Aussagenlogik
& Prädikatenlogik (FGdI II)
3. Übungsblatt

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Dr. Martin Otto
Felix Canavoi, Kord Eickmeyer

SoSe 2016
11. Mai 2016

Gruppenübung

Aufgabe G3.1 (Resolutionsverfahren)
Seien φ und ψ AL-Formeln in KNF. Wie kann man das Resolutionsverfahren benutzen, um zu überprüfen, ob

(a) φ unerfüllbar ist;
(b) φ erfüllbar ist;
(c) φ allgemeingültig ist;
(d) φ nicht allgemeingültig ist;
(e) $\varphi \models \psi$;
(f) eine endliche Menge Φ von AL-Formeln unerfüllbar ist;
(g) eine unendliche Menge Φ von AL-Formeln unerfüllbar ist?

Aufgabe G3.2 (Sequenzenkalkül)

(a) Leiten Sie die folgende Sequenz in $\mathcal{SK}$ ab:

$$\vdash ((\varphi \to \psi) \to \varphi) \to \varphi$$

(b) Zeigen Sie **semantisch**, d.h. indem Sie über Modelle argumentieren, dass die folgenden Sequenzenregeln für AL-Formeln φ, ψ korrekt sind:

$$\text{(i)} \quad \frac{\vdash \varphi \lor \psi}{\neg\psi \vdash \varphi} \qquad\qquad \text{(ii)} \quad \frac{\neg\varphi \vdash \neg\psi}{\psi \vdash \varphi}$$

Extra: Lässt sich die Regel (ii) in $\mathcal{SK}$ oder $\mathcal{SK}^+$ ableiten? *Hinweis:* Aufgabe 6.10 im Skript.

Aufgabe G3.3 (Berechnungen in Aussagenlogik modellieren)
Wir wollen in dieser Aufgabe Berechnungsmodelle mit aussagenlogischen Formeln modellieren. Dabei sei Σ ein endliches Alphabet.

(a) Sei $\mathcal{A} = (\Sigma, Q, q_0, \Delta, A)$ ein nichtdeterministischer endlicher Automat (NFA) und $w \in \Sigma^*$ ein Wort der Länge ℓ. Wir definieren eine Menge aussagenlogischer Variablen

$$\mathcal{V}_Q := \{p_{q,i} : q \in Q, i \geq 0\}.$$

Wir wollen einen Lauf

$$q_0 = q^{(0)} \to q^{(1)} \to q^{(2)} \to \cdots \to q^{(\ell)}$$

des Automaten $\mathcal{A}$ auf dem Wort w durch eine Interpretation $\mathfrak{I} : \mathcal{V}_Q \to \mathbb{B}$ kodieren, indem wir

$$\mathfrak{I}(p_{q,i}) = 1 \quad \Leftrightarrow \quad q^{(i)} = q$$

setzen. Geben Sie eine Formel $\varphi_{\mathcal{A},w} \in \mathrm{AL}(\mathcal{V}_Q)$ an, für die gilt:

$$\mathfrak{I} \models \varphi_{\mathcal{A},w} \quad \Leftrightarrow \quad \mathfrak{I} \text{ kodiert einen akzeptierenden Lauf von } \mathcal{A} \text{ auf } w.$$

Insbesondere gilt dann

$$\varphi_{\mathcal{A},w} \text{ erfüllbar} \quad \Leftrightarrow \quad \mathcal{A} \text{ akzeptiert } w$$

(b) Sei jetzt $\mathcal{M} = (\Sigma, Q, q_0, \delta, q^+, q^-)$ eine Turingmaschine. Wir wollen eine Formelmenge $\Phi_\mathcal{M}$ definieren, für die gilt:

$$\Phi_\mathcal{M} \text{ erfüllbar} \quad \Leftrightarrow \quad \square \xrightarrow{\mathcal{M}} \infty.$$

Die Menge $\Phi_\mathcal{M}$ soll also genau dann erfüllbar sein, wenn $\mathcal{M}$ auf dem leeren Band gestartet *nicht* hält. Außerdem soll die Menge $\Phi_\mathcal{M}$ aus einer geeigneten Kodierung der Turingmaschine $\mathcal{M}$ berechnet werden können (sonst könnten wir immer $\Phi_\mathcal{M} = \{\bot\}$ für oder $\Phi_\mathcal{M} = \{\top\}$ wählen, je nachdem, ob $\square \xrightarrow{\mathcal{M}}$ STOP oder nicht).
Anleitung: Wählen Sie als Variablenmenge

$$\mathcal{V}_\mathcal{M} := \{p_{a,t,i} : a \in \Sigma, t \geq 0, i \in \mathbb{Z}\} \cup \{h_{t,i,q} : t \geq 0, i \in \mathbb{Z}, q \in Q\}$$

mit folgender intendierter Bedeutung:

