Einführung in die Modelltheorie – Blatt 12

Lösungsvorschlag

Prof. I. Halupczok

Wie üblich sind alle Antworten zu begründen/beweisen.

Aufgabe 1 (5 Punkte):

Sei $L = \{0, s\}$, wobei s ein einstelliges Funktionssymbol ist, und sei T die L-Theorie, die folgendes besagt:

(i) s ist injektiv.

(ii) Das Bild von s ist alles außer 0.

(iii) s ist „zykelfrei", d. h. für jede feste natürliche Zahl $k \geq 1$ gilt die Aussage: $\forall x\colon \underbrace{s(\ldots(s(x))\ldots)}_{k \text{ mal}} \neq x$.

(Die natürlichen Zahlen mit der Nachfolger-Funktion s sind also ein Modell von T; aber wir wissen bisher nicht, ob T vollständig ist.)

Wir wollen überprüfen, dass T Quantorenelimination hat.

(a) Zeigen Sie zunächst: Jedes Modell $\mathcal{M} \models T$ besteht aus einer Kopie von $\mathbb{N}$ und beliebig vielen Kopien von $\mathbb{Z}$, wobei das Konstantensymbol 0 interpretiert wird als die 0 in der Kopie von $\mathbb{N}$. (Also formaler: $M \cong \mathbb{N} \cup (X \times \mathbb{Z})$ für eine beliebige Menge X, wobei $s^{\mathcal{M}}(n) = n + 1$ für $n \in \mathbb{N}$ und $s^{\mathcal{M}}(x, r) = r + 1$ für $x \in X$ und $r \in \mathbb{Z}$.)

Sei $\mathcal{M}$ ein Modell. Da s injektiv und zykelfrei ist, sind alle Elemente der Form $s^k(0)$ verschieden. Diese Elemente bilden eine Kopie von $\mathbb{N}$. Sei nun a ein Element von $\mathcal{M}$, das nicht in dieser Kopie von $\mathbb{N}$ liegt. Dann existiert ein eindeutiges $s^{-1}(a)$, das auch nicht in der Kopie von $\mathbb{N}$ liegt. Dies lässt sich iterieren. Insgesamt ist $\{s^k(a) \mid k \in \mathbb{Z}\}$ eine Kopie von $\mathbb{Z}$. Wir haben also gezeigt: Jedes Element von $\mathbb{M}$, dass nicht in der Kopie von $\mathbb{N}$ liegt, liegt in einer Kopie von $\mathbb{Z}$.

(b) Beschreiben Sie, welche Teilmengen eines Modells $\mathcal{M} \models T$ endlich erzeugte Unterstrukturen sind.

Wir identifizieren $\mathcal{M}$ mit $\mathbb{N} \cup (X \times \mathbb{Z})$. Sei $\mathcal{A}$ eine endl. erz. Unterstruktur.
Dann ist auf jeden Fall $\mathbb{N} \subseteq A$ (da $0 \in A$ und A unter Nachfolgern abgeschlossen ist).
Ist $(x_i, r_i) \in X \times \mathbb{Z}$ einer der Erzeuger, so ist außerdem $\{(x_i, s) \mid s \geq r_i\} \subseteq A$. Insgesamt besteht A also aus $\mathbb{N}$ und endlich vielen solchen Mengen.

(c) Wir nehmen nun an, dass $\mathcal{M}_1$ und $\mathcal{M}_2$ Modelle von T sind, $\mathcal{A}_i \subseteq \mathcal{M}_i$ endlich erzeute Unterstrukturen und $\alpha\colon \mathcal{A}_1 \to \mathcal{A}_2$ ein Isomorphismus. Zeigen Sie, dass sich α auf (geeignete) Modelle von T fortsetzen lässt, d. h. dass Unterstrukturen $\mathcal{B}_i \subseteq \mathcal{M}_i$ existieren mit $\mathcal{A}_i \subseteq \mathcal{B}_i$ und $\mathcal{B}_i \models T$, und so dass sich α zu einem Isomorphismus $\mathcal{B}_1 \to \mathcal{B}_2$ fortsetzen lässt.

Wir identifizieren $\mathcal{M}_i$ mit $\mathbb{N} \cup (X_i \times \mathbb{Z})$. Durch umnummerieren können wir außerdem annehmen, dass A_i die Form $\mathbb{N} \cup (Y_i \times \mathbb{N})$, für endliche Teilmengen $Y_i \subseteq X_i$. Ein Isomorphismus $\alpha\colon \mathcal{A}_1 \to \mathcal{A}_2$ muss natürlich $0^{\mathcal{A}_1}$ auf $0^{\mathcal{A}_2}$ abbilden und außerdem Elemente der Form $(x, 0) \in Y_1 \times \mathbb{N}$ auf Elemente der Form $(x', 0) \in Y_2 \times \mathbb{N}$ (da das die einzigen Elemente in $\mathcal{A}_i$ ohne Vorgänger sind). Insgesamt erhalten wir eine Bijektion $\beta\colon Y_1 \to Y_2$, und α bildet (x, n) auf $(\beta(x), n)$ ab, für $x \in Y_1$ und $n \in \mathbb{N}$.

