Theoretische Informatik 1 – Übungsblatt 7 (SS2006)

Aufgabe 7.1 Bestimmen Sie für folgende Formeln durch Angabe des Wahrheitswertverlaufs, ob sie gültig, erfüllbar, widerlegbar, bzw. unerfüllbar sind. Geben Sie, wo möglich, jeweils ein Modell bzw. ein Gegenbeispiel an.

a) $(A \equiv B) \not\equiv ((A \supset \mathbf{f}) \downarrow C)$

b) $(B \supset \neg A) \equiv (\neg A \supset B)$

c) $(C \supset (B \supset A)) \supset ((A \subset C) \subset (B \subset C))$

Lösung

a) Wir verwenden die Abkürzungen $F = (A \equiv B) \not\equiv ((A \supset \mathbf{f}) \downarrow C)$ und $G = (A \supset \mathbf{f}) \downarrow C$.

A	B	C	$A \equiv B$	$A \supset \mathbf{f}$	G	F
f	**f**	**f**	**t**	**t**	**f**	**t**
f	**f**	**t**	**t**	**t**	**f**	**t**
f	**t**	**f**	**f**	**t**	**f**	**f**
f	**t**	**t**	**f**	**t**	**f**	**f**
t	**f**	**f**	**f**	**f**	**t**	**t**
t	**f**	**t**	**f**	**f**	**f**	**f**
t	**t**	**f**	**t**	**f**	**t**	**f**
t	**t**	**t**	**t**	**f**	**f**	**t**

Die Formel ist also sowohl erfüllbar als auch widerlegbar, daher weder gültig noch unerfüllbar. Die erste Zeile der Tabelle liefert das Modell I mit $I(A) = \mathbf{f}$, $I(B) = \mathbf{f}$ und $I(C) = \mathbf{f}$. Die dritte Zeile liefert das Gegenbeispiel J mit $J(A) = \mathbf{f}$, $J(B) = \mathbf{t}$ und $J(C) = \mathbf{f}$.

b) Wir verwenden die Abkürzungen $F = (B \supset \neg A) \equiv (\neg A \supset B)$

A	B	$\neg A$	$B \supset \neg A$	$\neg A \supset B$	F
f	**f**	**t**	**t**	**f**	**f**
f	**t**	**t**	**t**	**t**	**t**
t	**f**	**f**	**t**	**t**	**t**
t	**t**	**f**	**f**	**t**	**f**

Die Formel ist also sowohl erfüllbar als auch widerlegbar, daher weder gültig noch unerfüllbar. Die erste Zeile der Tabelle liefert das Gegenbeispiel I mit $I(A) = \mathbf{f}$ und $I(B) = \mathbf{f}$. Die zweite Zeile liefert das Modell J mit $J(A) = \mathbf{f}$ und $J(B) = \mathbf{t}$.

c) Wir verwenden die Abkürzung $F = (C \supset (B \supset A)) \supset ((A \subset C) \subset (B \subset C))$ und $G = (A \subset C) \subset (B \subset C)$.

A	B	C	$B \supset A$	$C \supset (B \supset A)$	$A \subset C$	$B \subset C$	G	F
f	**f**	**f**	**t**	**t**	**t**	**t**	**t**	**t**
f	**f**	**t**	**t**	**t**	**f**	**f**	**t**	**t**
f	**t**	**f**	**f**	**t**	**t**	**t**	**t**	**t**
f	**t**	**t**	**f**	**f**	**f**	**t**	**f**	**t**
t	**f**	**f**	**t**	**t**	**t**	**t**	**t**	**t**
t	**f**	**t**	**t**	**t**	**t**	**f**	**t**	**t**
t	**t**	**f**	**t**	**t**	**t**	**t**	**t**	**t**
t	**t**	**t**	**t**	**t**	**t**	**t**	**t**	**t**

Die Formel ist also gültig und damit auch erfüllbar, aber weder widerlegbar noch unerfüllbar. Es gibt demnach keine Gegenbeispiele und jede Interpretation, z.B. I mit $I(A) = \mathbf{f}$, $I(B) = \mathbf{f}$ und $I(C) = \mathbf{f}$, ist ein Modell.

Aufgabe 7.2 Beweisen Sie Satz 3.28 (Deduktionstheorem) und Folgerung 3.29 aus dem Vorlesungsskriptum. *Hinweis:* Verwenden Sie vollständige Induktion.

