Übungsblatt 1

Aufgabe 1
Welche der folgenden Probleme sind entscheidbar, welche semi-entscheidbar?

(a) Ist eine prädiaktenlogische Formel F weder gültig noch unerfüllbar?

(b) Ist eine prädikatenlogische Formel F mit einem einstelligen Prädikatensymbol ohne Gleichheit und ohne Funktionssymbole erfüllbar?

(c) Ist eine prädikatenlogische Formel F in Pränexform ohne Allquantoren erfüllbar?

Lösung

(a) Dies ist nicht semi-entscheidbar. Nehmen wir an, es sei semi-entscheidbar, dass F nicht gültig, aber erfüllbar (d.h. nicht unerfüllbar) ist. Wir wissen bereits, dass die gültigen Formeln semi-entscheidbar sind. Man könnte nun folgendes Semi-Entscheidungsverfahren verwenden, um zu testen, ob eine Formel erfüllbar ist: Man testet parallel, ob sie gültig ist, und ob sie nicht gültig, aber erfüllbar ist. Divergiert der Algorithmus, so ist die Formel nicht gültig und nicht erfüllbar, d.h. nicht erfüllbar. Terminiert der Algorithmus, so ist die Formel gültig oder erfüllbar, d.h. erfüllbar. Wir wissen aber, dass es nicht semi-entscheidbar ist, ob eine Formel erfüllbar ist. Also kann es auch nicht semi-entscheidbar sein, ob eine Formel weder gültig noch unerfüllbar ist.

(b) Dies ist entscheidbar. Sei P einstellig und das einzige in F vorkommende Relationssymbol. Wir zeigen, dass wenn F erfüllbar ist, dann hat F auch ein Modell mit einem Universum der Größe höchstens zwei. Die Anzahl der Strukturen, die ausschließlich ein einstelliges Prädikatensymbol interpretieren und dessen Universen höchstens aus zwei Elementen bestehen sind (bis auf Isomorphie) endlich und damit lässt sich testen, welche von ihnen Modelle von F sind.

Um die Behauptung zu zeigen, nehmen wir zunächst an, dass F in *Negationsnormalform* ist, d.h. es gibt keine Negation in F außer in der Form $\neg P(x)$. Jede Formel besitzt eine zu ihr äquivalente Formel in Negationsnormalform. Sei $\mathcal{A} = (\mathcal{U}^{\mathcal{A}}, P^{\mathcal{A}})$ eine Struktur mit $\mathcal{A}[x_1/a_1, \ldots, x_n/a_n] \models F$, wobei $a_1, \ldots, a_n \in \mathcal{U}^{\mathcal{A}}$ und $n \geq 0$. Zu $a \in \mathcal{U}^{\mathcal{A}}$ definieren wir

$$a^{\sim} = \begin{cases} 0 & \text{falls } a \notin P^{\mathcal{A}}, \\ 1 & \text{falls } a \in P^{\mathcal{A}}. \end{cases}$$

Wir definieren dann die Struktur $\mathcal{A}_\sim = (\mathcal{U}^{\mathcal{A}_\sim}, P^{\mathcal{A}_\sim})$ wie folgt: Das Universum unserer Struktur ist definiert als das Bild unter $\sim$, also

$$\mathcal{U}^{\mathcal{A}_\sim} = \{x \in \{0,1\} \mid \exists a \in \mathcal{U}^{\mathcal{A}} : a^\sim = x\},$$

d.h. $\sim$ ist eine surjektive Abbildung von $\mathcal{U}^{\mathcal{A}}$ zu $\mathcal{U}^{\mathcal{A}_\sim}$. Des Weiteren definieren wir

$$P^{\mathcal{A}_\sim} = \begin{cases} \{1\} & \text{falls } 1 \in \mathcal{U}^{\mathcal{A}_\sim}, \\ \emptyset & \text{sonst.} \end{cases}$$

Wir zeigen per Induktion über den Formelaufbau, dass $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim] \models F$.

- Sei $F = P(x_i)$ mit $1 \leq i \leq n$. Da $\mathcal{A}[x_1/a_1, \dots, x_n/a_n] \models F$, gilt auch $a_i \in P^{\mathcal{A}}$, also $a_i^\sim = 1$ und somit $a_i^\sim \in P^{\mathcal{A}_\sim}$ und $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim] \models F$.
- Sei $F = \neg P(x_i)$ mit $1 \leq i \leq n$. Da $\mathcal{A}[x_1/a_1, \dots, x_n/a_n] \not\models F$, gilt auch $a_i \notin P^{\mathcal{A}}$, also $a_i^\sim = 0$ und somit $a_i^\sim \notin P^{\mathcal{A}_\sim}$ und $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim] \models F$.
- Sei $F = G \wedge H$. Da $\mathcal{A}[x_1/a_1, \dots, x_n/a_n] \models F$, gilt auch $\mathcal{A}[x_1/a_1, \dots, x_n/a_n] \models G$ und $\mathcal{A}[x_1/a_1, \dots, x_n/a_n] \models H$. Nach I.V. gilt, dass $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim] \models G$ und $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim] \models H$, also $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim] \models G \wedge H$.
- Sei $F = G \vee H$. Analog zum vorherigen Fall.
- Sei $F = \exists x G$. Da $\mathcal{A}[x_1/a_1, \dots, x_n/a_n] \models F$, gibt es ein $a \in \mathcal{U}^{\mathcal{A}}$ mit

