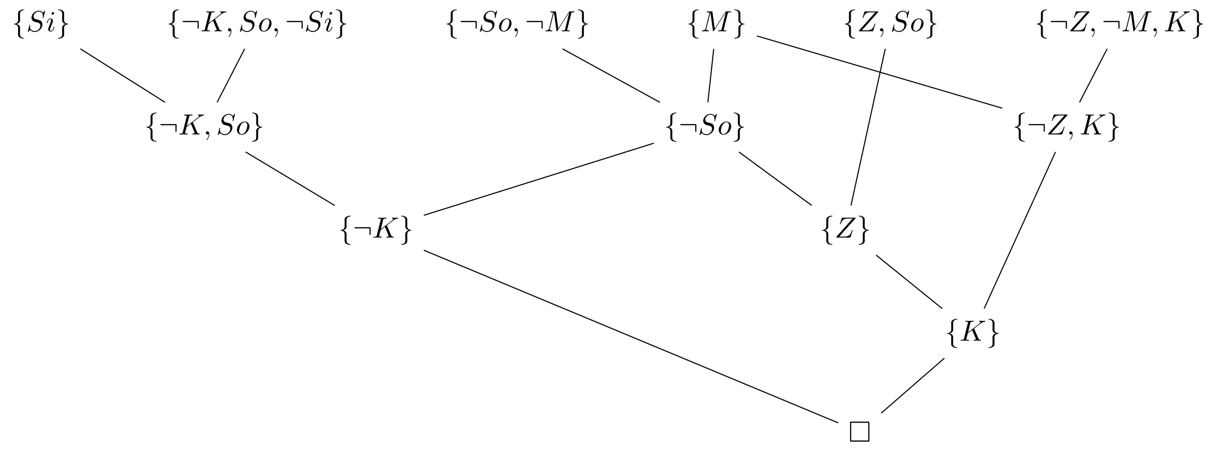
(b) Zeigen Sie mit Hilfe des Resolutionskalküls, dass ein solches Passwort nicht existieren kann.

Lösung zu Aufgabe 54

Formalisierung.

Das Passwort muss sicher sein, und man muss es sich merken können.	$Si \wedge M$
Passwörter beinhalten Zahlen oder Sonderzeichen oder beides.	$Z \vee So$
Ist das Passwort kurz und enthält keine Sonderzeichen, dann ist es nicht sicher.	$K \wedge \neg So \rightarrow \neg Si$
Ein Passwort mit Sonderzeichen kann man sich nicht merken.	$So \rightarrow \neg M$
Ein Passwort mit Zahlen muss kurz sein, damit man es sich merken kann.	$Z \wedge M \rightarrow K$

Beweis. Wir zeigen die Widersprüchlichkeit dieser Aussagen durch Ableitung einer leeren Klausel mit Resolution (vorher übersetzen wir die Formeln natürlich in Klauselform).



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!).

Lösung zu Aufgabe 55

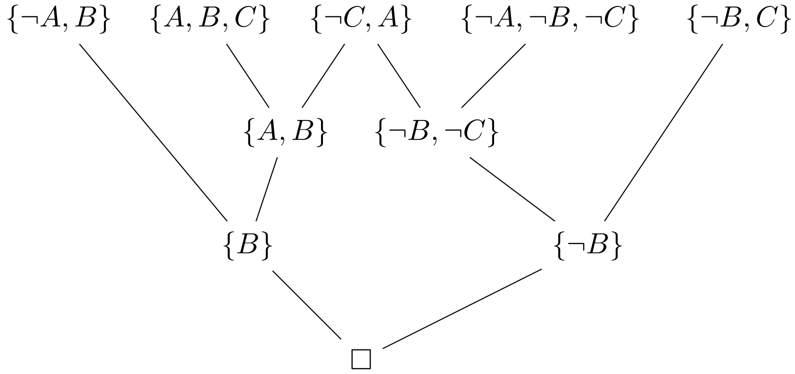
Diese Variante des Resolutionskalküls ist *nicht* vollständig, d.h., es gibt unerfüllbare Klauselmengen, aus denen nicht die leere Klausel abgeleitet werden kann.

Behauptung Die Klauselmenge

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

ist unerfüllbar, es gibt aber keine Resolutionsableitung, in der jede Klausel höchstens ein Mal benutzt wird.

Unerfüllbarkeit Folgender Resolutionsbeweis zeigt die Unerfüllbarkeit der Menge:



Zu zeigen: Es gibt keine Ableitung der leeren Klausel ohne mindestens eine Klausel mehrmals zu verwenden.

Folgendes ist dafür zu beobachten:

1. Bei jedem Resolutionsschritt nimmt die Anzahl der zur Verfügung stehenden Klauseln um genau eins ab.
2. Die leere Klausel kann in einem Schritt nur aus zwei Einerklauseln abgeleitet werden.

Wegen Punkt (i) kann bei fünf Ausgangsklauseln ein Beweis nur maximal *vier* Schritte umfassen, wobei nach dem vierten Schritt die leere Klausel entstehen muss. Wegen Punkt (ii) muss also wenigstens eine Einerklausel in einem Schritt (die andere dann in höchstens zwei) Schritten aus der Ausgangsmenge herleitbar sein. Resolviert man aber je zwei Klauseln aus der Menge, so stellt man fest, dass nie eine Einerklausel in einem Schritt herleitbar ist. Es gibt also keinen solchen Beweis.

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

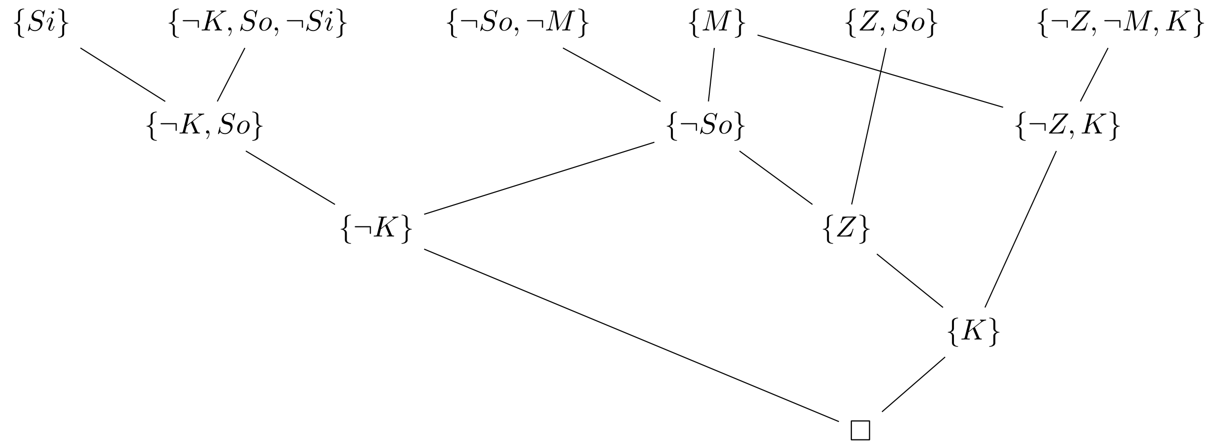
(b) Zeigen Sie mit Hilfe des Resolutionskalküls, dass ein solches Passwort nicht existieren kann.

Lösung zu Aufgabe 56

Formalisierung.

Das Passwort muss sicher sein, und man muss es sich merken können.	$Si \wedge M$
Passwörter beinhalten Zahlen oder Sonderzeichen oder beides.	$Z \vee So$
Ist das Passwort kurz und enthält keine Sonderzeichen, dann ist es nicht sicher.	$K \wedge \neg So \to \neg Si$
Ein Passwort mit Sonderzeichen kann man sich nicht merken.	$So \to \neg M$
Ein Passwort mit Zahlen muss kurz sein, damit man es sich merken kann.	$Z \wedge M \to K$

Beweis. Wir zeigen die Widersprüchlichkeit dieser Aussagen durch Ableitung einer leeren Klausel mit Resolution (vorher übersetzen wir die Formeln natürlich in Klauselform).



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.