$\mathfrak{I}(p_{a,t,i}) = 1 \Leftrightarrow$ in der i-ten Bandzelle steht nach t Schritten der Buchstabe a
$\mathfrak{I}(h_{t,i,q}) = 1 \Leftrightarrow$ nach t Schritten steht der Lesekopf auf der i-ten Bandzelle und die Maschine ist im Zustand q.

Dass das Band am Anfang der Berechnung leer ist, wird dann z.B. durch die Formelmenge

$$\{\neg p_{a,0,i} : a \in \Sigma, i \in \mathbb{Z}\}$$

ausgedrückt.

Diskutieren Sie: Ist das Erfüllbarkeitsproblem auch für unendliche Mengen von AL-Formeln algorithmisch loesbar? Was bedeutet das überhaupt? Ist, genauer, das Erfüllbarkeitsproblem für (unendliche) berechenbare bzw. entscheidbare Mengen von AL-Formeln entscheidbar oder aber rekursiv aufzählbar? Kann es eine (aus einer Kodierung von $\mathcal{M}$ berechenbare) Formelmenge $\Psi_\mathcal{M}$ geben, für die

$$\Psi_\mathcal{M} \text{ erfüllbar} \quad \Leftrightarrow \quad \square \xrightarrow{\mathcal{M}} \text{STOP}$$

gilt?

Hausübung

Hinweise zur Hausübung

Bitte geben Sie Ihre Lösungen zu dieser Hausübung in der **Übung am 01.06.2016** ab (**Name, Nummer der Übungsgruppe und Matrikelnummer** nicht vergessen). Wir unterstützen ausdrücklich das gemeinsame Arbeiten und Diskutieren in Gruppen, die gefundenen Lösungen sollte aber jeder selbst ausformulieren. Es darf also pro Abgabe nur ein Name auf dem Blatt stehen.

Aufgabe H3.1 (Resolution) (12 Punkte)

(a) Überprüfen Sie mit Hilfe der Resolutionsmethode, ob die folgende Formel unerfüllbar ist:

$$(q \lor s) \land (p \lor \neg s) \land (p \lor \neg q \lor r \lor s) \land (q \to (r \to s)) \land (r \lor s) \land ((p \land s) \to r) \land (\neg p \lor \neg r)$$

(b) Weisen Sie mit Hilfe der Resolutionsmethode die folgende Folgerungsbeziehung nach:

$$(p \lor \neg q \lor r) \land (\neg p \lor q \lor r) \models (\neg p \land q \land r) \lor (\neg p \land \neg q) \lor (\neg p \to 0)$$

(c) Bestimmen Sie das minimale Modell der folgenden Horn-Formelmenge:

$$H_0 = \{(p \land t) \to s, \quad r, \quad (q \land r) \to s, \quad t \to p, \quad t\}$$

Aufgabe H3.2 (Sequenzenkalkül) (12 Punkte)

(a) Finden Sie mittels Beweissuche im Sequenzenkalkül $\mathcal{SK}$ für folgende Formeln bzw. Sequenzen entweder eine Herleitung oder eine nicht-erfüllende Belegung.

i. $\vdash (p \land q) \lor \neg(q \lor r) \lor r \lor \neg p$

ii. $p, q \lor r \vdash (p \land q) \lor (p \land r)$

iii. $\vdash \neg(\neg(p \land q) \land r) \lor (q \land r)$

(b) Zeigen Sie semantisch, dass die folgenden Regeln korrekt sind.

i. $\dfrac{\Gamma, \varphi \vdash \Delta}{\Gamma \vdash \Delta, \neg\varphi}$

ii. $\dfrac{\Gamma \vdash \Delta, \varphi \qquad \Gamma, \psi \vdash \Delta}{\Gamma, \varphi \to \psi \vdash \Delta}$

Aufgabe H3.3 (Eigenschaften unendlicher Graphen) (12+3 Punkte)

Wir betrachten Graphen mit $\mathbb{N}$ als (unendlicher) Knotenmenge. Die Adjazenzmatrix eines solchen Graphen kodieren wir als Belegung der unendlichen Variablenmenge

$$\mathcal{V}_G := \{p_{ij} : 0 \leq i < j\},$$

wobei $\mathfrak{I}(p_{ij}) = 1$ für eine Interpretation $\mathfrak{I}$ gelten soll, falls in dem durch $\mathfrak{I}$ kodierten Graphen eine Kante zwischen den Knoten i und j existiert.

