Ludwig-Maximilians-Universität München SoSe 2009
Institut für Informatik
PD Dr. Martin Lange
Dipl.-Inf. Markus Latte 14. Mai 2009

Übung zur Vorlesung
Logik für Informatiker
Übungsblatt 4
Abgabe bis Freitag, 22. Mai 2009, 12h ct. vor der Übung
Besprechung am Freitag, 22. Mai 2009

Aufgabe 13. Entscheiden Sie für folgende Formeln, ob sie allgemeingültig sind. Geben Sie entweder einen Beweis im Sequenzenkalkül und eine falsifizierende Interpretation an.

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

(b) $((P \to Q) \to P) \to P$

(c) $P \wedge \neg P \to Q$

(d) $(A \to A) \to A \to A$.

(e) $(A \to A \wedge B \wedge C) \vee (B \to A \wedge B \wedge C) \vee (C \to A \wedge B \wedge C)$

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

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

Zusatzaufgabe: Formalisieren Sie Ihre Beweise in PVS. (Keine Abgabe.)

Aufgabe 14. Eine Regel heißt *korrekt*, wenn aus der Gültigkeit aller ihrer Prämissen, die Gültigkeit ihrer Konklusion folgt. Eine Regel heißt *invertierbar*, wenn aus der Gültigkeit ihrer Konklusion, die Gültigkeit aller ihrer Prämissen folgt. **Hinweis:** Korrektheit und Invertierbarkeit sind die beiden Richtungen des Ableitungslemmas aus der Vorlesung.

(a) Zeigen Sie, dass die Regel ($\to$-L) korrekt und invertierbar ist.

(b) Die sogenannte Abschwächungsregel

$$\frac{\Gamma \Longrightarrow \Delta}{\Gamma, \Gamma' \Longrightarrow \Delta, \Delta'} \text{ (weakening)}$$

ist zwar korrekt aber nicht invertierbar. Begründen Sie diesen Sachverhalt.

(c) Geben Sie für beide Seiten einer Sequenz jeweils eine korrekte und invertierbare Regel für die Biimplikation $\leftrightarrow$ an. Als Vorlage können Ihnen folgende Sequenzen dienen.

$$\Gamma \Longrightarrow \Delta, \alpha \leftrightarrow \beta \qquad \Gamma, \alpha \leftrightarrow \beta \Longrightarrow \Delta$$

Die Prämissen sollen nur in den Symbolen $\Longrightarrow, \Gamma, \Delta, \alpha$ und β ausgedrückt werden. Weisen Sie *eine* Ihrer Regeln als korrekt und invertierbar nach.

Aufgabe 15. Finden Sie eine Familie von Formeln, $(\varphi_n)_{n\in\mathbb{N}}$, so dass

(a) die Wahrheitstafel von φ_n *mindestens* 2^n Zeilen hat (für alle $n \in \mathbb{N}$),

(b) es aber für alle $n \in \mathbb{N}$ einen Beweis im Sequenzenkalkül von φ_n gilt, so dass *höchstens* linear viele Regeln angewendet werden.

Wie interpretieren Sie diesen Sachverhalt?

Aufgabe 16. In dieser Aufgabe sollen Sie zeigen, dass ein Resolutionsbeweis effizient in einen Sequenzenbeweis umgewandelt werden kann, siehe Teilaufgabe (b) für $C = \emptyset$. Im Folgenden bezeichnen C und D Klauseln (als Menge notiert) und $\mathcal{K}$ eine Klauselmenge. Für eine Klausel C bezeichne C^+ die Menge der Variablen von C, die in C positiv auftreten, und C^- solche, die negativ in C vorkommen; also beispielsweise $\{A, \neg B, C\}^+ = \{A, C\}$ und $\{A, \neg B, C\}^- = \{B\}$. Die Größe von Resolutions- und Sequenzenbeweisen bezeichne die Anzahl der Regel- und Axiomanwendungen. Beweisen Sie folgende Aussagen ohne Rückgriff auf Korrektheit oder Vollständigkeit eines der beiden Kalküle.

(a) Für alle Klauseln $C \in \mathcal{K}$ hat $\{\bigvee_{\ell\in D} \ell \mid D \in \mathcal{K}\}, C^- \Longrightarrow C^+$ einen Sequenzenbeweis der Größe $\leq 3(|C| + 1)$.

(b) Falls es einen Resolutionsbeweis aus der Klauselmenge $\mathcal{K}$ einer Klausel C gibt, der s Resolutionsschritte braucht, so gibt es einen Sequenzenbeweis der Größe $3s \cdot \max\{|D|+1 \mid D \in \mathcal{K}\}$ von $\{\bigvee_{\ell\in D} \ell \mid D \in \mathcal{K}\}, C^- \Longrightarrow C^+$. Der konstruierte Sequenzenbeweis darf die Schnittregeln (`Cut`) und (`Cut`*) aus der Vorlesung enthalten.