Lösung zu Aufgabe 57

Betrachten wir die Klauselmenge $\{\{P, Q\}, \{\neg P, \neg Q\}\}$, die z.B. durch die Interpretation I mit $I(P) = W$ und $I(Q) = F$ erfüllt wird, also nicht unerfüllbar ist.

Die „Doppelresolution“ würde jedoch in einem Schritt die leere Klausel $\Box$ ableiten. Widerspruch zur Erfüllbarkeit!

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.

Lösung zu Aufgabe 58

Wir beweisen die Aussage mit einer Variante des Vollständigkeitsbeweises aus der Vorlesung, bei der nur negative Resolutionsschritte erforderlich sind.

Wir ändern die induktive Definition der Belegung I folgendermaßen ab:

$$I(P_n) = W,$$

genau dann, wenn gilt:

M_0 enthält keine Klausel $C = C_1 \cup \{\neg P_n\}$, so daß in C_1 nur negative Literale $\neg P_i$ mit $i < n$ auftreten, und $val_I(C_1) = F$.

Wie zeigen, daß auch für diese Belegung I für alle Klauseln $C \in M_0$ gilt $val_I(C) = W$ durch Induktion über die Anzahl k der positiven Literale in C. Für den Induktionsanfang betrachten wir eine Klausel $C_0 \cup \{\neg P_n\}$ mit nur negativen Literalen, wobei alle Literale in C_0 einen kleineren Index als n haben. Falls $val_I(C_0) = W$ gilt so auch $val_I(C_0 \cup \{\neg P_n\}) = W$. Gilt $val_I(C_0) = F$ so erzwingt die Definition von I, daß $I(P_n) = F$ und damit ebenfalls $val_I(C_0 \cup \{\neg P_n\}) = W$ gilt.
Im Induktionsschritt betrachten wir eine Klausel $D \cup \{P_n\}$ mit $k > 0$ positiven Literalen und nehmen an, daß für alle Klauseln aus M_0 mit weniger als k vielen positiven Literalen $val_I(C) = W$ schon gezeigt ist. Gilt $I(P_n) = W$, so auch $val_I(D \cup \{P_n\}) = W$ und wir sind fertig. Gilt $I(P_n) = F$ dann gibt es nach Definition von I eine Klausel $C_0 \cup \{\neg P_n\}$ in M_0 mit nur negativen Literalen und $val_I(C_0) = F$. Da M_0 unter Resolventenbildung abgeschlossen ist, liegt auch die Resolvente $D \cup C_0$ von $D \cup \{P_n\}$ und $C_0 \cup \{\neg P_n\}$ in M_0. Da $D \cup C_0$ strikt weniger positive Literale als k enthält gilt nach Induktionsvoraussetzung $val_I(D \cup C_0) = W$. Wegen $val_I(C_0) = F$ folgt daraus $val_I(D) = W$ und wir sind fertig. $\square$

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.

Lösung zu Aufgabe 59

(a) Es gibt mehrere Möglichkeiten, einen linearen Beweis zu führen. Eine ist:

$$\begin{tikzcd}
\{A, D\} \arrow[d, dash] & \{\neg D, B\} \arrow[dl, dash] \\
\{A, B\} \arrow[d, dash] & \{\neg A, B\} \arrow[dl, dash] \\
\{B\} \arrow[d, dash] & \{\neg B\} \arrow[dl, dash] \\
\square &
\end{tikzcd}$$

(b) Auch hier gibt es mehrere Möglichkeiten. Wie in der Aufgabenstellung erwähnt, ist die Wahl der Startklausel von Bedeutung sein. Wählt man dafür z. B. $\{C, B\}$ aus, so gerät man in eine Sackgasse, man hat keine Möglichkeit, das Literal C loszubekommen, was daran liegt, dass C kein „Gegenstück“ in der Klauselmenge besitzt (solch ein Literal nennt man „pur“).

$$\begin{tikzcd} \{C, B\} \arrow[d, dash] & \{\neg B\} \arrow[dl, dash] \\ \{C\} & \end{tikzcd}$$

3.3 Resolutionskalkül für Prädikatenlogik

Aufgabe 60

Zeigen Sie die Unerfüllbarkeit der folgenden Klauselmenge mittels des Resolutionskalküls:

$$\{ \quad \{p(x_1, f(x_1))\}, \quad \{\neg p(x_2, x_3), \neg p(x_3, x_4), p(x_2, x_4)\}, \quad \{p(g(d), x_8)\},$$
$$\{\neg p(c, c), \neg p(d, g(x_7))\}, \ \{p(x_5, x_6), \neg p(x_6, x_5)\} \quad \}$$

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.

Lösung zu Aufgabe 60

Nummeriere die gegebenen Klauseln (1) bis (5).

(6)	$\{\neg p(f(x_1), x_4), p(x_1, x_4)\}$	[1, 2]	$\mu = \{x_2/x_1, x_3/f(x_1)\}$
(7)	$\{p(f(x_1), x_1)\}$	[1, 5]	$\mu = \{x_5/f(x_1), x_6/x_1\}$
(8)	$\{p(x_1, x_1)\}$	[6, 7]	$\mu = \{x_4/x_1\}$
(9)	$\{\neg p(d, g(x_7))\}$	[8, 4]	$\mu = \{x_1/c\}$
(10)	$\{\neg p(g(x_7, d))\}$	[9, 5]	$\mu = \{x_5/d, x_6/g(x_7)\}$
(11)	$\square$	[10, 3]	$\mu = \{x_8/d, x_7/d\}$

Hinweis: Es ist hilfreich, wenn man in einigen Klauseln Struktur erkennt: Klausel (2) besagt, dass p transitiv ist und (5), dass p symmetrisch ist. Dies kann man verwenden, um $p(x, x)$ zu resolvieren. Eine zweite Anwendung der Symmetrie sorgt dann für den endgültigen Abschluss.

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.

Lösung zu Aufgabe 61

Die kürzeste Ableitung ergibt sich durch Selbstresolution:

(1)	$\{p(a)\}$	
(2)	$\{\neg p(x), p(f(x))\}$	
(3)	$\{\neg p(f(f(f(f(a)))))\}$	
(4)	$\{\neg p(y), p(f(f(y)))\}$	$[2, 2, \mu = \{x/f(y)\}]$
(5)	$\{\neg p(z), p(f(f(f(f(z)))))\}$	$[4, 4, \mu = \{y/f(f(z))\}]$
(6)	$\{\neg p(a)\}$	$[3, 5, \mu = \{z/a\}]$
(7)	$\square$	$[1, 6, \mu = \{\}]$

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.

Lösung zu Aufgabe 62

Um eine Formel mit dem Resolutionskalkül als allgemeingültig zu beweisen, geht man folgendermaßen vor:

1. negieren der Formel
2. überführen der Formel in Pränexnormalform, Matrix in konjunktiver Form.
3. skolemisieren
4. resolvieren

Negieren und Überführen in PNF Nach einigen ereinfachenden Äquivalenzumformungen ist das Negat

$$\begin{aligned} &\big((\forall x_1\ p(x_1)) \to (\forall x_2\ q(x_2))\big) \\ \land\ &\big(\forall x_3(q(x_3) \to r(x_3))\big) \\ \land\ &\big(\forall x_4(\neg r(f(x_4)) \land p(x_4))\big) \end{aligned}$$

Wenn die Quantoren herausgezogen sind, lautet die Formel in PNF:

$$\begin{aligned} \exists x_1 \forall x_2 \forall x_3 \forall x_4 \quad &\big(\neg p(x_1) \lor q(x_2)\big) \\ \land\ &\big(\neg q(x_3) \lor r(x_3)\big) \\ \land\ &\big(\neg r(f(x_4)) \land p(x_4)\big) \end{aligned}$$

Skolemisieren Die Skolemisierung führt ein neues Funktionssymbol c für x_1 ein. Die erfüllbarkeitsäquivalente Formel lautet nun:

$$\begin{aligned} &\big(\neg p(c) \lor q(x_2)\big) \\ \land\ &\big(q(x_3) \lor r(x_3)\big) \\ \land\ &\neg r(f(x_4)) \quad \land \quad p(x_4) \end{aligned}$$

wobei die Allquantoren als implizit angenommen und daher weggelassen wurden.