Setze nun $\mathcal{B}_i := \mathbb{N} \cup (Y_i \times \mathbb{Z}) \subseteq \mathcal{M}_i$. Das sind Modelle von T, und α setzt sich fort zu $\mathcal{B}_1 \to \mathcal{B}_2$, $(x, r) \mapsto (\beta(x), r)$, für $r \in \mathbb{Z}$.

(d) Zeigen Sie nun, dass T das Quantoreneliminations-Kriterium aus Satz 4.2.4 erfüllt.

Hinweis: Indem Sie (c) anwenden, können Sie sich das Leben leichter machen: Falls das b aus Satz 4.2.4 in B_1 ist, können sie b' mit Hilfe von (c) finden, völlig unabhängig von ϕ. Wenn das b nicht in B_1 liegt, kann man zeigen, dass die Formel $\phi(\underline{a}, y)$ eine Form hat, die sich „besonders leicht realisieren lässt".

Wir verwenden die Notationen von (c). Sei $\phi(\underline{a}, x)$ eine Konjunktion von $L(A_1)$-Literalen und sei $b \in \mathcal{M}_1$ mit $\mathcal{M}_1 \models \phi(\underline{a}, b)$.

Falls $b \in B_1$ ist, setze $b' := \alpha(b)$. Da ϕ quantorenfrei ist, gilt $\mathcal{M}_1 \models \phi(\underline{a}, b) \iff \mathcal{B}_1 \models \phi(\underline{a}, b) \iff \mathcal{B}_2 \models \phi(\alpha(\underline{a}), b') \iff \mathcal{M}_2 \models \phi(\alpha(\underline{a}), b)$.

Falls $b \notin B_1$ ist, hat b also die Form (x, r) für ein $x \notin Y_1$. Daraus folgt, dass kein $a \in A_1$ existiert und keine natürlichen Zahlen m, n mit $s^m(b) = s^n(a)$. Alle Literale in ϕ, in denen y vorkommt, müssen also die Form $s^m(y) \neq s^n(a)$ haben (oder $s^m(y) = s^m(y)$). Insbesondere schließt $\phi(\alpha(\underline{a}), y)$ nur endlich viele Elemente für y aus. Da $\mathcal{M}_2$ unendlich ist, existiert ein $b' \in M_2$, das $\phi(\alpha(\underline{a}), y)$ realisiert.

Aufgabe 2 (5 Punkte):

Wir betrachten $\mathbb{Z}$ in der Sprache $L := L_{\text{agrp}} \cup \{1\}$.

(a) Zeigen Sie, dass sich $2\mathbb{Z}$ nicht quantorenfrei definieren lässt.

(Vorbemerkung: Man könnte einen trickreichen Beweis finden mit einem Isomorphismus von Unterstrukturen, der ein Element von $2\mathbb{Z}$ auf ein Element außerhalb von $2\mathbb{Z}$ abbildet… allerdings nicht in $\mathbb{Z}$ selbst, sondern in einer elementaren Erweiterung. Genauer gesagt kann man dafür genau den Isomorphismus α aus der untigen Lösung zu (c) wählen. Statt desssen gebe ich hier eine elementare Lösung an:)

Wir zeigen, dass jede Menge $\phi(\mathbb{Z})$, die durch eine quantorenfreie Formel $\phi(x)$ in einer Variablen definiert wird, bereits endlich oder co-endlich ist.
Wir machen Induktion über den Aufbau von ϕ:
Falls ϕ atomar ist: Der Fall $\phi = \perp$ ist klar. Sei also ϕ (o.E.) von der Form $t(x) = 0$, für einen L-Term t. Jeder solche L-Term ist äquivalent zu einem Term der Form $rx + m$, mit $r, m \in \mathbb{Z}$. Falls $r = 0$ ist $\phi(x)$ immer wahr oder immer falsch (je nach m); ansonsten $\phi(x)$ für maximal ein x wahr. In jedem der Fälle ist $\phi(\mathbb{Z})$ endlich oder co-endlich.
Falls $\phi = \neg\psi$: Wenn $\psi(\mathbb{Z})$ endlich ist, ist $\phi(\mathbb{Z})$ co-endlich und umgekehrt.
Falls $\phi = \psi_1 \wedge \psi_2$: Wenn beide $\psi_i(\mathbb{Z})$ co-endlich sind, dann auch $\phi(\mathbb{Z})$; wenn mindestens ein $\psi_i(\mathbb{Z})$ endlich ist, dann auch $\phi(\mathbb{Z})$.

(b) Hier ist der Versuch eines Beweises, dass $\mathbb{Z}$ in der obigen Sprache L Quantorenelimination hat. Welche(r) der Schritte ist/sind falsch?

