Fachbereich Mathematik
Martin Otto
Achim Blumensath
Tobias Löw

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Sommersemester 2006
25. April 2006

Formale Grundlagen der Informatik II

Lösungshinweise zum ersten Übungsblatt

Hausübungen

Abgabe in der Vorlesung am 23. Mai 2006

(H 1)

Sei $n \in \mathbb{N}$. Konstruieren Sie induktiv über n aussagenlogische Formeln

$$\varphi_n(x_0, \ldots, x_n, y_0, \ldots, y_n, z_0, \ldots, z_n, z_{n+1}),$$

welche genau dann wahr sind, wenn die Summe der in $\bar{x}$ und $\bar{y}$ kodierten Binärzahlen gleich $\bar{z}$ ist.
($\bar{x}$ kodiert die Zahl $\sum_i x_i 2^i$.)

Lösung:

Falls $n = 0$, dann definieren wir

$$\varphi_0 = ((x_0 \leftrightarrow y_0) \leftrightarrow \neg z_0) \wedge ((x_0 \wedge y_0) \leftrightarrow z_1).$$

Man prüft leicht nach, dass genau die Tupel $(0,0,0,0)$, $(1,0,1,0)$, $(0,1,1,0)$ und $(1,1,0,1)$ die Formel φ_0 erfüllen.
Im Induktionsschritt setzen wir ($\varphi_n[z_{n+1} := 0]$ sei die Formel φ_n bei der jedes Vorkommen von z_{n+1} durch 0 ersetzt wurde. Analog für $\varphi_n[z_{n+1} := 1]$.)

$$\begin{aligned}\varphi_{n+1} = &(\varphi_n \wedge (x_{n+1} \leftrightarrow y_{n+1}) \wedge (x_{n+1} \leftrightarrow z_{n+2})) \vee \\ &(\neg\varphi_n \wedge \varphi_n[z_{n+1} := 0] \wedge \neg(x_{n+1} \leftrightarrow y_{n+1}) \wedge \neg z_{n+2}) \vee \\ &(\neg\varphi_n \wedge \varphi_n[z_{n+1} := 1] \wedge \neg(x_{n+1} \leftrightarrow y_{n+1}) \wedge z_{n+2})\end{aligned}$$

wobei die erste Zeile den Fall behandelt, dass $x_0, \ldots, x_n, y_0, \ldots, y_n, z_0, \ldots, z_n, z_{n+1}$ korrekt aufsummiert sind und demnach x_{n+1}, y_{n+1} und z_{n+2} alle 0 oder alle 1 sein müssen, die zweite Zeile den Fall behandelt, in dem z_{n+1} gesetzt ist, obwohl kein Überlauf an der n-ten Stelle entsteht. Dann muss entweder x_{n+1} oder y_{n+1} gleich 1 und z_{n+2} muss 0 sein. Die dritte Zeile behandelt den Fall , in dem z_{n+1} nicht gesetzt ist, obwohl ein Überlauf an der n-ten Stelle entsteht. Dann muss entweder x_{n+1} oder y_{n+1} gleich 1 und z_{n+2} muss 1 sein.

(H 2)

Wir definieren folgende partielle Ordnung auf aussagenlogischen $\mathcal{V}_n$-Interpretationen:

$$\mathfrak{I} \leq \mathfrak{I}' \quad \text{:gdw.} \quad \mathfrak{I}(p) \leq \mathfrak{I}'(p) \quad \text{für alle Variablen } p \in \mathcal{V}_n$$

Eine AL_n-Formel φ heißt *monoton*, wenn für alle Interpretationen $\mathfrak{I} \leq \mathfrak{I}'$ gilt:

$$\varphi^{\mathfrak{I}} \leq \varphi^{\mathfrak{I}'}.$$

Beweisen Sie per Induktion über den Formelaufbau, dass jede aussagenlogische Formel φ, in der kein Negationszeichen vorkommt, monoton ist.
Bemerkung: Jede monotone Formel ist äquivalent zu einer Formel ohne Negationszeichen.