(a) Geben Sie zu endlichem Graphen G_0 mit Knotenmenge $V(G_0) \subset \mathbb{N}$ eine Formel $\varphi_{G_0} \in \mathrm{AL}(\mathcal{V}_G)$ an, für die gilt: $\mathfrak{I} \models \varphi_{G_0}$ genau dann, wenn $\mathfrak{I}$ einen Graphen G kodiert, dessen Kanten zwischen den Knoten in $V(G_0)$ genau mit denjenigen von G_0 übereinstimmen, d.h., dass für $u, v \in V(G_0)$ gilt: u ist mit v in G verbunden gdw. u mit v in G_0 verbunden ist. (D.h. G_0 ist Teilgraph von G.)

(b) Geben Sie eine Formelmenge $\Psi_1 \subseteq \mathrm{AL}(\mathcal{V}_G)$ an, für die gilt:

$$\mathfrak{I} \models \Psi_1 \quad \Leftrightarrow \quad \mathfrak{I} \text{ kodiert einen 3-färbbaren Graphen.}$$

Zeigen Sie, dass es keine Formelmenge $\Psi_2 \subseteq \mathrm{AL}(\mathcal{V}_G)$ gibt, für die gilt:

$$\mathfrak{I} \models \Psi_2 \quad \Leftrightarrow \quad \mathfrak{I} \text{ kodiert einen nicht 3-färbbaren Graphen.}$$

Hinweise: Erinnern Sie sich, dass

i. ein Graph 3-färbbar ist falls sich seine Knotenmenge V in drei Teilmengen (Farbklassen) zerlegen lässt, sodass keine Kante zwei Knoten innerhalb derselben Teilmenge (derselben Farbe) verbindet.
ii. ein Graph genau dann 3-färbbar ist, wenn jeder endliche Teilgraph 3-färbbar ist, d.h., wenn keiner der durch geeignete endliche Anfangsabschnitte von $\mathfrak{I}$ kodierten Teilgraphen ein Hindernis für die 3-Färbbarkeit darstellt (warum?).

Die Formelmenge Ψ_1 muss keine 3-Färbung eines Graphen in irgendeiner Form kodieren, sondern lediglich sicherstellen, dass kein Hindernis für die Existenz einer solchen Färbung besteht.

(c) Zwei Knoten $u, v \in V$ in einem Graph $G = (V, E)$ heißen *verbunden*, wenn $u = v$ oder es eine Folge von Knoten $u = v^{(0)}, v^{(1)}, \dots, v^{(\ell)} = v$ gibt, so dass $v^{(i-1)}v^{(i)} \in E$ für $i = 1, \dots, \ell$. Der Graph G heißt *zusammenhängend*, wenn alle Paare u, v von Knoten verbunden sind.
Zeigen Sie: Es gibt weder eine Menge $\Phi_1 \subseteq \mathrm{AL}(\mathcal{V}_G)$, für die gilt

$$\mathfrak{I} \models \Phi_1 \quad \Leftrightarrow \quad \mathfrak{I} \text{ kodiert einen zusammenhängenden Graphen}$$

noch eine Menge $\Phi_2 \subseteq \mathrm{AL}(\mathcal{V}_G)$, für die gilt

$$\mathfrak{I} \models \Phi_2 \quad \Leftrightarrow \quad \mathfrak{I} \text{ kodiert einen nicht zusammenhängenden Graphen.}$$

(d) *Bonus*: Seien $G_1 = (\mathbb{N}, E_1), \dots, G_k = (\mathbb{N}, E_k)$ Graphen mit Knotenmenge $\mathbb{N}$, also

$$E_i \subseteq \{\{u, v\} : u, v \in \mathbb{N} \text{ und } u \neq v\}.$$

Geben Sie eine Formelmenge $\Phi \subseteq \mathrm{AL}(\mathcal{V}_G)$ an, so dass

$$\mathfrak{I} \models \Phi \quad \Leftrightarrow \quad \mathfrak{I} \text{ kodiert einen der Graphen } G_1, \dots, G_k.$$