Beispiele von Quantorenelimination

November 8, 2018

Quantoreneliminationkriterium

Erinnerung:

Theorem 3.11. *Eine Theorie T besitzt Quantorenelimination genau denn, wenn es für alle Modelle $M_1, M_2 \vDash T$ mit einer gemeinsamen endlich erzeugten Unterstruktur $A \subseteq M_1, M_2$ (wo $A = \langle\,\rangle = \emptyset$ erlaubt ist), und für alle primitiven Existenzformeln mit Parametern in A*

$$\psi = \exists y. \bigwedge_i \theta_i(y)$$

(mit θ_i basic) gilt

$$M_1 \vDash \psi \Leftrightarrow M_2 \vDash \psi.$$

T_∞

Sei T_∞ die Theorie in der leeren Sprache

$$T_\infty := \{\exists x_1, \ldots, x_n. \bigwedge_{i=1}^{n} \bigwedge_{j=i+1}^{n} x_i \neq x_j : n \in \mathbb{N}\}.$$

Theorem 3.12. *T_∞ ist vollständig und besitzt Quantorenelimination.*

Beweis. Vollständigkeit folgt aus Quantorenelimination, weil die Sprache keine Konstante besitzt.

Sei $M_i \vDash T_\infty$ und $A = \{a_1, \ldots, a_n\} \subseteq M_1, M_2$ eine endliche gemeinsame Teilmenge.

Sei $\exists y.\phi(y)$ eine primitive Existenzformel mit Parametern in A. Angenommen, dass $b \in M_1$ existiert, so dass $M_1 \vDash \phi(b)$. Wir müssen ein $b' \in M_2$ finden, so dass $M_2 \vDash \phi(b')$.

Falls $b \in A$, setze $b' := b$. Sonst: weil $M_2 \vDash T_\infty$, ist M_2 unendlich. Setze $b' \in M_2 \setminus A$.

Dann gelten die gleichen Identitäten in $(b, a_1, \ldots, a_n)$ als in $(b', a_1, \ldots, a_n)$, daher $M_2 \vDash \phi(b')$. □

T_{DLO}

Theorem 3.13. *T_{DLO} ist vollständig und besitzt Quantorenelimination.*

Beweis. Vollständigkeit folgt aus Quantorenelimination, weil die Sprache keine Konstante besitzt.

Sei $M_i \vDash T_{\mathrm{DLO}}$ und $A = \{a_1, \ldots, a_n\} \subseteq M_1, M_2$ eine endliche gemeinsame Unterstruktur mit $a_1 < a_2 < \ldots < a_n$.

Sei $\exists y.\phi(y)$ eine primitive Existenzformel mit Parametern in A. Angenommen, dass $b \in M_1$ existiert, so dass $M_1 \vDash \phi(b)$. Wir finden ein $b' \in M_2$ mit $M_2 \vDash \phi(b')$.

Es gibt vier Fälle:

(i) $b \in A$: dann setze $b' = b$.

(ii) $b < a_1$: dann sei $b' \in M_2$ so dass $b' < a_1$ (b' existiert, weil M_2 keinen Endpunkt hat).

(iii) $b > a_n$: dann sei $b' \in M_2$ so dass $b' > a_n$ (b' existiert, weil M_2 keinen Endpunkt hat).

(iv) $a_i < b < a_{i+1}$: dann sei $b' \in M_2$ so dass $a_i < b' < a_{i+1}$ (b' existiert, weil M_2 dicht ist).

In alle Fällen ist $A \cup \{b\}$ zu $A \cup \{b'\}$ über A isomorph als angeordnete Menge. Daher $M_2 \vDash \phi(b')$. □

T_{AAK}

Theorem 3.14. *T_{AAK} besitzt Quantorenelimination.*

Beweis. Sei $K_i \vDash T_{\mathrm{AAK}}$ und $R = \langle a_1, \ldots, a_n \rangle \subseteq K_1, K_2$ ein endlicher erzeugter gemeinsamer Unterring.

Sei $\exists y.\phi(y)$ eine primitive Existenzformel mit Parametern in R. Angenommen, dass $b \in K_1$ existiert, so dass $K_1 \vDash \phi(b)$. Wir zeigen, dass $K_2 \vDash \exists y.\phi(y)$.