Lösung:

Angenommen φ ist eine aussagenlogische Formel, in der kein Negationszeichen vorkommt und $\mathfrak{I}$, $\mathfrak{I}'$ sind Interpretationen mit $\mathfrak{I} \leq \mathfrak{I}'$. Wir beweisen mit Induktion, dass $\varphi^{\mathfrak{I}} \leq \varphi^{\mathfrak{I}'}$ gilt.

- $\varphi = 0$, $\varphi = 1$ sind klar.
- $\varphi = p \in \mathcal{V}_n$: weil $\mathfrak{I} \leq \mathfrak{I}'$ gilt $\mathfrak{I}(p) \leq \mathfrak{I}'(p)$, also $\varphi^{\mathfrak{I}} \leq \varphi^{\mathfrak{I}'}$.

- $\varphi = \neg\psi$ kann nicht sein, da in φ kein Negationszeichen vorkommt.
- $\varphi = \psi \wedge \chi$: nach I.V. gilt $\psi^{\mathfrak{I}} \leq \psi^{\mathfrak{I}'}$ und $\chi^{\mathfrak{I}} \leq \chi^{\mathfrak{I}'}$. Also gilt $\min(\psi^{\mathfrak{I}}, \chi^{\mathfrak{I}}) \leq \min(\psi^{\mathfrak{I}'}, \chi^{\mathfrak{I}'})$, und es folgt $(\psi \wedge \chi)^{\mathfrak{I}} \leq (\psi \wedge \chi)^{\mathfrak{I}'}$.
- $\varphi = \psi \vee \chi$: nach I.V. gilt $\psi^{\mathfrak{I}} \leq \psi^{\mathfrak{I}'}$ und $\chi^{\mathfrak{I}} \leq \chi^{\mathfrak{I}'}$. Also gilt $\max(\psi^{\mathfrak{I}}, \chi^{\mathfrak{I}}) \leq \max(\psi^{\mathfrak{I}'}, \chi^{\mathfrak{I}'})$, und es folgt $(\psi \vee \chi)^{\mathfrak{I}} \leq (\psi \vee \chi)^{\mathfrak{I}'}$.

(H 3)

(a) Überprüfen Sie mit Resolution, ob folgende AL-Formeln erfüllbar sind

(i) $(p \vee q \vee \neg s) \wedge (p \rightarrow r) \wedge \neg((r \wedge \neg s) \vee q) \wedge (r \leftrightarrow s)$

LÖSUNG:

Umformen in KNF: $(p \vee q \vee \neg s) \wedge (\neg p \vee r) \wedge (\neg r \vee s) \wedge \neg q \wedge (\neg r \vee s) \wedge (\neg s \vee r)$ und wir erhalten die Klauselmenge

$$\{\{p, q, \neg s\}, \{\neg p, r\}, \{\neg r, s\}, \{\neg q\}, \{\neg s, r\}\}$$

Aus Gründen der Übersichtlichkeit, lassen wir Klauseln, in denen sowohl ein Literal p als auch $\overline{p}$ vorkommt weg. Durch Resolution erhält man im ersten Schritt zusätzlich die Klauseln

$$\{q, \neg s, r\}, \{p, q, \neg r\}, \{p, \neg s\}, \{\neg p, s\}$$

im nächsten Schritt kommt noch die Klausel

$$\{q, \neg r, s\}, \{q, \neg p, r\}$$

und schließlich noch

$$\{q, \neg p, s\}$$

hinzu. Da keine neuen Klauseln mehr hinzukommen folgt, dass die Formel erfüllbar ist.

