Formale Grundlagen der Informatik II
7. Übungsblatt

TECHNISCHE UNIVERSITÄT DARMSTADT

Fachbereich Mathematik
Prof. Dr. Martin Otto
Julian Bitterlich, Felix Canavoi, Kord Eickmeyer, Daniel Günzel

SoSe 2015
15. Juli 2015

Aufgabe G1 (Quiz)
Für die folgenden Mengen geben Sie jeweils an, ob sie

- entscheidbar,
- rekursiv aufzählbar, aber nicht entscheidbar,
- nicht rekursiv aufzählbar

sind.

(a) $\mathrm{SAT(AL)} := \{\varphi \in \mathrm{AL} \mid \varphi \text{ erfüllbar}\}$

(b) $\{(\varphi,\psi) \in \mathrm{AL} \times \mathrm{AL} \mid \varphi \models \psi\}$

(c) $\mathrm{SAT(FO)} := \{\varphi \in \mathrm{FO} \mid \varphi \text{ erfüllbar}\}$

(d) $\mathrm{VAL(FO)} := \{\varphi \in \mathrm{FO} \mid \varphi \text{ allgemeingültig}\}$

(e) $\overline{\mathrm{SAT(FO)}} := \{\varphi \in \mathrm{FO} \mid \varphi \text{ unerfüllbar}\}$

(f) $\mathrm{FINSAT(FO)} := \{\varphi \in \mathrm{FO} \mid \varphi \text{ hat ein endliches Modell}\}$

(g) $\mathrm{INF(FO)} := \{\varphi \in \mathrm{FO} \mid \varphi \text{ ist erfüllbar und hat nur unendliche Modelle}\}$

Lösung:

(a) SAT(AL) ist entscheidbar. *Begründung:* Zugehörigkeit zu dieser Menge kann man mit Wahrheitstafeln entscheiden.

(b) $\{(\varphi,\psi) \in \mathrm{AL} \times \mathrm{AL} \mid \varphi \models \psi\}$ ist entscheidbar. *Begründung:* Zugehörigkeit zu dieser Menge kann man mit Wahrheitstafeln entscheiden.

(c) SAT(FO) ist nicht semi-entscheidbar. *Begründung:* Diese Menge ist nicht entscheidbar (Satz von Church und Turing, S. 37 im Skript). $\overline{\mathrm{SAT(FO)}}$ besteht aus den Sätzen φ, die nicht erfüllbar sind, oder, anders gesagt, aus den Sätzen φ, für die $\neg\varphi$ allgemeingültig ist. Das Komplement von SAT(FO) ist also wegen des Vollständigkeitssatzes semi-entscheidbar. Da eine semi-entscheidbare Menge, deren Komplement auch semi-entscheidbar ist, entscheidbar ist, kann SAT(FO) also nicht semi-entscheidbar sein.

(d) VAL(FO) ist semi-entscheidbar, aber nicht entscheidbar. *Begründung:* Wegen des Vollständigkeitssatzes ist diese Menge semi-entscheidbar. Sie ist nicht entscheidbar, da eine Formel φ erfüllbar ist, genau dann wenn $\neg\varphi$ nicht allgemeingültig ist. Erfüllbarkeit ist für FO aber nicht entscheidbar.

(e) $\overline{\mathrm{SAT(FO)}}$ ist semi-entscheidbar, aber nicht entscheidbar. *Begründung:* Eine Formel φ ist unerfüllbar genau dann, wenn $\neg\varphi$ allgemeingültig ist, also ist diese Menge nach (d) semi-entscheidbar. Sie ist nach (c) nicht entscheidbar, da eine Formel unerfüllbar ist, genau dann wenn sie nicht erfüllbar ist.

(f) FINSAT(FO) ist semi-entscheidbar, aber nicht entscheidbar. *Begründung:* Diese Menge ist semi-entscheidbar. Mittels einer unbeschränkten, erschöpfenden Suche generiert man alle endlichen Strukturen (bis auf Isomorphie) und überprüft, ob diese Modelle von φ sind. Nach dem Satz von Traktenbrot (S. 37 im Skript) ist diese Menge aber nicht entscheidbar.