  $$\mathcal{A}[x_1/a_1, \dots, x_n/a_n, x/a] \models G.$$

  Nach I.V. gilt $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim, x/a^\sim] \models G$, d.h. es gibt $u \in \mathcal{U}^{\mathcal{A}_\sim}$ mit

  $$\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim, x/u] \models G,$$

  also $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim] \models \exists x G$.
- Sei $F = \forall x G$. Da $\mathcal{A}[x_1/a_1, \dots, x_n/a_n] \models F$, gilt für alle $a \in \mathcal{U}^{\mathcal{A}}$, dass

  $$\mathcal{A}[x_1/a_1, \dots, x_n/a_n, x/a] \models G.$$

  Nach I.V. gilt, dass $\mathcal{A}_\sim[x_1/a_1^\sim, \dots, x_n/a_n^\sim, x/a^\sim] \models G$. Da die Abbildung $a \to a^\sim$ surjektiv ist, gilt auch für alle $u \in \mathcal{U}^{\mathcal{A}_\sim}$, dass

  $$\mathcal{A}[x_1/a_1^\sim, \dots, x_n/a_n^\sim, u] \models G$$

  und somit auch, dass $\mathcal{A}[x_1/a_1^\sim, \dots, x_n/a_n^\sim] \models \forall x G$.

(c) Dies ist entscheidbar. F ist genau dann erfüllbar, wenn ihre Skolemform erfüllbar ist. Die Skolemform einer Formel ohne Allquantoren ist im Prinzip eine aussagenlogische Formel. Für diese ist es entscheidbar, ob sie erfüllbar sind.

Aufgabe 2
Sei $(\mathbb{N}, +, \cdot)$ die Struktur mit

- Trägermenge $\mathbb{N}$,
- zwei zweistelligen Funktionssymbolen $+$ und $\cdot$, die mit Addition und Multiplikation interpretiert werden
- und dem zweistelligen Relationssymbol $=$, das mit Gleichheit interpretiert wird.

Formulieren Sie folgende Aussagen in $(\mathbb{N}, +, \cdot)$ mit Hilfe der Prädikatenlogik:

(a) x ist eine Primzahl (mit freier Variable x).

(b) z ist der ggT von x und y (mit freien Variablen x, y und z).

(c) x und y sind teilerfremd (mit freien Variablen x und y).

(d) Es gibt keine größte Primzahl.

(e) Jede Zahl außer 1 ist das Produkt einer Primzahl und einer natürlichen Zahl.

(f) Jede Primzahl außer 2 ist ungerade.

(g) Jede gerade Zahl, die größer als 2 ist, ist Summe zweier Primzahlen.

(h) Es gibt unendlich viele Primzahlen p so, dass $p + 2$ auch eine Primzahl ist.

Lösung

(a) Wir definieren zunächst $x = 1$ für eine Variable x mit Hilfe der Formel $\forall y(x \cdot y = y)$. Die gesuchte Formel ist dann

$$\text{prim}(x) := \neg(x = 1) \wedge \forall u \forall v\, ((u \cdot v = x) \rightarrow ((u = 1) \vee (v = 1)))$$

(b) Wir definieren zunächst $x \leq y$ mit Hilfe der Formel $\exists z(x+z = y)$. Außerdem definieren wir $z|x, y$ (z ist Teiler von x und von y) als $\exists u \exists v((x = u \cdot z) \wedge (y = v \cdot z))$. Dann ist die gesuchte Formel

$$z = \text{ggT}(x, y) := (z|x, y) \wedge \forall u((u|x, y) \rightarrow (z \leq u)).$$

(c) $(z = 1) \wedge (z = \text{ggT}(x, y))$

(d) Wir definieren zunächst $x < y$ mit Hilfe der Formel $(x \leq y) \wedge \neg(x = y)$. Dann ist die gesuchte Formel

$$\forall x(\text{prim}(x) \rightarrow \exists y(\text{prim}(y) \wedge (x < y))).$$

(e) $\forall x(\neg(x = 1) \rightarrow \exists y \exists z(\mathrm{prim}(y) \wedge (x = y \cdot z)))$

(f) Wir definieren zunächst $\mathrm{odd}(x)$ (x ist ungerade) mit Hilfe der Formel $\neg\exists y(x = y + y)$. Außerdem definieren wir $x = 2$ mit Hilfe der Formel $\exists y((y = 1) \wedge (x = y + y))$. Die gesuchte Formel ist dann

$$\forall x(\neg(x = 2) \rightarrow (\mathrm{prim}(x) \rightarrow \mathrm{odd}(x)))$$

(g) Wir definieren zunächst $\mathrm{even}(x) = \neg\mathrm{odd}(x)$ (x ist gerade). Dann ist die gesuchte Formel

$$\forall x((\mathrm{even}(x) \wedge \exists y((y = 2) \wedge (y < x))) \rightarrow \exists p \exists q(\mathrm{prim}(p) \wedge \mathrm{prim}(q) \wedge (x = p + q)))$$

(h) Wir definieren zunächst $x = y + 2$ mit Hilfe der Formel $\exists w(w = 2 \wedge x = y + w)$. Dann ist die gesuchte Formel

$$\forall x(\mathrm{prim}(x) \rightarrow \exists y(\mathrm{prim}(y) \wedge (x < y) \wedge \exists z(\mathrm{prim}(z) \wedge (z = y + 2))))$$