Rekursive und primitiv-rekursive Funktionen

Patrik Lengacher

02. Mai 2012

Dieses Handout richtet sich nach Kapitel 6.1 in [R]. Grundsätzlich wird dieselbe Notation wie in den vorhergehenden Vorträgen verwendet.
Im Folgenden bezeichnen nebst k, l, m, n auch a, b jeweils natürliche nichtnegative Zahlen. Weiter bezeichnet $\mathbb{N}$ die Menge der nichtnegativen Zahlen. Die Menge aller n-stelligen Funktionen mit Argumenten aus $\mathbb{N}^n$ und Werten aus $\mathbb{N}$ werde mit $\mathbf{F}_n$ bezeichnet. Die Menge $\mathbf{F}_0$ bezeichnet alle Konstanten, d.h. $\mathbf{F}_0 \cong \mathbb{N}$. Sind $h \in \mathbf{F}_m$ und $g_1, ..., g_m \in \mathbf{F}_n$, so heisse

$$f : \vec{a} \mapsto h(g_1\vec{a}, ..., g_m\vec{a})$$

die durch *Komposition* aus h und g_i entstehende Funktion, kurz $f = h[g_1, ..., g_m]$. Die Stellenzahl von f ist n. Analog sei $P[g_1, ..., g_m]$ für $P \subseteq \mathbb{N}^m$ das m-stellige Prädikat $\{\vec{a} \in \mathbb{N}^m | P(g_1\vec{a}, ..., g_m\vec{a})\}$.

Intuitiv gesprochen ist $f \in \mathbf{F}_n$ berechenbar, wenn es einen Algorithmus gibt, der zu jedem $\vec{a} \in \mathbb{N}^n$ den Wert $f\vec{a}$ in endlich vielen Schritten berechnet. Als Beispiele können Summen und Produkte betrachtet werden. Es gibt überabzählbar viele einstellige Funktionen über $\mathbb{N}$; davon können aber wegen der Endlichkeit einer jeden Berechnungsvorschrift nur abzählbar viele berechenbar sein.
Die im intuitiven Sinne berechenbaren Funktionen mit Argumenten und Werten aus $\mathbb{N}$ haben ganz offensichtlich die Eigenschaften

Oc: Mit $h \in \mathbf{F}_m$ und $g_1, \ldots, g_m \in \mathbf{F}_n$ ist auch $f = h[g_1, \ldots, g_m]$ berechenbar.

Op: Sind $g \in \mathbf{F}_n$ und $h \in \mathbf{F}_{n+2}$ berechenbar, so auch $f \in \mathbf{F}_{n+1}$, bestimmt durch

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

die sogenannten *Rekursionsgleichungen*. Weiter heisst f die aus g, h durch primitive Rekursion entstehende Funktion und werde auch als $f = \mathbf{Op}(g, h)$ notiert.

Definition 1. Sei $g \in \mathbf{F}_{n+1}$ und es gilt $\forall\vec{a}\exists b g(\vec{a}, b) = 0$, so bezeichnet $\mu_b[g(\vec{a}, b) = 0]$ das kleinste b mit $g(\vec{a}, b) = 0$.

Oμ: Ist $g \in \mathbf{F}_{n+1}$ und gilt $\forall\vec{a}\exists b g(\vec{a}, b) = 0$, so ist auch $\mu_b[g(\vec{a}, b) = 0]$ berechenbar.

Die Eigenschaften **Oc** ,**Op** und **O**μ können als Erzeugungsoperationen zur Gewinnung neuer Funktionen gesehen werden.

Definition 2. Die Menge der *primitiv-rekursiven* (p.r.) Funktionen bestehe aus allen Funktionen über $\mathbb{N}$, die sich mittels **Oc** und **Op** erzeugen lassen aus folgenden *Anfangsfunktionen* bzw. *Basisfunktionen*:

- die Konstante 0,
- die Nachfolgerfunktion $\mathtt{S} : \mathbb{N} \to \mathbb{N}, a \mapsto a + 1$,
- die Projektionsfunktion $I^n_\nu \in \mathbf{F}_n, (a_1, \dots a_n) \mapsto a_\nu, \quad 1 \leq \nu \leq n$.

Definition 3. Die Menge der p.r. rekursiven Funktionen zusammen mit der Operation $\mathbf{O}\mu$ erhält man die Menge aller *rekursiven* Funktionen, auch μ-rekursiven Funktionen genannt.