Resolution Die Ausgangs-Klauselmenge lautet nun:

1. $\{\neg p(c), q(x_2)\}$
2. $\{\neg q(x_3), r(x_3)\}$
3. $\{\neg r(f(x_4))\}$
4. $\{p(x_4)\}$

Weitere Resolution ergibt:

5.	$\{q(x_2)\}$	1,4	$\sigma = \{x_4/c\}$
6.	$\{r(x_3)\}$	5,2	$\sigma = \{x_2/x_4\}$
7.	$\square$	6,3	$\sigma = \{x_4/f(x_4)\}$

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.

Lösung zu Aufgabe 63

Wegen $Res'(M) \subseteq Res(M)$ ist der modifizierte Kalkül auf jeden Fall noch korrekt. Er ist aber nicht mehr vollständig. Die Formelmenge $\{\forall x(p(x, f(x))), \neg\exists x(p(a, x))\}$ ist sicherlich unerfüllbar. Nach Umwandlung in Klauselnormalform erhalten wir $\{\{p(x, f(x))\}, \{\neg p(a, x)\}\}$. Die beiden Einerklauseln $\{p(x, f(x))\}$, $\{\neg p(a, x)\}$ sind allerdings nicht resolvierbar, da die Unifikation von x mit $f(x)$ in der zweiten Argumentstelle von p nicht möglich ist. Dagegen liefert die Resolution von $\{p(x, f(x))\}$ mit $\{\neg p(a, y)\}$ sofort die leere Klausel.

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

Lösung zu Aufgabe 64

Abbildung 3.1 zeigt Tableaubeweise für beide Teilaufgaben. Das Tableau für Teilaufgabe (a) lässt sich schließen, die Allgemeingültigkeit der Formel φ_a ist damit bewiesen.

Das Tableau für die Formel $\neg\varphi_b$ lässt sich auch im erschöpften Zustand nicht schließen, daher ist $\neg\varphi_b$ erfüllbar, φ_b also nicht allgemeingültig.

Die Abbildungen sind mit der Vorzeichen-Variante des Kalküls aus der Vorlesung erstellt und die Regelanwendungen darin markiert. Dabei steht eine rote Kante für eine α- und eine blaue für eine β-Erweiterung. Die jeweils letzten Formeln im Tableau von (b) gehen aus der β-Formel $1B \to C$ hervor.

Ein erschöpftes, nicht geschlossenes Tableau hat einen Ast, der nicht geschlossen werden kann. Dieser Erlaubt das Ablesen einer Interpretation, die die Wurzelformel erfüllt: Setze für jede Variable $P \in \Sigma$

- wenn $0P$ auf dem Ast vorkommt $I(P) := F$,
- wenn $1P$ auf dem Ast vorkommt $I(P) := W$.
- andernfalls $I(P)$ beliebig.

Zur Begründung siehe Lemma 3.34 im Skript.

Insbesondere wird die Wurzel des Baumes erfüllt, das Negat der Formel, die auf Allgemeingültigkeit überprüft werden soll. Für diese Formel ist die Belegung also ein Gegenbeispiel zur Allgemeingültigkeit.

Für (b) ist das der Fall für die Belegung I mit $I(A) = I(B) = I(C) = F$. Denn dann gilt: $\text{val}_I(\phi_b) = F$.

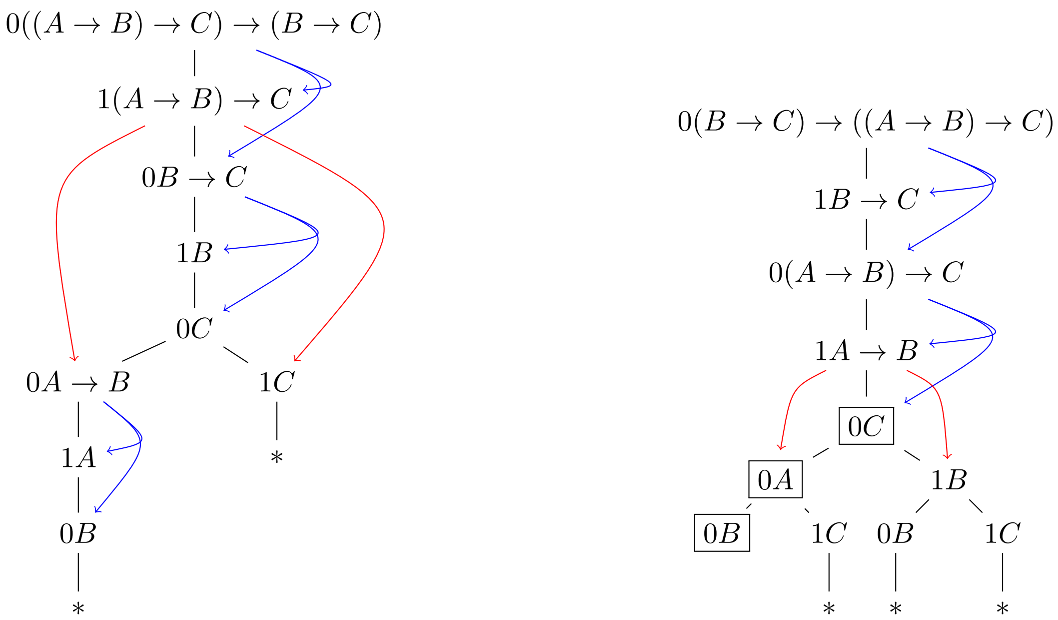


Abbildung 3.1: Tableaubeweise zu Aufgabe 64(a) (links) und 64(b) (rechts)

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).

Lösung zu Aufgabe 65

(a)

$$\begin{array}{c} 1sh(P_1,P_2,P_3) \\ \hline \begin{array}{r|l} 1P_1 & 0P_1 \\ 1P_3 & 1P_2 \end{array} \end{array} \qquad\qquad \begin{array}{c} 0sh(P_1,P_2,P_3) \\ \hline \begin{array}{r|l} 1P_1 & 0P_1 \\ 0P_3 & 0P_2 \end{array} \end{array}$$

(b) Es ist zu zeigen: Für eine beliebige Interpretation I gilt

$$\mathrm{val}_I(1sh(P_1,P_2,P_3)) = W \qquad \text{gdw.} \qquad \begin{array}{c} \mathrm{val}_I(1P_1) = W \text{ und } \mathrm{val}_I(1P_3) = W \\ \text{oder} \\ \mathrm{val}_I(0P_1) = W \text{ und } \mathrm{val}_I(1P_2) = W \end{array}$$

Dabei ist die Richtung $\Rightarrow$ der Korrektheits- und die Richtung $\Leftarrow$ der Vollständigkeitsteil des Beweises.

Die Behauptung ergibt sich aus:

$$\begin{array}{ll} & \mathrm{val}_I(1sh(P_1,P_2,P_3)) = W \\ \text{gdw.} & \mathrm{val}_I(sh(P_1,P_2,P_3)) = W \\ \text{gdw.} & \mathrm{val}_I(P_1 \wedge P_3 \vee \neg P_1 \wedge P_2) = W \\ \text{gdw.} & \mathrm{val}_I(P_1 \wedge P_3) = W \text{ oder } \mathrm{val}_I(\neg P_1 \wedge P_2) = W \\ \text{gdw.} & \mathrm{val}_I(P_1) = W \text{ und } \mathrm{val}_I(P_3) = W \text{ oder } \mathrm{val}_I(\neg P_1) = W \text{ und } \mathrm{val}_I(P_2) = W \\ \text{gdw.} & \mathrm{val}_I(1P_1) = W \text{ und } \mathrm{val}_I(1P_3) = W \text{ oder } \mathrm{val}_I(0P_1) = W \text{ und } \mathrm{val}_I(1P_2) = W \end{array}$$