Lösung

Das Deduktionstheorem lautet: $F_1, \ldots, F_n \models G$ genau dann, wenn $F_1, \ldots, F_{n-1} \models F_n \supset G$.
Wir beweisen diesen Satz durch Induktion nach n.
Induktionsanfang: $F_1 \models G$ bedeutet, laut Definition, dass für alle Interpretationen I gilt, dass wenn $\mathcal{M}_{AF}(I, F_1) = \mathbf{t}$ dann auch $\mathcal{M}_{AF}(I, G) = \mathbf{t}$. Anders formuliert: $F_1 \models G$ gilt gdw. für alle I entweder $\mathcal{M}_{AF}(I, F_1) = \mathbf{f}$ oder $\mathcal{M}_{AF}(I, G) = \mathbf{t}$. Letzteres ist aber, gemäß der Defintion der Semantik von '$\supset$' (MAF4), genau die Bedingung dafür, dass $\mathcal{M}_{AF}(I, F_1 \supset G) = \mathbf{t}$. Mit anderen Worten: $F_1 \models G$ gdw. $F_1 \supset G$ gültig ist, wobei letzteres gleichbedeutend mit $\models F_1 \supset G$ ist.
Induktionsannahme: $F_1, \ldots, F_n \models G$ gdw. $F_1, \ldots, F_{n-1} \models F_n \supset G$.
Induktionsschritt: Wie müssen zeigen, dass $F_1, \ldots, F_n, F_{n+1} \models G$ gdw. $F_1, \ldots, F_n \models F_{n+1} \supset G$.
Wir benützen die Tatsache, dass folgende Aussage eine Instanz der Induktionsannahme ist:
$F_1 \wedge F_2, F_3 \ldots, F_n, F_{n+1} \models G$ gdw. $F_1 \wedge F_2, F_3 \ldots, F_n \models F_{n+1} \supset G$ (wobei $n \geq 2$).
Es bleibt dann nur mehr zu zeigen, dass, ganz allgemein für alle Formeln $H_1, \ldots, H_m, E$ gilt:
$H_1 \wedge H_2, H_3 \ldots, H_m \models E$ gdw. $H_1, H_2, H_3, \ldots, H_m \models E$.
Letzteres folgt aber aus der Definition von '$\models$' und '$\wedge$'. Das sieht man am deutlichsten, wenn man folgende äquivalente Umformung von Definition 3.27 betrachtet (vgl. Definition 3.35):

$F_1, \ldots, F_n \models G$ gdw. $\mathcal{M}_{AF}(I, G) = \mathbf{t}$ oder $\mathcal{M}_{AF}(I, F_i) = \mathbf{f}$ für mindestens ein $F_i \in \{F_1, \ldots, F_n\}$.

Weil $\mathcal{M}_{AF}(I, H_1 \wedge H_2) = \mathbf{f}$ gdw. $\mathcal{M}_{AF}(I, H_1) = \mathbf{f}$ oder $\mathcal{M}_{AF}(I, H_2) = \mathbf{f}$, ist die Bedingung '$\mathcal{M}_{AF}(I, H) = \mathbf{f}$ für mindestens ein $H \in \{H_1, H_2, H_3 \ldots, F_n\}$' gleichbedeutend mit:
'$\mathcal{M}_{AF}(I, H) = \mathbf{f}$ für mindestens ein $H \in \{H_1 \wedge H_2, H_3 \ldots, F_n\}$'.
Zusammenfassend erhält man daher (für $n \geq 2$):
$F_1, F_2, F_3, \ldots, F_n, F_{n+1} \models G$ gdw. $F_1 \wedge F_2, F_3 \ldots, F_n, F_{n+1} \models G$ gdw. (Induktionsannahme)
$F_1 \wedge F_2, F_3 \ldots, F_n \models F_{n+1} \supset G$ gdw. $F_1, F_2, F_3 \ldots, F_n \models F_{n+1} \supset G$.

Durch n-malige Anwendung des Deduktionstheorems erhält man die Folgerung: $F_1, \ldots, F_n \models G$ gdw. $\models F_1 \supset (F_2 \supset \cdots (F_n \supset G) \cdots)$.
Hinweis für TutorInnen: Man sollte erwähen, dass man jeden Beweis der Form 'Durch wiederholte Anwendung von ...' auch als Induktionsbeweis verstehen kann.

