Seminar über mathematische Logik
Der Repräsentationssatz

Dimitri Wyss

16. 5. 2012

Die folgenden Ausführungen sind eine geringfügig veränderte Exposition des Abschnitts 6.4 aus [1].

Das wichtigste Resultat dieses Abschnitts wird folgender Satz sein.

Satz 1 (Repräsentationssatz)**.** *Jede rekursive Funktion und somit auch jedes rekursive Prädikat ist in* ***PA*** *repräsentierbar.*

Im Folgenden soll *repräsentierbar* immer *repräsentierbar in* ***PA*** bedeuten. Unter natürlichen Zahlen verstehen wir die Menge $\mathbb{N} = \{0, 1, 2, \dots\}$.
Einige Resultate, die wir für den Beweis von Satz 1 brauchen, wurden bereits im Vortrag über *Repräsentierbarkeit arithmetischer Prädikate* bewiesen. Wir fassen diese hier noch einmal zusammen:

Lemma 2. *(a) Es sei* $P \subset \mathbb{N}^{n+1}$ *repräsentiert durch* $\alpha(\vec{x}, y)$*, sowie* $z \notin frei\alpha$*. Dann repräsentieren* $(\exists z \leq y)\alpha(\vec{x}, z)$ *und* $(\forall z \leq y)\alpha(\vec{x}, z)$ *die Prädikate* Q *und* R *mit*

$$Q(\vec{a}, b) \Leftrightarrow (\exists c \leq b)P(\vec{a}, c) \text{ bzw. } R(\vec{a}, b) \Leftrightarrow (\forall c \leq b)P(\vec{a}, c).$$

(b) Die Menge aller repräsentierbaren Funktionen ist abgeschlossen unter $\boldsymbol{O\mu}$.

(c) Die Menge aller repräsentierbaren Funktionen ist abgeschlossen unter $\boldsymbol{Oc}$.

Wegen (b) und (c) müssen wir für den Beweis von Satz 1 also nur noch die Repräsentierbarkeit der Anfangsfunktionen und Abgeschlossenheit unter $\boldsymbol{Op}$ nachweisen. Für Letzteres brauchen wir einige Vorbereitungen.

Wir werden nun eine repräsentierbare Funktion $\boldsymbol{\beta} \in \boldsymbol{F}_2$ konstruieren mit der Eigenschaft, dass zu jedem $n \in \mathbb{N}$ und jeder Zahlenfolge $c_0, \ldots, c_n$ eine Zahl c existiert mit $\boldsymbol{\beta}(c, i) = c_i$ für $i = 0, \ldots, n$. Die Idee dazu liefert folgender Satz aus der Zahlentheorie:

Proposition 3 (Chinesischer Restsatz)**.** *Gegeben seien natürliche Zahlen $c_i < d_i$ für $i = 0, \ldots, n$ und seien $d_0, \ldots, d_n$ paarweise teilerfremd. Dann existiert ein $a \in \mathbb{N}$ mit rest$(a, d_i) = c_i$ für $i = 0, \ldots, n$.*

Beweis. Für $n = 0$ folgt die Aussage mit $a = c_0$. Wir schliessen nun induktiv und nehmen an, dass $a \in \mathbb{N}$ existiert mit $\mathrm{rest}(a.d_i) = c_i$ für alle $i < n$. Da $k = \mathrm{kgV}\{d_i \mid i < n\}$ und d_n teilerfremd sind, existieren nach dem Lemma von Bézout $x, y \in \mathbb{N}$ mit $xk + 1 = yd_n$. Multipliziert man beide Seiten mit $c_n(k-1) + a$ folgt $x'k + c_n(k-1) + a = y'd_n$ mit neuen Werten $x', y' \in \mathbb{N}$. Setze $a' = (x' + c_n)k + a = y'd_n + c_n$. Dann ist $\mathrm{rest}(a', d_i) = \mathrm{rest}(a, d_i) = c_i$ für alle $i < n$, aber auch $\mathrm{rest}(a', d_n) = c_n$, denn $c_n < d_n$. □

Als nächstes konstruieren wir zu gegebenen $c_0, \ldots, c_n$ Zahlen $d_0, \ldots, d_n$, sodass die Voraussetzungen für Proposition 3 erfüllt sind. Seid dazu $m = \max\{n, c_0, \ldots, c_n\}$ und $b = \mathrm{KgV}\{i + 1 \mid i < m\}$. Dann gilt

Lemma 4. *Die Zahlen $d_i = 1 + (1 + i)b$ für $i = 0, \ldots, n$ sind paarweise teilerfremd und $d_i > c_i$.*