Bemerkung 4. Man erkennt, dass die p.r. Funktionen mit einem im Prinzip abschätzbarem Aufwand berechenbar sind. Während die Existenzbedingung $\forall \vec{a} \exists m P(\vec{a}, m)$ der rekursiven Funktionen nicht konstruktiv sein kann, so dass selbst grobe Abschätzungen über den Berechnungsaufwand unmöglich sind.

Beispiel 5. Ein berühmtes Beispiel für eine rekursive aber nicht p.r. Funktion, ist die *Ackermann-Funktion* $\circ \in \mathbf{F}_2$ definiert durch

$$0 \circ b = \mathtt{S}b \quad ; \quad \mathtt{S}a \circ 0 = a \circ 1 \quad ; \quad \mathtt{S}a \circ \mathtt{S}b = a \circ (\mathtt{S}a \circ b)$$

Für den Beweis wird auf [F] verwiesen.

Bemerkung 6. Man sieht leicht, dass mit jeder Funktion f auch jede Funktion p.r. bzw. rekursiv ist, die aus f durch *Vertauschung, Hinzufügen von fiktiven Argumenten oder Gleichsetzung* hervorgeht. Hierbei geht $h : \mathbb{N} \to \mathbb{N}$ aus $f : \mathbb{N}^2 \to \mathbb{N}$ durch Gleichsetzung hervor, falls $h := f[I^1_1, I^1_1]$ gilt.

Beweis. Sei $f \in \mathbf{F}_2$. Für $g := f[I^2_2, I^2_1]$ ist dann $g(a, b) = f(b, a)$. Für $h := f[I^1_1, I^1_1]$ ist $ha = f(a, a)$, und für $f' := f[I^3_1, I^3_2]$ ist $f'(a, b, c) = f(a, b)$, wobei hier die fiktive Variable c hinzugefügt wurde. Analog für höherstellige Funktionen. □

Beispiel 7. Sei $\mathtt{S}^0 = I^1_1$ und $S^{k+1} = \mathtt{S}[\mathtt{S}^k]$, so offenbar

$$\begin{aligned} \mathtt{S}^k : \mathbb{N} &\to \mathbb{N} \\ a &\mapsto a + k. \end{aligned}$$

Diese einstelligen Funktionen sind nach **Oc** alle p.r.

Fakt 8. Die n-stelligen konstanten Funktionen

$$\begin{aligned} K^n_c : \mathbb{N} &\to \mathbb{N} \\ \vec{a} &\mapsto c \end{aligned}$$

sind primitiv rekursiv.

Beweis. Mit **Op** sieht man leicht dass, $K^0_0 = 0$, $K^0_c = \mathtt{S}^c[0]$, sowie $K^1_c 0 = K^0_c = c$ und $K^1_c \mathtt{S}b = I^2_2(b, K^1_c b)$. Für $n > 1$ hat man $K^n_c = K^1_c[I^n_1]$. □

Fakt 9. Die Additionsfunktion $f : \mathbb{N}^2 \to \mathbb{N}$ definiert durch $g(x, y) = x + y$ ist p.r.

Beweis. Sei $g(y) := I_1^1(y) = y$ und $hh(x,y,z) := \mathtt{S}(I_3^3(x,y,z))(= \mathtt{S}(z))$. Da h_1 eine Basisfunktion ist, ist sie auch primitiv rekursiv. Analog ist h eine Komposition von Basisfunktionen, also auch primitiv rekursiv. Nun definieren wir $f(x,y)$ durch primitive Funktionen mittels **Op**:

$$\begin{aligned} f(0,y) &= g(y) = y \text{ und} \\ f(x+1,y) = h(x,y,g(x,y)) &= \mathtt{S}(f(x,y)) = f(x,y)+1. \end{aligned}$$

Folglich ist auch $f(x,y)$ p.r. □

Fakt 10. Die Multiplikationsfunktion $f : \mathbb{N}^2 \to \mathbb{N}$ definiert durch $f(x,y) = x \cdot y$ ist p.r.

