Rogers Kap 1–7

Nach einem Abschnitt über Notation beginnt Rogers mit dem Konzept der Algorithmen und nimmt als Beispiel die primitiv-rekursiven Funktionen. Das konkrete Modell ist irrelevant, denn es geht um den Begriff der berechenbaren Funktion als solche. Interessant sind 5 Merkmale, die allen Algorithmen gemeinsam sind und 5 Fragen, die man üblicherweise beantworten muß. (*1 .. *10)

§1.3 stellt fest, daß man zwischen Algorithmen (intensional) und berechenbaren Funktionen (extensional) unterscheiden muß. Letztere werden durch ihre Eigenschaften beschrieben und es ist nicht immer klar, wie man einen Algorithmus findet – wenn dies überhaupt möglich ist. §1.4 erklärt die Beweismethode der Diagonalisierung am Beispiel, daß es keine universelle primitiv-rekursive Funktion geben kann.

1 Formale Berechenbarkeitsbegriffe

Turingmaschinen sind bis auf notationelle Abweichungen bekannt und für die Kapitel ab $5 irrelevant. Wir brauchen sie nur, um einen Beweis des UTM und SMN Theorems geben zu

Kleene's Ansatz ist uns nicht so bekannt, aber es lohnt sich nicht, länger darauf einzugehen. Programme sind *Rekursionsgleichungen*, die durch Einsetzen ausgewertet werden.

Satz: *Die Berechenbarkeitsbegriffe von Turing, Kleene und anderen sind äquivalent und können effektiv ineinander übersetzt werden.*

Definition: Die Funktionen der obigen Klasse heißen *(partiell) rekursive Funktionen*. Läßt man das Wort "partiell"weg, so ist bei Rogers meist "total" gemeint. Ich verwende zur Äbkürzung manchmal $\mathcal{R}$ bzw. $\mathcal{TR}$

Church's These besagt daß die Klasse der rekursiven Funktionen genau die Klasse der intuitiv berechenbaren Funktionen beschreibt. Statt "rekursiv"sagt man auch effektiv, berechenbar etc.

Berechenbarkeit auf anderen Mengen als $\mathbb{N}$ kann durch Codierungen (oder *Numerierungen*) beschrieben werden. Hierzu benötigt man eine Bijektion $\gamma{:}C{\to}\mathbb{N}$.

Definition: Eine Funktion $g : C{\to}C$ ist *γ-berechenbar* (oder kurz *berechenbar / rekursiv*), wenn es eine rekursive Funktion $f : \mathbb{N}{\to}\mathbb{N}$ gibt, so daß $g = \gamma^{-1} f \gamma$ ist.

Zur Illustration nimmt man Diagramme, so wie auf Seite 28.

1.1 Standardnumerierung berechenbarer Funktionen

Dies haben wir in der Vorlesung ausführlich besprochen. Wir codieren Turingmaschinen als Wörter, zählen alle Wörter über dem entsprechenden Alphabet auf und eliminieren solche, die keine Turingmaschinen darstellen. Dies liefert eine bijektive Numerierung aller Turingmaschinen: M_i sei die Turingmaschine, deren Codierung hierbei an i-ter Stelle erscheint.

Daraus leiten wir eine Numerierung der berechenbaren Funktionen ab. Es sei $r_b{:}\mathbb{N}{\to}\{0,1\}^*$ die Binärcodierung der natürlichen Zahlen. Die Standardnumerierung $\varphi{:}\mathbb{N}{\to}\mathcal{R}$ der berechenbaren Funktionen ist definiert durch $\varphi(i) = r_b^{-1}{\circ}f_{M_i}{\circ}r_b$. Die Schrittzahlfunktion $\Phi{:}\mathbb{N}{\to}\mathcal{R}$ ist definiert durch $\Phi(i)(n) = t_{M_i}(r_b(n))$. Anstelle von $\varphi(i)$ und $\Phi(i)$ schreiben wir meist φ_i bzw. Φ_i. Die Nummer i wird auch die *Gödelnummer* oder *Index* von φ_i genannt. Rogers geht auf derartige Details nicht ein, sondern nimmt einfach an, daß wir eine solche Numerierung der berechenbaren Funktionen haben.

Satz: *es gibt abzählbar unendlich viele (partiell) rekursive Funktionen.*

Satz: *es gibt Funktionen auf $\mathbb{N}$, die nicht rekursiv sind.*

Satz: *jede (partiell) rekursive Funktion hat abzählbar unendlich viele Indizes (Gödelnummern)*

UTM Theorem: *Die Funktion $u{:}\mathbb{N}{\to}\mathbb{N}$ mit $u\langle i,n\rangle{=}\varphi_i(n)$ ist rekursiv.*

SMN Theorem: *Es gibt Funktion $s \in \mathcal{TR}$ mit $\varphi_{s\langle m,n\rangle}(i) = \varphi_m\langle n,i\rangle$ für alle $m,n,i \in \mathbb{N}$.*

Hiervon gibt es viele Variationen. Die gängigsten sind

Satz: *Für jede Funktion $h \in \mathcal{R}$ gibt es ein $g \in \mathcal{TR}$ mit der Eigenschaft $\varphi_{g(i)}(n) = h\langle i,n\rangle$ für alle $n,i \in \mathbb{N}$.*

Satz: *Es gibt Funktion $h \in \mathcal{TR}$ mit $\varphi_{h\langle i,j\rangle} = \varphi_i \circ \varphi_j$*

Kleene Normalform Theorem: *Es gibt rekursive Funktionen $p:\mathbb{N}\to\mathbb{N}$ und $t:\mathbb{N}^3\to\mathbb{N}$, so daß $\varphi_i(x) = g(\mu_y[t(i,x,y)=0]$ für alle $i,x\in\mathbb{N}$ gilt.*

Das Theorem gilt analog für mehrstellige Funktionen, aber das ist wegen der Standard-Tupelfunktion eigentlich nicht weiter wichtig. Rogers gibt auch einen Beweis nahe an Kleene's Original.

