Karlsruher Institut für Technologie
Institut für Theoretische Informatik
Prof. Dr. B. Beckert
Thorsten Bormer

Formale Systeme, WS 2010/2011

Lösungen zum Übungsblatt 3

Dieses Blatt wurde in der Übung am 12.11.2010 besprochen.

Zu Aufgabe 1

(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

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

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

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

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

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

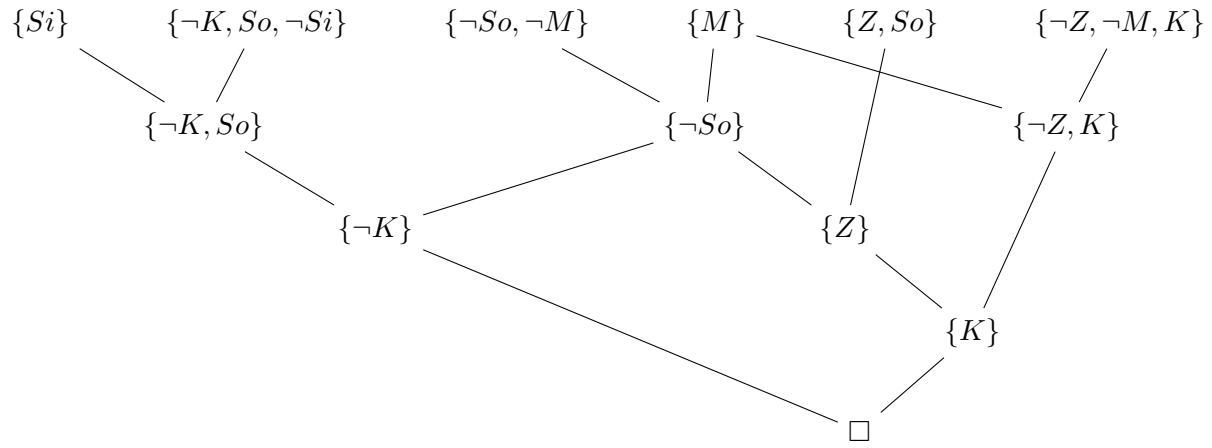
Anmerkung: Die Frage war nur, ob der Kalkül korrekt bzw. vollständig sein *kann*. Daraus folgt aber nicht, dass der Kalkül auch tatsächlich korrekt (im Falle von R_2) und vollständig (im Falle von R_1 oder R_2) ist. Der Standard-Hilbertkalkül H0 aus der Vorlesung hat diese Eigenschaften. Aber da wir 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.

Zu Aufgabe 2

Formalisierung.

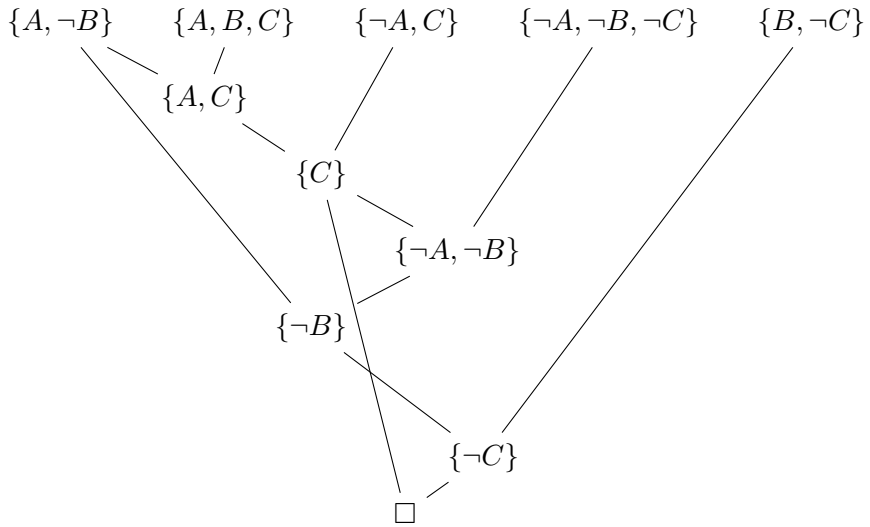
Das Passwort muss sicher sein, und man muss es sich merken können.	$Si \wedge M$
Passwörter beinhalten Zahlen oder Sonderzeichen oder beides.	$Z \vee So$
Ist das Passwort kurz und enthält keine Sonderzeichen, dann ist es nicht sicher.	$K \wedge \neg So \rightarrow \neg Si$
Ein Passwort mit Sonderzeichen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