(g) INF(FO) ist nicht semi-entscheidbar. *Begründung:* Wäre diese Menge semi-entscheidbar, dann wäre auch $\mathrm{SAT(FO)} = \mathrm{FINSAT(FO)} \cup \mathrm{INF(FO)}$ semi-entscheidbar, im Widerspruch zu (c).

Aufgabe G2 (Graphen und FO)
Ein Pfad in einem Graphen $\mathcal{G} = (V, E)$ ist eine Sequenz $\langle x_0, x_1, \ldots, x_n \rangle$ von Knoten, so dass $(x_i, x_{i+1}) \in E$ für alle $i < n$. Der Graph heißt *zusammenhängend*, wenn es für alle Paare von Knoten (x, y) einen Pfad $\langle x_0, x_1, \ldots, x_n \rangle$ gibt, mit $x = x_0$ und $y = x_n$. Zeigen Sie, dass es keine FO-Formelmenge Γ in der Sprache der Graphen, d.h. in der Signatur $\{E\}$, gibt, sodass $\mathcal{G} \models \Gamma$ genau dann, wenn $\mathcal{G}$ zusammenhängend ist.

Lösung: Wir verwenden, dass man eine Formel $\varphi_n(x, y)$ definieren kann, die aussagt, dass es einen Pfad der Länge n von x nach y gibt:

$$\varphi_n(x, y) = \exists x_0, \ldots, x_n ((x_0 = x) \wedge (x_n = y) \wedge \bigwedge_{i<n} E x_i x_{i+1}).$$

Nehmen wir an, dass es eine Formelmenge Γ gibt in der Sprache der Graphen, sodass ein Graph $\mathcal{G}$ ein Modell von Γ ist genau dann, wenn $\mathcal{G}$ zusammenhängend ist. Wir erweitern die Signatur um zwei Konstanten c und d und betrachten die folgende Formelmenge in der erweiterten Sprache

$$\Gamma_\infty = \Gamma \cup \left\{ \neg\varphi_n(c, d) \;\middle|\; n \in \mathbb{N} \right\}.$$

Die Formelmenge Γ_∞ is unerfüllbar, da man in einem Modell $\mathcal{G}$ die Konstanten c und d nicht widerspruchsfrei interpretieren kann: einerseits soll der Knoten $d^{\mathcal{G}}$ von $c^{\mathcal{G}}$ aus erreichbar sein, da Γ erfüllt ist und der Graph $\mathcal{G}$ deshalb zusammenhängend sein muss; andererseits kann $d^{\mathcal{G}}$ nicht von $c^{\mathcal{G}}$ aus erreichbar sein: dann würde es einen Pfad von $c^{\mathcal{G}}$ nach $d^{\mathcal{G}}$ geben; dieser Pfad hat eine bestimmte Länge n, was unmöglich ist, da $\mathcal{G} \models \neg\varphi_n(c, d)$.
Also ist (nach Kompaktheitssatz) schon eine endliche Teilmenge von Γ_∞ unerfüllbar und insbesondere ist schon eine Teilmenge von der Form

$$\Gamma_n = \Gamma \cup \left\{ \neg\varphi_k(c, d) \;\middle|\; k < n \right\}$$

unerfüllbar (da jede endliche Teilmenge in einem Γ_n enthalten ist). Aber jedes Γ_n hat ein Modell, einen zusammehängenden Graphen $\mathcal{G}$, wobei es keinen Pfad der Länge kürzer als n von $c^{\mathcal{G}}$ nach $d^{\mathcal{G}}$ gibt. (Ein Modell könnte so aussehen:

$$0 \longleftrightarrow 1 \longleftrightarrow \ldots \longleftrightarrow n-1 \longleftrightarrow n$$

wobei wir c als der 0-Knoten und d als der n-Knoten interpretieren.)
Also haben wir einen Widerspruch und schließen, dass es keine Formelmenge Γ geben kann, die den Zusammenhang eines Graphen ausdrückt.

