Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. Bernhard Beckert
Thorsten Bormer, Dr. Vladimir Klebanov, Dr. Mattias Ulbrich

Formale Systeme, WS 2014/2015

Übungsblatt 7

Dieses Übungsblatt wird in der Übung am 12.12.2014 besprochen.

Aufgabe 1

Zeigen Sie mit Hilfe des Hilbertkalküls aus der Vorlesung die Aussage

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

Verwenden Sie dabei das in der Vorlesung vorgestellte Deduktionstheorem.

Lösung zu Aufgabe 1

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.

Die Ableitung im Hilbertkalkül ist:

	$\vdash$	$\neg A \to (\neg B \to \neg A)$	(1)	(Ax1)
$\{\neg A\}$	$\vdash$	$\neg B \to \neg A$	(2)	(DT 1)
	$\vdash$	$(\neg B \to \neg A) \to (A \to B)$	(3)	(Ax3)
$\{\neg A\}$	$\vdash$	$A \to B$	(4)	(MP 2,3)
	$\vdash$	$\neg A \to (A \to B)$	(5)	(DT 4)

Aus der Korrektheit des Hilbertkalküls folgt die Behauptung.

Aufgabe 2

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

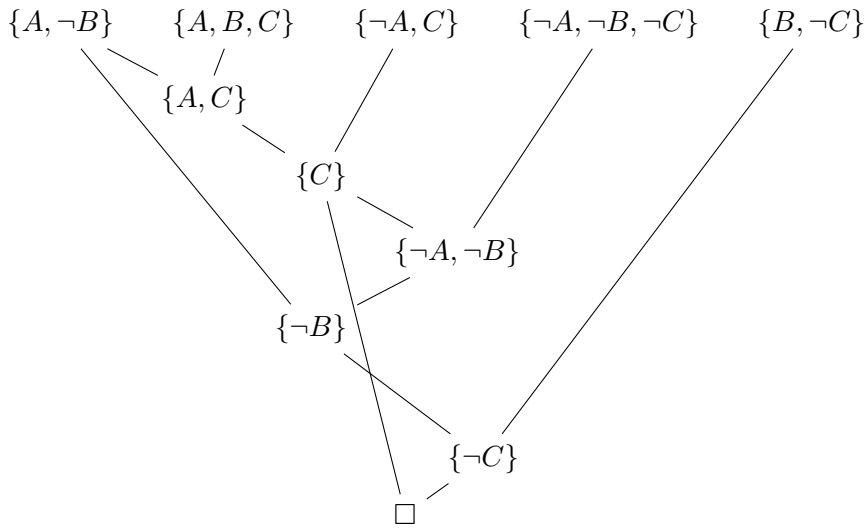
$$\neg A \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge \neg D) \vee (D \wedge B) \vee (\neg B \wedge C) \ ,$$