1.2 Unentscheidbare Probleme

Das Halteproblem $H = \{\langle i,n\rangle \mid n \in \text{domain}(\varphi_i)\} = \{\langle i,n\rangle \mid \varphi_i(n)\ konvergiert\}$

Satz: *Das Halteproblem ist unentscheidbar.*

Formulierung a'la Rogers: *es gibt keine rekursive Funktion h mit* $h\langle i,n\rangle = \begin{cases} 1 & \varphi_i(n)\ konvergiert \\ 0 & sonst \end{cases}$

Beweis durch Diagonalsisierung

Selbstanwendbarkeitsproblem: $S = \{i \mid i \in \text{domain}(\varphi_i)\} = \{i \mid \varphi_i(i)\ konvergiert\}$

Satz: *Das Selbstanwendbarkeitsproblem ist unentscheidbar*

Totalitätsproblem: $TR = \{i \mid \varphi_i \text{ total}\}$

Satz: *Das Totalitätsproblem ist unentscheidbar*

Theorem XI wird formuliert als Aussage über ein beliebiges Berechnungsmodell um Frage *10 zu beantworten. Bei terminierenden Berechnungen gibt es keine berechenbare obere Rechenzeitgrenze. Reformuliert in Φ-Notation heißt dies

Satz: *Es gibt keine berechenbare Funktion $f:\mathbb{N}^2\to\mathbb{N}$ mit $\Phi_i(x)\le f(i,x)$ für alle $i\in\mathbb{N}$, $x\in domain(\varphi_i)$.*

2 Weitere unlösbare Probleme

Rogers erwähnt, daß es zwei Arten gibt, Unlösbarkeit zu zeigen – direkt, üblicherweise mit *Diagonalisierung* – und indirekt, d.h. mit *Reduktion*. Letztere wird §6–9 ausführlich diskutiert und verfeinert. Im Rest dieses Kapitels führt er eine Reihe von unlösbaren Problemen aus verschiedenen Bereichen auf und gibt Beweise. Anstelle von *entscheidbar* verwendet er *recursively unsolvable*. Die Probleme werden verbal beschrieben. Ich gebe stattdessen formale kurze Beschreibungen

Satz: *Die Menge* $CONST = \{i \mid \exists k\ \forall j\ \ \varphi_i(j) = k\}$ *ist unentscheidbar*

Beweis Sei $h:\mathbb{N}\to\mathbb{N}$ definiert durch $h\langle i,n\rangle = \begin{cases} 0 & \varphi_i(i)\ konvergiert \\ \perp & sonst \end{cases}$

Dann ist $h = c_0^1 \circ u \circ (pr_1^2, pr_1^2)$, also berechenbar. Nach dem smn-Theorem gibt es also eine berechenbare totale Funktion $g{:}\mathbb{N}\to\mathbb{N}$ mit der Eigenschaft $\varphi_{g(i)}(n) = h\langle i,n\rangle$ für alle $n,i\in\mathbb{N}$,

also $\varphi_{g(i)} = \begin{cases} c_0^1 & \varphi_i(i)\ konvergiert \\ f_\perp & sonst \end{cases}$ bzw. $\begin{cases} \varphi_{g(i)} \in CONST & i\in S \\ \varphi_{g(i)} \notin CONST & sonst \end{cases}$

Wäre $CONST$ entscheidbar, dann wären χ_{CONST} und $\chi_{CONST}\circ g$ totale berechenbare Funktionen und wir hätten $(\chi_{CONST}\circ g)(i)) = \begin{cases} 1 & i\in S \\ 0 & sonst \end{cases}$. Damit wäre die charakteristische Funktion des Selbstanwendbarkeitsproblems berechenbar, was bekanntlich nicht der Fall ist. □

Satz: *Die Menge* $RG = \{\langle i,j\rangle \mid j \in range(\varphi_i)\}$ *ist unentscheidbar*

Satz: *Die Menge* $CORRECT = \{\langle i,j,k\rangle \mid \varphi_i(j) = k\}$ *ist unentscheidbar*

Satz: *Die Menge* $EQ = \{\langle i,j\rangle \mid \varphi_i = \varphi_j\}$ *ist unentscheidbar*

Satz: *Die Menge* $RG_j = \{i \mid j \in range(\varphi_i)\}$ *ist unentscheidbar*

Satz: *Die Menge* $RG_i = \{j \mid j \in range(\varphi_i)\}$ *ist für manche i entscheidbar, für andere nicht*

Die anderen Beweise sind ebenfalls Reduktionsbeweise. Im Prinzip sind all diese Mengen Spezialfälle des Satz von Rice, den wir in der Vorlesung bewiesen hatten.

Satz von Rice: *Für $\emptyset \neq P \subset \mathcal{R}$ ist $L_P = \{i \mid \varphi_i \in P\}$ unentscheidbar*

Der Beweis ist so ähnlich wie der oben angegebene. In Rogers ist das eine Übungsaufgabe.

§2.2 erwähnt unlösbare Probleme aus der Mathematik wie Gödels Unvollständigkeitssätze oder Hilbert's zehntes Problem. Dies wird aber nicht weiter vertieft und erst am Ende des Buches wieder aufgegriffen. §2.3 diskutiert weitere unlösbare Probleme, die das Verhalten partiell-rekursiver Funktionen betreffen, die eher pathologischer Natur sind. So gibt es partiell-rekursive Funktionen, die sich nicht zu einer total-rekursiven Funktion fortsetzen lassen.

Satz: *Es gibt eine partiell-rekursive Funktion $g{:}\mathbb{N}{\to}\mathbb{N}$ so daß für jede total-rekursive Funktion $f{:}\mathbb{N}{\to}\mathbb{N}$ ein $i \in domain(g)$ existiert mit $g(i) \neq f(i)$*

Beweis Wir konstruieren g durch Diagonalisierung.

Sei $g : \mathbb{N}{\to}\mathbb{N}$ definiert durch $g(i) = \begin{cases} \varphi_i(i){+}1 & \varphi_i(i)\ konvergiert \\ \perp & sonst \end{cases}$ und $f{:}\mathbb{N}{\to}\mathbb{N}$ total-rekursiv, also $f = \varphi_j$. Da f total ist, konvergiert $\varphi_j(j)$ und wir haben $g(j) = \varphi_j(j){+}1 \neq \varphi_j(j) = f(j)$. □

Satz: *Es gibt eine Funktion $g \in \mathcal{R}$ so daß für jede total-rekursive Funktion $f : \mathbb{N}^2{\to}\mathbb{N}$ gilt $g \neq \mu f$.*

Beweis Sei $g : \mathbb{N}{\to}\mathbb{N}$ definiert durch $g(i) = \begin{cases} i & \varphi_i(i)\ konvergiert \\ \perp & sonst \end{cases}$ und $f : \mathbb{N}^2{\to}\mathbb{N}$ total-rekursiv mit $g = \mu f$. Dann ist $f(i,i) = 0$, wenn $\varphi_i(i)$ konvergiert, und $f(i,j) \neq 0$ für alle j, wenn $\varphi_i(i)$ nicht konvergiert, insbesondere also auch $f(i,i) \neq 0$. Damit wäre $\chi_S = f \circ (pr_1^1, pr_1^1)$ berechenbar, was bekanntlich nicht der Fall ist. □

In §3 bespricht Rogers die Ziele des Buches. Diese werden wir im Laufe des Seminars der Reihe nach ansprechen. Es gibt keine technischen Aussagen, Definitionen oder Sätze.

