Aufgabe 1 (a)

Beweis durch logische Umformung

Schreibweise:

$F \equiv G$ für „die Formeln F und G sind äquivalent“.

Übungen

zur Vorlesung

Formale Systeme

Wintersemester 2000/2001

Dr. Bernhard Beckert

beckert@ira.uka.de

Zimmer 309

Institut für Logik, Komplexität
und Deduktionssysteme

Universität Karlsruhe (TH)

$$A = \underbrace{(\neg P \land Q \land \neg R)}_{1} \lor \underbrace{(P \land Q \land \neg R)}_{2} \lor \underbrace{(P \land Q \land R)}_{3} \lor \underbrace{(\neg P \land \neg Q \land R)}_{4} \lor \underbrace{(P \land \neg Q \land R)}_{5}$$

$$A' = \underbrace{(\neg Q \land R)}_{A'_1} \lor \underbrace{(Q \land \neg R)}_{A'_2} \lor \underbrace{(P \land R)}_{A'_3}$$

A

$\equiv$ (Kommutativität von $\land$ und $\lor$, Idempotenz von $\lor$)

$$\underbrace{(A'_1 \land \neg P)}_{4'} \lor \underbrace{(A'_1 \land P)}_{5'} \lor \underbrace{(A'_2 \land \neg P)}_{1'} \lor \underbrace{(A'_2 \land P)}_{2'} \lor \underbrace{(A'_3 \land \neg Q)}_{5''} \lor \underbrace{(A'_3 \land Q)}_{3'}$$

Web-Seite

Web-Seite zu den Übungen:

`http://i12www.ira.uka.de/~beckert/Lehre/FS-Uebungen/`

A

$\equiv$

$(A'_1 \land \neg P) \lor (A'_1 \land P) \lor (A'_2 \land \neg P) \lor (A'_2 \land P) \lor (A'_3 \land \neg Q) \lor (A'_3 \land Q)$

$\equiv$ (Distributivität von $\land$ über $\lor$)

$(A'_1 \land (\neg P \lor P)) \lor (A'_2 \land (\neg P \lor P)) \lor (A'_3 \land (\neg Q \lor Q))$

$\equiv$ (Tertium non datur)

$(A'_1 \land \mathit{true}) \lor (A'_2 \land \mathit{true}) \lor (A'_3 \land \mathit{true})$

$\equiv$ (true neutrales Element bzgl. $\land$)

$A'_1 \lor A'_2 \lor A'_3 \overset{\text{def}}{=} A'$

Aufgabe 1 (b) und (c)

Primimplikanten von A:

1. $\neg Q \land R$ (essentiell)
2. $Q \land \neg R$ (essentiell)
3. $P \land R$ (nicht essentiell)
4. $P \land Q$ (nicht essentiell)

Aufgabe 2

Craig's Interpolationstheorem. Seien A_1 und A_2 äquivalente aussagenlogische Formeln. Dann gibt es eine zu A_1 und A_2 äquivalente Formel A, so daß jede in A vorkommende aussagenlogische Variable sowohl in A_1 als auch in A_2 vorkommt.

Wir beweisen zunächst:

Lemma. Ein Primimplikant einer Formel B enthält nur aussagenlogische Variablen, die auch in B vorkommen.

Beweis.

Angenommen, die Aussage des Lemmas wäre falsch.

Also: Ein Primimplikant von B enthält eine Variable, die in B nicht vorkommt.

Dieser Primimplikant kann nicht leer sein
(denn er enthält eine Variable).

Also: Er ist von der Form $P \land L$, wobei o.B.d.A. L ein Literal ist, dessen Variable in B nicht vorkommt.

Sei I beliebige Interpretation, in der P wahr ist.

Sei $\overline{I}$ die Struktur, die sich von S nur dadurch unterscheidet, daß der Wahrheitswert der Variablen in L zu seinem Komplement verändert ist.

Dann gilt: $P \land L$ ist entweder in I oder in $\overline{I}$ wahr.

Also: B in I oder in $\overline{I}$ wahr.

Wahrheitswert von B hängt nicht von der Belegung der Variablen in L ab.
(Denn diese kommt in B nicht vor.)

Also: B sowohl in I als auch in $\overline{I}$ wahr,
insbesondere in I.

Damit: P ein Implikant von B.

Widerspruch dazu, daß $P \land L$ ein *Prim*implikant von B ist.

Also: Annahme falsch.

$P \land L$ enthält nur Variablen, die in B vorkommen.

Craig's Interpolationstheorem. Seien A_1 und A_2 äquivalente aussagenlogische Formeln. Dann gibt es eine zu A_1 und A_2 äquivalente Formel A, so daß jede in A vorkommende aussagenlogische Variable sowohl in A_1 als auch in A_2 vorkommt.

