Formale Grundlagen der Informatik II
5. Übungsblatt

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Dr. Ulrich Kohlenbach
Alexander Kreuzer
Pavol Safarik

SS 2012

Gruppenübung

Aufgabe G1

(a) Zeigen Sie mit dem Resolutionskalkül, dass die folgenden Formelmengen unerfüllbar sind:

i. $\{\, (p \vee q) \to x, (x \vee y) \to z, p \vee q \vee y, \neg z \,\}$

ii. $\{\, \forall x \forall y (Rxy \to (Px \wedge \neg Py)), \forall x \forall y (Rxy \to \exists z (Rxz \wedge Rzy)), \forall x Rxfx \,\}$

iii. $\{\, \forall x \forall y \forall z (Rxy \vee Rxz \vee Ryz), \forall x \forall y \forall z ((Rxy \wedge Ryz) \to Rxz),$
$\forall x \forall y (Rxy \to Rfxfy), \forall x \neg Rxffx \,\}$

(b) Untersuchen Sie für jede der obigen Formelmengen, ob es auch echte Teilmengen gibt, die schon unerfüllbar sind.

Lösungsskizze:

(a) i. Klauseln: $\{\neg p, x\}, \{\neg q, x\}, \{\neg x, z\}, \{\neg y, z\}, \{p, q, y\}, \{\neg z\}$

$$\begin{tikzcd}
\{\neg z\} \arrow[dr] & \{\neg y, z\} \arrow[d] & \{\neg x, z\} \arrow[dr] & \{\neg z\} \arrow[d] & \\
\{p, q, y\} \arrow[dr] & \{\neg y\} \arrow[d] & \{\neg q, x\} \arrow[d] & \{\neg x\} \arrow[dl] \arrow[dd] & \{\neg p, x\} \arrow[ddl] \\
 & \{p, q\} \arrow[dr] & \{\neg q\} \arrow[d] & & \\
 & & \{p\} \arrow[d] & \{\neg p\} \arrow[dl] & \\
 & & \square & &
\end{tikzcd}$$

ii. Die zweite Formel hat folgende Skolemnormalform: $\forall x \forall y (Rxy \to Rxg(x,y) \wedge Rg(x,y)y)$
Klauseln: $\{\neg Rxy, Px\}, \{\neg Rxy, \neg Py\}, \{\neg Rxy, Rxg(x,y)\}, \{\neg Rxy, Rg(x,y)y\}, \{Rxfx\}$

$$\begin{tikzcd}
\{\neg Rxfx, \neg Pfx\} \arrow[dr] & \{Rxfx\} \arrow[d] & \{Rfxffx\} \arrow[d] & \{\neg Rfxffx, Pfx\} \arrow[dl] \\
 & \{\neg Pfx\} \arrow[d] & \{Pfx\} \arrow[dl] & \\
 & \square & &
\end{tikzcd}$$

iii. Klauseln: $\{Rxy, Rxz, Ryz\}$, $\{\neg Rxy, \neg Ryz, Rxz\}$, $\{\neg Rxy, Rfxfy\}$, $\{\neg Rxffx\}$

$$
\begin{tikzcd}
 & \{\neg Rxffx\} \arrow[dr] & \{\neg Rxfx, \neg Rfxffx, Rxffx\} \arrow[d] \\
\{\neg Rxfx, Rfxffx\} \arrow[dr] & & \{\neg Rxfx, \neg Rfxffx\} \arrow[dl] \\
\{Rxfx, Rxffx, Rfxffx\} \arrow[dr] & \{\neg Rxfx\} \arrow[d] \arrow[dr] & \\
 & \{Rxffx, Rfxffx\} \arrow[d] & \{\neg Rfxffx\} \arrow[dl] \\
\{\neg Rxffx\} \arrow[dr] & \{Rxffx\} \arrow[d] & \\
 & \square &
\end{tikzcd}
$$