4 Rekursive Invarianz

Ziel dieses Kapitels ist es, bestimmte Eigenschaften von Mengen, Funktionen und partiellen Funktionen über natürlichen Zahlen, die in den späteren Kapiteln immer wieder zur Sprache kommen, isoliert zu besprechen. Dabei geht es speziell um *Räume* (Mengen) und *Gruppen* von Transformatione auf diesen Räumen, die wir mit $\mathcal{K}$ und $\mathcal{G}$ bezeichnen.

Eine Eigenschaft auf Mengen heißt *$\mathcal{G}$-invariant*, wenn sie unter Anwendung von Transformationen aus $\mathcal{G}$ erhalten bleibt. Die Theorie der $\mathcal{G}$-invarianten Eigenschaften wird von Rogers als *$\mathcal{G}$-Theorie* bezeichnet. Diese Vorgehensweise dient i.w. dazu einen prägnanten Begriffsapparat einzuführen, der später das Argumentieren erleichtern soll.

Zwei Teilmengen A und B von $\mathcal{K}$ heißen *$\mathcal{G}$-isomorph* (im Zeichen $A \equiv_{\mathcal{G}} B$), wenn $B = g(A)$ für ein $g \in \mathcal{G}$ ist. Da $\mathcal{G}$ eine Gruppe ist, ist $\equiv_{\mathcal{G}}$ eine Äquivalenzrelation und die Äquivalenzklassen von $\mathcal{K}$ unter $\equiv_{\mathcal{G}}$ heißen *$\mathcal{G}$-isomorphe Typen*. Damit sind $\mathcal{G}$-invariante Eigenschaften genau die Eigenschaften die unter $\mathcal{G}$-Isomorphie wohldefiniert sind - sie gelten für alle Elemente eines $\mathcal{G}$-isomorphen Typs $\mathcal{J}$ oder für keine. Die Menge aller Eigenschaften, die für $\mathcal{J}$ gelten, sind die *vollständige Menge der Invarianten für $\mathcal{J}$*.

Mann kann all diese Begriffe auch auf Relationen über $\mathcal{K}$ fortsetzen.

Definition: $\mathcal{G}^* = \{f \in \mathcal{TR} \mid f \text{ bijektiv}\}$ ist die Gruppe der *rekursiven Permutationen*
Zwei Mengen $A \subseteq \mathbb{N}$ und $B \subseteq \mathbb{N}$ heißen *rekursiv isomorph* (im Zeichen $A \equiv B$), wenn $A \equiv_{\mathcal{G}^*} B$.
$\mathcal{G}^*$-isomorphe Typen heißen *rekursiv isomorphe Typen*. *Rekursive Invarianz* ist $\mathcal{G}^*$-invarianz.

Die Begriffe gelten analog für Mengen von Tupeln, Relationen und auch für Funktionen (die man ja als Mengen betrachten kann). Nahezu alle Konzepte, die wir im Laufe des Seminars diskutieren werden, sind rekursiv invariant. Beispiele auf Seite 52.

Satz: *Zwei partielle Funktionen f und g sind rekursiv isomorph, wenn $f = h^{-1}\circ g\circ h$ für ein $h\in\mathcal{G}^*$.*

Beweis Ist $f\equiv g$, dann gilt $g{=}h(f)$ für ein $h\in\mathcal{G}^*$, d.h. $\{(x, g(x)) \mid x\in\mathbb{N}\} = \{h(z, f(z)) \mid z\in\mathbb{N}\} = \{(h(z), h(f(z))) \mid z\in\mathbb{N}\} = \{(x, h(f(h^{-1}(x)))) \mid x\in\mathbb{N}\}$, also $g(x) = h(f(h^{-1}(x)))$ für alle $x\in\mathbb{N}$ bzw. $g = h\circ f\circ h^{-1}$, woraus die Behauptung folgt. □

Ein etwas schwächeres Konzept als Isomorphie ist Ähnlichkeit

Definition: *g ähnelt f*, wenn $f = h^{-1}\circ g\circ h'$ für zwei $h, h'\in\mathcal{G}^*$.

Auch dies ist eine Äquivalenzrelation, die zu *Ähnlichkeitsklassen* führt.

Rogers will nun das Konzept der *universellen Funktion* so verallgemeinern, daß es rekursiv invariant ist. Was nicht funktioniert ist eine Definition wie $\psi\in\mathcal{R}^{(2)}$ *ist universell, wenn* $\forall x, y.\psi(x, y) = \varphi_x(y)$, da die hierzu isomorphe Funktion $\psi' = h^{-1}\circ\psi\circ h$ nicht mehr universell wäre.

Definition: *$\psi\in\mathcal{R}^{(1)}$ ist universell, wenn $\forall x, y.\psi(f(x, y)) = \varphi_x(y)$ für ein $f\in\mathcal{TR}$ ist.*

Satz: *Wenn ψ universell ist und $h, h'\in\mathcal{G}^*$, dann ist $\psi' = h^{-1}\circ\psi\circ h'$ universell.*

Beweis Sei $\forall x, y.\psi(f(x, y)) = \varphi_x(y)$. Wegen des smn-Theorems gibt es $g\in\mathcal{TR}$ mit $\varphi_{g(x)} = h\circ\varphi_x$ für alle x. Definiere $f'(x, y) = h'^{-1}(f(g(x), y))$. Dann ist $f'\in\mathcal{TR}$ und für beliebige x, y:

$$\begin{aligned}\psi'(f'(x, y)) &= h^{-1}\circ\psi\circ h\circ h'^{-1}(f(g(x), y)) = h^{-1}\circ\psi(f(g(x), y)) = h^{-1}(\varphi_{g(x)}(y)) \\ &= h^{-1}(h(\varphi_x(y))) = \varphi_x(y)\end{aligned}$$

□

Damit ist Universalität abgeschlossen unter Ähnlichkeit und insbesondere rekursiv invariant.