Aufgabe G3 (Nichtstandardmodelle)

(a) Zeigen Sie, dass es keine FO(S) Formelmenge Φ gibt, die ein unendliches Modell besitzt, und die Eigenschaft hat, dass in jedem Modell $\mathcal{A}$ von Φ alle Elemente durch veriablenfreie S-Terme ausgedrückt werden können, d.h., dass es für jedes a in der Trägermenge von $\mathcal{A}$ einen Term $t \in T_0(S)$ gibt, sodass $a = t^{\mathcal{A}}$.

(b) Sei $S = \{+, \cdot, <, 0, 1\}$ die Signatur der Arithmetik und $\mathcal{N} = (\mathbb{N}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, <^{\mathbb{N}}, 0^{\mathbb{N}}, 1^{\mathbb{N}})$ das Modell der natürlichen Zahlen. Folgern Sie aus (a) die Existenz eines Nichtstandardmodells $\mathcal{N}^*$ von $\mathcal{N}$ (vgl. Seite 21 im Skript).

Im folgenden sei $\mathcal{N}^* = (\mathbb{N}^*, +^*, \cdot^*, <^*, 0^*, 1^*)$ ein Nichtstandardmodell von $\mathcal{N}$ und $\underline{\cdot} \colon \mathbb{N} \to T_0(S)$ eine Kodierung von natürlichen Zahlen in S-terme induktiv definiert durch $\underline{0} = 0$ und $\underline{n+1} = \underline{n} + 1$.

(c) Zeigen, Sie dass die Abbildung $\widehat{\cdot} \colon \mathbb{N} \mapsto \mathbb{N}^*; n \mapsto \widehat{n} := \underline{n}^{\mathcal{N}^*}$ ein injektiver, nicht surjektiver Homomorphismus ist.

(d) Zeigen Sie, dass alle Elemente, die nicht in $\widehat{\mathbb{N}} := \{\widehat{n} \mid n \in \mathbb{N}\}$ liegen, größer als jedes Element in $\widehat{\mathbb{N}}$ sind.

(e) Zeigen Sie, dass es eine Teilmenge von $\mathbb{N}^*$ gibt, die kein kleinstes Element hat.

(f) Was zeigt ein Beweis von $\varphi(x) \in$ FO(S) durch vollständige Induktion, wenn x über die Elemente von $\mathbb{N}^*$ läuft?

(g) Extra: Folgern sie aus (b) und (c) die Aussage aus G2.
Hinweis: Nehmen Sie an, dass ein geeignetes Γ existiere. Substituieren Sie dann alle Atome der Form Exy in Γ durch $x = y + 1 \vee y = x + 1$. Dann wäre $\mathcal{N}$ ein Modell des resultierenden Γ', nicht aber $\mathcal{N}^*$.

Lösung:

(a) Nehmen wir an, dass es eine Formelmenge Φ gibt, die ein unendliches Modell besitzt und für alle Modelle $\mathcal{A}$ von Φ die Abbildung $t \mapsto t^{\mathcal{A}}$ von $T_0(S)$ in die Trägermenge von $\mathcal{A}$ surjektiv ist. Wir erweitern die Signatur S um eine Konstante c und betrachten die folgende Formelmenge in der erweiterten Signatur

$$\Phi_c = \Phi \cup \left\{ \neg c = t \;\middle|\; t \in T_0(S) \right\}$$

Die Formelmenge Φ_c ist unerfüllbar, da man in einem Modell $\mathcal{A}$ die Konstante c nicht widerspruchsfrei interpretieren kann: einerseits soll $c^{\mathcal{A}} = t^{\mathcal{A}}$ für ein $t \in T_0(S)$ sein, da Φ erfüllt ist; andererseits gilt $c^{\mathcal{A}} \neq t^{\mathcal{A}}$, für alle $t \in T_0(S)$.

Also ist (nach Kompaktheitssatz) schon eine endliche Teilmenge von Φ_c unerfüllbar und insbesondere ist eine Teilmenge der Form

$$\Phi_T = \Phi \cup \{\neg c = t \mid t \in T\}$$

für ein endliches $T \subseteq T_0(S)$ unerfüllbar (da jede endliche Teilmenge von Φ_c in einem geeigneten Φ_T enthalten ist). Aber jedes Φ_T hat ein Modell, nämlich ein unendliches Modell $\mathcal{A}$ von Φ erweitert zu einer Struktur $\mathcal{A}'$ in der Signatur $S \cup \{c\}$, sodass $c^{\mathcal{A}'}$ ein Element ungleich allen $(t^{\mathcal{A}})_{t\in T}$ ist (warum kann man c so interpretieren?).