Beweis. Durch $a \cdot 0 = h(a,0) = K_0^1 a = 0$ sowie $f(a,\mathtt{S}b) = a \cdot \mathtt{S}b = a \cdot b + a = I_3^3(a,b,a\cdot b) + I_1^3(a,b,a\cdot b)$ gewinnt man die Multiplikation, i.e. durch Anwendung von **Op, Oc** und Fakt 9. □

Fakt 11. Die „gestutzte“ Subtraktion definiert durch

$$a \dot{-} b = \begin{cases} a-b & \text{,falls } b \le a \\ 0 & \text{,sonst} \end{cases}$$

ist primitiv rekursiv. Insbesondere ist auch die absolute Differenz primitiv rekursiv, denn

$$|a-b| = (a \dot{-} b) + (b \dot{-} a).$$

Beweis. Die Vorgängerfunktion $\mathtt{R}$ definiert durch

$$\mathtt{R}0 := 0 \quad ; \quad \mathtt{R}(\mathtt{S}b) := I_1^2(b, \mathtt{R}b) = b$$

ist primitiv rekursiv.

Mit den Rekursionsgleichungen schreibt man

$$\begin{aligned} a \dot{-} 0 &= I_1^1(a) = a \text{ und} \\ a \dot{-} \mathtt{S}b &= \mathtt{R}(a \dot{-} b) = \mathtt{R}I_3^3(a,b,a \dot{-} b). \end{aligned}$$

□

Fakt 12. Mit $f \in \mathbf{F}_{n+1}$ ist auch $(\vec{a},b) \mapsto \prod_{k<b} f(\vec{a},k)$ primitiv rekursiv, definiert durch

$$\begin{aligned} \prod_{k<0} f(\vec{a},k) &= 1 \\ \prod_{k<\mathtt{S}b} f(\vec{a},k) &= \left(\prod_{k<b} f(\vec{a},k)\right) \cdot f(\vec{a},b). \end{aligned}$$

Ebenso ist $(\vec{a},b) \mapsto \sum_{k<b} f(\vec{a},k)$ primitiv rekursiv, definiert durch

$$\begin{aligned} \sum_{k<0} f(\vec{a},k) &= 0 \\ \sum_{k<\mathtt{S}b} f(\vec{a},k) &= \left(\sum_{k<b} f(\vec{a},k)\right) + f(\vec{a},b). \end{aligned}$$

Definition 13.
- Die δ-Funktion wird definiert durch $\delta 0 = 1$ und $\delta \mathtt{S} n = 0$.
- Weiter wird die sg-Funktion definiert durch $\operatorname{sg} 0 = 0$, und $\operatorname{sg} \mathtt{S} n = 1$.

Nach Definition sind beide Funktionen primitiv rekursiv.

Definition 14. Ein Prädikat $P \subseteq \mathbb{N}^n$ heisst *p.r. bzw. rekursiv*, wenn die charakteristischte Funktion

$$\mathcal{X}_P : \vec{a} \mapsto \begin{cases} 1 & , \vec{a} \in P \\ 0 & , sonst \end{cases}$$

p.r. bzw. rekursiv ist.

Fakt 15.
- Das Prädikat $=$ ist p.r.
- Jede endliche Teilmenge ist p.r.
- Das Prädikat $\neq$ ist p.r.

Beweis. Das Prädikat $=$ kann man mittels Identitätsrealtion schreiben als $\mathcal{X}_=(a,b) = \delta|a-b|$ und ist folglich primitiv rekursiv. Das wiederum impliziert, dass jede endliche Teilmenge $E = \{a_1, \ldots, a_n\}$ von $\mathbb{N}$, wobei , a_i paarweise verschieden sind, ist primitiv rekursiv. Denn $\mathcal{X}_\emptyset = K_0^1$ und $\mathcal{X}_E(a) = \mathcal{X}_=(a, a_1) + \cdots + \mathcal{X}_=(a, a_n)$ für $E \neq \emptyset$. Das Prädikat $\neq$ ist prmitiv rekursiv, weil $\mathcal{X}_\neq(a,b) = \operatorname{sg}|a-b|$. □

Die δ-Funktion ergibt die Abgeschlossenheit der p.r. bzw. rekursiven Funktionen gegenüber Definition durch p.r. (bzw. rekursive) Fallunterscheidung:

Lemma 16. [Fallunterscheidung] Mit P, g, g' ist auch h p.r. (bzw. rekursiv), definiert durch

$$h\vec{a} = g\vec{a} \cdot \mathcal{X}_P(\vec{a}) + g'\vec{a} \cdot \delta(\mathcal{X}_P(\vec{a})), \text{ d.h.}$$

$$h\vec{a} = \begin{cases} g\vec{a}, & \text{falls } P\vec{a}, \\ g'\vec{a}, & \text{falls } \neg P\vec{a}. \end{cases}$$