5 Entscheidbare und Aufzählbare Mengen

In diesem Kapitel werden einige Begriffe präzisiert, die bisher implizit genutzt werden. Die meisten sind aus der Vorlesung TI-2 bekannt.

Definition: Eine Menge A ist *rekursiv* (oder *entscheidbar*), wenn χ_A rekursiv ist

Rekursive Mengen sind abgeschlossen unter Komplement, Vereinigung, Durchschnitt, Differenz, und Urbild total-rekursiver Funktionen.

Definition: Eine Menge A ist *rekursiv aufzählbar* wenn $A = \emptyset$ oder $A = range(f)$ für ein $f\in\mathcal{TR}$

Rekursiv aufzählbare Mengen sind abgeschlossen unter Vereinigung, Durchschnitt sowie und Bild und Urbild total-rekursiver Funktionen, aber nicht unter Differenz oder Komplement. Die Zusammenhänge zwischen den beiden Begriffen sind aus der Vorlesung bekannt.

Satz: *A rekursiv $\Rightarrow$ A rekursiv aufzählbar*

Satz: *A rekursiv $\Leftrightarrow$ A und $\bar{A}$ rekursiv aufzählbar*

Definition: Eine Menge A ist *rekursiv aufzählbar in nichtabsteigender Reihenfolge*,
wenn $A = range(f)$ für ein $f\in\mathcal{TR}$ mit $\forall x, y\ x < y \Rightarrow f(x)\leq f(y)$

Definition: Eine Menge A ist *rekursiv aufzählbar in aufsteigender Reihenfolge*
wenn $A = range(f)$ für ein $f\in\mathcal{TR}$ mit $\forall x, y\ x < y \Rightarrow f(x) < f(y)$

Satz: *$A{\neq}\emptyset$ rekursiv $\Leftrightarrow$ A rekursiv aufzählbar in nichtabsteigender Reihenfolge*

Satz: *(A rekursiv $\wedge$ A unendlich) $\Leftrightarrow$ A rekursiv aufzählbar in aufsteigender Reihenfolge*

Satz: *Jede unendliche rekursiv aufzählbare Menge A hat eine unendliche rekursive Teilmenge*

Beweis Sei $A = range(f)$ und definiere $g : \mathbb{N}\to\mathbb{N}$ durch $g(i) = \begin{cases} f(0) & i = 0 \\ f(\mu_y[f(y){>}g(i{-}1)]) & sonst \end{cases}$

Dann ist $g\in\mathcal{TR}$ streng monoton und $B = range(g)$ unendlich, rekursiv und Teilmenge von A. □

Alle o.g. Konzepte sind rekursiv invariant

Satz: *A rekursiv aufzählbar $\Leftrightarrow$ $\exists x.A = domain(\varphi_x)$*

Korollar: *A rekursiv aufzählbar $\Leftrightarrow$ $\exists x.A = range(\varphi_x)$*

Der Beweis wurde in der Vorlesung geführt. Diese Charakterisierung führt zu einer Numerierung rekursiv aufzählbarer Mengen.

Definition: $W_x = domain(\varphi_x)$

Korollar: *Es gibt* $f, g, \in \mathcal{TR}$ *mit* $range(\varphi_{f(x)}) = domain(\varphi_x)$ *und* $domain(\varphi_{g(x)}) = range(\varphi_x)$

Beweis Sei Sei $h : \mathbb{N}^2 \to \mathbb{N}$ definiert durch $h(i,j) = \begin{cases} j & \varphi_i(j)\ konvergiert \\ \perp & sonst \end{cases}$

Nach dem smn-Theorem gibt es ein $f \in \mathcal{TR}$ mit $\varphi_{f(i)}(j) = h(i,j)$ für alle i, j. Es folgt $range(\varphi_{f(i)}) = \{j \mid \varphi_i(j)\ konvergiert\} = domain(\varphi_i)$

Die Konstruktion von g benötigt dovetailing. Bei Eingabe von (i,j) zählen wir den Bildbereich von φ_i auf und testen, ob j darin vorkommt. Dies gibt eine rekursive Funktion $h' : \mathbb{N}^2 \to \mathbb{N}$ mit der Eigenschaft $h'(i,j) = \begin{cases} j & \exists \langle n,t \rangle . \Phi_i(n) = t \wedge \varphi_i(n) = j \\ \perp & sonst \end{cases}$ Nach dem smn-Theorem gibt es ein $g \in \mathcal{TR}$ mit $\varphi_{g(i)}(j) = h'(i,j)$ für alle i, j und es folgt $domain(\varphi_{g(i)}) = range(\varphi_i)$ □

Es gibt noch zwei Varianten dieses Satzes auf Seite 62. In der ersten wird zwischen Bild- und Definitionsbereich umgerechnet und man erhält totale Funktionen, wenn A nicht leer ist. In der zweiten werden zusätzlich injektive Funktionen erzeugt, deren Definitionsbereiche *Initialsegmente von* $\mathbb{N}$ sind. Dies ist in sich nicht so interessant aber für manche Beweise hilfreich.

Die Menge $S = \{i \mid i \in \text{domain}(\varphi_i)\} = \{i \mid i \in W_i\}$ wird im Buch mit K bezeichnet. Sie ist rekursiv aufzählbar aber nicht rekursiv. Der Beweis für die Unentscheidbarkeit ist aber sehr elegant.

Beweis Wir nehmen an K sei rekursiv. Dann ist $\bar{K}$ rekursiv aufzählbar, also $\bar{K} = W_i$ für ein i. Es folgt $i \in K \Leftrightarrow_{def} i \in W_i \Leftrightarrow i \in \bar{K} \Leftrightarrow i \notin K$ □

Der Begiff der Entscheidbarkeit und Aufzählbarkeit läßt sich leicht auf Mengen von Tupeln und Relationen fortsetzen. Rogers führt hierzu die Standardtupelfunktion $\langle , \rangle$ *ein, die wir aus der Vorlesung zu primitiv-rekursiven Funktionen kennen. In §5.4 führt er dann Projektionen ein.*

Definition: Für $B \subseteq \mathbb{N}^2$ heißt $A = \{j \mid \exists i\ \langle i,j \rangle \in B\}$ *Projektion von* B *(in der ersten Komponente)*.