Oder:

$$
\begin{tikzcd}
\{Rxfx, Rxffx, Rfxffx\} \arrow[dr] & \{\neg Rxffx\} \arrow[d] & \\
\{\neg Rxfx, Rfxffx\} \arrow[dr] & \{Rxfx, Rfxffx\} \arrow[d] & \\
 & \{Rfxffx\} \arrow[d] \arrow[dddr, bend left] & \\
\{\neg Rfxffx, \neg Rffxfffx, Rfxfffx\} \arrow[dr] & \{Rffxfffx\} \arrow[d] & \\
 & \{\neg Rfxffx, Rfxfffx\} \arrow[dr] & \\
 & \{\neg Rfxfffx\} \arrow[dr] & \{Rfxfffx\} \arrow[d] \\
 & & \square
\end{tikzcd}
$$

(b) Die Formelmengen in (i) und (iii) haben nur echte Teilmengen die erfüllbar sind (insbesondere ist $\{\, \forall x \forall y \forall z (Rxy \lor Rxz \lor Ryz), \forall x \forall y \forall z ((Rxy \land Ryz) \to Rxz), \forall x \neg Rxffx \,\}$ erfüllbar: wir nehmen z.B. die natürliche Zahlen als Trägermenge und interpretieren f als die Nachfolgerfunktion $f(x) = x + 1$ und R wie folgt:

$$(x, y) \in R \text{ gdw. } (x \in P \Leftrightarrow y \in P),$$

wobei $P = \{0, 1, 4, 5, 8, 9, \ldots\}$.)
In (ii) ist $\{\, \forall x \forall y (Rxy \to (Px \land \neg Py)), \forall x Rxfx \,\}$ schon unerfüllbar, wie wir oben gezeigt haben.

Aufgabe G2

Sei $G = (V, E)$ ein ungerichteter Graph (ohne Schleifen, d.h. es gibt keine Kante von einem Knoten zu sich selbst).

Wir nennen G 3-*färbbar*, wenn es eine Abbildung $f\colon V \to \{1, 2, 3\}$ gibt, so dass für jede Kante $(u, v) \in E$ gilt $f(u) \neq f(v)$.

(a) Erstellen Sie eine Formelmenge $\Phi(G)$, welche genau dann erfüllbar ist, wenn G 3-färbbar ist.

Hinweis: Führen Sie zu jedem Knoten $v \in V$ eine Konstante c_v ein und zu jeder Farbe $i \in \{1, 2, 3\}$ ein Prädikat P_i.

(b) Zeigen Sie mit Hilfe des Kompaktheitssatzes, dass ein Graph G genau dann 3-färbbar ist, wenn jeder endliche Teilgraph 3-färbbar ist. ($H = (V_0, E_0)$ ist ein Teilgraph von G, wenn $V_0 \subseteq V$ und $E_0 \subseteq E$ ist.)

Lösungsskizze:

(a) Wir führen zu jedem Knoten $v \in V$ eine Konstante c_v ein, zu jeder Farbe $i \in \{1, 2, 3\}$ ein Prädikat P_i und eine Kantenrelation E.

$$\begin{aligned}\Phi(G) \quad := \quad & \{\, \forall x\big((P_1x \vee P_2x \vee P_3x) \wedge \neg(P_1x \wedge P_2x) \wedge \neg(P_1x \wedge P_3x) \wedge \neg(P_2x \wedge P_3x)\big) \,\} \cup \\ & \{\, Ec_uc_v \mid (u, v) \in E \,\} \cup \{\, \neg c_u = c_v \mid u, v \in V, u \neq v \,\} \cup \\ & \{\, \forall xy\big(Exy \to \neg((P_1x \wedge P_1y) \vee (P_2x \wedge P_2y) \vee (P_3x \wedge P_3y))\big) \,\}\end{aligned}$$

(b) Eine Färbung $f : V \to \{1, 2, 3\}$ von G liefert Färbungen $f|_{V_0} : V_0 \to \{1, 2, 3\}$ jedes endlichen Teilgraphen (V_0, E_0) von G.