Lösungsvorschlag. (a) Setze Γ als Abkürzung für $\{\bigvee_{\ell\in D} \ell \mid D \in \mathcal{K}\}$. Eigentlich möchten wir die Behauptung durch Induktion über $|C|$ zeigen. Jedoch verändern wir im Induktionschritt die entsprechende Menge Γ. Daher zeigen wir folgende Aussage, welche die Behauptung impliziert.

> Für alle $k \in \mathbb{N}$, alle (endlichen) Klauselmengen $\mathcal{K}$ und alle Klauseln $C \in \mathcal{K}$ mit $|C| = k$ gilt: Wenn es einen Resolutionsbeweis aus der Klauselmenge $\mathcal{K}$ einer Klausel C gibt, der s Resolutionsschritte braucht, so gibt es einen Sequenzenbeweis der Größe $3s \cdot \max\{|D| + 1 \mid D \in \mathcal{K}\}$ von $\Gamma, C^- \Longrightarrow C^+$.

Induktionsbasis $|C| = 0$. Zu finden ist eine Herleitung der Sequenz

$$\Gamma \Longrightarrow \emptyset$$

der Größe ≤ 3. Da in diesem Fall C die leere Klausel ist, befindet sich $\bot \in \Gamma$. Also reicht hier die Regel $(\bot_L)$.

Induktionsbasis $|C| = 1$, so besteht C entweder aus einem positiven oder einem negativen Vorkommen einer Variable X. Im ersten Szenario, müssen wir einen Beweis der Sequenz

$$\Gamma \Longrightarrow X$$

der Größe ≤ 6 finden. Da X bereits in Γ enthalten ist, reicht hier das Axiom (Ax). Im anderen Szenario genügt folgende Herleitung.

$$\dfrac{\dfrac{}{\Gamma, X \Longrightarrow X}\,(Ax)}{\underbrace{\Gamma}_{\neg X\in}, X \Longrightarrow \emptyset}\,(\neg_L)$$

In beiden Szenarien reichen also zwei Schritte aus.

Induktionsschritt $|C| \geq 2$**.** Also lässt sich C als $\{c\} \dot\cup \widetilde{C}$ schreiben, wobei c das erste Literal in C ist in der für die Definition von $\bigvee$ maßgeblichen Ordnung. Mit der Abkürzung $\widetilde{\Gamma} := \left\{\bigvee_{\ell\in D} \ell \mid D \in \mathcal{K} \setminus \{C\}\right\}$ und der Induktionhypothese für $|\widetilde{C}| < |C|$ und $\widetilde{\Gamma} \cup \{\bigvee_{\ell\in\widetilde{C}} \ell\}$ erhalten wir die folgende Herleitung[1].

$$\dfrac{\begin{array}{cc}\vdots \text{ wie Fall “}|C|=1\text{”} & \vdots \text{ Ind.hyp.}\\ \widetilde{\Gamma}, c,\ \{c\}^- \Longrightarrow \{c\}^+ & \widetilde{\Gamma}, \bigvee_{\ell\in\widetilde{C}} \ell,\ \widetilde{C}^- \Longrightarrow \widetilde{C}^+\end{array}}{\underbrace{\widetilde{\Gamma}, \underbrace{c \vee \bigvee_{\ell\in\widetilde{C}} \ell}_{=\bigvee_{\ell\in C}},\ \underbrace{\{c\}^-, \widetilde{C}^-}_{=C^-} \Longrightarrow \underbrace{\{c\}^+, \widetilde{C}^+}_{=C^+}}_{=\Gamma}}\,(\vee_L)$$

Also hat die Herleitung die Länge $\leq 1 + 2 + 3(|\widetilde{C}| + 1) \leq 3(|C| + 1)$.

Bemerkung: Die Verrenkung mit den zwei Basisfällen $|C| = 0$ und $|C| = 1$ rührt von der Sonderrolle von $\bot$ in der Definition von $\bigvee D$ her. Würde $\bot$ immer vorkommen, also z.B. $\bigvee\{A, B, C\} = A \vee (B \vee (C \vee \bot))$, bräuchte man nur einen Basisfall, nämlich $|C| = 0$, betrachten und der andere Basisfall würde im Schrittfall aufgehen.

(b) Zur Abkürzung seien $m := 3 \cdot \max\{|D| + 1 \mid D \in \mathcal{K}\}$ und $\Gamma := \left\{\bigvee_{\ell\in D} \ell \mid D \in \mathcal{K}\right\}$. Wir beweisen die Behauptung durch Induktion über den Resolutionsbaum.

Induktionbasis. Es liegt also ein Blatt mit der Beschriftung $C \in \mathcal{K}$ vor. Laut Aufgabenteil (a) gibt es die gewünschte Herleitung in der Größe $\leq 3(|C| + 1) \leq s$, da $C \in \mathcal{K}$.