Höhere Projektionen und Projektionen in anderen Komponenten sind analog definiert. Der folgende Satz wurde in der Vorlesung für den Spezialfall der Projektion von B in der ersten Komponente definiert und gilt analog für andere Projektionen.

Satz: *Eine Menge* A *ist rekursiv aufzählbar g.d.w. sie Projektion einer rekursiven Menge* B *ist.*

Satz: *Jede Projektion einer rekursiv aufzählbaren Menge ist rekursiv aufzählbar.*

Die Projektionssätze sind sehr wichtige Hilfsmittel in vielen Beweisen. Ein weiteres wichtiges Mittel sind Projektionen, bei denen ein Argument festgehalten wird.

Definition: Für $B \subseteq \mathbb{N}^k$, $i \in \mathbb{N}$ heißt $A = \{\langle x_2, .., x_k \rangle \mid \langle i, x_2, .., x_k \rangle \in B\}$ *Sektion von* B *an der Stelle* n.

Jede rekursiv ausfzählbare Menge läßt sich effektiv als Sektion einer entscheidbaren Menge beschreiben.

Satz: *Es gibt eine rekursive Menge* $A \subseteq \mathbb{N}^3$ *mit der Eigenschaft* $W_i = \{j \mid \exists k\ (i,j,k) \in A\}$.

Beweis Sei $A = \{(i,j,k) \mid \Phi_i(j) \leq k\}$. Dann ist A rekursiv und $W_i = \{j \mid \exists k\ (i,j,k) \in A\}$.

Die Abschlußeigenschaften rekursiver und rekursiv aufzählbarer Mengen sind *effektiv* in folgendem Sinne: *es gibt ein* $g \in \mathcal{TR}$ *mit* $W_{g(i,j)} = W_i \cap W_j$ und analog für die anderen Operationen. Bei den rekursiven Mengen gilt die Effektivität in Bezug auf die W-Indizes, allerdings nicht für das Komplement, da wir sonst $\bar{K}$ rekursiv aufzählen könnten.

Anstelle der W-Indizes kann man zur Numerierung der rekursiven Mengen auch die φ-Indizes ihrer charakteristischen Funktionen verwenden (der sogenannte *charakteristische Index*). Beide Numerierungen sind *partiell*. Man kann charakteristische Indizes in W-Indizes umrechnen aber nicht umgekehrt.

Auch für endliche Mengen gibt es eine kanonische Aufzählung, was wir im folgenden öfter benötigen werden. Die konkrete Aufzählung ist eigentlich unbedeutend. Die einfachste Form ist eine Art Binär-Aufzählung der Elemente in kanonischer Reihenfolge.

Definition: Der *kanonische Index* einer endlichen Menge $A = \{x_1, ..x_k\}$ mit $x_i{<}x_j$ für $i{<}j$ ist die Zahl $x = \sum_{i=1}^{k} 2^{x_i}$. Die endliche Menge mit dem kanonischen Index x wird mit D_x bezeichnet.

Jede endliche Menge hat einen eindeutigen kanonischen Index und daher ist die Numerierung D total und bijektiv. Die Kardinalität von D_x kann effektiv bestimmt werden, aber nicht die Kardinalität der endlichen Menge mit dem charakteristischen Index x.

Satz: *Es gibt ein $f \in \mathcal{TR}$ mit $f(x) = |D_x|$ für alle x.*

Satz: *Es gibt kein $g \in \mathcal{R}$ so daß für jede endliche Menge A gilt:*
ist $\varphi_x = \chi_A$ dann ist $x \in domain(g)$ und $g(x) = |A|$.

Beweis Nach dem smn-Theorem gibt es ein $h \in \mathcal{TR}$ mit der Eigenschaft $\varphi_{h(i)}(j) = \begin{cases} 1 & \Phi(i,i) = j \\ 0 & sonst \end{cases}$

Für alle i ist $\varphi_{h(i)}$ eine charakteristische Funktion einer endlichen Menge A, die genau ein Element enthält, wenn $\varphi_i(i)$ definiert ist und sonst keines.
Würde g existieren, dann wäre $g{\circ}h \in \mathcal{TR}$ und $g{\circ}h(i) = \begin{cases} 1 & i \in K \\ 0 & sonst \end{cases}$ □

Damit kann man charakteristische Indizes (und damit auch W-Indizes) endlicher Mengen nicht in kanonische Indizes umrechnen.

Der letzte Abschnitt betrachtet *einwertige Mengen*, also Mengen, die Graphen partieller Funktionen beschreiben. Die W-Indizes dieser Mengen liefern eine Numerierung der partiell-rekursiven Funktionen. Allerdings ist die Menge dieser Indizes nicht entscheidbar, ja nicht einmal aufzählbar. Möglich ist es aber, für einwertigen Mengen mindestens einen Index effektiv zu generieren.

Definition: Eine Menge A ist einwertig, wenn für alle x höchstens ein y mit $\langle x, y\rangle \in A$ existiert. Für solche Mengen ist definiert *domain(A)* $=\{x \mid \exists y\ \langle x, y\rangle \in A\}$

Satz: *Es gibt ein $f \in \mathcal{TR}$ so daß für alle $i \in \mathbb{N}$*
1. *$W_{f(i)}$ ist einwertig*
2. *$W_{f(i)} \subseteq W_i$*
3. domain($W_{f(i)}$) = domain(W_i)
4. *W_i einwertig $\Rightarrow$ $W_{f(i)} = W_i$*

Beweis Es gibt ein $g \in \mathcal{TR}$, so daß $W_i = range(\varphi_{g(i)})$ für alle i, wobei $\varphi_{g(i)}$ auf einem Initialsegment von $\mathbb{N}$ definiert und injektiv ist.