Also haben wir einen Widerspruch und schließen, dass solch eine Formelmenge Φ nicht existiert.

(b) Wir betrachten $\mathrm{Th}(\mathcal{N}) := \{\varphi \in \mathrm{FO}_0(S) \mid \mathcal{N} \models \varphi\}$. Nach (a) gibt es aber ein Modell $\mathcal{N}^*$ von $\mathrm{Th}(\mathcal{N})$, sodass die Funktion $t \mapsto t^{\mathcal{N}^*}$ von $T_0(S)$ in die Trägermenge von $\mathcal{N}^*$ nicht surjektiv ist. Angenommen es gibt einen Isomorphismus f von $\mathcal{N}$ nach $\mathcal{N}^*$, dann ist die Komposition der surjektiven Funktionen $t \mapsto t^{\mathcal{N}}$ und f auch surjektiv aber diese ist gerade $t \mapsto t^{\mathcal{N}^*}$, da $f(t^{\mathcal{N}}) = t^{\mathcal{N}^*}$. Wir erhalten somit einen Widerspruch, demnach sind $\mathcal{N}^*$ und $\mathcal{N}$ nicht isomorph.

(c) Per Induktion zweigt man leicht, dass $\underline{n}^{\mathcal{N}} = n$. Nun zeigen wir, dass $\widehat{\cdot}$ die Konstanten respektiert. Da $\mathcal{N} \models 0 = \underline{0}$ gilt auch $\mathcal{N}^* \models 0 = \underline{0}$ und somit $0^* = \widehat{0}$. Genauso zeigt man, dass $1^* = \widehat{1}$.

Um die Erhaltung der Operationen und der Ordnung zu beweisen, benutzen wir, dass für alle Formeln $\phi(x_1, \dots, x_n)$ und $n_1, \dots, n_k \in \mathbb{N}$ (Definition von $\phi[\dots]$ wie im Skript Seite 10)

$$\mathcal{N} \models \phi[n_1, \dots, n_k] \text{ gdw. } \mathcal{N}^* \models \phi[\widehat{n}_1, \dots, \widehat{n}_k].$$

gilt, denn

$$\begin{aligned}\mathcal{N} \models \phi[n_1, \dots, n_k] \Leftrightarrow \mathcal{N} \models \phi[\underline{n_1}^{\mathcal{N}}, \dots, \underline{n_k}^{\mathcal{N}}] \Leftrightarrow \mathcal{N} \models \phi(\underline{n_1}, \dots, \underline{n_k}) \Leftrightarrow \\ \mathcal{N}^* \models \phi(\underline{n_1}, \dots, \underline{n_k}) \Leftrightarrow \mathcal{N}^* \models \phi[\underline{n_1}^{\mathcal{N}^*}, \dots, \underline{n_k}^{\mathcal{N}^*}] \Leftrightarrow \mathcal{N}^* \models \phi[\widehat{n}_1, \dots, \widehat{n}_k].\end{aligned}$$

Dass die Operation $+$ von $\widehat{\cdot}$ erhalten wird, zeigen wir durch Zuhilfenahme der Formel $\phi_+(x, y, z) := x + y = z$. Für natürliche Zahlen $n, m, k \in \mathbb{N}$ gilt nun

$$n +^{\mathbb{N}} m = k \Leftrightarrow \mathcal{N} \models \phi_+[n, m, k] \Leftrightarrow \mathcal{N}^* \models \phi_+[\widehat{n}, \widehat{m}, \widehat{k}] \Leftrightarrow \widehat{n} +^* \widehat{m} = \widehat{k}$$

und damit $\widehat{n} +^* \widehat{m} = \widehat{n +^{\mathbb{N}} m}$. Analog zeigt man dies für $\cdot$ und $<$.

