Formale Grundlagen der Informatik II
7. Übungsblatt

Fachbereich Mathematik
Prof. Dr. Martin Ziegler
Alexander Kreuzer
Carsten Rösnick

SS 2011
13.07.11

Gruppenübung

Aufgabe G1

Leiten Sie die folgenden Sequenzen her:

(a) $\forall x Rx\, fx \vdash \exists x Rfx\, ffx$.

(b) $\exists y \forall x Rxy \vdash \forall x \exists y Rxy$.

(c) $\forall x(\varphi \vee \psi) \vdash \forall x \varphi \vee \psi$, vorausgesetzt, dass $x \notin \text{frei}(\psi)$.

(d) $\forall x(Px \to Pfx) \vdash \forall x(Px \to Pffx)$.

Aufgabe G2

Sei $S = (+, \cdot, 2^x, <, 0, 1)$ die Signatur der Arithmetik mit Exponentation. In dieser Aufgabe bezeichnet $\mathcal{N}$ das Modell der natürliche Zahlen mit Exponentation über S, also $\mathcal{N} = (\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, (2^x)^{\mathbb{N}}, <^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}})$.

(a) Zeigen Sie, dass für einen quantorfreien Satz $\varphi[u]$ (mit Parameter u) entscheidbar ist, ob $\mathbb{N} \vDash \varphi[u]$, d.h. dass die Funktion

$$\chi(n) := \begin{cases} 0 & \text{falls } \mathcal{N} \nvDash \varphi[\underbrace{1 + 1 + \cdots + 1}_{n\text{-mal}}] \\ 1 & \text{falls } \mathcal{N} \vDash \varphi[\underbrace{1 + 1 + \cdots + 1}_{n\text{-mal}}] \end{cases}$$

berechenbar ist.

Bemerken Sie, dass diese Ergebnis auf für Erweiterungen

$$\mathcal{N}(f_1, f_2, \dots) = (\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, (2^x)^{\mathbb{N}}, <^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}}, f_1, f_2, \dots)$$

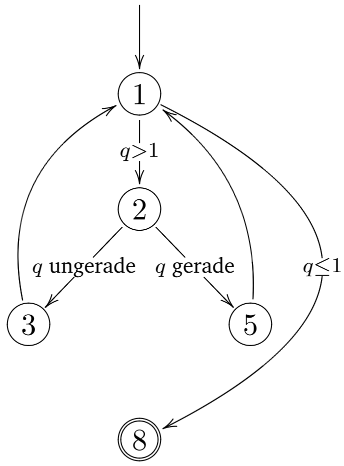
über der Signatur $S \cup (f_1, f_2, \dots)$ gilt, wenn die Funktionen $f_1, f_2, \dots$ berechenbar sind.

Hinweis: Betrachten Sie zuerst atomare Formeln.

Wir modellieren nun in $\mathcal{N}$ den Ablauf von Programmen.

Betrachten Sie das folgend Programm und den dazugehörigen Control-Flow-Graphen

Require: $q \in \mathbb{N}$
1: **while** $q > 1$ **do**
2: **if** q ungerade **then**
3: $q \leftarrow 3 \cdot q + 1$
4: **else**
5: $q \leftarrow q \div 2$
6: **end if**
7: **end while**
8: **return**

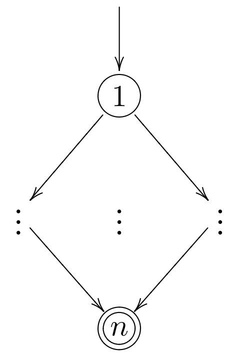


Man kann nun den Lauf des Programms bei der Eingabe von q durch zwei Funktionen $f(q,n)$, $g(q,n)$ kodieren, wobei $f(q,n)$ das Statment (i.e. in diesem Fall die Programmzeile), bei dem das Programm nach n Schritten bei der Eingabe q ist, beschreibt und $g(q,n)$ den Wert der Variable q zu diesem Zeitpunkt. Falls das Programm bei Eingabe q hält, dann beschreibt $f(q,\cdot)$ einen Pfad von 1 nach 8 im Contorl-Flow-Graphen, wenn nicht dann einen unendliche Pfad, der bei 1 startet.

(b) Definieren Sie (durch simultane Rekursion) die Funktionen f, g für das oben gegebene Programm.

(c) Betrachten Sie nun ein beliebiges Programm (mit einer Variable q), das ein Control-Flow-Graphen der Form wie rechts angegeben hat und bei dem n der einzige Endzustand ist.
Geben Sie einen Sätze ψ_1, ψ_2 an so dass
- $\mathcal{N}(f,g) \models \psi_1$ genau dann wenn das Programm hält,
- $\mathcal{N}(f,g) \models \psi_2$ genau dann wenn das Programm lineare Laufzeit (in der Länger, d.h. Anzahl der Bits, der Eingabe) hat.