Sei $A_i = \{\langle x, y\rangle \in W_i \mid \exists j\ \varphi_{g(i)}(j) = \langle x, y\rangle \wedge (\forall j', y'\ \varphi_{g(i)}(j') = \langle x, y'\rangle \Rightarrow j{<}j')\}$. Per Konstruktion ist A_i rekursiv aufzählbar, einwertig (a), eine Teilmenge von W_i (b) und hat denselben Domain wie W_i (c). (d) folgt unmittelbar aus (b) und (c). Nach dem smn Theorem gibt es ein $f \in \mathcal{TR}$ mit $W_{f(i)} = A_i$. □

Der soeben bewiesene Satz ist ein gutesHilfsmittel für den Beweis wichtiger Eigenschaften. So kann man z.B. leicht zeigen, daß rekursiv-aufzählbare Mengen effektiv separiert werden können.

Satz: *Für jedes paar A, B rekursiv aufzählbarer Mengen gibt es rekursiv aufzählbarer Mengen $A' \subseteq A$ und $B' \subseteq B$ mit $A \cup B = A' \cup B'$ und $A' \cap B' = \emptyset$.*

Beweis Aufgrund der Abschlußeigenschaften rekursiv-aufzählbarer Mengen gibt es ein i, so daß $C = A{\times}\{0\} \cup B{\times}\{1\} = W_i$. Sei $C' = W_{f(i)}$, wobei $f \in \mathcal{TR}$ aus dem Einwertigkeitssatz, und h die durch C' beschriebene partiell-rekursive Funktion. Dann gilt $h(i) = 0 \Rightarrow i \in A$ und $h(i) = 1 \Rightarrow i \in B$. Wir wählen $A' = h^{-1}(0)$ und $B' = h^{-1}(1)$. Dann folgt $A' \subseteq A$ und $B' \subseteq B$, $A' \cap B' = \emptyset$ wegen der Einwertigkeit und $A \cup B = A' \cup B'$ wegen Teil (c) des Einwertigkeitssatzes. □

Satz: *Es gibt ein $g \in \mathcal{R}$, so daß für alle $i \in \mathbb{N}$*
1. *$g(i)$ konvergiert $\Leftrightarrow$ $\exists j \in W_i\ W_j \neq \emptyset$*
2. *$g(i)$ konvergiert $\Rightarrow$ $g(i) \in W_i \wedge W_{g(i)} \neq \emptyset$*

Beweis Sei $A = \{\langle i, j\rangle \mid j \in W_i \wedge W_j \neq \emptyset\} = \{\langle i, j\rangle \mid \exists x\ j \in W_i \wedge x \in W_j\}$. Aufgrund des Projektionssatzes ist A rekursiv aufzählbar. Mithilfe des Einwertigkeitssatzes können wir nun ein einwertiges $A' \subseteq A$ und hieraus die partiell rekursive Funktion $g \in \mathcal{R}$ konstruieren, die per Konstruktion die gewünschten Eigenschaften hat. □

6 Reduzierbarkeit

In diesem kurzen Kapitel gibt Rogers eine Übersicht über das Konzept der Reduzierbarkeit als solches. Probleme werden, wie in der Vorlesung als Mengen von Zahlen beschrieben und ein Problem gilt als *lösbar* wenn diese Menge entscheidbar ist. Für die Untersuchung der Abstufungen von Unlösbarkeit müssen die unlösbaren Mengen in Äquivalenzklassen unterteilt werden. Dazu dient das Konzept der Reduzierbarkeit.

Wir werden in den folgenden Kapiteln mehrere mögliche konkrete Definitionen kennnenlernen. All diesen ist gemeinsam, daß ein Problem auf ein anderes reduzierbar ist, wenn eine Lösung des anderen zu einer Lösung des Originalproblems führt. Hierzu gibt Rogers auf Seite zwei informale Beispiele.

Wir kürzen reduzierbarkeit immer als $A \leq_r B$ ab, wobei der Index r die Art der Reduzierbarkeit kennzeichnet. Aus der Vorlesung kennen wir Reduzierbarkeit unter einer berechenbaren totalen Funktion – was in Kapitel 7 als m-reduzierbar bezeichnet wird – und polynomielle Reduzierbarkeit, was wir in diesem Seminar nicht weiter betrachten. Alle Reduzierbarkeitsrelationen sind *reflexiv und transitiv* und *rekursiv invariant*, also invariant unter berechenbaren Bijektionen. Sie führen zu einer Äquivalenzrelation $A \equiv_r B$, definiert als $A \leq_r B \wedge B \leq_r A$. $\leq_r$ liefert damit auch eine partielle Ordnung auf diesen Äquivalenzklassen, die im Endeffekt ihren "Schwierigkeitsgrad" vergleicht. Die Äquivalenzklassen werden auch als *Grade der Unlösbarkeit* bezeichnet. Das liegt daran, daß alle interessanten Äquivalenzklassen Klassifizierungen rekursiv-aufzählbarer Mengen oder noch komplizierter Mengen charakterisieren und die entscheidbaren Mengen im Endeffekt immer nur eine Äquivalenzklasse bilden. Man kann also die Ordnung auf diesen Äquivalenzklasse immer als "hat einen höheren Grad der Unlösbarkeit" ansehen.

Der Fokus des Buches wird auf der Untergliederung der rekursiv-aufzählbaren Mengen liegen, die bis jetzt die erste Stufe der Unlösbarkeit beschreiben, aber eigentlich sehr verschieden schwere Mengen enthalten. Dieser Aspekt ist für viele Anwendungen, z.B. in der Logik interessant. Auch jenseits rekursiv-aufzählbarer Mengen kann man noch Abstufungen vornehmen, die charakterisieren, wie schwierig Probleme sein können, die nicht einmal aufzählbar aber immer noch leichter als andere sind.

Dabei wird inspesondere das Konzept der Vollständigkeit wichtig, das wir in der Vorlesung nur im Rahmen der $\mathcal{NP}$-Vollständigkeit kennengelernt haben. Die Definition ist im Prinzip dieselbe. Eine Menge A ist *vollständig bezüglich $\leq_r$*, wenn sie selbst rekursiv aufzählbar ist und jede andere r.a. Menge B auf A reduziert werden kann. In dem Sinne haben vollständige Mengen den größten Grad der Unlösbarkeit. Aus der Definition folgt auch sofort, daß zwei *vollständige Mengen äquivalent* sind und daß jede r.a. Menge, auf die eine vollständige Menge reduzierbar ist, ebenfalls vollständig ist. All dies kennen wir in ähnlicher Form für $\mathcal{NP}$-vollständige Mengen.