Sei F_i der Quotientenkörper in K_i von R. Dann definiert $F_1 \ni \frac{r}{s} \to \frac{r}{s} \in F_2$ einen Isomorphismus $f : F_1 \to F_2$.

Nun sei G_i der algebraische Abschluss von F_i in K_i, d.h. die Menge aller Lösungen von Polynomgleichungen mit Koeffizienten in F_i.

Weil der algebraisch Abschluss von F_1 eindeutig bis auf F_1-Isomorphie ist, erweitert sich f zu einen Isomorphismus $g : G_1 \to G_2$.

Falls $b \in G_1$, dann $K_2 \vDash \phi(g(b))$.

Sonst: b ist transzendent über G_1, und $G_1(b)$ ist isomorph über G_1 zum rationalen Funktionkörper $G_1(X)$. Sei K_2' eine elementare Erweiterung von K_2, so dass $K_2' \neq G_2$. Dann gibt es $b' \in K_2' \setminus G_2$. Wieder ist $G_2(b')$ isomorph über G_2 zum rationalen Funktionkörper $G_2(X)$. Deshalb erweitert sich g zu einen Isomorphismus $h : G_1(b) \to G_2(b')$ mit $h(b) = b'$. Deswegen folgt $K_2' \vDash \phi(b')$, und deshalb $K_2' \vDash \exists y.\phi(y)$, daher folgt schließlich $K_2 \vDash \exists y.\phi(y)$. □

Für $p \in \mathbb{N}$ prim, sei $T_{\mathrm{AAK}_p} := T_{\mathrm{AAK}} \cup \{\ulcorner p \urcorner \doteq 0\}$, wobei $\ulcorner p \urcorner$ der Term $1 + 1 + \ldots + 1$ (p Mal) ist.

Sei $T_{\mathrm{AAK}_0} := T_{\mathrm{AAK}} \cup \{\ulcorner n \urcorner \neq 0 : n \in \mathbb{N}_{>0}\}$.

Theorem 3.15. *Die Vervollständigungen von T_{AAK} sind T_{AAK_p} für $p = 0$ und für p prim.*

Beweis. p bestimmt die Unterstruktur, die von $\emptyset$ erzeugt ist, d.h. die Primkörper $\mathbb{F}_p$ oder $\mathbb{Q}$, und deshalb bestimmt es welche quantorenfreien Aussagen gelten. Deswegen impliziert Quantorenelimination Vollständigkeit von jedem T_{AAK_p}.

Die Charakteristik eines Körper ist 0 oder prim, deshalb gibt es keine andere Vervollständigung. □

Presburger Arithmetik

Betrachten Sie die Struktur $\langle \mathbb{Z}; +, < \rangle$. Wir wollen ein vollständiges Axiomsystem für ihre Theorie finden. Um dies zu tun finden wir eine Sprache, in der die Theorie Quantorenelimination hat. Sie besitzt nicht Quantorenelimination in $\{+, <\}$, weil für $n > 1$ die Untermenge $n\mathbb{Z} \subseteq \mathbb{Z}$ nicht quantorfrei definierbar ist. Wir zeigen, dass dies das einzige Problem ist.

Sei T_{Pr} die Theorie in die Sprache $\{0, 1, +, -, <, (P_n)_{n>1}\}$, die aus den folgenden Axiomen besteht:

(I) die Axiome angeordneter abelscher Gruppen in der Sprache $\{0, +, <\}$;

(II) $0 < 1 \wedge \forall x.(x \leq 0 \vee x \geq 1)$;

(III) für jedes $n > 1$, $\forall x.(P_n(x) \leftrightarrow \exists y.x \doteq ny)$;

(IV) für jedes $n > 1$, $\forall x. \bigvee_{0 \leq i < n}(x \equiv_n \ulcorner i \urcorner \wedge \bigwedge_{0 \leq j < n; j \neq i} x \not\equiv_n \ulcorner j \urcorner)$ wobei wir $x \equiv_n y$ für $P_n(x - y)$ schreiben ("jedes x ist mod n zu genau einem von $0, \ldots, n-1$ kongruent")

Theorem 3.16. *T_{Pr} ist vollständig und besitzt Quantorenelimination.*

Beweis. Die Unterstruktur jedes Modell von T_{Pr}, die von $\emptyset$ erzeugt ist, ist $\mathbb{Z}$. Daher folgt Vollständigkeit aus Quantorenelimination.