Folgern Sie, dass $\mathcal{N}(f_1,\dots) \models \varphi$ für f_i berechenbar im Allgemeinen nicht entscheidbar ist.



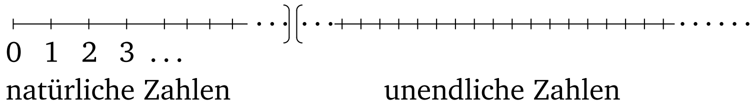
Aufgabe G3

Sei nun $S = \{+,\cdot,<,0,1\}$ die Signatur 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 $\mathrm{FO}(S)$-Sätze über der Signatur S, 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 dieser Kopie von $\mathcal{N}$ gehört, größer ist als jedes Element in dieser Kopie, 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

$$^*(-) : \mathbb{N} \to {}^*\mathbb{N} : n \mapsto {}^*n = \begin{cases} 0^{*\mathbb{N}} & \text{wenn } n = 0 \\ (\underbrace{1^{*\mathbb{N}} +^{*\mathbb{N}} 1^{*\mathbb{N}} +^{*\mathbb{N}} \ldots +^{*\mathbb{N}} 1^{*\mathbb{N}}}_{n-\mathrm{mal}}) & \text{sonst.} \end{cases}$$

(a) Zeigen Sie, dass diese Abbildung $^*(-)$ ein injektiver Homomorphismus ist, d.h. dass die Abbildung die Interpretationen der Konstanten $0, 1$ in $\mathcal{N}$ auf die entsprechenden Interpretationen in ${}^*\mathcal{N}$ abbildet, und dass die Operationen $+, \cdot$ und die Ordnung $<$ erhalten werden.

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 in $\mathcal{N}$ wahr ist *und sich durch einen Satz in der Logik 1. Stufe ausdrücken lässt*, auch in ${}^*\mathcal{N}$ wahr ist 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 unendliches Element x in ${}^*\mathbb{N}$ ein anderes unendliches Element y gibt, so dass $2y \leq x$.

Hausübung

Aufgabe H1 (Nim-Spiel)

Betrachten Sie das folgende Spiel: Gegeben seien zwei Spieler, w und s, sowie h Streichhölzer. Beide Spieler nehmen abwechselnd mindestens ein, maximal aber drei Streichhölzer pro Zug. Der Spieler, der am Ende die letzten Streichhölzer nimmt, verliert.

(a) Überlegen Sie sich für $h = 4$ Streichhölzer alle möglichen Spielsituationen, und ob es eine Lösungsstrategie für den beginnenden Spieler (dies sei ohne Einschränkung w) gibt. Können Sie daraus für 5 Streichhölzer ableiten, ob w eine Gewinnstrategie besitzt?

Hinweis: Stellen Sie die Spielzüge durch ein Transitionssystem (FGdI I) dar.

(b) Geben Sie eine FO-Formel $\psi(h)$ an die beschreibt, ob Spieler w bei anfänglich h Streichhölzern eine Gewinnstrategie besitzt. (Sie können dafür eine geeignete Signatur wählen.)

(c) Geben Sie ein Prolog-Programm für $\psi(h)$ an und bestimmen Sie für $h = 1, \ldots, 20$ an, ob Spieler w eine Gewinnstrategie besitzt.

Aufgabe H2

(a) Welche der folgenden Mengen sind entscheidbar, welche sind rekursiv aufzählbar?

(i) $\mathrm{SAT(AL)} := \{\varphi \in \mathrm{AL} : \varphi$ erfüllbar$\}$

(ii) $\{(\varphi, \psi) \in \mathrm{AL} : \varphi \models \psi\}$

(iii) $\mathrm{SAT(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ erfüllbar$\}$

(iv) $\mathrm{VAL(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ allgemeingültig$\}$

(v) $\mathrm{UNSAT(FO)} := \{\varphi \in \mathrm{FO} : \varphi$ unerfüllbar$\}$

(b) Für eine Klasse L von FO-Sätzen gelte die folgende „Endliche-Modell-Eigenschaft“:
Jeder erfüllbare Satz $\varphi \in L$ hat ein endliches Modell.

Argumentieren Sie, dass Erfüllbarkeit für Sätze aus L entscheidbar ist.

Hinweis: Man erinnere sich, dass eine Menge entscheidbar ist, falls man die Menge selbst und auch ihr Komplement aufzählen kann (warum?). Diesen Sachverhalt kann man für $\mathrm{SAT}(L)$ und $L \setminus \mathrm{SAT}(L)$ ausnutzen.

(c) Zeigen Sie, dass Erfüllbarkeit für universell-pränexe FO-Sätze in einer Symbolmenge ohne Funktionssymbole (nur Relationen und Konstanten) entscheidbar ist.

Hinweis: Man überlege sich, zunächst für Sätze ohne Gleichheit, wie deren Herbrand-Modelle aussehen.