Zu Aufgabe 3

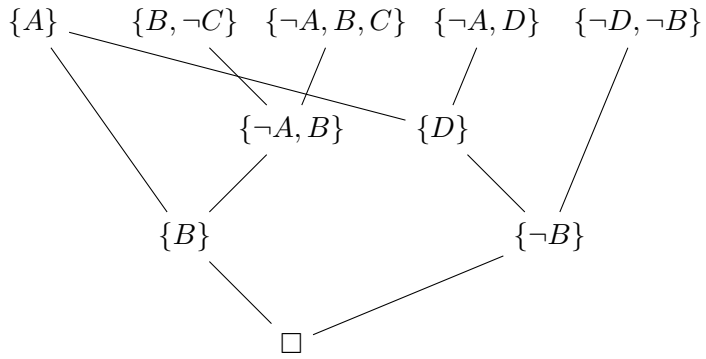
(a) 1. Schritt: Resolution



(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



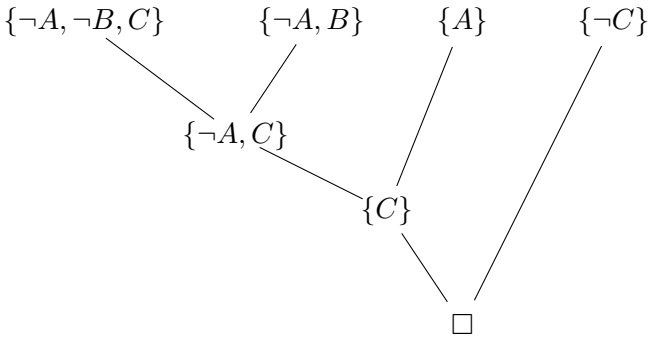
(c) 1. Schritt: Formel negieren

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

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



Zu Aufgabe 4

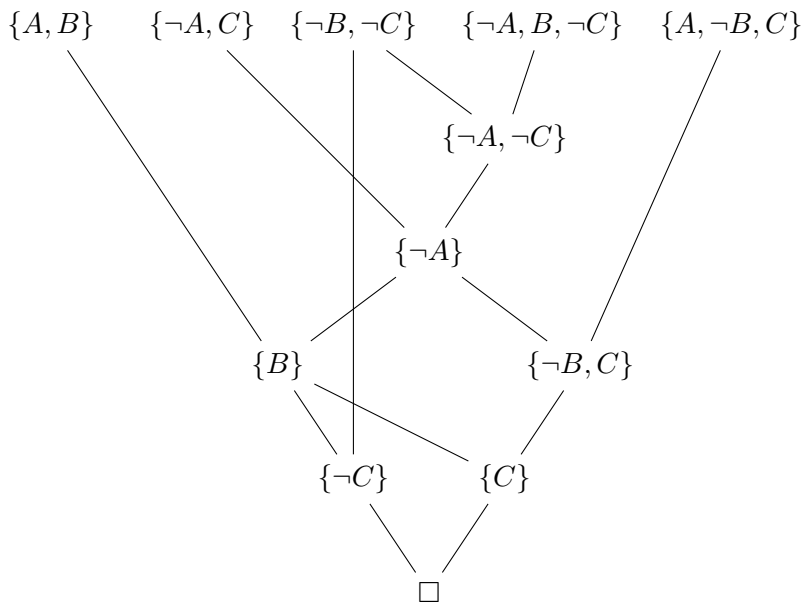
Diese Variante des Resolutionskalküls ist *nicht* vollständig, d.h., es gibt unerfüllbare Klauselmengen, aus denen nicht die leere Klausel abgeleitet werden kann.

Behauptung Die Klauselmenge

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

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 eins Klausel mehrmals zu verwenden.

Folgendes ist dafür zu beobachten:

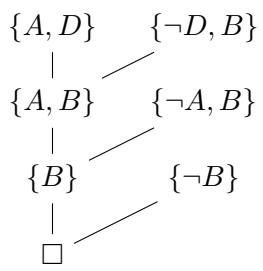
1. Bei jedem Resolutionsschritt nimmt die Anzahl der zur Verfügung stehenden Klauseln um genau eins ab.

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.

Zu Aufgabe 5

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



(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“).