Analog für ist für die zweite Regel zu zeigen, dass

$$\mathrm{val}_I(0sh(P_1,P_2,P_3)) = W \qquad \text{gdw.} \qquad \begin{array}{c} \mathrm{val}_I(1P_1) = W \text{ und } \mathrm{val}_I(0P_3) = W \\ \text{oder} \\ \mathrm{val}_I(0P_1) = W \text{ und } \mathrm{val}_I(0P_2) = W \end{array}$$

Das ergibt sich aus:

$$\begin{array}{ll} & \mathrm{val}_I(0sh(P_1,P_2,P_3)) = W \\ \text{gdw.} & \mathrm{val}_I(sh(P_1,P_2,P_3)) = F \\ \text{gdw.} & \mathrm{val}_I((P_1 \to P_3) \wedge (\neg P_1 \to P_2)) = F \\ \text{gdw.} & \mathrm{val}_I((\neg P_1 \vee P_3) \wedge (P_1 \vee P_2)) = F \\ \text{gdw.} & \mathrm{val}_I(\neg P_1 \vee P_3) = F \text{ oder } \mathrm{val}_I(P_1 \vee P_2) = F \\ \text{gdw.} & \mathrm{val}_I(\neg P_1) = F \text{ und } \mathrm{val}_I(P_3) = F \text{ oder } \mathrm{val}_I(P_1) = F \text{ und } \mathrm{val}_I(P_2) = F \\ \text{gdw.} & \mathrm{val}_I(1P_1) = W \text{ und } \mathrm{val}_I(0P_3) = W \text{ oder } \mathrm{val}_I(0P_1) = W \text{ und } \mathrm{val}_I(0P_2) = W \end{array}$$

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.

Lösung zu Aufgabe 66

Die Formalisierung der Regeln ergibt:

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.

$$A_1 \equiv \forall x \forall y \ ((m(x) \wedge m(y) \wedge r(x, y)) \rightarrow \forall z \ (m(z) \rightarrow r(z, x)))$$

2. Vier der Mitglieder sind: Guido, Lorenzo, Petrucio und Cesare.

$$A_2 \equiv m(g) \wedge m(l) \wedge m(p) \wedge m(c)$$

3. Guido rasiert Cesare.

$$A_3 \equiv r(g, c)$$

4. Petrucio rasiert Lorenzo.

$$C \equiv r(p, l)$$

$$1\ \forall x.\forall y.((m(x) \wedge (m(y) \wedge r(x,y))) \rightarrow \forall z.(m(z) \rightarrow r(z,x)))\ {\scriptstyle 1}$$

$$1\ (m(g) \wedge (m(l) \wedge (m(p) \wedge m(c))))\ {\scriptstyle 2}$$

$$1\ r(g,c)\ {\scriptstyle 3}$$

$$0\ r(p,l)\ {\scriptstyle 4}$$

$$1\ m(g)\ {\scriptstyle 5[\alpha(2)]}$$

$$1\ (m(l) \wedge (m(p) \wedge m(c)))\ {\scriptstyle 6[\alpha(2)]}$$

$$1\ m(l)\ {\scriptstyle 7[\alpha(6)]}$$

$$1\ (m(p) \wedge m(c))\ {\scriptstyle 8[\alpha(6)]}$$

$$1\ m(p)\ {\scriptstyle 9[\alpha(8)]}$$

$$1\ m(c)\ {\scriptstyle 10[\alpha(8)]}$$

$$1\ \forall y.((m(X_1) \wedge (m(y) \wedge r(X_1,y))) \rightarrow \forall z.(m(z) \rightarrow r(z,X_1)))\ {\scriptstyle 11[\gamma(1)]}$$

$$1\ ((m(X_1) \wedge (m(X_2) \wedge r(X_1,X_2))) \rightarrow \forall z.(m(z) \rightarrow r(z,X_1)))\ {\scriptstyle 12[\gamma(11)]}$$

$$0\ (m(X_1) \wedge (m(X_2) \wedge r(X_1,X_2)))\ {\scriptstyle 13[\beta(12)]} \qquad 1\ \forall z.(m(z) \rightarrow r(z,X_1))\ {\scriptstyle 14[\beta(12)]}$$

$$0\ m(X_1)\ {\scriptstyle 15[\beta(13)]} \qquad 0\ (m(X_2) \wedge r(X_1,X_2))\ {\scriptstyle 16[\beta(13)]} \qquad 1\ (m(X_3) \rightarrow r(X_3,X_1))\ {\scriptstyle 19[\gamma(14)]}$$

$$0\ m(X_2)\ {\scriptstyle 17[\beta(16)]} \qquad 0\ r(X_1,X_2)\ {\scriptstyle 18[\beta(16)]} \qquad 0\ m(X_3)\ {\scriptstyle 20[\beta(19)]} \qquad 1\ r(X_3,X_1)\ {\scriptstyle 21[\beta(19)]}$$

$$1\ \forall y.((m(X_4) \wedge (m(y) \wedge r(X_4,y))) \rightarrow \forall z.(m(z) \rightarrow r(z,X_4)))\ {\scriptstyle 22[\gamma(1)]}$$

$$1\ ((m(X_4) \wedge (m(X_5) \wedge r(X_4,X_5))) \rightarrow \forall z.(m(z) \rightarrow r(z,X_4)))\ {\scriptstyle 23[\gamma(22)]}$$

$$0\ (m(X_4) \wedge (m(X_5) \wedge r(X_4,X_5)))\ {\scriptstyle 24[\beta(23)]} \qquad 1\ \forall z.(m(z) \rightarrow r(z,X_4))\ {\scriptstyle 25[\beta(23)]}$$

$$0\ m(X_4)\ {\scriptstyle 26[\beta(24)]} \qquad 0\ (m(X_5) \wedge r(X_4,X_5))\ {\scriptstyle 27[\beta(24)]} \qquad 1\ (m(X_6) \rightarrow r(X_6,X_4))\ {\scriptstyle 30[\gamma(25)]}$$

$$0\ m(X_5)\ {\scriptstyle 28[\beta(27)]} \qquad 0\ r(X_4,X_5)\ {\scriptstyle 29[\beta(27)]} \qquad 0\ m(X_6)\ {\scriptstyle 31[\beta(30)]} \qquad 1\ r(X_6,X_4)\ {\scriptstyle 32[\beta(30)]}$$

Abbildung 3.2: Lösung zu Aufgabe 66

Zu beweisen ist: $\{A_1, A_2, A_3\} \models C$. Um dies mit Hilfe des Tableaukalküls nachzuweisen, zeigen wir $\{A_1, A_2, A_3\} \cup \neg C \vdash \mathbf{0}$

Abbildung 3.2 zeigt ein Tableau für $\{A_1, A_2, A_3\} \cup \neg C$.

Das Tableau aus Abb. 3.2 ist noch nicht geschlossen (damit die freien Variablen sichtbar bleiben). Durch die Substitution

$$\mu = \{X_1/g, X_2/c, X_3/l, X_4/l, X_5/g, X_6/p\}$$

kann es aber geschlossen werden.

Aufgabe 67

Zeigen Sie mit Hilfe des prädikatenlogischen Tableaukalküls, dass die Formel

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

unerfüllbar ist.

Lösung zu Aufgabe 67

Ein geschlossenes Tableau zu der Vorzeichenformel

$$1\ \forall y \forall x \forall z \big((p(x,z) \to p(y,z)) \to q(x,y)\big) \land \neg\exists y \forall x (q(x,x) \lor r(y))$$

ist in in Abbildung 3.3 dargestellt. Die schließende Substitution ist dabei: $\{X_2 = f(X_1), X_3 = f(X_1)\}$

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:

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

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

Lösung zu Aufgabe 68

siehe Abbildung 3.4.

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.

Lösung zu Aufgabe 69

Betrachte $\phi = (\forall x(p(x) \lor q(x))) \to (p(a) \lor q(b))$.