Beispiel 17. Der Divisionsrest von $a|b$ wird definiert durch

$$\operatorname{rest}(0, b) := 0,$$

$$\operatorname{rest}(\mathtt{S}a, b) := \begin{cases} \mathtt{S} \operatorname{rest}(a,b) \text{ für } \operatorname{rest}(a,b) < b \dot{-} 1 \\ \operatorname{rest}(\mathtt{S}a, b) = 0 \text{ sonst.} \end{cases}$$

Es bleibt zu zeigen, dass rest p.r. ist. Sei $h(a,b,c) = \mathtt{S}c$, falls $c < b \dot{-} 1$ und $h(a,b,c) = 0$ sonst, ist nach Lemma 16 primitiv rekursiv. Wir können nun rest mit h und den Rekursionsgleichungen schreiben als $\operatorname{rest}(\mathtt{S}a, b) = h(a, b, \operatorname{rest}(a,b))$.

Von grundlegender Bedeutung, speziell für die Gewinnung von Unentscheidbarkeitsresultaten, ist die Hypothese, dass die rekursiven Funktionen alle irgendwie berechenbaren Funktionen über $\mathbb{N}$ bereits ausschöpfen, die sogenannte *Churchsche These*. Der Definition der rekursiven Funktionen ist dies kaum anzusehen, aber alle auf unterschiedliche Weise definierten Berechenbarkeitskonzepte erwiesen sich als äquivalent und stützen die These.

Nun kommen wir zu einer Zusammenstellung beweisbarer Grundfakten über primitiv und μ-rekursive Prädikate. P, Q, R bezeichnen jetzt aussschliesslich Prädikate über $\mathbb{N}^n$. Um die formale Niederschrift von Eigenschaften solcher Prädikate zu erleichtern, benutzen wir weitere metasprachliche Abkürzungen wie $\exists$ und $\forall$.

Definition 18. Man sagt $P' \subseteq \mathbb{N}^{n+1}$ gehe aus $P \subseteq \mathbb{N}^n$ durch *Hinzufügung von fiktiven Argumenten* hervor, falls $P' = \{(p_1, \ldots, p_{n+1}) | (p_1, \ldots, p_n) \in P\}$.

Lemma 19. Die Menge der p.r. bzw. rekursiven Prädikate ist abgeschlossen gegenüber Komplementbildung, Vereinigung, und Durchschnitt von Prädikaten derselben Stellenzahl. Weiter ist diese Menge abgeschlossen gegenüber Einsetzung p.r. bzw. rekursiver Funktionen sowie gegenüber Gleichsetzung, Vertauschung und Hinzufügung von fiktiven Argumenten.

Beweis. Für $P \subseteq \mathbb{N}^n$ ist $\delta[\mathcal{X}_P]$ gerade die charakteristische Funktion von $\neg P = \mathbb{N}^n \setminus P$; ferner ist offenbar $\mathcal{X}_{P \cup Q} = \mathrm{sg}[\mathcal{X}_P + \mathcal{X}_Q]$, $\mathcal{X}_{P \cap Q} = \mathcal{X}_P \cdot \mathcal{X}_Q$ und $\mathcal{X}_{P[g_1,\ldots,g_m]} = \mathcal{X}_P[g_1, \ldots, g_m]$. Die übrigen Abgeschlossenheitseigenschaften folgen einfach aus den entsprechenden Eigenschaften der charakteristischen Funktionen und Bemerkung 6. □

Definition 20. Seien $P, Q, \cdots \subseteq \mathbb{N}^{n+1}$. Ist

$$\begin{aligned} Q(\vec{a}, b) &\Leftrightarrow (\forall k < b) P(\vec{a}, k) \\ R(\vec{a}, b) &\Leftrightarrow (\exists k < b) P(\vec{a}, k) \\ Q'(\vec{a}, b) &\Leftrightarrow (\forall k \leq b) P(\vec{a}, k) \text{ und} \\ R'(\vec{a}, b) &\Leftrightarrow (\exists k \leq b) P(\vec{a}, k) \end{aligned}$$

sagt man Q, R, Q', R' entstünden aus P durch beschränkte Quantifizierung.