Wir zeigen nun noch: $F_1, \ldots, F_n \models G$ gdw. $\models (F_1 \wedge \cdots \wedge F_n) \supset G$.
Dies kann man entweder direkt – wie in unserem Beweis des Deduktionstheorems – tun, oder man kann – auf Grund der vorhergehenden Folgerung – statt dessen die Äquivalenz von $F_1 \supset (F_2 \supset \cdots (F_n \supset G) \cdots)$ und $(F_1 \wedge \cdots \wedge F_n) \supset G$ zeigen.
Wir gehen den zuletzt genannten Weg und beweise die Äquivalenz durch Induktion nach n:
Induktionsanfang: Es bleibt nichts zu zeigen da man für $n = 1$ in beiden Fällen $F_1 \supset G$ erhält.
Induktionsannahme: $F_1 \supset (F_2 \supset \cdots (F_n \supset G) \cdots) = (F_1 \wedge \cdots \wedge F_n) \supset G$.
Induktionsschritt: Wir wenden die Induktionsannahme auf die Teilformel $(F_2 \supset \cdots (F_n \supset G) \cdots)$ in $F_1 \supset (F_2 \supset \cdots (F_n \supset G) \cdots)$ an und erhalten $F_1 \supset ((F_2 \wedge \cdots \wedge F_n) \supset G)$. Wir müssen nun noch $F_1 \supset (H \supset G) = (F_1 \wedge H) \supset G$ zeigen, wobei $H = (F_2 \wedge \cdots \wedge F_n)$. Diese Äquivalenz gilt ganz allgemein, wie folgende Wahrheitstafel zeigt:

A	B	C	$B \supset C$	$A \wedge B$	$A \supset (B \supset C)$	$(A \wedge B) \supset C$
f	**f**	**f**	**t**	**f**	**t**	**t**
f	**f**	**t**	**t**	**f**	**t**	**t**
f	**t**	**f**	**f**	**f**	**t**	**t**
f	**t**	**t**	**t**	**f**	**t**	**t**
t	**f**	**f**	**t**	**f**	**t**	**t**
t	**f**	**t**	**t**	**f**	**t**	**t**
t	**t**	**f**	**f**	**t**	**f**	**f**
t	**t**	**t**	**t**	**t**	**t**	**t**

Um unsere spezielle Instanz der Äquivalenz zu erhalten können wir auf Folgerung 3.23 des Vorlesungsskriptums verweisen.

Aufgabe 7.3 Zeigen Sie, dass folgende Formeln H_1, H_2, H_3 paarweise äquivalent sind. Verwenden Sie dazu Satz 3.21 und Folgerung 3.23 aus dem Vorlesungsskriptum.

$H_1 = \neg((G \uparrow D) \downarrow K) \supset (C \equiv (E \downarrow D))$

$H_2 = (C \equiv (E \downarrow D)) \vee ((G \uparrow D) \downarrow K)$

$H_3 = (C \equiv (E \downarrow D)) \subset \neg((G \uparrow D) \downarrow K)$

Lösung Es sei σ die Substitution $[\genfrac{}{}{0pt}{}{(G\uparrow D)\downarrow K}{A} \genfrac{}{}{0pt}{}{C\equiv(E\downarrow D)}{B}]$, sowie $F_1 = \neg A \supset B$, $F_2 = B \vee A$ und $F_3 = B \subset \neg A$. Dann gilt $H_i = F_i\sigma$ für alle $i \in \{1,2,3\}$. Laut Satz 3.20 und Folgerung 3.22 genügt es daher, die paarweise Äquivalenz von F_1, F_2 und F_3 zu zeigen. Diese läßt sich unmittelbar aus folgender Wahrheitswertabelle ablesen:

A	B	$\neg A \supset B$	$B \vee A$	$B \subset \neg A$	$F_1 \equiv F_2$	$F_1 \equiv F_3$	$F_2 \equiv F_3$
f	**f**	**f**	**f**	**f**	**t**	**t**	**t**
f	**t**	**t**	**t**	**t**	**t**	**t**	**t**
t	**f**	**t**	**t**	**t**	**t**	**t**	**t**
t	**t**	**t**	**t**	**t**	**t**	**t**	**t**

Aufgabe 7.4 Finden Sie konjunktive und disjunktive Normalformen zur Formel

$$F = (\neg\neg A \not\supset B) \uparrow ((\mathbf{f} \downarrow C) \subset (B \vee \neg A))$$

indem Sie sowohl die syntaktische als auch die semantische Methode zur Normalformenbildung anwenden. Geben Sie die KNF von F auch in Mengennotation an.