Sei $M_i \vDash T_{\mathrm{Pr}}$ und $G \subseteq M_1, M_2$ ein endliche erzeugte gemeinsame Unterstruktur.

Sei $\phi(y) = \bigwedge_i \theta_i(y)$ mit θ_i Basicformeln mit Parametern in G. Angenommen, dass $b \in K_1$ existiert, so dass $M_1 \vDash \phi(b)$. Wir zeigen, dass $M_2 \vDash \exists y.\phi(y)$.

Jedes $\theta_i(y)$ ist äquivalent mod T_{Pr} zu eins von

(1) $my \doteq g$

(1') $my \not\doteq g$

(2) $my \equiv_n g$

(2') $my \not\equiv_n g$

(3) $my < g$

(3') $g < my$

wobei $n, m \in \mathbb{N}$ und $g \in G$.

M_i sind torsionfrei, weil sie angeordnet sind. Daher können wir annehmen, dass es ein gemeinsames m für alle θ_i gibt, weil für $m, k \in \mathbb{N}$,

$$T_{\mathrm{Pr}} \vdash \forall y.(my = g \leftrightarrow kmy = kg)$$
$$T_{\mathrm{Pr}} \vdash \forall y.(my \equiv_n g \leftrightarrow kmy \equiv_{kn} kg)$$
$$T_{\mathrm{Pr}} \vdash \forall y.(my < g \leftrightarrow kmy < kg)$$

gelten.

Sei θ_i', so dass $T_{\mathrm{Pr}} \vdash \forall y.(\theta_i(y) \leftrightarrow \theta_i'(my))$. Z.B., wenn θ_i in Fall (1) fallt mit $\theta_i(y)$ äquivalent mod T_{Pr} zu $my \doteq g$, nehmen wir $\theta_i'(z) := z \doteq g$.

Sei $\phi' := \bigwedge_i \theta_i'$. Daher $M_1 \vDash \phi'(mb)$.

Behauptung 3.17. *Es gibt $h \in G$, so dass $G \vDash \phi'(h) \wedge P_m(h)$ gilt.*

Beweis. Schreibe $\phi' = \phi_1' \wedge \phi_2' \wedge \phi_3'$, wobei ϕ_k' besteht die Konjunkte θ_i', die Form (k) oder (k') haben.

Dann ist $\phi_3'(z)$ äquivalent mod T_{Pr} zu $g_1 < z < g_2$ für bestimmte $g_i \in G \cup \{-\infty, \infty\}$. Angenommen, dass $g_1, g_2 \in G$ sind (die anderen Fälle sind ähnlich).

Sei $N \in \mathbb{N}$, so dass m und alle n, die in ϕ_2' erscheinen, N teilen.

Wenn es $i \in \mathbb{N}$ gibt mit $g_2 = g_1 + \ulcorner i \urcorner$, gilt $mb \in G$, daher ist $h := mb$ wie gefordert. Ähnlich, wenn es eine Formel von Form (1) gibt.

Angenommen, dass wir uns im keinen der gerade behandelten Fälle befinden. Nun folgt es aus (IV), dass es unendliche viele $h \in g_1 + \mathbb{N}_{>0} \subseteq G$ gibt, so dass $h \equiv_N mb$. Daher gibt es ein solches h mit auch $G \vDash \phi_1'(h)$. Es folgt aus (II), dass $h < g_2$. Dann ist h wie gewünscht. □

Nun $M_2 \vDash P_m(h)$, deshalb gibt es $b' \in M_2$ mit $mb' = h$, und daher $M_2 \vDash \phi(b')$. □

Corollary 3.18. $\mathrm{Th}(\mathbb{Z}; +, <)$ *ist entscheidbar.*

Beweis. Das obene Axiomsystem T_{Pr} ist entscheidbar. Weil es vollständig ist, ist die erzeugte Theorie $\mathrm{Th}(\mathbb{Z}; 0, 1, +, -, <, (P_n)_n)$ auch entscheidbar, und insbesondere ist $\mathrm{Th}(\mathbb{Z}; +, <)$ entscheidbar. □