Der Homomorphismus ist injektiv, weil für alle $n, m \in \mathbb{N}$ mit $\phi_{\neq} = \neg x = y$ gilt

$$n \neq m \iff \mathcal{N} \models \phi_{\neq}[n, m] \iff \mathcal{N}^* \models \phi_{\neq}[\widehat{n}, \widehat{m}] \iff \widehat{n} \neq \widehat{m}.$$

Der Homomorphismus ist nicht surjektiv, da er sonst ein Isomorphismus wäre.

(d) Sei $a \in \mathbb{N}^* \setminus \widehat{\mathbb{N}}$, dann gilt für jede natürliche Zahl $n \in \mathbb{N}$, dass $\widehat{n} = a, a <^* \widehat{n}$ oder $\widehat{n} <^* a$, da $<^*$ eine lineare Ordnung ist. Das erste kann nicht gelten, da a nicht im Bild von $\widehat{\cdot}$ liegt. Das Zweite ebenso nicht, da aus

$$\mathcal{N} \models \forall x \left(x < \underline{n} \longrightarrow \bigvee_{0 \le k < n} x = \underline{k} \right)$$

folgt, dass $a = \widehat{k}$ für ein $k < n$. Also ist $\widehat{n} < a$.

(e) Wir betrachten die Menge $M = \mathbb{N}^* \setminus \widehat{\mathbb{N}}$. Angenommen M hat ein kleinstes Element a. Dann kann a nicht 0^* sein, da $0^* = \widehat{0} \notin M$. Also gibt es ein $b \in \mathbb{N}^*$ mit $b \notin M$ und $a = b + 1$. Demnach ist also $b = \widehat{k}$ für ein geeignete Zahl $k \in \mathbb{N}$ und damit $a = \widehat{k + 1} \notin M$. Wir erhalten einen Widerspruch. Also hat M kein kleinstes Element.

(f) Ein Beweis von $\varphi(x)$ über vollständige Induktion zeigt die Aussage a priori nur für Elemente in $\widehat{N}$. Trotzdem gilt φ für alle $a \in \mathbb{N}^*$. Ist nämlich $n \in \mathbb{N}$, dann gilt $\mathcal{N}^* \models \varphi[\widehat{n}]$ und demnach $\mathcal{N} \models \varphi[n]$. Also gilt $\mathcal{N} \models \forall x\ \varphi(x)$ und damit wiederum $\mathcal{N} \models \forall x\, \varphi(x)$

(g) Wir zeigen zuerst, dass $\mathcal{N}$ ein Modell von Γ' ist. Dafür müssen wir zeigen, dass der Graph $(\mathbb{N}, E)$ mit der Kantenrelation $E = \{(a, b) \in \mathbb{N} \times \mathbb{N} \mid a = b + 1 \text{ oder } b = a + 1\}$ zusammenhängend ist. Sind $a, b \in \mathbb{N}$, wobei ohne Beschränkung der Allgemeinheit $b = a + k$ für eine Zahl $k \in \mathbb{N}$ gilt, dann ist $\langle a, a + 1, \ldots, a + (k - 1), a + k\rangle$ ein Pfad von a nach b.

Umgekehrt, ist $(\mathbb{N}^*, E^*)$ mit $E^* = \{(a, b) \in \mathbb{N}^* \times \mathbb{N}^* \mid a = b +^* 1 \text{ oder } b = a +^* 1\}$ nicht zusammenhängend. Dafür zeigen wir per Induktion, dass wenn 0^* einen Pfad nach a hat, dann ist $a \in \widehat{\mathbb{N}}$. Für Pfade der Länge 0 gilt die Aussage trivialer Weise. Angenommen $\langle x_0, \ldots, x_{n+1}\rangle$ ist ein Pfad der Länge $n + 1$ von 0 nach a. Dann ist nach Induktionsvoraussetzung $x_n = \widehat{k}$ für eine natürliche Zahl $k \in \mathbb{N}$. Es gilt nun $(x_n, x_{n+1}) \in E^*$, also $a = x_n +^* 1$ oder $x_n = a +^* 1$ damit gilt auch $a = \widehat{k+1}$ oder $a = \widehat{k-1}$. Damit gilt die Behauptung. Da $\mathbb{N}^* \setminus \widehat{\mathbb{N}}$ nicht-leer ist, ist 0^* nicht mit jedem Element in $\mathbb{N}^*$ verbunden.

