Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. Peter H. Schmitt
Dr. V. Klebanov, Dr. M. Ulbrich, C. Scheben

Formale Systeme, WS 2013/2014

Lösungen zu Übungsblatt 7

Dieses Übungsblatt wurde in der Übung am 13.12.2013 besprochen.

Aufgabe 1

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

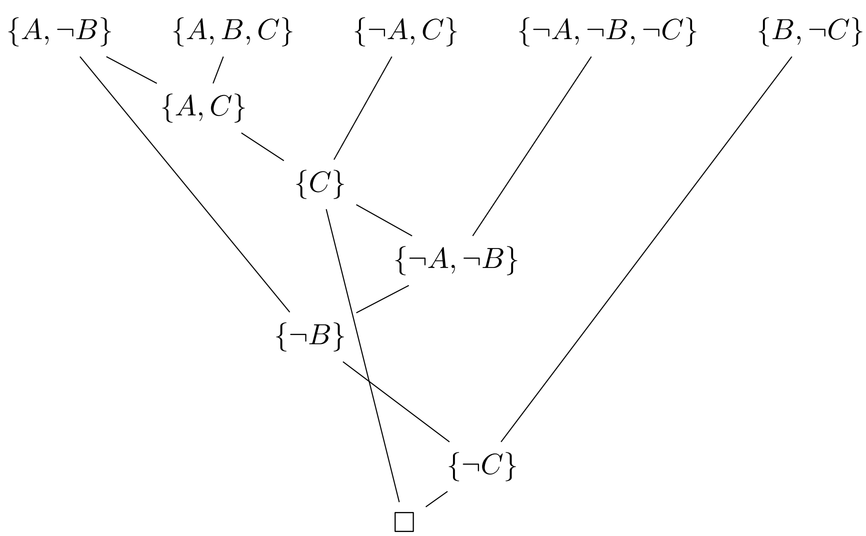
$$\neg A \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge \neg D) \vee (D \wedge B) \vee (\neg B \wedge C) \ ,$$

(c) die Allgemeingültigkeit der Formel

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

Lösung zu Aufgabe 1

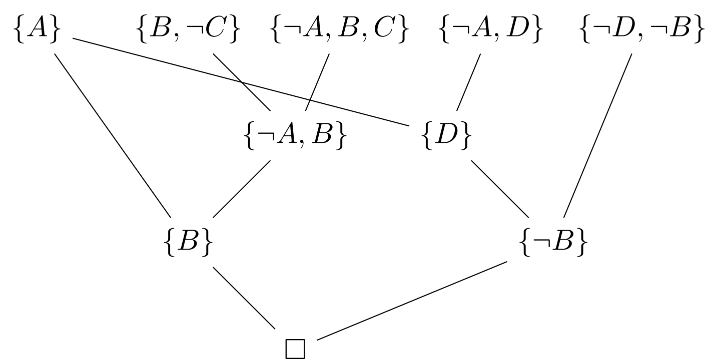
(a) 1. Schritt: Resolution



(b) <u>1. Schritt:</u> Formel negieren

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

<u>2. Schritt:</u> Klauselschreibweise und Resolution



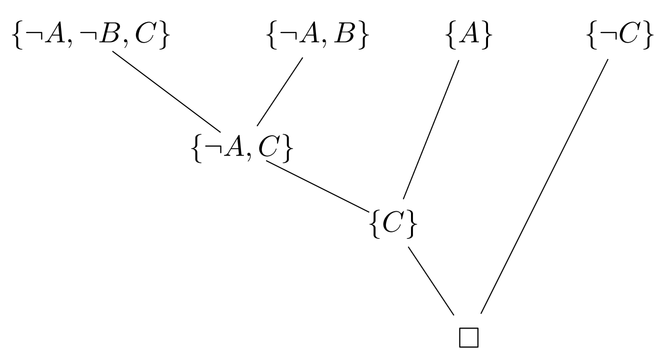
(c) <u>1. Schritt:</u> Formel negieren

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

<u>2. Schritt:</u> In KNF transformieren

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

<u>3. Schritt:</u> Klauselschreibweise und Resolution



Aufgabe 2

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

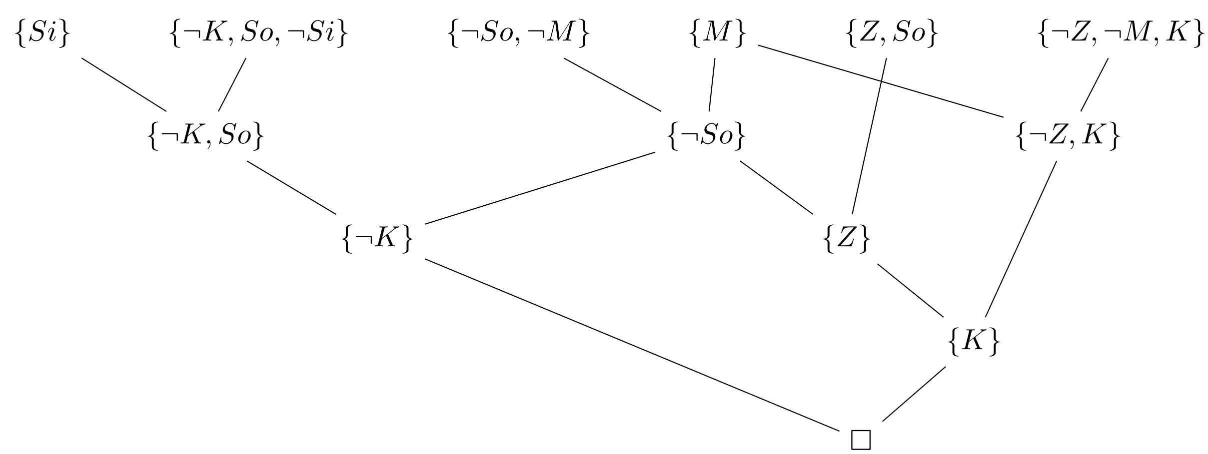
(b) Zeigen Sie mit Hilfe des Resolutionskalküls, dass ein solches Passwort nicht existieren kann.

Lösung zu Aufgabe 2

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 3

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 3

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 4

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 4

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. $\Box$

Aufgabe 5

Zeigen Sie die Unerfüllbarkeit der folgenden Klauselmenge mittels des Resolutionskalküls:

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

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 5

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 6

Betrachten wir - nur für diese Übungsaufgabe - die folgende geänderte Version der Definition von $Res(M)$ aus Definition 5.23 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 6

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.