Beweis. Nach Konstruktion ist sicher $b_i > c_i$ für $i = 0, \ldots, n$. Nehme nun an p sei ein Primteiler von d_i und d_j für $i < j$. Dann gilt $p | d_j - d_i = (j - i)b$. Wegen $j - i \leq n \leq m$ gilt auch $j - i | b$, also insgesamt $p | b$. Andererseits gilt auch $b | d_i - 1$ und somit $p | d_i - 1$, ein Widerspruch. □

Dies motiviert die Definition einer Funktion $\boldsymbol{\alpha} \in \boldsymbol{F}_3$ als

$$\boldsymbol{\alpha}(a, b, i) = \mathrm{rest}(a, (1 + (1 + i)b)),$$

welche repräsentierbar ist, da das dazugehörige Prädikat gegeben ist durch

$$\boldsymbol{\alpha}(a, b, i) = k \Leftrightarrow (\exists c \leq a)[a = c(1 + (1 + i)b) + k \wedge k < 1 + (1 + i)b].$$

Um schliesslich eine Funktion $\boldsymbol{\beta} \in \boldsymbol{F}_2$ zu erhalten, verwenden wir noch die Tatsache, dass es eine repräsentierbare Bijektion zwischen $\mathbb{N}^2$ und $\mathbb{N}$ gibt. Dies liefert zum Beispiel die Funktion

$$\mathfrak{p}(a, b) = a + \frac{1}{2}(a + b)(a + b + 1),$$

welche durch folgende Formel repräsentiert wird

$$\mathfrak{p}(a,b) = c \Leftrightarrow 2c = 2a + (a+b)(a+b+1).$$

Wir bezeichnen mit $\mathfrak{x}_1, \mathfrak{x}_2$ die Umkehrfunktionen von $\mathfrak{p}$, das heisst $\mathfrak{p}(\mathfrak{x}_1 k, \mathfrak{x}_2 k) = k$. Die explizite Darstellung von $\mathfrak{x}_1, \mathfrak{x}_2$ ist hier unwichtig, man beachte aber die Ungleichungen $\mathfrak{x}_1 k, \mathfrak{x}_2 k \leq k$. Somit erhalten wir schliesslich

Proposition 5 (Die β-Funktion)**.** *Die Funktion $\boldsymbol{\beta} \in \boldsymbol{F}_2$ definiert als*

$$\boldsymbol{\beta}(c,i) = \boldsymbol{\alpha}(\mathfrak{x}_1 c, \mathfrak{x}_2 c, i),$$

ist repräsentierbar und erfüllt die folgende Eigenschaft:
Zu jedem $n \in \mathbb{N}$ und jeder Folge von natürlichen Zahlen $c_0, \ldots, c_n$ existiert eine Zahl c mit $\boldsymbol{\beta}(c,i) = c_i$ für $i = 0, \ldots, n$.

Beweis. Es gilt

$$\boldsymbol{\beta}(c,i) = k \Leftrightarrow (\exists a \leq c)(\exists b \leq c)[\mathfrak{p}(a,b) = c \wedge \boldsymbol{\alpha}(a,b,i) = k],$$

also ist $\boldsymbol{\beta}$ repräsentierbar. Sind nun $c_0, \ldots, c_n$ gegeben, so wählen wir zunächst b und $d_0, \ldots, d_n$ wie in Lemma 4 und anschliessend verwenden wir Proposition 3 um ein passendes a zu erhalten. Dann gilt für $c = \mathfrak{p}(a,b)$ schliesslich

$$\boldsymbol{\beta}(c,i) = \boldsymbol{\alpha}(a,b,i) = \mathrm{rest}(a,d_i) = c_i.$$

□

Beweis von Satz 1. Für die Anfangsfunktionen $0, S, I_k^n$ haben wir die Formeln $v_0 = 0, v_1 = Sv_0$ und $v_n = v_k$. Wie bereits erwähnt, müssen wir wegen Lemma 2 nur noch zeigen, dass die Menge der repräsentierbaren Funktionen unter $\boldsymbol{Op}$ abgeschlossen ist. Seien also g, h repräsentierbar und f bestimmt durch

$$f(\vec{a}, 0) = g\vec{a} \text{ und } f(\vec{a}, Sb) = h(\vec{a}, b, f(\vec{a}, b)).$$

Definiere nun das Prädikat P als

$$P(\vec{a}, b, c) \Leftrightarrow \boldsymbol{\beta}(c,0) = g\vec{a} \wedge (\forall v < b)\boldsymbol{\beta}(c, Sv) = h(\vec{a}, v, \boldsymbol{\beta}(c,v)).$$