Das Halteproblem $H = \{\langle i,n\rangle \mid n \in W_i\}$ muß vollständig sein, denn jede für jede r.a. Menge $B = W_i$ gilt $x \in B$ genau dann, wenn $\langle i,x\rangle \in H$ und somit haben wir eine Reduktion von B auf H, ohne daß es nennenswert Formalia bedarf.

7 1- und m-Reduzierbarkeit, Kreative Mengen

Dieses Kapitel widmet sich der Reduzierbarkeit, die wir aus der Vorlesung kennen (die sogenannte m-Reduzierbarkeit), sowie eine injektive Variante davon.

Definition: A ist 1-reduzierbar auf B ($A \leq_1 B$), wenn es eine injektive total-rekursive Funktion f gibt mit $A = f^{-1}(B)$ (d.h. $\forall x\ x \in A \Leftrightarrow f(x) \in B$).

Definition: A ist m-reduzierbar auf B ($A \leq_m B$), wenn es ein $f \in \mathcal{TR}$ gibt mit $A = f^{-1}(B)$.

Wenn man genau sein will sagt man auch A ist reduzierbar auf B via f. Man beachte, daß $A = f^{-1}(B)$ äquivalent ist zu $\chi_A = \chi_B \circ f$, woraus direkt gewisse Abschlußeigenschaften folgen.

Satz:

1. *$\leq_1$ und $\leq_m$ sind reflexiv und transitiv*
2. *$\leq_1$ impliziert $\leq_m$*
3. *$A{\leq_1}B \Rightarrow \bar{A}{\leq_1}\bar{B}$ und $A{\leq_m}B \Rightarrow \bar{A}{\leq_m}\bar{B}$*
4. *$A{\leq_m}B$ und B entscheidbar (bzw. r.a) $\Rightarrow$ A entscheidbar (bzw. r.a) und analog für $\leq_1$*

Definition: $A\equiv_1 B$ = $A{\leq_1}B \wedge B{\leq_1}A$, $\quad A\equiv_m B$ = $A{\leq_m}B \wedge B{\leq_m}A$

$\equiv_1$ und $\equiv_m$ sind Äquivalenzrelationen, deren Klassen *1-Grade* bzw. *m-Grade* genannt werden. Grade, die eine entscheidbare Menge enthalten, bestehen nur aus entscheidbaren Mengen und das gleiche gilt für r.a. Mengen. Man spricht daher auch von *rekursiven Graden* bzw *rekursiv-aufzählbarenen Graden*.

Für den Beweis des nächsten Theorems brauchen wir den Begriff der disjunktion Summe (*join*).

Definition: $A{+}B$ = $\{2x \mid x \in A\} \cup \{2x{+}1 \mid x \in B\}$

Aus dieser Definition ergibt sich, daß $A{\leq_m}A{+}B$ via $\lambda x.2x$ und $B{\leq_m}A{+}B$ via $\lambda x.2x{+}1$ gilt. Damit ist $A{+}B$ in der $\leq_m$-Ordnung eine obere Schranke von A und B. Außerdem gilt: wenn $A{\leq_m}C$ via f und $B{\leq_m}C$ via g, dann ist $A{+}B{\leq_m}C$ via h für die Funktion h mit $h(2x) = f(x)$ und $h(2x{+}1) = g(x)$, d.h. $A{+}B$ ist die kleinste obere Schranke.

Satz:

1. *Es gibt zwei unentscheidbare Mengen, die bezüglich $\leq_m$ und $\leq_1$ unvergleichbar sind.*
2. *$A{\leq_m}B$ impliziert nicht $A{\leq_m}\bar{B}$*
3. *m-Reduzierbarkeit ist ein Halbverband mit (eindeutigem) Supremum. Das Supremum zweier rekursiv-aufzählbarer Grade ist rekursiv-aufzählbar.*

Beweis

1. Als Beispiel wähle man K und $\bar{K}$. Da $\bar{K}$ nicht r.a. ist, kann $\bar{K}{\leq_m}K$ nicht gelten und nach obigem Satz (3) auch nicht $K{\leq_m}\bar{K}$.
2. Als Gegenbeispiel wähle man $A = B = K$
3. Für eine Menge X sei $d(X)$ der m-Grad von X. Die Grade sind partiell geordnet und für je zwei Grade $d(A)$ und $d(B)$ ist $d(A{+}B)$ das Supremum. □

7.1 1-/m-vollständige Mengen

Definition: Eine Menge $A{\subseteq}\mathbb{N}$ ist *1-vollständig*, wenn A r.a. ist und $B{\leq_1}A$ für jede r.a. Menge B gilt.

Definition: Eine Menge $A{\subseteq}\mathbb{N}$ ist *m-vollständig*, wenn A r.a. ist und $B{\leq_m}A$ für jede r.a. Menge B gilt.

Satz: *$H = \{\langle i,n\rangle \mid n \in W_i\}$ ist 1-vollständig*

Beweis $H = \{\langle i,n\rangle \mid \exists t.\Phi_i(n){\leq}t\}$ ist nach dem Projektionssatz r.a. Ist B r.a., dann gibt es ein i mit $B = W_i$ und $x \in B$ genau dann, wenn $\langle i,x\rangle \in H$. Also $B{\leq_1}H$ via $\lambda x.\langle i,x\rangle$ □

Satz: *$K = \{i \mid i \in W_i\}$ ist 1-vollständig*

Beweis K ist wie H r.a. Wir zeigen $H{\leq_1}K$. Dafür zeigen wir $H{\leq_m}K$ und modifizieren dann die Reduktionsfunktion. Nach dem smn-Theorem gibt es ein $f \in \mathcal{TR}$ mit $\varphi_{f\langle i,n\rangle}(x) = \begin{cases} 1 & \varphi_i(n) \text{ konvergiert} \\ \perp & \text{sonst} \end{cases}$

Es folgt $\langle i,n\rangle \in H \Leftrightarrow f\langle i,n\rangle \in K$, da $\varphi_{f\langle i,n\rangle}$ nicht von der Eingabe abhängt.

Um f injektiv zu machen, verwenden wir eine Technik namens *padding*, mit der wir schrittweise größere Gödelnummern derselben Funktion konstruieren. Es gibt eine Funktion $t \in \mathcal{TR}$ mit $\varphi_{t\langle i,j\rangle} = \varphi_i$ für alle j und t ist injektiv in j. Wir konstruieren eine Funktion $t' \in \mathcal{TR}$ durch $t'(0){=}t(0)$ und (für $0{<}\langle i,j\rangle$) $t'\langle i,j\rangle = t(i,\ \mu_z[t\langle i,z\rangle{\neq}t'(k)$ *für alle* $k{<}\langle i,j\rangle])$. Dann ist t' injektiv und $\varphi_{t'\langle i,j\rangle} = \varphi_i$ für alle j.