Aufgabe G4

(a) Drücken Sie die folgenden "Tatsachen" durch Sätze der Logik erster Stufe in einer passenden Signatur aus:
   i. Ein Drache ist glücklich, wenn alle seine Kinder fliegen können.
   ii. Grüne Drachen können fliegen.
   iii. Ein Drache ist grün, wenn mindestens einer seiner Elterndrachen grün ist.
   iv. Alle grünen Drachen sind glücklich.

   Hinweis: Überlegen Sie sich u. a., was Sie in der Signatur benötigen, um "ist Kind von" ausdrücken zu können.

(b) Leiten sie argumentativ die vierte Aussage aus den ersten drei her.

(c) Zeigen Sie mittels des Resolutionsverfahrens, dass die vierte Aussage aus den ersten drei folgt.
   Hinweis: Beachten Sie, dass man auf eine Skolemfunktion geführt wird, die ggf. "nicht fliegende Kinder" liefert.

Lösung:

(a) Eine mögliche Signatur ist $S = (G, F, L, C)$, wobei G (green), F (can fly) und H (happy) einstellige Relationssymbole sind, und C (child of) ein zweistelliges Relationssymbol ist.
   Obige Aussagen entsprechen folgenden FO(S)-Sätzen:
   i. $\varphi_1 := \forall x(\forall y(Cyx \to Fy) \to Hx)$
   ii. $\varphi_2 := \forall x(Gx \to Fx)$
   iii. $\varphi_3 := \forall x(\exists y(Cxy \wedge Gy) \to Gx)$
   iv. $\varphi_4 := \forall x(Gx \to Hx)$

(b) Angenommen g ist ein grüner Drache, und c ist ein Kind von g. Dann ist c grün (wegen (iii)) und kann damit auch fliegen (wegen (ii)). Also können alle Kinder von g fliegen, also ist g (wegen (i)) glücklich.

(c) Wir wollen zeigen, dass die Satzmenge $\{\varphi_1, \varphi_2, \varphi_3, \neg\varphi_4\}$ unerfüllbar ist. Dazu bringen wir diese Sätze in Skolemnormalform:
   i. $\forall x(\forall y(Cyx \to Fy) \to Hx) \equiv \forall x \exists y((Cyx \to Fy) \to Hx)$
      Skolemnormalform: $\forall x((Cfxx \to Ffx) \to Hx)$.
   ii. Ist bereits in Skolemnormalform: $\forall x(Gx \to Fx)$
   iii. $\forall x(\exists y(Cxy \wedge Gy) \to Gx) \equiv \forall x \forall y((Cxy \wedge Gy) \to Gx)$
      Skolemnormalform: $\forall x \forall y((Cxy \wedge Gy) \to Gx)$.
   iv. $\neg\forall x(Gx \to Hx) \equiv \exists x(Gx \wedge \neg Hx)$
      Skolemnormalform: $Gc \wedge \neg Hc$.

   Es ergibt sich die folgende Klauselmenge:

$$\begin{array}{cl} \{Cfxx, Hx\}, \{\neg Ffx, Hx\} & \text{von (i)} \\ \{\neg Gx, Fx\} & \text{von (ii)} \\ \{\neg Cxy, \neg Gy, Gx\} & \text{von (iii)} \\ \{Gc\}, \{\neg Hc\} & \text{von (iv)} \end{array}$$

   Damit lässt sich zum Beispiel wie folgt die leer Klausel ableiten:

$$\begin{tikzcd}
\{Cfcc, Hc\} \arrow[dr] & \{\neg Hc\} \arrow[d] & & & \\
\{\neg Cfcc, \neg Gc, Gfc\} \arrow[dr] & \{Cfcc\} \arrow[d] & & \{\neg Ffc, Hc\} \arrow[d] & \{\neg Hc\} \arrow[dl] \\
\{Gc\} \arrow[dr] & \{\neg Gc, Gfc\} \arrow[d] & & \{\neg Ffc\} \arrow[d] & \{\neg Gfc, Ffc\} \arrow[dl] \\
& \{Gfc\} \arrow[dr] & & \{\neg Gfc\} \arrow[dl] & \\
& & \square & &
\end{tikzcd}$$