(c) die Allgemeingültigkeit der Formel

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

Lösung zu Aufgabe 2

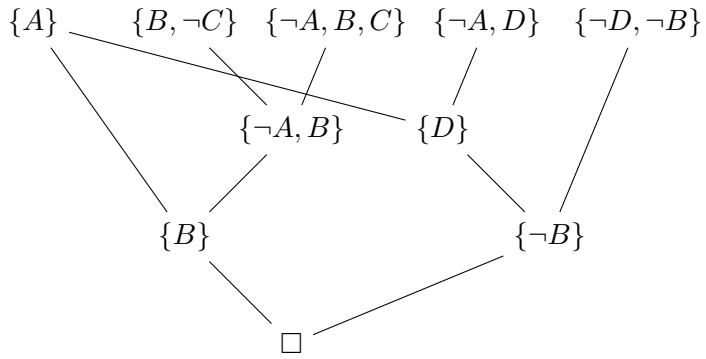
(a) 1. Schritt: Resolution



(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



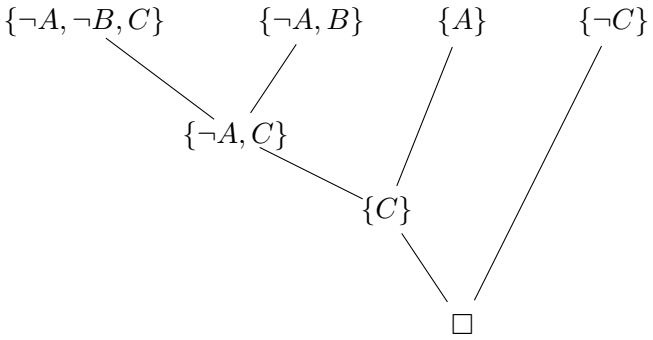
(c) 1. Schritt: Formel negieren

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

2. Schritt: In KNF transformieren

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

3. Schritt: Klauselschreibweise und Resolution



Aufgabe 3

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

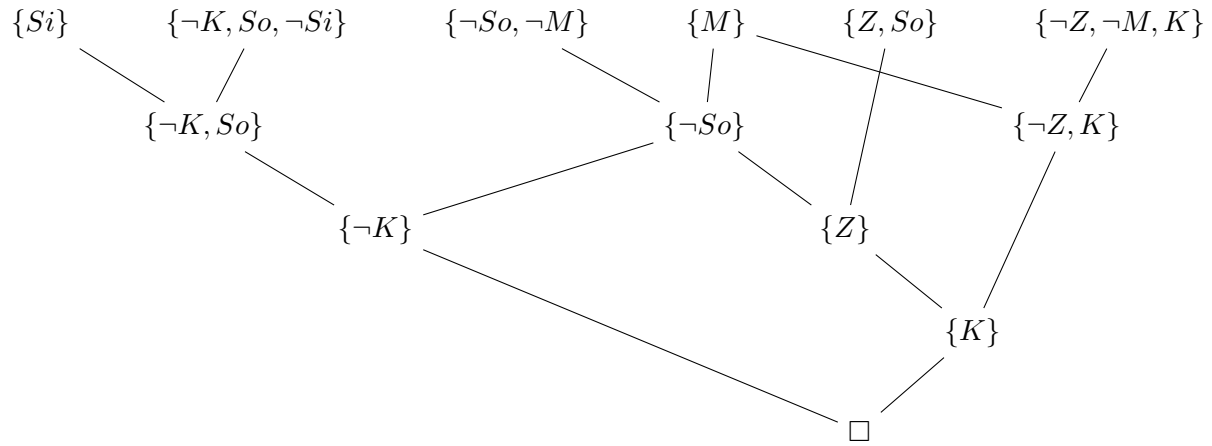
(b) Zeigen Sie mit Hilfe des Resolutionskalküls, dass ein solches Passwort nicht existieren kann.

Lösung zu Aufgabe 3

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 4

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 4

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 $\square$ ableiten. Widerspruch zur Erfüllbarkeit!

Aufgabe 5 (Zusatzaufgabe für Knobelbegeisterte)

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 5

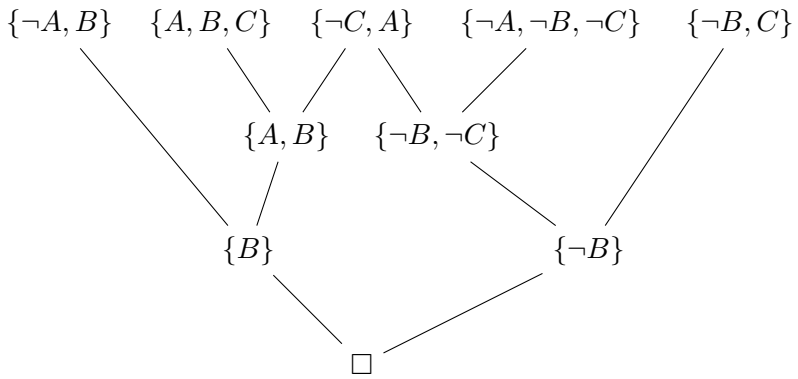
Diese Variante des Resolutionskalküls ist *nicht* vollständig, d.h., es gibt unerfüllbare Klauselmengen, aus denen nicht die leere Klausel abgeleitet werden kann.

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.