Tableau für 0ϕ:

[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.

$$1\ (\forall y.\forall x.\forall z.((p(x,z) \to p(y,z)) \to q(x,y)) \wedge \neg\exists y.\forall x.(q(x,x) \vee r(y)))\ _{1}$$

$$1\ \forall y.\forall x.\forall z.((p(x,z) \to p(y,z)) \to q(x,y))\ _{2[\alpha(1)]}$$

$$1\ \neg\exists y.\forall x.(q(x,x) \vee r(y))\ _{3[\alpha(1)]}$$

$$0\ \exists y.\forall x.(q(x,x) \vee r(y))\ _{4[\alpha(3)]}$$

$$0\ \forall x.(q(x,x) \vee r(X_1))\ _{5[\gamma(4)]}$$

$$0\ (q(f(X_1),f(X_1)) \vee r(X_1))\ _{6[\delta(5)]}$$

$$0\ q(f(X_1),f(X_1))\ _{7[\alpha(6)]}$$

$$0\ r(X_1)\ _{8[\alpha(6)]}$$

$$1\ \forall x.\forall z.((p(x,z) \to p(X_2^*,z)) \to q(x,X_2^*))\ _{9[\gamma(2)]}$$

$$1\ \forall z.((p(X_3^*,z) \to p(X_2^*,z)) \to q(X_3^*,X_2^*))\ _{10[\gamma(9)]}$$

$$1\ ((p(X_3^*,X_4) \to p(X_2^*,X_4)) \to q(X_3^*,X_2^*))\ _{11[\gamma(10)]}$$

$$\begin{array}{cc}
0\ (p(X_3^*,X_4) \to p(X_2^*,X_4))\ _{12[\beta(11)]} & 1\ q(X_3^*,X_2^*)\ _{13[\beta(11)]} \\
 & *_{[7,13]} \\
1\ p(X_3^*,X_4)\ _{14[\alpha(12)]} & \\
0\ p(X_2^*,X_4)\ _{15[\alpha(12)]} & \\
*_{[14,15]} &
\end{array}$$

Abbildung 3.3: Tableau für Aufg. 67

$$1\forall x.\exists y.r(x,y) \quad {\scriptstyle 1}$$

$$1\forall x.\forall y.\forall z.((r(x,y)\wedge r(y,z)) \rightarrow r(x,z)) \quad {\scriptstyle 2}$$

$$1\forall x.\forall y.(r(x,y) \rightarrow r(y,x)) \quad {\scriptstyle 3}$$

$$0\forall x.r(x,x) \quad {\scriptstyle 4}$$

$$0r(c,c) \quad {\scriptstyle 5[\delta(4)]}$$

$$1\exists y.r(X_1,y) \quad {\scriptstyle 6[\gamma(1)]}$$

$$1r(X_1,f(X_1)) \quad {\scriptstyle 7[\delta(6)]}$$

$$1\forall y.(r(X_2,y) \rightarrow r(y,X_1)) \quad {\scriptstyle 8[\gamma(3)]}$$

$$1(r(X_2,X_3) \rightarrow r(X_3,X_2)) \quad {\scriptstyle 9[\gamma(8)]}$$

$$0r(X_2,X_3) \quad {\scriptstyle 10[\beta(9)]} \qquad\qquad 1r(X_3,X_2) \quad {\scriptstyle 11[\beta(9)]}$$

$$*_{[7,10]}$$

$$1\forall y.\forall z.((r(X_4,y)\wedge r(y,z)) \rightarrow r(X_4,z)) \quad {\scriptstyle 12[\gamma(2)]}$$

$$1\forall z.((r(X_4,X_5)\wedge r(X_5,z)) \rightarrow r(X_4,z)) \quad {\scriptstyle 13[\gamma(12)]}$$

$$1((r(X_4,X_5)\wedge r(X_5,X_6)) \rightarrow r(X_4,X_6)) \quad {\scriptstyle 14[\gamma(13)]}$$

$$0(r(X_4,X_5)\wedge r(X_5,X_6)) \quad {\scriptstyle 15[\beta(14)]} \qquad 1r(X_4,X_6) \quad {\scriptstyle 16[\beta(14)]}$$

$$*_{[5,16]}$$

$$0r(X_4,X_5) \quad {\scriptstyle 17[\beta(15)]} \qquad 0r(X_5,X_6) \quad {\scriptstyle 18[\beta(15)]}$$

$$*_{[7,17]} \qquad\qquad *_{[11,18]}$$

Substitution: $\sigma = \{X_1/c, X_2/c, X_3/f(c), X_4/c, X_5/f(c), X_6/c\}$

Abbildung 3.4: Tableau für Aufgabe 68

$$
\begin{array}{ccc}
 & 0\phi & (0) \\
 & | & \\
 & 1\forall x(p(x) \vee q(x)) & (1)\ [\alpha(0)] \\
 & | & \\
 & 0(p(a) \vee q(b)) & (2)\ [\alpha(0)] \\
 & | & \\
 & 0p(a) & (3)\ [\alpha(2)] \\
 & | & \\
 & 0q(b) & (4)\ [\alpha(2)] \\
 & | & \\
 & 1p(X) \vee q(X) & (5)\ [\gamma(1)] \\
\end{array}
$$

$$
(6)\ [\beta(5)] \quad 1p(X) \qquad\qquad 1q(X) \quad (7)\ [\beta(5)]
$$

Der linke Ast kann nun durch die Substitution X/a geschlossen werden. Wird diese nur lokal (d.h. auf dem Ast) angewendet, kann der rechte Ast durch X/b geschlossen werden.

Die Formel ϕ ist aber nicht allgemeingültig, wie folgende (Herbrand-)Interpretation (D, I) beweist:

$$
\begin{array}{rcl}
D & = & \{a, b\} \\
I(p) & = & \{b\} \\
I(q) & = & \{a\}
\end{array}
$$

Es gilt $\mathrm{val}_I(\forall x(p(x) \vee q(x))) = W$ aber $\mathrm{val}_I(p(a)) = F$ und $\mathrm{val}_I(q(b)) = F$

Aufgabe 70

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

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

$$
\begin{array}{c}
1\,\neg p(a, b) \rightarrow \exists x\,(p(b, x) \vee q(a, x))\ {}_1 \\
| \\
0\,\exists y\,\exists x\,(p(x, y) \vee \exists z\, q(x, z))\ {}_2
\end{array}
$$

Lösung zu Aufgabe 70

Eine Möglichkeit, das Tableau zu vervollständigen, ist in Abbildung 3.5 dargestellt. Die schließende Substitution ist dabei $\{X_1/sk_1, X_2/b, X_3/b, X_4/a, X_5/sk_1\}$.

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.

- $1\,\neg p(a,b) \rightarrow \exists x\,(p(b,x) \vee q(a,x))$ ${}_{1}$
- $0\,\exists y\,\exists x\,(p(x,y) \vee \exists z\,q(x,z))$ ${}_{2}$
- $0\,\exists x\,(p(x,X_1) \vee \exists z\,q(x,z))$ ${}_{3[\gamma(2)]}$
- $0\,(p(X_2,X_1) \vee \exists z\,q(X_2,z))$ ${}_{4[\gamma(3)]}$
- $0\,p(X_2,X_1)$ ${}_{5[\alpha(4)]}$
- $0\,\exists z\,q(X_2,z)$ ${}_{6[\alpha(4)]}$
- $0\,\exists x\,(p(x,X_3) \vee \exists z\,q(x,z))$ ${}_{7[\gamma(2)]}$
- $0\,(p(X_4,X_3) \vee \exists z\,q(X_4,z))$ ${}_{8[\gamma(7)]}$
- $0\,p(X_4,X_3)$ ${}_{9[\alpha(8)]}$
- $0\,\exists z\,q(X_4,z)$ ${}_{10[\alpha(8)]}$
    - $0\,\neg p(a,b)$ ${}_{11[\beta(1)]}$
        - $1\,p(a,b)$ ${}_{13[\neg\neg(11)]}$
        - $\boxed{\star_{[9,13]}}$
    - $1\,\exists x\,(p(b,x) \vee q(a,x))$ ${}_{12[\beta(1)]}$
        - $1\,(p(b,sk_1) \vee q(a,sk_1))$ ${}_{14[\delta(12)]}$
            - $1\,p(b,sk_1)$ ${}_{15[\beta(14)]}$
                - $\boxed{\star_{[5,15]}}$
            - $1\,q(a,sk_1)$ ${}_{16[\beta(14)]}$
                - $0\,q(X_4,X_5)$ ${}_{17[\gamma(10)]}$
                - $\boxed{\star_{[16,17]}}$

Abbildung 3.5: Tableau für Aufg. 70

Lösung zu Aufgabe 71

Der Wurzelknoten eines Sequenzenbeweises für eine Formel φ ist markiert mit " $\rightarrow \varphi$".