Umgekehrt nehmen wir an, dass jeder endliche Teilgraph 3-färbbar ist. Um zu zeigen, dass dann auch G 3-färbbar ist, reicht es nach (a), die Erfüllbarkeit von $\Phi(G)$ nachzuweisen. Dazu benutzen wir den Kompaktheitssatz. Sei $\Phi_0 \subseteq \Phi(G)$ eine endliche Teilmenge. Sei $V_0 \subseteq V$ die Menge der Knoten von G, die in Φ_0 erwähnt werden. Dann ist V_0 endlich und $\Phi_0 \subseteq \Phi(H)$, wobei $H := (V_0, E_0)$ der Teilgraph von G ist mit $E_0 := E \cap (V \times V)$. Nach Annahme ist H 3-färbbar. Also ist $\Phi(H)$ und damit auch Φ_0 erfüllbar. Wir haben gezeigt, dass jede endliche Teilmenge von $\Phi(G)$ erfüllbar ist. Nach dem Kompaktheitssatz ist deshalb auch $\Phi(G)$ erfüllbar.

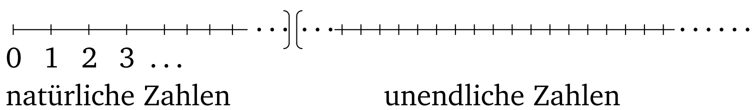
Aufgabe G3

Sei $L = \{+, \cdot, <, 0, 1\}$ die Sprache der Arithmetik und und $\mathcal{N} = (\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, <^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}})$ das Modell der natürlichen Zahlen. Dieses Modell wird auch *Standardmodell* genannt. Weiterhin sei

$$T = Th(\mathcal{N})$$

die Menge der Formeln in der Sprache L, die wahr sind in $\mathcal{N}$. Wie in der Vorlesung besprochen (siehe Skript 4.3) beschreibt T das Modell $\mathcal{N}$ nicht eindeutig, d.h. es gibt auch anderen Modelle von T. Solche Modelle werden *Nichtstandardmodelle* genannt.

Wir zeigen in dieser Aufgabe, dass jedes Nichtstandardmodell eine Kopie von $\mathcal{N}$ enthält. Wir zeigen weiter, dass jedes Element, das nicht zu $\mathcal{N}$ gehört, größer ist als jedes Element in $\mathcal{N}$, d.h. dass diese Zahlen „unendlich“ sind. Nichtstandardmodelle haben damit die Form:



Sei nun ${}^*\mathcal{N} = ({}^*\mathbb{N}, +^{{}^*\mathbb{N}}, \cdot^{{}^*\mathbb{N}}, <^{{}^*\mathbb{N}}, 0^{{}^*\mathbb{N}}, 1^{{}^*\mathbb{N}})$ ein Nichtstandardmodell. Betrachten Sie die Abbildung

$$^*(-) : \mathbb{N} \to {}^*\mathbb{N} : n \mapsto {}^*n = (\underbrace{1 + 1 + \ldots + 1}_{n-\mathrm{mal}})^{{}^*\mathbb{N}}.$$

(a) Zeigen Sie, dass diese Abbildung $^*(-)$ ein injektiver Homomorphismus ist, d.h. dass die Abbildung $0, 1$, die Operation $+, \cdot$ und die Ordnung $<$ erhält.
Das Bild von $^*(-)$ verhält sich also wie $\mathcal{N}$ und ist damit eine Kopie von $\mathcal{N}$ in ${}^*\mathcal{N}$.
Hinweis: Verwenden Sie hier und in den nächsten Teilaufgaben, dass alles, was wahr ist in $\mathcal{N}$ *und sich in der Logik 1. Stufe ausdrücken lässt,* auch wahr ist in ${}^*\mathcal{N}$ und umgekehrt.

(b) Zeigen Sie, dass alle Elemente, die nicht im Bild von $^*(-)$ liegen, größer als jedes ${}^*n$ (für $n \in \mathbb{N}$) sein müssen.
Diese Elemente von ${}^*\mathcal{N}$ sind die *unendlichen* Zahlen.