Bemerkung 21. Die Menge der p.r. bzw. rekursiven Funktionen ist abgeschlossen bezüglich beschränkter Quantifizierung. Mit P p.r. sind alle diese Prädikate p.r. So ist $\mathcal{X}_Q(\vec{a}, b) = \prod_{k<b} \mathcal{X}_P(\vec{a}, k)$ und $\mathcal{X}_R(\vec{a}, b) = \mathrm{sg}(\sum_{k<b} \mathcal{X}_P(\vec{a}, k))$ sowie $\mathcal{X}'_Q(\vec{a}, b) = \prod_{k<\mathtt{S}b} \mathcal{X}_P(\vec{a}, k)$ und $\mathcal{X}'_R(\vec{a}, b) = \mathrm{sg}(\sum_{k<\mathtt{S}b} \mathcal{X}_P(\vec{a}, k))$.

Fakt 22. Das Prädikat „a teilt b“ kurz $a|b$ ist p.r.

Beweis. Das Prädikat $a|b$ schreibt man mittels beschränkter Quantifizierung als $a|b \Leftrightarrow (\exists k \leq b)[a \cdot k = b]$. □

Beispiel 23. Das Prädikat „prim“ ist p.r, da $\mathrm{prim}\, p \Leftrightarrow p \neq 0, 1 \& (\forall k < p)[k|p \Rightarrow k = 1]$ p.r., denn $a|p \Rightarrow a = 1$ ist gleichwertig zu $a \nmid p \vee a = 1$ und als Vereinigung p.r. Prädikate wieder p.r.

Wir wollen abschliessend den Unterschied zwischen den p.r. und rekursiven Funktionen etwas deutlicher machen.

Fakt 24. Erfülle $P \subseteq \mathbb{N}^{n+1}$ die Bedingung $\forall \vec{a} \exists m P(\vec{a}, m)$. Sei $\mu_k[P(\vec{a}, k)]$ die Funktion $\mathbb{N}^n \to \mathbb{N}$, welche $\vec{a}$ das kleinste k mit $P(\vec{a}, k)$ zuordnet. Dann mit $\mathbf{O}\mu$ ist auch $\mu_k[\delta \mathcal{X}_P(\vec{a}, k) = 0]$; rekursiv, in der Regel aber nicht p.r.

Andererseits können wir die beschränkten μ-Operationen

$$\mu_{k \leq m}[P(\vec{a}, k)] = \begin{cases} \text{kleinstes } k \leq m \text{ mit } P(\vec{a}, k), \text{ falls ein solches } k \text{ existiert,} \\ m \text{ sonst, d.h. } \neg P(\vec{a}, k) \text{ für alle } k \leq m \end{cases}$$

betrachten.

Lemma 25. Mit P ist auch $\mu_{k \leq m}[P(\vec{a}, k)]$ primitiv rekursiv.

Beweis. Schreibe $f := \mu_{k\leq m}[P(\vec{a},k)]$. So ist $f(\vec{a},0) = 0$, sowie $f(\vec{a},\mathtt{S}m) = f(\vec{a},m)$ falls $(\exists k \leq m)P(\vec{a},k)$, und sonst ist $f(\vec{a},\mathtt{S}m) = \mathtt{S}m$. In der normierten Notation $f = \mathbf{Op}(g,h)$ bedeutet dies wie bei rest eine p.r. Fallunterscheidung in der Definition von h. Also ist f p.r.

□

Beispiel 26. Ist p eine Primzahl, so ist $p!+1$ gewiss durch keine Primzahl $q \leq p$ teilbar; denn $q|p!+1$ und $q|p!$ liefern den Widerspruch $q|1$. Ein Primteiler von $p!+1$ ist also eine neue Primzahl. Daher ist die kleinste auf p folgende Primzahl $\leq p!+1$. Also ist $n \mapsto p_m$ wohldefiniert und charakterisiert durch

$$p_0 = 2 \quad ; \quad p_{n+1} = \mu_{q\leq p_n!+1}[q\,\mathrm{prim}\,\&q > p_n] \tag{1}$$

Die Gleichung (1) ist eine Anwendung von **Op**. Denn mit $f : (a,b) \mapsto \mu_{q\leq b}[q\,\mathrm{prim}\,\&q > a]$ ist auch $g : a \mapsto f(a,a!+1)$ p.r. und die zweite Gleichung in (1) lässt sich einfach schreiben als $p_{n+1} = g(p_n)$. Folglich ist die Primzahlaufzählung $n \mapsto p_n$ p.r.

Literatur

[R] W. Rautenberg, Einführung in die Mathematisch Logik, Vieweg-Teubner, 2008

[F] W. Felscher, Berechenbarkeit, Springer, 1993