Wenn man die Regeln aus der Vorlesung/Skript anwendet, kommt man zu einem Beweisbaum ähnlich zu dem in Abbildung 3.6. Da alle Blätter des Beweises Axiome sind, ist die Ausgangsformel damit bewiesen.

Im Baum ist jeweils die Formel markiert, auf die die nachfolgende Regel angewendet wird.

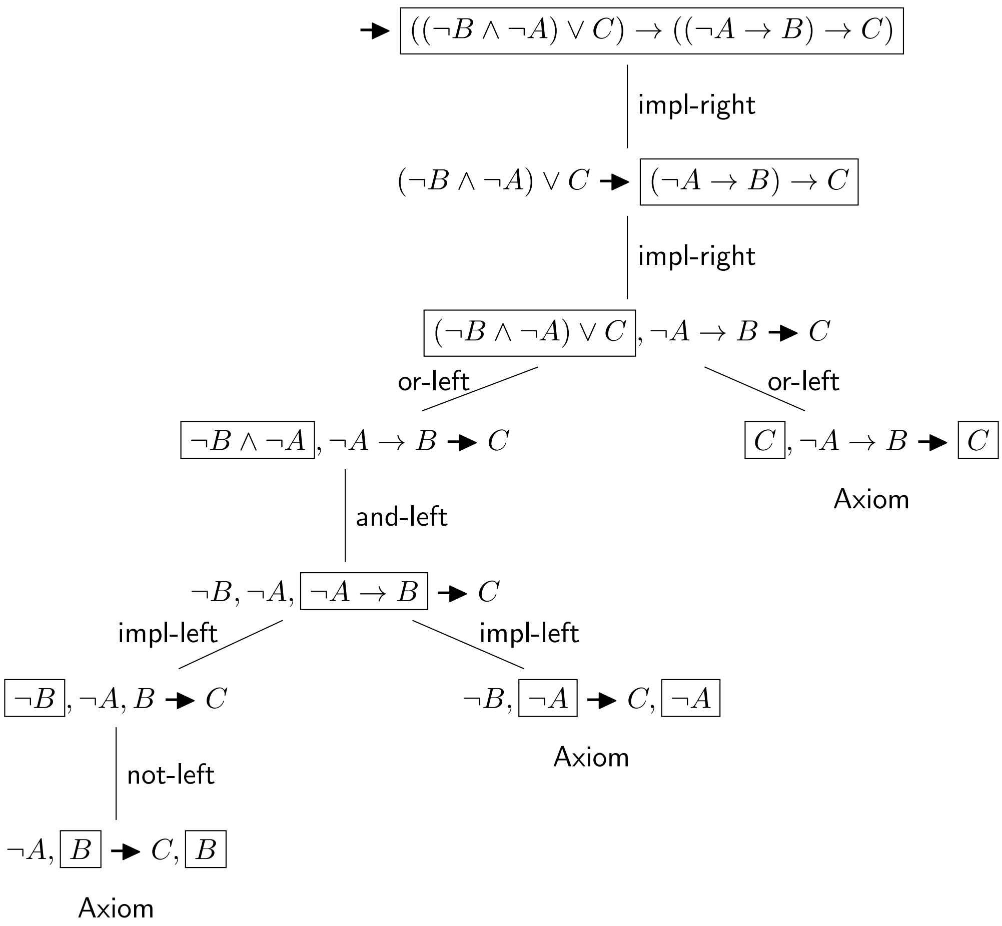


Abbildung 3.6: Sequenzenbeweisbaum zu Aufgabe 5

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;
  @*/
```

Lösung zu Aufgabe 72

(a) Die Forderung, dass die Methode "in jedem Zustand aufgerufen werden" darf, beschreiben wir in JML durch die allgemeingültige Vorbedingung `true`[1].

```
/*@ public normal_behaviour
  @   requires true;
  @   ensures age == \old(age) + 1;
  @   assignable age;
  @*/
void celebrateBirthday() { ... }
```

(b) Folgender Vertrag beschreibt das Verhalten der Methode möglichst präzise:

```
/*@ public normal_behaviour
  @   ensures child.mother == isFemale ? this : \old(child.mother);     (1)
  @   ensures child.father == isFemale ? \old(child.father) : this;     (2)
  @   ensures children.length == \old(children.length) + 1;             (3)
  @   ensures (\forall int i; 0<=i && i<children.length-1;              (4)
  @                children[i] == \old(children[i]));
  @   ensures children[children.length-1] == child;                     (5)
  @   assignable children, child.father, child.mother;                  (6)
  @*/
void becomeParentTo(Person child) { ... }
```

Einige Beobachtungen dazu:

- Bei (1) und (2) fällt auf, dass nicht nur beschrieben werden muss, wie sich `child.mother` and `child.father` *ändern*, sondern auch unter welchen Bedingungen sie sich *nicht ändern*.
- Für das Feld `this.children` muss sowohl die Änderung der Länge beschrieben werden (3), also auch der neue Inhalt (4), (5).

[1] Wird keine Vorbedingung angegeben, so wird als Standard `true` verwendet, so dass wir in diesem Fall auch auf eine Vorbedingung ganz verzichten hätten können.

- Die Methode ändert (6) die Referenz auf `children` und die Felder `father` und `mother` für die Referenz `child`. Beachten Sie: Der Inhalt des *alten* Feldes `children`, also die Speicherstellen, die durch `children[*]` bezeichnet werden, werden von dieser Implementierung in keinem Fall verändert.

(c)
```
/*@ public normal_behaviour
  @  ensures \result.length == children.length + 1;
  @  ensures (\forall int i; 0 <= i && i < children.length;
  @               \result[i] == children[i]);
  @  ensures \result[children.length] == child;
  @  assignable \nothing;
  @*/
```

Die `assignable`-Klausel mag im ersten Moment ungewöhnlich erscheinen: Wie kann die Methode nichts verändern, wenn sie doch ein neues Objekt auf dem Speicher anlegt? Antwort: Assignable-Klauseln beziehen sich auf den schon existierenden Teil des Speichers. Die Methode darf neuen Speicher belegen, aber *nichts* an den schon existierenden Speicherstellen manipulieren.

Alle anderen Teile des Systems hängen nur von schon existierenden Speicherstellen ab, daher kann die Methode das System nicht "verändern".

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.

Lösung zu Aufgabe 73

Das folgende annotierte Programm beinhaltet die Lösung für beide Teilaufgaben.

```
public class ZeroFinder {

    /*@ public normal_behaviour
      @   requires true;
      @   ensures -1 <= \result && \result < array.length;
      @   ensures \result >= 0 ==> array[\result] == 0 &&
      @              (\forall int i; 0<=i && i<\result; array[i] != 0);
      @   ensures \result == -1 ==>
      @              (\forall int i; 0<=i && i<array.length; array[i] != 0);
      @   assignable \nothing;
      @*/
    public int findZero(int[] array) {
        int k = 0;

        while(k < array.length) {
            if(array[k] == 0) {
                return k;
```

```
            }
            k++;
        }

        return -1;
    }
}
```

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?

Lösung zu Aufgabe 74

(a) Die Normalisierung kann direkt als 3 Ungleichungen formuliert werden, die die Bereiche für die Felder `euros` and `cents` einschränken.