(ii) $(p \wedge q \wedge r) \leftrightarrow (p \vee q \vee r)$

LÖSUNG:

Umformen in KNF:

$$\begin{aligned}
(p \wedge q \wedge r) \leftrightarrow (p \vee q \vee r) &= (\neg(p \wedge q \wedge r) \vee (p \vee q \vee r)) \wedge (\neg(p \vee q \vee r) \vee (p \wedge q \wedge r)) \\
&= (\neg p \vee \neg q \vee \neg r \vee p \vee q \vee r) \wedge ((\neg p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r)) \\
&= (\neg p \wedge \neg q \wedge \neg r) \vee (p \wedge q \wedge r) \\
&= (\neg p \vee q) \wedge (\neg p \vee r) \wedge (\neg q \vee p) \wedge (\neg q \vee r) \wedge (\neg r \vee p) \wedge (\neg r \vee q)
\end{aligned}$$

und wir erhalten die Klauselmenge

$$\{\{\neg p, q\}, \{\neg p, r\}, \{\neg q, p\}, \{\neg q, r\}, \{\neg r, p\}, \{\neg r, q\}\}$$

Man sieht leicht, dass keine neuen Klauseln mehr hinzukommen. Also ist die Formel erfüllbar.

(b) Gegeben seien folgende AL-Formeln:

$$\begin{aligned}
\varphi &:= (p \vee \neg r) \vee \neg(\neg p \vee q) \\
\psi &:= q \wedge r \wedge (\neg p \rightarrow r)
\end{aligned}$$

Zeigen Sie mit Resolution, dass $p \wedge q$ ist eine Folgerung aus der Formelmenge $\{\varphi, \psi\}$.

LÖSUNG:

Wir müssen zeigen, dass die Formelmenge $\Box \in \text{Res}^*(\{\varphi, \psi, \neg(p \wedge q)\})$. Wir erhalten die KNF Formeln

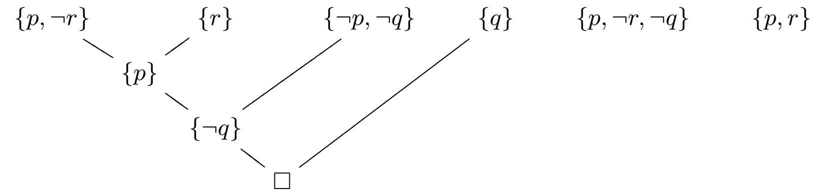
$$\varphi = (p \vee \neg r) \vee (p \wedge \neg q) = (p \vee \neg r) \wedge (p \vee \neg r \vee \neg q)$$

$$\begin{aligned}
\psi &= q \wedge r \wedge (p \vee r) \\
\neg(p \wedge q) &= \neg p \vee \neg q
\end{aligned}$$

und demnach die Klauselmenge

$$\{\{p, \neg r\}, \{p, \neg r, \neg q\}, \{q\}, \{r\}, \{p, r\}, \{\neg p, \neg q\}\}$$

und wir erhalten den Resolutionsbaum



Also gilt $\{\varphi, \psi\} \vDash p \wedge q$.

(H 4)

Gegeben sei die folgende Menge von nicht-negativen Hornklauseln:

$$M := \{\{\neg t, q\}, \{r\}, \{\neg r, t\}, \{p, \neg u, \neg s\}, \{\neg t, \neg q, r, \neg s\}, \{\neg r, \neg p, u\}, \{\neg t, s, \neg r, \neg q\}\}$$

(a) Bestimmen Sie eine minimale Belegung für M.

Lösung:

Wir erhalten nacheinander: $r \mapsto 1$, $t \mapsto 1$, $q \mapsto 1$, $s \mapsto 1$.
Die minimale Belegung ist also: $r \mapsto 1$, $t \mapsto 1$, $q \mapsto 1$, $s \mapsto 1$, $p \mapsto 0$, $u \mapsto 0$.

(b) Betrachten Sie nun folgende Mengen von negativen Hornklauseln:

$$N_1 := \{\{\neg p\}, \{\neg t, \neg u\}\}, \qquad N_2 := \{\{\neg u, \neg t, \neg s\}, \{\neg q, \neg u\}, \{\neg s, \neg r, \neg t\}\}\,.$$

Überprüfen Sie für $i \in \{1, 2\}$, ob die minimale Belegung aus (a) die Klauselmenge $M \cup N_i$ erfüllt.