(c) Zeigen Sie, dass es für jedes unendliche Element x in ${}^*\mathbb{N}$ ein anderes unendliches Element y gibt, so dass $2y \leq x$.

Lösungsskizze:

(a) 0, 1 werden per Definition auf die gleichen Konstanten in ${}^*\mathcal{N}$ abgebildet.
Die Operation $+$ wird erhalten, weil

$${}^*m + {}^*n = {}^*k \iff {}^*\mathcal{N} \models {}^*m + {}^*n = {}^*k \iff \mathcal{N} \models m + n = k \iff m + n = k.$$

Analog zeigt man dies für $\cdot$ und $<$.
Der Homomorphismus ist injektiv, weil er $<$ erhält. (Aus $n \neq m$ folgt, dass $\mathcal{N} \models n < m \vee m < n$ und damit auch dass ${}^*\mathcal{N} \models n < m \vee m < n$, was das gleiche ist wie ${}^*n \neq {}^*m$.)

(b) $\mathcal{N} \models \forall x \forall y (x < y \;\vee\; y < x \;\vee\; x = y)$, also ist auch ${}^*\mathcal{N}$ eine lineare Ordnung. Neue Elemente sind deshalb entweder kleiner als 0, liegen zwischen ${}^*n$ und ${}^*(n+1)$ oder sind größer als alle ${}^*n$. Die ersten beiden Fälle sind unmöglich, da die Formeln $\neg\exists x(x \leq 0 \wedge \neg x = 0)$ und $\neg\exists x(n \leq x \wedge x \leq n + 1 \wedge \neg x = n \wedge \neg x = n + 1)$ in $\mathcal{N}$ wahr sind und deshalb auch in ${}^*\mathcal{N}$ wahr seien müssen.

(c) Die Formel $\forall x \exists y (y + y = x \vee (y + y) + 1 = x)$ ist wahr in $\mathcal{N}$, also muss sie auch wahr sein in ${}^*\mathcal{N}$. Also gibt es für jedes unendliche Element x ein Element y, so dass $y + y = x$ oder $(y + y) + 1 = x$. Dieses Element y muss unendlich sein, da sonst auch $y + y$ und $(y + y) + 1$ endlich wären.

Hausübung

Aufgabe H1 (6 Punkte)

Betrachten Sie die Signatur $S = (\leq)$. In dieser Aufgabe behandeln wir partielle Ordnungen. Zur Erinnerung: partielle Ordnungen sind S-Strukturen, die die folgenden Sätze erfüllen:

$$\forall x \forall y \; ((x \leq y \wedge y \leq x) \leftrightarrow x = y)$$
$$\forall x \forall y \forall z \; ((x \leq y \wedge y \leq z) \rightarrow x \leq z)$$

(a) Geben Sie für die folgenden partiellen Ordnungen $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3, \mathcal{A}_4$ Sätze $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ an, so dass für jedes $i \in \{1, 2, 3, 4\}$

$$\mathcal{A}_i \vDash \varphi_i \qquad \text{und für } j \neq i \qquad \mathcal{A}_j \nvDash \varphi_i.$$

D.h. mit den Sätzen φ_i können die Strukturen unterschieden werden.

i. $\mathcal{A}_1 = (\mathbb{N}, \leq^{\mathbb{N}})$
ii. $\mathcal{A}_2 = (\mathbb{Q}, \leq^{\mathbb{Q}})$

iii. $\mathcal{A}_3 = (\Sigma^*, \preccurlyeq)$ mit $\Sigma = \{a, b\}$, wobei $\preccurlyeq$ die Präfixrelation beschreibt, d.h. für die Wörter $e_0 e_1 \dots e_n \in \Sigma^*$ und $f_0 f_1 \dots f_m \in \Sigma^*$ gilt

$$e_0 e_1 \dots e_n \preccurlyeq f_0 f_1 \dots f_m,$$

falls $n \leq m$ und $e_i = f_i$ für alle $i \leq n$.

iv. $\mathcal{A}_4 = (\mathcal{P}(\mathbb{N}), \subseteq)$

(b) Geben Sie eine S-Struktur an, die *keine* partielle Ordnung ist.