```
/*@ invariant 0 <= euros && 0 <= cents && cents < 100;  */
```

(b) Der "Wert" eines Betrages ist `100*euros + cents`. Im Vertrag muss also gefordert werden, dass der Wert des Ergebnisses gerade die Summe aus dem Wert von `b` und `this` ist. Der Vertrag lautet also:

```
/*@ ensures \result.euros*100 + \result.cents ==
  @    this.euros*100 + this.cents + a.euros*100 + a.cents;
  @ assignable \nothing;
  @*/
```

Die `assignable`-clause `\nothing` erlaubt, dass neue Objekte erstellt werden und deren Felder geändert werden.

(c) Das Problem ist, dass nach der Ausführung des Konstruktors am Ende der Methode `add` die Invariante des neu erzeugten Objektes unter Umständen verletzt ist und die Spezifikation damit nicht erfüllt wird. Die Klasseninvariante muss schließlich von jedem Konstruktor etabliert werden.

Um dem Problem zu entgehen, müssen die Argumente für den Konstruktor normalisiert werden. Dies kann z. B. erreicht werden, indem die zusätzliche Anweisung

```
if(c >= 100) {
   c -= 100;
   e ++;
}
```

direkt vor der `return`-Anweisung der Methode `add` eingebaut wird.

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 $\succ$),

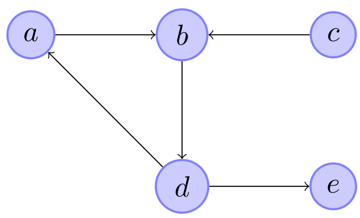
(ii) $\xrightarrow{+}$ (die transitive Hülle von $\succ$) und

(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.

Lösung zu Aufgabe 75



(a)

$$\begin{aligned}\text{Die transitive Hülle } \xrightarrow{+} = \{&(a,a),(a,b),(a,d),(a,e),\\ &(b,a),(b,b),(b,d),(b,e),\\ &(c,a),(c,b),(c,d),(c,e),\\ &(d,a),(d,b),(d,d),(d,e)\} \ .\end{aligned}$$

$$\begin{aligned}\text{Die reflexive, transitive Hülle } \rightarrow = \{&(a,a),(a,b),(a,d),(a,e),\\ &(b,a),(b,b),(b,d),(b,e),\\ &(c,a),(c,b),\boldsymbol{(c,c)},(c,d),(c,e),\\ &(d,a),(d,b),(d,d),(d,e),\\ &\boldsymbol{(e,e)}\} \ .\end{aligned}$$

$$\text{Die reflexive, transitive, symmetrische Hülle } \leftrightarrow = \{a,b,c,d,e\} \times \{a,b,c,d,e\} \ .$$

(b) Die Knoten a, b, c, e haben nicht mehr als einen Nachfolger bzgl. $\succ$: an diesen Stellen ist somit keine Divergenz möglich.

Der Knoten d hat zwei unmittelbare Nachfolger: a und e. Wegen $a \overset{+}{\to} e$ (s.o.) ist $\succ$ lokal konfluent.

Ebenfalls ist $\succ$ konfluent, da von allen Knoten aus, die von d erreichbar sind (a, b, d, e), der Knoten e erreichbar ist.

(Nota bene: Der Satz, dass jedes noethersche und lokal konfluente Reduktionssystem konfluent ist, ist hier nicht anwendbar, da die Relation nicht noethersch ist.)

(c) Wir fügen einen neuen Knoten f, sowie das Paar (a, f) hinzu. Die einzige neue Divergenz ist $f \prec a \succ b$. Wegen $b \overset{+}{\to} a \overset{+}{\to} f$ bleibt $\succ$ lokal konfluent. Die neue Relation ist aber nicht konfluent, da $b \overset{+}{\to} e$ gilt, und weder f noch e Nachfolger bzgl. $\succ$ haben.

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.

Lösung zu Aufgabe 76

Betrachten wir zunächst nur $(N, \succ)$

(a) Es gilt:

$$6 \succ 2, \; 6 \succ 3$$

Aber 2 und 3 sind irreduzible Elemente, weil sie keine echten Teiler größer 1 haben. Also ist das Reduktionssystem **nicht** lokal konfluent.

(b) ... und damit natürlich auch nicht konfluent.

(c) Aus $n \succ m$ folgt, dass $n > m$. In $\mathbb{N}$ kann es aber keine unendliche absteigende Kette geben ($(\mathbb{N}, >)$ ist noethersch), also ist $(N, \succ)$ noethersch.

(d) Die irreduziblen Elemente sind gerade die natürlichen Zahlen, die keine natürlichen Teiler haben außer 1 und sich selbst, also die Primzahlen.

Hier fällt der Begriff irreduzibel mit dem aus der Algebra/Zahlentheorie zusammen.

Desweiteren nun die Betrachtung für $(N', \succ)$: 1 ist Teiler jeder positiven natürlichen Zahl, also gilt, dass: $n \succ 1$ für alle $n \in N'$.

(a) folgt aus (b).

(b) Sei $n \succ m_1$ und $n \succ m_2$. Dann ist wegen $m_1 \succ 1$ und $m_2 \succ 1$ die Konfluenz gegeben.

(c) Das Argument von oben greift auch hier.

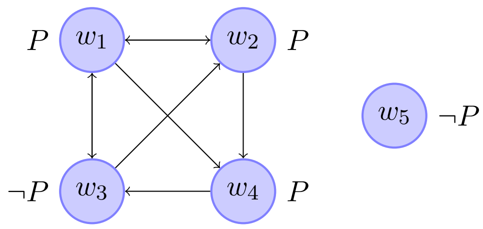
(d) 1 ist das einzig irreduzible Element.

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 $[\![\Box\Box P]\!]$.

Lösung zu Aufgabe 77

(a) Die Unterscheidungsformeln sind (eine Möglichkeit):

$$\phi_{w_5} = \Box\mathbf{0}$$

$$\phi_{w_4} = P \wedge \Box\neg P \qquad \phi_{w_3} = \neg P \wedge \Diamond P \qquad \phi_{w_2} = \Box P \wedge P \qquad \phi_{w_1} = \wedge_{i=w_2}^{w_5} \neg\phi_i$$

(b) Die Extensionen in diesem Modell sind:

$$[\![\Box P]\!] = \{w_2, w_3, w_5\} \qquad [\![\Diamond\Box P]\!] = \{w_1, w_3, w_4\}$$

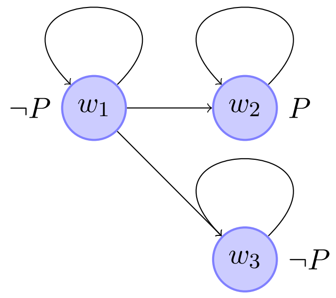
$$[\![\Diamond\Diamond P]\!] = \{w_1, w_2, w_3, w_4\} \qquad [\![\Box\Box P]\!] = \{w_4, w_5\}$$

Aufgabe 78

Wir betrachten die Klasse **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 **T**-Struktur $\mathcal{K}$ an, so daß $\mathcal{K} \models P \to \Box\Diamond P$, jedoch $\mathcal{K} \not\models \Diamond P \to \Box\Diamond P$.

Lösung zu Aufgabe 78

Sei $\mathcal{K}$ der folgende reflexive Kripkerahmen:



Es gilt $\mathcal{K} \models P \to \Box\Diamond P$ wegen $w_2 \models \Box\Diamond P$, da w_2 genau sich selbst als Nachfolger hat. Gleichzeitig $w_1 \not\models \Diamond P \to \Box\Diamond P$, da $w_1 \models \Diamond P$ (wegen $w_1 \to w_2$), aber $w_1 \not\models \Box\Diamond P$ wegen $w_3 \not\models \Diamond P$.

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) $\Diamond A \wedge \Diamond B \to \Diamond((A \wedge \Diamond B) \vee (\Diamond A \wedge B) \vee (A \wedge B))$

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

Lösung zu Aufgabe 79

(a) ist nicht allgemeingültig.

Gegenbeispiel: Sei $S = \{0\}$ und $R = \emptyset$, dann ist $0 \models \Box A$, aber nicht $0 \models \Diamond A$.

(b) ist nicht allgemeingültig.

In der unten stehenden Struktur gilt $0 \models \Diamond A$, aber nicht $0 \models \Diamond\Diamond A$.

(c) ist allgemeingültig.

Sei $t_0 \in S$ eine Kripkewelt.