Induktionsschritt. O.B.d.A. sind wir in der Situation

$$\dfrac{\begin{array}{cc}\vdots & \vdots\\ C_1 & C_2\end{array}}{C_1 \setminus \{X\} \ \cup\ C_2 \setminus \{\neg X\}}$$

mit $X \in C_1$ und $\neg X \in C_2$. Die Größe des linken bzw. rechten Teilbaums seien s_1 bzw. s_2. Insbesondere ist $s = 1 + s_1 + s_2$. Mit der Induktionhypothese für die beiden Teilbäume herhalten wir folgende Herleitung.

$$\dfrac{\begin{array}{cc}\vdots & \vdots\\ \Gamma, C_1^- \Longrightarrow C_1^+ & \Gamma, C_2^- \Longrightarrow C_2^+\end{array}}{\Gamma, C_1^-, C_2^- \setminus \{X\} \Longrightarrow C_1^+ \setminus \{X\}, C_2^+}\,(\texttt{Cut}^*)$$

weil $X \in C_1^+$ und $X \in C_2^-$. Die untere Sequenz ist in der Tat $\Gamma, C^- \Longrightarrow C^+$, da

$$(C_1 \setminus \{X\} \ \cup\ C_2 \setminus \{\neg X\})^+ = (C_1 \setminus \{X\})^+ \ \cup\ (C_2 \setminus \{\neg X\})^+ = C_1^+ \setminus \{X\} \ \cup\ C_2^+$$

und analog für den anderen Operator. Mit der Induktionshypothese können wir die Größe des Beweis abschätzen durch $\leq 1 \ +\ s_1 \cdot m \ +\ s_2 \cdot m \leq (1 + s_1 + s_2) \cdot m = s \cdot m$, da $m \geq 1$.

[1] Eigentlich ist dies nicht die Regel $(\vee_L)$ aus der Vorlesung, sonderen eine Version davon mit eingebautem Weakening. Jedoch lässt sich jedes Weakening zu den Blättern des Beweisbaumes verschieben, wo es von den Axiomen absorbiert wird. Bei dieser Transformation ändert sich die Anzahl der Regelanwendung nicht. Alternativ könnte man das Weakening auch gleich in die Aussage einbauen, über die wir den Induktionsbeweis führen: … so gibt es einen Sequenzenbeweis … von $\{\bigvee_{\ell\in D} \ell \mid D \in \mathcal{K}\}, C^-, \Phi \Longrightarrow C^+, \Psi$ *für beliebige (endliche) Formelmengen* Φ *und* Ψ.

Beispiel zu Aufgabe 16.
Die Klauselmenge $\mathcal{K} := \{\{\neg A, B, \neg E\}, \{\neg A, \neg B\}, \{A, B\}, \{A, \neg B\}, \{E\}\}$ hat folgenden Resolutionsbeweis (für ihre Unerfüllbarkeit).

$$\dfrac{\dfrac{\dfrac{\boxed{\neg A, B, \neg E}_{(I)} \qquad \boxed{\neg A, \neg B}_{(II)}}{\boxed{\neg A, \neg E}_{(III)}} \qquad \dfrac{A, B \qquad A, \neg B}{A}}{\neg E} \qquad E}{\emptyset}$$

Mit der Setzung $\Gamma := \{\bigvee_{\ell \in D} \ell \mid D \in \mathcal{K}\} = \{\neg A \vee (B \vee \neg E), \neg A \vee \neg B, A \vee B, A \vee \neg B, \neg E\}$ kann obiger Resolutionsbeweis in einen Sequenzenbeweis umgeformt werden, der auszugsweise wie folgt aussieht.

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma, A, E \Longrightarrow A, B} \quad \dfrac{}{\Gamma, B, A, E \Longrightarrow B} \quad \dfrac{}{\Gamma, A, E \Longrightarrow B, E}}{\Gamma, \neg A, A, E \Longrightarrow B} \quad \dfrac{}{\Gamma, \neg E, A, E \Longrightarrow B}}{\Gamma, B \vee \neg E, A, E \Longrightarrow B}}{\Gamma, \neg A \vee (B \vee \neg E), A, E \Longrightarrow B}_{(I)} \qquad \boxed{\begin{array}{c}\vdots \\ \Gamma, A, B \Longrightarrow \emptyset\end{array}}_{(II)}}{\boxed{\Gamma, A, E \Longrightarrow \emptyset}_{(III)}}$$

$$\vdots$$

In der Sequenz $\Gamma, \neg A \vee (B \vee \neg E), \neg A, E \Longrightarrow B$ wurde $\neg A \vee (B \vee \neg E)$ nur deutlichkeitshalber nochmal explizit genannt. Die Formel liegt ja bereits in Γ.