(i) Es reicht, das Kriterium aus Satz 4.2.4 zu prüfen. Seien also $\mathcal{M}_1 = \mathcal{M}_2 = \mathbb{Z}$, seien $\mathcal{A}_i \subseteq \mathcal{M}_i$ endlich erzeugte Unterstrukturen und sei $\alpha\colon \mathcal{A}_1 \to \mathcal{A}_2$ ein L-Isomorphismus. (ii) Da 1 ein Konstanten-Symbol von L ist und 1 die ganze Gruppe $\mathbb{Z}$ erzeugt, muss schon $\mathcal{A}_i = \mathcal{M}_i$ gelten. (iii) Außerdem muss $\alpha(1) = 1$ sein. (iv) Daraus folgt, dass α die Identität ist. (v) Ist nun $\psi(\underline{a}, y)$ eine quantorenfreie $L(A_1)$-Formel, und existiert ein $b_1 \in \mathcal{M}_1 = \mathbb{Z}$ mit $\mathcal{M}_1 \models \psi(\underline{a}, b_1)$, so gilt trivialerweise auch $\mathcal{M}_2 \models \psi(\alpha(\underline{a}), b_1)$. (vi) Wir können also $b_2 := b_1$ setzen und haben damit das Kriterum aus dem Satz gezeigt.

Für das Kriterium aus Satz 4.2.4 muss man für $\mathcal{M}_1$ und $\mathcal{M}_2$ beliebige Modelle einer Theorie erlauben, in diesem Fall also beliebige Modelle von $\mathrm{Th}(\mathbb{Z})$ (und nicht nur $\mathbb{Z}$ selbst).

(c) Geben Sie ein (möglichst) konkretes Beispiel an, das zeigt, dass das Kriterium aus Satz 4.2.4 nicht erfüllt ist.
Sei $\mathcal{M}_1 = \mathcal{M}_2 \succ \mathbb{Z}$ eine beliebige echte elementare Erweiterung. Wir werden gleich zwei geeignete Elemente $a_1, a_2 \in \mathcal{M}_1 \setminus \mathbb{Z}$ wählen. Danach setzen wir $\mathcal{A}_1 := \langle a_1 \rangle_L$, $\mathcal{A}_2 := \langle a_2 \rangle_L$.
Behauptung: Für $i = 1, 2$ ist $\mathcal{A}_i$ ist isomorph zu $\mathbb{Z} \times \mathbb{Z}$, erzeugt von a_i und 1.
Beweis der Behauptung: $\mathbb{Z}$ ist abelsch und torsionsfrei.[1] Dies lässt sich durch L-Aussagen ausdrücken, also ist auch $\mathcal{M}_i$ abelsch und torionsfrei, also auch die Untergruppe $\mathcal{A}_i$. Als Gruppe ist $\mathcal{A}_i$ erzeugt von zwei Elementen (nämlich a_i und 1), also ist $\mathcal{A}_i$ isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z} \times \mathbb{Z}$. Wir müssen nur noch den Fall $\mathcal{A}_i \cong \mathbb{Z}$ ausschließen. In diesem Fall gäbe es natürliche Zahlen $m, m' \geq 1$ mit $m \cdot a_i = m' \cdot 1$. Wenn m kein Teiler von m' ist, sagt $\mathrm{Th}(\mathbb{Z})$, dass gar kein x existiert mit $m \cdot x = m' \cdot 1$. Wenn m ein Teiler von m' ist, sagt $\mathrm{Th}(\mathbb{Z})$, dass nur ein solches x existiert (nämlich m'/m). Das liegt aber in $\mathbb{Z}$, und wir hatten $a_i \notin \mathbb{Z}$ gewählt.
Aus der Behauptung folgt, dass ein Isomorphismus $\alpha\colon \mathcal{A}_1 \to \mathcal{A}_2$ existiert mit $a_1 \mapsto a_2$ (und $1 \mapsto 1$).
Jetzt müssen wir nur noch a_1 und a_2 so wählen, dass $\mathcal{M}_1 \models \exists y\colon 2y = a_1$ gilt aber $\mathcal{M}_2 \not\models \exists y\colon 2y = a_2$. Das können wir z.B. machen, indem wir erstmal $a_0 \mathcal{M}_1 \setminus \mathbb{Z}$ beliebig wählen und dann $a_1 := 2a_0$ und $a_2 := 2a_0 + 1$ setzen. Dass a_1 durch 2 teilbar ist, ist klar. Dass a_2 nicht durch 2 teilbar ist, liegt daran, dass in $\mathbb{Z}$ (und damit auch in $\mathcal{M}_2$) gilt: Es gibt kein x, so dass $2x + 1$ durch 2 teilbar ist.

[1] Torsionsfrei heißt: Alle Elemente außer 0 haben Ordnung ∞.