Beweis.

Sei A die Disjunktion aller Primimplikanten von A_1.

A ist äquivalent zu A_1
(wie in der Vorlesung bewiesen)
und damit auch zu A_2.

Jeder in A vorkommende Primimplikant von A_1 ist auch Primimplikant von A_2
(wegen der Äquivalenz von A_1 und A_2).

Aus dem Lemma folgt:
A enthält nur Variablen, die sowohl in A_1 als auch in A_2 vorkommen.

Aufgabe 3

Lemma (Korollar zu Satz 3.58 im Skriptum)

Die Formel

$$A_1 \leftrightarrow (A_2 \leftrightarrow \cdots (A_{k-1} \leftrightarrow A_k) \cdots)$$

ist genau dann in einer Interpretation I wahr, wenn die Zahl der A_i, die in I *falsch* sind, *gerade* ist.

Daraus folgt:

Da entweder P_1 oder $\neg P_1$ falsch ist, ist

$$C_n = \neg(P_1 \leftrightarrow (P_2 \leftrightarrow \cdots (P_{n-1} \leftrightarrow (P_n \leftrightarrow \neg P_1) \cdots))$$

wahr genau dann,

wenn eine *gerade* Anzahl der $P_2, \ldots, P_n$ *falsch* ist.

Teilaufgabe 3 (a)

Antwort: Nein.

Schon
$$C_2 = \neg(P_1 \leftrightarrow (P_2 \leftrightarrow \neg P_1))$$
ist keine Tautologie.

Aus der Überlegung folgt, daß C_2 genau dann falsch ist, wenn P_2 falsch ist,

also beispielsweise in einer Interpretation I mit

$$\begin{array}{rcl} val_I(P_1) & = & W \\ val_I(P_2) & = & F \end{array}$$

Teilaufgabe 3 (b)

Aus der Überlegung folgt, daß folgende Formel in *disjunktiver* Normalform zu C_n äquivalent ist:

$$\bigvee_{\substack{I \subseteq \{2,\ldots,n\} \\ \#I \text{ gerade}}} \Big(\bigwedge_{i \in I} \neg P_i \wedge \bigwedge_{j \in \{2,\ldots,n\} \setminus I} P_j \Big)$$

Durch Anwendung der de Morganschen Gesetze
(die Negation „nach innen schieben"):

Folgende Formel in *konjunktiver* Normalform ist zu $\neg C_n$ äquivalent:

$$\bigwedge_{\substack{I \subseteq \{2,\ldots,n\} \\ \#I \text{ gerade}}} \Big(\bigvee_{i \in I} P_i \vee \bigvee_{j \in \{2,\ldots,n\} \setminus I} \neg P_j \Big)$$

Teilaufgabe 3 (c)

$$C_n = \overbrace{\neg(P_1 \leftrightarrow \underbrace{(P_2 \leftrightarrow \cdots \underbrace{(P_{n-1} \leftrightarrow \overbrace{(P_n \leftrightarrow \neg P_1)}^{Q_n})}_{Q_{n-1}} \cdots)}_{Q_2})}^{Q_1}$$

1. Schritt: Einführung neuer Atome

$$\begin{array}{ccc}
Q_1 & \leftrightarrow & \neg(P_1 \leftrightarrow Q_2) \\
Q_2 & \leftrightarrow & (P_2 \leftrightarrow Q_3) \\
\vdots & \vdots & \vdots \\
Q_{n-1} & \leftrightarrow & (P_{n-1} \leftrightarrow Q_n) \\
Q_n & \leftrightarrow & (P_n \leftrightarrow \neg P_1) \\
Q_1 & &
\end{array}$$

Zur Auflösung der Äquivalenzen verwenden wir folgende Abkürzungen:

$$\begin{aligned}
F(A,B,C) := {} & (\ \ A \lor \ \ B \lor \ \ C) \land \\
& (\ \ A \lor \neg B \lor \neg C) \land \\
& (\neg A \lor \ \ B \lor \neg C) \land \\
& (\neg A \lor \neg B \lor \ \ C)
\end{aligned}$$

$$\begin{aligned}
G(A,B,C) := {} & (\neg A \lor \neg B \lor \neg C) \land \\
& (\ \ A \lor \ \ B \lor \neg C) \land \\
& (\ \ A \lor \neg B \lor \ \ C) \land \\
& (\neg A \lor \ \ B \lor \ \ C)
\end{aligned}$$

Es gilt (Übung!):

$$\begin{array}{rcl}
F(A,B,C) & \equiv & A \leftrightarrow (B \leftrightarrow C) \\
G(A,B,C) & \equiv & \neg F(A,B,C)
\end{array}$$