Lösung:

Durch einfache Überprüfung erhält man, dass die minimale Belegung $M \cup N_1$, jedoch nicht $M \cup N_2$ erfüllt.

(H 5)

Zu gegebener unendlicher Folge $s := (a_i)_{i \in \mathbb{N}}$ von Zeichen aus einem Alphabet Σ bezeichnen wir für $i \in \mathbb{N}$ mit $s(i)$ das Wort $a_0 a_1 \dots a_{i-1} a_i$.

(a) Zeigen Sie, dass es zu jedem (endlichen) Alphabet Σ und unendlicher Sprache $L \subsetneq \Sigma^*$ eine unendliche Folge s von Zeichen gibt, sodass für unendlich viele $i \in \mathbb{N}$ das Wort $s(i)$ Präfix eines Wortes aus L ist.

Hinweis: Betrachten Sie die Sprache $\hat{L}$ aller Präfixe von Wörtern in L. Die Bedingung an s besagt, dass $s(i) \in \hat{L}$ für alle $i \in \mathbb{N}$.

Lösung:

Betrachten wir die Sprache $\hat{L}$. Man kann die Elemente von $\hat{L}$ bezüglich der Präfix-Ordnung in einem Baum anordnen. Da das Alphabet endlich ist, ist der Baum an jedem Knoten endlich verzweigend. Ein unendlicher Baum, der nur endlich verzweigend ist, muss nach Königs-Lemma einen unendlichen Pfad besitzen. Die Elemente entlang dieses Pfades bilden gerade die gesuchte Folge $s(i)$.
Angenommen $s(i)$ wäre für nur endlich viele $i \in \mathbb{N}$ Präfix eines Wortes aus L, dann gäbe es ein größtes $i' \in \mathbb{N}$ mit dieser Eigenschaft, und es folgt $s(i) \notin \hat{L}$ für $i > i'$. Widerspruch.

(b) Gilt die Aussage in (a) auch, wenn man fordert, dass für unendlich viele $i \in \mathbb{N}$ das Wort $s(i)$ in L liegt (anstatt ein Präfix zu sein)?

Lösung:

Nein. Ein Gegenbeispiel ist die Sprach $L(a^*b)$. Damit $s(i) \in L$ gilt muss $a_i = b$ sein. Da alle Wörter in $L(a^*b)$ genau ein b enthalten, folgt $s(j) \notin L(a^*b)$ für $j \neq i$.

(H 6)

(a) Zeigen Sie, dass folgende Regeln korrekt sind.

(i) $\dfrac{\Gamma \vdash \emptyset}{\Gamma \vdash \varphi}$ (ex falso quodlibet) (ii) $\dfrac{\Gamma, \varphi \vee \psi \vdash \chi}{\Gamma, \varphi \vdash \chi}$

LÖSUNG:

Zu Regel (i): Angenommen $\Gamma \vdash \emptyset$ ist allgemeingültig. Dann gilt $\bigwedge \Gamma \vDash 0$, d. h. es gilt $(\bigwedge \Gamma)^{\mathfrak{I}} = 0$ für alle Interpretationen $\mathfrak{I}$. Also ist $(\bigwedge \Gamma)^{\mathfrak{I}} \leq \varphi^{\mathfrak{I}}$ für alle Interpretationen $\mathfrak{I}$, und es folgt, dass $\Gamma \vdash \varphi$ allgemeingültig ist.