Mit Lemma 2 (a) und (c) folgt, dass P repräsentierbar ist. Wenn wir nun die Definition von f einsetzen lässt sich P auch schreiben als

$$P(\vec{a}, b, c) \Leftrightarrow \boldsymbol{\beta}(c,i) = f(\vec{a}, i) \text{ für } i = 0, \ldots, b.$$

Nun wenden wir Proposition 5 mit $c_i = f(\vec{a}, i)$ an und erhalten $\forall \vec{a} \forall b \exists c P(\vec{a}, b, c)$. Nach Lemma 2 (b)ist deshalb $f' : (\vec{a}, b) \longmapsto \mu c P(\vec{a}, b, c)$ repräsentierbar und somit auch $\boldsymbol{\beta}(f'(\vec{a}, b), b) = f(\vec{a}, b)$. □

Definition 6. Der *Gödelterm* von $\phi \in \boldsymbol{\mathcal{L}}_{ar}$ ist $\ulcorner\phi\urcorner = \underline{n}$, wobei $n = \dot{\phi}$ die Gödelzahl von ϕ ist.

Beispielsweise ist $\ulcorner v_0 = 0\urcorner = \underline{\dot{v_0}\tilde{=}\dot{0}} = \underline{2^{22} \cdot 3^2 \cdot 5^{14}}$. Analog ist auch $\ulcorner\Phi\urcorner$ für einen Beweis Φ definiert, indem man einfach seine entsprechende Gödelzahl als Term in **PA** auffasst.
Als Korollar der Representationssatzes betrachten wir die Prädikate bew_T und bwb_T aus dem Vortrag über die *Gödelisierung von Formeln*. Dort wurde gezeigt, dass bew_T p.r. ist und daher nach Satz 1 repräsentierbar, sagen wir durch $\text{bew}(x, y)$. Definiere weiter $\text{bwb}(x) = \exists y\, \text{bew}(y, x)$. Dann gilt

Korollar 7. *Für $\phi \in \boldsymbol{\mathcal{L}}_{ar}$ gilt $\vdash \phi \Rightarrow \vdash \text{bew}(\underline{n}, \ulcorner\phi\urcorner)$ für ein n (daher $\vdash \phi \Rightarrow \text{bwb}(\ulcorner\phi\urcorner)$) und $\nvdash \phi \Rightarrow\ \neg\,\text{bew}(\underline{n}, \ulcorner\phi\urcorner)$ für alle n.*

Beiwes. Per Definition von $\vdash \phi$ existiert ein Beweis Φ mit den Axiomen aus **PA**, also $bew(\dot{\Phi}, \phi)$. Dann können wir $\underline{n} = \ulcorner\Phi\urcorner$ wählen. Die Umkehrung folgt durch Kontraposition. □

Als nächstes wollen wir untersuchen, wann die Umkehrung von Satz 1 gilt. Auch dazu müssen wir zuerst ein wenig ausholen.
Die *Churchsche Theses* besagt, dass die rekursiven Funktionen bereits alle "berechenbaren"Funktionen ausschöpfen. Dabei stellen wir uns eine Funktion f als berechenbar vor, falls es einen Algorithmus gibt, der zu jedem $a \in \mathbb{N}$ den Wert fa in endlich vielen Schritten berechnet. Die These ist also keine exakte mathematische Aussage, allerdings liefert sie oft sehr intuitive "Beweise". Wir wollen dies an folgendem Satz erläutern, welcher auch in einem späteren Vortrag noch einmal wichtig wird.

Satz 8. *Jede vollständig axiomatisierbare Theorie T ist rekursiv*

Wir erklären nun zuerst, wie man dies mit Hilfe der Churchschen These "beweisen"könnte. Als erstes bemerken wir, dass es eine Aufzählung $\alpha_0, \alpha_1, \ldots$ aller in T beweisbaren Aussagen gibt, da T axiomatisierbar ist (Dies ist eine Interpretation von Satz 6.2.4 aus [1]). Unser Entscheidungsverfahren besteht nun darin, für gegebenes $\alpha \in \boldsymbol{\mathcal{L}}^0$ die Aussagen α und $\neg\alpha$ im n-ten Schritt mir α_n zu vergleichen. Dieses Verfahren terminiert wegen der Vollständigkeit von T. Daher ist T entscheidbar, i.e. χ_T ist berechenbar, was mit der Churchschen These gleichbedeutend ist mit rekursiv.
Dieses Argument lässt sich auch formalisieren:

Beweis. Wegen der Vollständigkeit ist die Funktion f mit

$$f(a) = \mu b[a \in \dot{\boldsymbol{\mathcal{L}}}^0 \Rightarrow\ bew(b, a) \vee bew(b, \tilde{\neg}a)]$$

wohldefiniert. Denn bezeichnet $P(a,b)$ das p.r. Prädikat in eckigen Klammern, gilt offenbar $\forall a \exists b P(a,b)$, wobei für $a \notin \dot{\boldsymbol{\mathcal{L}}}^0$ bereits $P(a,0)$ zutrifft. Gemäss $\boldsymbol{O\mu}$ ist f also rekursiv. Es genügt nun zu zeigen

$$a \in \dot{T} \Leftrightarrow a \in \dot{\boldsymbol{\mathcal{L}}}^0 \wedge bew(fa,a).$$

Sei zuerst $a \in \dot{T}$, dann gilt sicher $a \in \dot{\boldsymbol{\mathcal{L}}}^0$. Da T konsistent ist, gibt es überhaupt kein b mit $bew(b, \dot{\neg} a)$ und daher insbesondere $bew(fa,a)$. Die Rückrichtung $\Leftarrow$ ist offensichtlich. □

Schliesslich kommen wir zur Umkehrung von Satz 1.

Satz 9. *Jedes repräsentierbare Prädikat $P \subset \mathbb{N}^n$ ist rekursiv.*

Sei $\alpha(\vec{x})$ eine repräsentierende Formel für P. Da **PA** axiomatisierbar ist, können wir wieder eine Liste aller beweisbaren Aussagen erstellen. Für gegebenes $\vec{a}$ können wir dann einfach warten, bis entweder $\alpha(\underline{\vec{a}})$ oder $\neg\alpha(\underline{\vec{a}})$ erscheint. Also ist P entscheidbar.
In [1] wird erwähnt, dass man diesen Beweis ähnlich wie in Satz 8 formalisieren kann. Dem Autor ist allerdings nicht klar, wie das genau funktioniert.

Schliesslich kommen wir noch einmal auf die Substitution zurück. Im Vortrag über die *Gödelisierung von Formeln*, wurde die p.r. Funktion $(m,i,k) \longmapsto [m]_i^k$ definiert, mit der Eigenschaft

$$[\dot{\xi}]_{\dot{x}}^{\dot{t}} = (\dot{\xi}\frac{\dot{t}}{x}) \text{ für } \xi \in \boldsymbol{\mathcal{T}} \cup \boldsymbol{\mathcal{L}}, x \in \mathrm{Var}, t \in \boldsymbol{\mathcal{T}}.$$

Weiter bezeichne zf $a = \underline{\dot{a}}$ die Gödelzahl der Terms $\underline{a} = S^a 0$. Dann ist $a \longmapsto$ zf a p.r., da zf $0 = \underline{\dot{0}}$ und zf $Sa = \dot{S} * \text{zf } a$. Sei $\mathrm{sb}_x(m,a) = [m]_{\dot{x}}^{\text{zf } a}$, sowie $\mathrm{sb}_{\vec{x}} \in \boldsymbol{F}_{n+1}$ induktiv über die Länge von $\vec{x} \in \mathrm{Var}^n$, erklärt durch $\mathrm{sb}_\emptyset(m) = m$ und $\mathrm{sb}_{\vec{x}x}(m,\vec{a}a) = \mathrm{sb}_x(\mathrm{sb}_{\vec{x}}(m,\vec{a}),a)$. Dabei seien $x_1,\ldots,x_m,x$ paarweise verschieden. Als Verknüpfung von p.r. Funktionen sind alle $\mathrm{sb}_{\vec{x}}$ ebenfalls p.r. Schliesslich definieren wir noch $\dot{\alpha}(\underline{\vec{a}})$ als die Gödelzahl von $\alpha(\underline{\vec{a}})$. Dann gilt

Satz 10. *Für beliebiges $\alpha(\vec{x}) \in \boldsymbol{\mathcal{L}}$ und für alle $\vec{a} \in \mathbb{N}^n$ ist $sb_{\vec{x}}(\dot{\alpha},\vec{a}) = \dot{\alpha}(\underline{\vec{a}})$*

Beweis. Weil $\alpha(\underline{\vec{a}})$ durch schrittweise Ausführung einfacher Substitutionen entsteht, müssen wir lediglich $\mathrm{sb}_x(\dot{\alpha},a) = \dot{\alpha}(\underline{a})$ für alle $a \in \mathbb{N}$ zeigen. Dies gilt wegen $\mathrm{sb}_x(\dot{\alpha},a) = [\dot{\alpha}]_{\dot{x}}^{\text{zf } a} = [\dot{\alpha}]_{\dot{x}}^{\dot{\underline{a}}} = [\dot{\alpha}]_{\dot{x}}^{\underline{a}} = (\dot{\alpha}(\underline{a})) = \dot{\alpha}(\underline{a})$.

□

Literatur

[1] W. Rautenberg, „Einführung in die Mathematische Logik", Vieweg-Teubner, 2008