Zudem verwenden wir:

$$\begin{array}{rcl}
A \leftrightarrow \neg B & \equiv & \neg A \leftrightarrow B \\
& \equiv & \neg(A \leftrightarrow B)
\end{array}$$

Ergebnis des 1. Schrittes war:

$$\begin{array}{ccc}
Q_1 & \leftrightarrow & \neg(P_1 \leftrightarrow Q_2) \\
Q_2 & \leftrightarrow & (P_2 \leftrightarrow Q_3) \\
\vdots & \vdots & \vdots \\
Q_{n-1} & \leftrightarrow & (P_{n-1} \leftrightarrow Q_n) \\
Q_n & \leftrightarrow & (P_n \leftrightarrow \neg P_1) \\
Q_1 & &
\end{array}$$

Endergebnis: $(C_n)_{kknf}$ ist die Konjunktion von

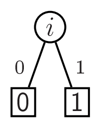
$$\begin{array}{c}
G(Q_1, P_1, Q_2) \\
F(Q_2, P_2, Q_3) \\
\vdots \\
F(Q_{n-1}, P_{n-1}, Q_n) \\
G(Q_n, P_n, P_1) \\
Q_1
\end{array}$$

Aufgabe 4

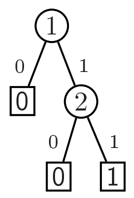
Achtung:

Eine Formel der Form $sh(P_1, P_2, P_3)$ ist *nicht* normiert, da P_2 und P_3 keine normierten sh-Formeln sind.

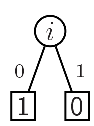
(a) $P_i \equiv sh(P_i, 0, 1)$



(b) $P_1 \land P_2 \equiv sh(P_1, 0, sh(P_2, 0, 1))$

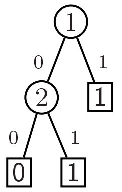


(c) $\neg P_i \equiv sh(P_i, 1, 0)$



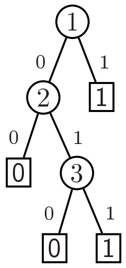
Aufgabe 4

(d) $P_1 \vee P_2 \quad \equiv \quad sh(P_1, sh(P_2, 0, 1), 1)$



(e) $P_1 \vee \neg P_1 \quad \equiv \quad 1$

(f) $P_1 \vee (P_2 \wedge P_3) \quad \equiv$
$sh(P_1, sh(P_2, 0, sh(P_3, 0, 1)), 1)$



Aufgabe 5

Man zeige, daß

$$\begin{aligned} A &= sh(sh(P_1, P_2, P_3), P_4, P_5) \\ B &= sh(P_1, sh(P_2, P_4, P_5), sh(P_3, P_4, P_5)) \end{aligned}$$

äquivalent sind.

Beweis

Sei eine beliebige Interpretation I gegeben.

Wir zeigen: $val_I(A) = val_I(B)$

Fallunterscheidung

1. Fall: $val_I(P_1) = W$

Dann gilt: $val_I(sh(P_1, P_2, P_3)) \;=\; val_I(P_3)$

Also: $val_I(A) \;=\; val_I(sh(P_3, P_4, P_5))$

Ebenso: $val_I(B) \;=\; val_I(sh(P_3, P_4, P_5))$

2. Fall: $val_I(P_1) = F$

Analog.

Frage

Gibt es eine kurze *disjunktive* Normalform?

Genauer:

Kann zu jeder aussagenlogischen Formel F eine Formel F' in disjunktiver Normalform berechnet werden, deren Länge polynomiell in der Länge von F ist und die genau dann erfüllbar ist, wenn F erfüllbar ist?

Antwort: Ja.

Man kann nämlich $true$ für erfüllbare und $false$ für unerfüllbare Formeln benutzen. Da die Erfüllbarkeit einer Formel entscheidbar ist, ist diese Normalform berechenbar.

Allerdings: Das ist uninteressant.

Präzisere Frage

Gibt es eine in *polynomieller Zeit berechenbare* kurze disjunktive Normalform?

Genauer:

Gibt es einen Algorithmus mit polynomieller Komplexität, der zu jeder aussagenlogischen Formel F eine Formel F' in disjunktiver Normalform berechnet, die genau dann erfüllbar ist, wenn F erfüllbar ist?

Antwort: Das ist ein offenes Problem.

Allerdings: Wahrscheinlich nicht. Denn da die Erfüllbarkeit von AL-Formeln ein NP-vollständiges Problem ist, die Erfüllbarkeit einer Formel in DNF aber in polynomieller Zeit entschieden werden kann, würde aus der Existenz eines solchen Algorithmus P=NP folgen!