Zu Regel (ii): Angenommen $\Gamma, \varphi \vee \psi \vdash \chi$ ist allgemeingültig und $\mathfrak{I}$ eine (beliebige) Interpretation. Dann gilt $(\bigwedge \Gamma) \wedge (\varphi \vee \psi) \vDash \chi$, d. h. es gilt $((\bigwedge \Gamma) \wedge (\varphi \vee \psi))^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$. Also ist $(\bigwedge \Gamma)^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$ oder $(\varphi \vee \psi)^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$.
Falls $(\bigwedge \Gamma)^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$, dann folgt sofort $\min((\bigwedge \Gamma)^{\mathfrak{I}}, \varphi^{\mathfrak{I}}) = ((\bigwedge \Gamma) \wedge \varphi)^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$. Falls $(\varphi \vee \psi)^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$, dann folgt wegen $(\varphi \vee \psi)^{\mathfrak{I}} = \max(\varphi^{\mathfrak{I}}, \psi^{\mathfrak{I}})$, dass $\varphi^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$, also $\min((\bigwedge \Gamma)^{\mathfrak{I}}, \varphi^{\mathfrak{I}}) = ((\bigwedge \Gamma) \wedge \varphi)^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$.
In beiden Fällen folgt $((\bigwedge \Gamma) \wedge \varphi)^{\mathfrak{I}} \leq \chi^{\mathfrak{I}}$, also ist $\Gamma, \varphi \vdash \chi$ allgemeingültig.

(b) Geben Sie ein Verfahren an, das eine $\mathcal{SK}$-Ableitung von $\Gamma \vdash \emptyset$ in eine $\mathcal{SK}$-Ableitung von $\Gamma \vdash \varphi$ transformiert.

LÖSUNG:

Wir müssen eine allgemeinere Aussage zeigen, nämlich: wie man aus einer $\mathcal{SK}$-Ableitung von $\Gamma \vdash \Delta$ eine $\mathcal{SK}$-Ableitung von $\Gamma \vdash \Delta \cup \{\varphi\}$ macht.
Dies zeigen wir mit Induktion: Angenommen wir haben eine $\mathcal{SK}$-Ableitung von $\Gamma \vdash \Delta$, falls die letzte Regel ein Axiom war, dann ersetzen wir Δ durch $\Delta \cup \{\varphi\}$ (und erhalten wieder ein Axiom), anderfalls ersetzen wir alle Δ durch $\Delta \cup \{\varphi\}$ und benutzen die Induktionshypothese.

(c) Geben Sie eine „direkte Simulation“ von Regel (ii) in $\mathcal{SK}^+$ an, d. h. geben Sie einen Ableitungsbaum in $\mathcal{SK}^+$ mit Wurzel $\Gamma, \varphi \vdash \chi$ an, dessen Blätter nur mit Axiomen oder $\Gamma, \varphi \vee \psi \vdash \chi$ beschriftet sind.

LÖSUNG:

$$\dfrac{\dfrac{\dfrac{}{\varphi \vdash \varphi, \psi}\,(\text{Ax})}{\varphi \vdash \varphi \vee \psi}\,(\vee\text{R}) \qquad \dfrac{\vdots}{\Gamma, \varphi \vee \psi \vdash \chi}}{\Gamma, \varphi \vdash \chi}\,(\text{modus ponens})$$

(d) Begründen Sie, warum Regel (ii) in $\mathcal{SK}$ nicht direkt simulierbar ist. D. h. zeigen Sie, dass es keinen $\mathcal{SK}$ Ableitungsbaum mit Wurzel $\Gamma, \varphi \vdash \chi$ gibt, dessen Blätter nur mit Axiomen oder $\Gamma, \varphi \vee \psi \vdash \chi$ beschriftet sind.

Hinweis: Betrachten Sie hierfür die Länge der Formeln von Prämisse und Konklusion der $\mathcal{SK}$ Regeln.

LÖSUNG:

In $\mathcal{SK}$-Ableitungen kommen alle Formeln, die in einer Regel oben stehen im unteren Teil als ganzes oder Teilformel vor, demzufolge kann Regel (ii) (da wir nicht wissen, wie Γ, φ, ψ und χ aussehen) nicht herleitbar sein.