Gelte $\mathcal{K}, t_0 \models \Diamond A \wedge \Diamond B$, dann gibt es zwei Welten $t_A > t_0$ und $t_B > t_0$, so dass $\mathcal{K}, t_A \models A$ und $K, t_B \models B$. Nun werden wir in einer (erschöpfenden) Fallunterscheidung drei Fälle nebeneinander stellen:

$t_A < t_B$: Dann gilt $\mathcal{K}, t_A \models A \wedge \Diamond B$, also in t_o auch $\mathcal{K}, t_0 \models \Diamond(A \wedge \Diamond B)$.

$t_A = t_B$: Dann gilt $\mathcal{K}, t_A \models A \wedge B$, also in t_o auch $\mathcal{K}, t_0 \models \Diamond(A \wedge B)$.

$t_A > t_B$: Dann gilt $\mathcal{K}, t_B \models \Diamond A \wedge B$, also in t_o auch $\mathcal{K}, t_0 \models \Diamond(\Diamond A \wedge B)$.

Da immer eine der drei Möglichkeiten erfüllt sein muss, ist insgesamt

$$\begin{array}{rcl} \mathcal{K}, t_0 & \models & \Diamond(A \wedge \Diamond B) \vee \Diamond(\Diamond A \wedge B) \vee \Diamond(A \wedge B) \\ \iff \mathcal{K}, t_0 & \models & \Diamond((A \wedge \Diamond B) \vee (\Diamond A \wedge B) \vee (A \wedge B)) \end{array}$$

Diese Aussage gilt weil die Welten durch die strikte Totalordnung alle „in einer Kette“ liegen. Es gibt keine Verzweigungsmöglichkeiten, so dass auf einem Pfad A und einem anderen B gelten könnte. Die beiden Welten t_A und t_B müssen bezgl. R in Beziehung zu einander stehen.

Die Implikation gilt auch in der Rückrichtung, so daß wir ingesamt erhalten:

$$\begin{array}{rcl} \mathcal{K}, t_0 & \models & \Diamond((A \wedge \Diamond B) \vee (\Diamond A \wedge B) \vee (A \wedge B)). \\ \iff \mathcal{K}, t_0 & \models & \Diamond(A \wedge \Diamond B) \vee \Diamond(\Diamond A \wedge B) \vee \Diamond(A \wedge B). \end{array}$$

Falls $\mathcal{K}, t_0 \models \Diamond(A \wedge B)$, so gilt $\mathcal{K}, t_0 \models \Diamond A \wedge \Diamond B$.
Falls $\mathcal{K}, t_0 \models \Diamond(A \wedge \Diamond B)$ ($\mathcal{K}, t_0 \models \Diamond(\Diamond A \wedge B)$ analog), so gilt wegen der Transitivität (d.h. $\Diamond\Diamond A \to \Diamond A$) auch $\mathcal{K}, t_0 \models \Diamond A \wedge \Diamond B$.

[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.

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:

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

Lösung zu Aufgabe 80

Zunächst die Transformation einer modallogischen Struktur $\mathcal{K} = (S, R, I)$ über der Signatur Σ in eine prädikatenlogische Struktur $\mathcal{K}' = (D_{\mathcal{K}'}, I_{\mathcal{K}'})$ über $\Sigma_{\mathcal{K}'}$.

$$\begin{aligned}
D_{\mathcal{K}'} &= S \\
\Sigma_{\mathcal{K}'} &= (\emptyset, \Sigma \cup \{r\}, \alpha) \\
\alpha(p) &= 1 \text{ für } p \in \Sigma \\
\alpha(r) &= 2 \\
I_{\mathcal{K}'}(p) &= \{s \in S : I(p, s) = W\} \\
I_{\mathcal{K}'}(r) &= R
\end{aligned}$$

Das PL-Universum entspricht der Menge der möglichen Welten der Kripkestruktur. Für eine modallogische Formel φ suchen wir daher nun eine PL-Formel $\tilde{\varphi}$, die eine freie Variable x besitzt. Die Belegung von x bestimmt die Welt, in der die Formel „ausgewertet“ werden soll. Dazu transformieren wir durch die folgende, rekursiv anzuwendende Abbildung:

Modallogik φ	Prädikatenlogik $\tilde{\varphi}$	
p	$p(x)$	AL-Atome werden zu Anwendungen von Prädikaten
$\psi \circ \chi$	$\tilde{\psi} \circ \tilde{\chi}$	AL-Verknüpfungen bleiben erhalten
$\Box\psi$	$\forall y(r(x,y) \to \tilde{\psi}[x \leftarrow y])$	$\Box$ wird zum Allquantor, wobei die Variable y neu gewählt sein muss, also in $\tilde{\psi}$ nicht auftreten darf.
$\Diamond\psi$	$\exists y(r(x,y) \wedge \tilde{\psi}[x \leftarrow y])$	$\Diamond$ wird zum Existenzquantor, wobei die Variable y neu gewählt sein muss, also in $\tilde{\psi}$ nicht auftreten darf.

Offensichtlich enthält jedes $\tilde{\varphi}$ genau eine freie Variable: x. Diese entspricht dem Zustand, in dem die Formel ausgewertet werden soll. Entsprechend bedeutet z.B. die Übersetzung des $\Box$-Operators, dass eine Formel in allen Zuständen y, für die $r(x,y)$ wahr ausgewertet wird, auch wahr ausgewertet werden muss.

Die Aussage $\mathcal{K}, s \models \varphi$ ist damit genau dann wahr, wenn die Aussage $\mathcal{K}', I'_{\mathcal{K}'}, \beta_x^s \models \tilde{\varphi}$ wahr ist. Die Aussage ist in jeder Kripkewelt gültig ($\mathcal{K} \models \varphi$), wenn $\mathcal{K}', I'_{\mathcal{K}'} \models \forall x\ \tilde{\varphi}$ wahr ist. Setze also $\varphi' := \forall x\ \tilde{\varphi}$.

Da umgekehrt aus jeder PL-Interpretation auch eine Kripkestruktur abgeleitet werden kann, gilt sogar die Aussage:

> φ ist allgemeingültig in allen Kripkestrukturen gdw. φ' ist prädikatenlogisch allgemeingültig.

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

Lösung zu Aufgabe 81

(a) Diese Aussage gilt nicht in allen ω-Strukturen.

Gegenbeispiel:

$$\xi(0) = \{A\}, \quad \xi(1) = \{B\}, \quad \xi(2) = \{C\}$$

Dann gilt:

$$\xi \models (A \vee B)\,\mathbf{U}\,C \text{ aber weder } \xi \models A\,\mathbf{U}\,C \text{ noch } \xi \models B\,\mathbf{U}\,C$$

(b) + (c) gilt.

Sei ξ beliebige ω-Struktur, dann gilt:

$\xi \models A\,\mathbf{V}\,(B \wedge C)$ gdw. Für alle $n \in \mathbb{N}$ gilt: $\xi_n \models B \wedge C$ oder es existiert ein $k \in \mathbb{N}, k < n$ mit $\xi_k \models A$.

gdw. Für alle $n \in \mathbb{N}$ gilt: ($\xi_n \models B$ und $\xi_n \models C$) oder es existiert ein $k \in \mathbb{N}, k < n$ mit $\xi_k \models A$.

gdw. Für alle $n \in \mathbb{N}$ gilt: ($\xi \models B$ oder es existiert ein $k \in \mathbb{N}, k < n$ mit $\xi_k \models A$) und ($\xi \models C$ oder es existiert ein $k \in \mathbb{N}, k < n$ mit $\xi_k \models A$).

gdw. (Für alle $n \in \mathbb{N}$ gilt: $\xi \models B$ oder es existiert ein $k \in \mathbb{N}, k < n$ mit $\xi_k \models A$), und (für alle $n \in \mathbb{N}$ gilt: $\xi \models C$ oder es existiert ein $k \in \mathbb{N}, k < n$ mit $\xi_k \models A$).

gdw. $\xi \models (A\,\mathbf{V}\,B) \wedge (A\,\mathbf{V}\,C)$