Lösung

Syntaktische Methode:

Schritt 1 — Alle Operatoren auf $\wedge$, $\vee$, $\neg$ zurückführen:

$$\begin{aligned}
F &= (\neg\neg A \not\supset B) \uparrow ((\mathbf{f} \downarrow C) \subset (B \vee \neg A)) \\
&= \neg(\neg\neg A \not\supset B) \vee \neg((\mathbf{f} \downarrow C) \subset (B \vee \neg A)) \\
&= \neg(\neg\neg A \wedge \neg B) \vee \neg((\mathbf{f} \downarrow C) \subset (B \vee \neg A)) \\
&= \neg(\neg\neg A \wedge \neg B) \vee \neg((\neg\mathbf{f} \wedge \neg C) \subset (B \vee \neg A)) \\
&= \neg(\neg\neg A \wedge \neg B) \vee \neg((\neg\mathbf{f} \wedge \neg C) \vee \neg(B \vee \neg A))
\end{aligned}$$

Schritt 2 — Negationen nach innen ziehen:

$$\begin{aligned}
&= (\neg\neg\neg A \vee \neg\neg B) \vee \neg((\neg\mathbf{f} \wedge \neg C) \vee \neg(B \vee \neg A)) \\
&= (\neg A \vee B) \vee (\neg(\neg\mathbf{f} \wedge \neg C) \wedge \neg\neg(B \vee \neg A)) \\
&= (\neg A \vee B) \vee (\neg\neg\mathbf{f} \vee \neg\neg C) \wedge \neg\neg(B \vee \neg A)) \\
&= (\neg A \vee B) \vee ((\mathbf{f} \vee C) \wedge (B \vee \neg A))
\end{aligned}$$

Schritt 3 – Konstanten eliminieren:

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

Schritt 4 — Ausdistribuieren: Die DNF von F erhält man, in diesem Fall, durch einmaliges Anwenden des entsprechenden Distributivgesetzes:

$$\begin{aligned}
&(\neg A \vee B) \vee (C \wedge (B \vee \neg A)) \\
&= (\neg A \vee B) \vee ((C \wedge B) \vee (C \wedge \neg A))
\end{aligned}$$

Berücksichtigt man die Assoziativität und Kommutativität der Disjunktion so erhalten wir

$$\mathrm{DNF}(F) = \neg A \vee B \vee (B \wedge C) \vee (\neg A \wedge C)$$

($\mathrm{DNF}(F)$ ist zur einfacheren Formel $\neg A \vee B$ äquivalent.)

Auch die KNF von F erhält man, in diesem Fall, durch einmaliges Anwenden des entsprechenden Distributivgesetzes:

$$\begin{aligned}&(\neg A \vee B) \vee (C \wedge (B \vee \neg A))\\ =\ &((\neg A \vee B) \vee C) \wedge ((\neg A \vee B) \vee (B \vee \neg A))\end{aligned}$$

Berücksichtigt man die Assoziativität, Idempotenz und Kommutativität der Disjunktion so erhalten wir

$$\mathrm{KNF}(F) = (\neg A \vee B \vee C) \wedge (\neg A \vee B)$$

bzw. in Mengennotation

$$\mathrm{KNF}(F) = \{\{\neg A, B, C\},\ \{\neg A, B\}\}$$

Durch Anwendung von Subsumtion lässt sich dies vereinfachen zu

$$\mathrm{KNF}(F) = \{\{\neg A, B\}\}$$

Semantische Methode:

Wir verwenden die Abkürzungen $G = \neg\neg A \not\supset B$ und $H = (\mathbf{f} \downarrow C) \subset (B \vee \neg A)$.

A	B	C	$\neg A$	$\neg\neg A$	G	$\mathbf{f} \downarrow C$	$B \vee \neg A$	H	F	K_I	D_I
f	**f**	**f**	**t**	**f**	**f**	**t**	**t**	**t**	**t**	$\neg A \wedge \neg B \wedge \neg C$	
f	**f**	**t**	**t**	**f**	**f**	**f**	**t**	**f**	**t**	$\neg A \wedge \neg B \wedge C$	
f	**t**	**f**	**t**	**f**	**f**	**t**	**t**	**t**	**t**	$\neg A \wedge B \wedge \neg C$	
f	**t**	**t**	**t**	**f**	**f**	**f**	**t**	**f**	**t**	$\neg A \wedge B \wedge C$	
t	**f**	**f**	**f**	**t**	**t**	**t**	**f**	**t**	**f**		$\neg A \vee B \vee C$
t	**f**	**t**	**f**	**t**	**t**	**f**	**f**	**t**	**f**		$\neg A \vee B \vee \neg C$
t	**t**	**f**	**f**	**t**	**f**	**t**	**t**	**t**	**t**	$A \wedge B \wedge \neg C$	
t	**t**	**t**	**f**	**t**	**f**	**f**	**t**	**f**	**t**	$A \wedge B \wedge C$	