Lösungsskizze:

(a) i. Es gibt ein kleinstes Element *und* alle Elemente sind vergleichbar:

$$\varphi_1 \equiv \exists x \forall y \forall z \, (x \leq y \wedge x \leq z \wedge [y \leq z \vee z \leq y])$$

ii. Für je zwei Elemente gibt es stets ein Drittes, welches zwischen diesen beiden liegt:

$$\varphi_2 \equiv \forall x \forall y \exists z \, ((\neg(x = y) \wedge x \leq y) \to [x \leq z \wedge z \leq y \wedge \neg(z = x) \wedge \neg(z = y)])$$

iii.

$$\varphi_3 \equiv \neg(\varphi_1 \wedge \varphi_2 \wedge \varphi_4)$$

iv. Für gibt ein größtes Element.

$$\varphi_4 \equiv \exists x \forall y (y \leq x)$$

(b) S-Struktur $\mathcal{S} = (\{a, b, c\}, \leq^{\mathcal{S}})$ mit der Interpretation $\leq^{\mathcal{S}} := \{(a, b), (b, c), (c, b)\}$.

Aufgabe H2 (Zusatzaufgabe†) (10 Punkte)

Betrachten Sie die folgende FO-Theorie $\mathcal{T}$ mit Gleichheit (Beispiele dieser Art gehen auf Statman, Orevkov, Pudlak oder Zhang zurück):

- Die Sprache $\mathcal{L}(\mathcal{T})$ beinhaltet die Konstanten 0 und 1, die Funktionssymbole $+$, $2^{(\cdot)}$ und ein einstelliges Predikat $I(\cdot)$.
- Die Theorie $\mathcal{T}$ beinhaltet die zusätzlichen Axiome $x + (y + z) = (x + y) + z$, $y + 0 = y$, $2^0 = 1$, $2^x + 2^x = 2^{1+x}$, $I(0)$, $I(x) \to I(1 + x)$. Man beachte, dass der $\forall$-Abschluss der Konjunktion dieser Axiome als ein Universeller Satz $\forall \underline{x} \; \varphi_{\text{qf}}(\underline{x})$, wobei φ_{qf} eine quantorenfreie Formel ist, geschrieben werden kann.

Im folgenden benutzen wir die abkürzende Schreibweise

$$2_0 := 0, \quad 2_{k+1} := 2^{2_k}.$$

(a) Zeigen Sie mit dem Satz von Herbrand für offene Theorien, dass es für jedes $k \in \mathbb{N}$ eine Herbrand-Disjunktion geben muss, so dass

$$\bigvee_{i=1}^{n} \big(\varphi_{\text{qf}}(\underline{t}_i) \to I(2_k)\big),$$

wobei $\underline{t}_i$ geschlossene Terme von $\mathcal{T}$ sind.

(b) Geben Sie einen kurzen (informellen) Beweis für $\exists \underline{x} \; \big(\varphi_{\text{qf}}(\underline{x}) \to I(2_k)\big)$ für jedes $k \in \mathbb{N}$.
Hinweis: Definieren Sie hierzu eine Relationen R_i mit $R_0 :\equiv I$ und $R_{i+1}(x) :\equiv \forall y \; \big(R_i(y) \to R_i(2^x + y)\big)$.
Man kann zeigen, dass es einen ($\mathcal{SK}$-)Beweis gibt der nur polynomiel in k viele Schritte benötigt.

(c) Zeigen Sie, dass jede Herbrand-Disjunktion von $\exists \underline{x} \; \big(\varphi_{\text{qf}}(\underline{x}) \to I(2_k)\big)$ mindestens die Länge 2_k hat.

†Punkte zählen für den Klausurbonus, aber nicht für die Bestimmung der Basis der 50% Schranke.