Es gilt also:

$$\begin{aligned}\mathrm{DNF}(F) = \bigvee_{I \in INT, \mathcal{M}_{AF}(I,F)=\mathbf{t}} K_I = \;&(\neg A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge B \wedge \neg C)\\ &\vee (\neg A \wedge B \wedge C) \vee (A \wedge B \wedge \neg C) \vee (A \wedge B \wedge C)\end{aligned}$$

(Die DNF ist natürlich wiederum zu $\neg A \vee B$ äquivalent.)

$$\mathrm{KNF}(F) = \bigwedge_{I \in INT, \mathcal{M}_{AF}(I,F)=\mathbf{f}} D_I = (\neg A \vee B \vee C) \wedge (\neg A \vee B \vee \neg C)$$

bzw. in Mengenform: $\mathrm{KNF}(F) = \{\{\neg A, B, C\},\ \{\neg A, B, \neg C\}\}$.
(Die KNF ist wiederum äquivalent zu $\{\{\neg A, B\}\}$.)

Aufgabe 7.5 Finden Sie durch Konstruktion geeigneter Ableitungsversuche im Sequentialkalkül jeweils entweder ein Gegenmodell oder den Nachweis, dass die Formel gültig ist.

a) $((\neg A \wedge D) \supset (D \supset (\neg B \vee B))) \supset A$

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

Lösung

a) Wir bilden folgenden Ableitungsversuch:

$$\cfrac{\cfrac{\cfrac{\cfrac{\overset{\text{Axiom}}{A \vdash A}}{\vdash \neg A, A}\,\neg\text{-r} \qquad \overset{\text{Anti-Axiom}}{\vdash D, A}}{\vdash \neg A \wedge D, A}\,\wedge\text{-r} \qquad \cfrac{\vdots}{D \supset (\neg B \vee B) \vdash A}}{(\neg A \wedge D) \supset (D \supset (\neg B \vee B)) \vdash A}\,\supset\text{-l}}{\vdash ((\neg A \wedge D) \supset (D \supset (\neg B \vee B))) \supset A}\,\supset\text{-r}$$

Das Anti-Axiom gibt an, dass jede Interpretation I mit $I(A) = \mathbf{f}$ und $I(D) = \mathbf{f}$ ein Gegenmodell zu $((\neg A \wedge D) \supset (D \supset (\neg B \vee B))) \supset A$ ist; also, z.B., eine Interpretation I, die *alle* Aussagenvariable falsch macht.
(Da bereits ein Zweig, der in einem Anti-Axiom endet, zum Nachweis der Widerlegbarkeit aussreicht, muss der Rest des Ableitungsversuchs nicht weiter ausgeführt werden.)

b) Der Sequent $\vdash ((A \supset D) \supset (B \wedge C)) \supset (\neg C \supset (\neg(A \supset D) \vee B))$ ist ableitbar und daher ist die entsprechende Formel — wegen der Korrektheit des Sequentialkalküls — gültig:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\genfrac{}{}{0pt}{}{\text{Axiom}}{A \supset D \vdash A \supset D, C, B} \qquad \dfrac{\genfrac{}{}{0pt}{}{\text{Axiom}}{B, C, A \supset D \vdash C, B}}{B \wedge C, A \supset D \vdash C, B}\ \wedge\text{-l}}{(A \supset D) \supset (B \wedge C), A \supset D \vdash C, B}\ \supset\text{-l}}{(A \supset D) \supset (B \wedge C) \vdash C, \neg(A \supset D), B}\ \neg\text{-r}}{(A \supset D) \supset (B \wedge C), \neg C \vdash \neg(A \supset D), B}\ \neg\text{-l}}{(A \supset D) \supset (B \wedge C), \neg C \vdash \neg(A \supset D) \vee B}\ \vee\text{-r}}{(A \supset D) \supset (B \wedge C) \vdash \neg C \supset (\neg(A \supset D) \vee B)}\ \supset\text{-r}}{\vdash ((A \supset D) \supset (B \wedge C)) \supset (\neg C \supset (\neg(A \supset D) \vee B))}\ \supset\text{-r}
$$