Sei $f' = \lambda x.t'\langle f(x),x\rangle$. Dann ist f' injektiv und $\varphi_{f'(x)} = \varphi_{t'\langle\langle f(x),x\rangle,x\rangle} = \varphi_{f(x)}$ und somit $\langle i,n\rangle \in H \Leftrightarrow f'\langle i,n\rangle \in K$, also $H{\leq_1}K$ via f'. □

Korollar: $K \equiv_1 H$

Der obige Beweis wirft einige Fragen auf: *Sind 1-Vollständigkeit und m-Vollständigkeit identisch?*, *Ist jede nichtentscheidbare, r.a. Menge m-vollständig? Sind $\leq_1$ und $\leq_m$ auf nichtentscheidbaren, r.a. Menge identisch?* Die letzten beiden Fragen werden in Kapitel 8 negativ beschieden. Um zu zeigen, daß die erste Frage tatsächlich eine positive Antwort hat, brauchen wir ein Lemma über Mengen mit m-Grad über K.

Lemma: *Wenn A r.a. und $K \leq_m A$ gilt, dann gibt es ein $g \in \mathcal{TR}$ mit* $g(x) \in \begin{cases} A - D_x & \emptyset \neq D_x \subseteq A \\ \bar{A} - D_x & \emptyset \neq D_x \subseteq \bar{A} \end{cases}$.

Beweis Es sei $K \leq_m A$ via f. Dann ist $f(K)$ unendlich, da ansonsten $K = f^{-1}(f(K))$ entscheidbar wäre, und es gibt ein $f' \in \mathcal{TR}$ mit $f(K) = range(f')$.

Da A r.a ist, gibt es ein $h \in \mathcal{TR}$ mit $\varphi_{h(x)}(i) = \begin{cases} 1 & (f(i) \in D_x \wedge D_x \cap A = \emptyset) \vee D_x \cap A \neq \emptyset \\ \perp & sonst \end{cases}$

Wir definieren $g(x) = \begin{cases} f(h(x)) & f(h(x)) \notin D_x \\ f'(\mu_z[f'(z) \notin D_x]) & sonst \end{cases}$ Dann ist $g \in \mathcal{TR}$ und $g(x) \notin D_x$ für alle x.

Sei $\emptyset \neq D_x \subseteq A$. Dann ist $W_{h(x)} = \mathbb{N}$, also $h(x) \in W_{h(x)}$, d.h. $h(x) \in K$ und damit $g(x) = f(h(x)) \in f(K) \subseteq A$.

Sei $\emptyset \neq D_x \subseteq \bar{A}$. Dann ist $W_{h(x)} = f^{-1}(D_x)$ und $h(x) \notin f^{-1}(D_x)$, denn andernfalls wäre $f(h(x)) \in D_x$ und $h(x) \in W_{h(x)}$, $h(x) \in K$, $f(h(x)) \in A$, also $D_x \cap A \neq \emptyset$. Es folgt $h(x) \in \bar{K}$ und wegen $h(x) \notin f^{-1}(D_x)$ auch $g(x) = f(h(x)) \in f(\bar{K}) \subseteq \bar{A}$ □

Satz: *A m-vollständig $\Leftrightarrow$ A 1-vollständig*

Beweis Die $\Leftarrow$-Richtung ist trivial. Für die Gegenrichtung nehmen wir ann, daß A m-vollständig ist, also insbesondere $K \leq_m A$ via einem f gilt und zeigen unter Verwendung der obigen Funktion g, daß $K \leq_1 A$ gilt. Aus der 1-Vollständigkeit von K folgt dann die von A.

Dazu definieren wir eine Funktion f' durch $f'(0) = f(0)$ und $f'(n+1) = f(n+1)$, falls $f(n+1)$ neu ist (d.h. $f(n+1) \notin \{f'(0), ..f(n)\}$). Ansonsten sei x_0 so daß $D_{x_0} = \{f(n+1)\}$. Wenn $g(x_0)$ neu ist, setze $f'(n+1) = g(x_0)$. Ansonsten sei x_1 so daß $D_{x_1} = \{f(n+1), g(x_0)\}$. Wenn $g(x_1)$ neu ist, setze $f'(n+1) = g(x_1)$. etc. nach spätestens $n+1$ Schritten haben wir mit diesem Prozess einen neuen Wert für $f'(n+1)$ gefunden und damit ist $f' \in \mathcal{TR}$ injektiv.

Per Konstruktion gilt $0 \in K \Leftrightarrow f'(0) \in A$ (wegen $K \leq_m A$ via f) und $n+1 \in K \Leftrightarrow f'(n+1) \in A$ ($\Rightarrow$ per Konstruktion, $\Rightarrow$ ebenso über das Komplement), also insgesamt $K \leq_1 A$ via f'. □

7.2 Produktive und Kreative Mengen

Die Tatsache, daß $\bar{K} = \{i \mid i \notin W_i\}$ nicht r.a. ist, läßt sich – ähnlich wie beim zweiten Gödelschen Unvollständigkeitssatz – auf eine sehr konstruktive Weise eindrucksvoll demonstrieren. Per Definition muß für jede r.a. Teilmenge W_x von $\bar{K}$ die Zahl x selbst in $\bar{K} - W_x$ liegen. Der Index produziert also einen konstruktiven Beweis, warum $\bar{K}$ nicht diese r.a. Menge sein kann. Mengen mit dieser Eigenschaft nennt man *produktiv*. Die folgende Definition gibt eine rekursiv invariante Formulierung des Begriffs.

Definition: A ist *produktiv*, wenn es ein $f \in \mathcal{R}$ gibt mit $\forall x\ W_x \subseteq A \Rightarrow x \in domain(f) \wedge f(x) \in A - W_x$.
f heißt *produktive Funktion für A*

Definition: A ist *kreativ*, wenn A r.a. und $\bar{A}$ produktiv ist.

Die Menge K ist, wie oben demonstriert, kreativ. Ein weiteres Beipiel ist die Menge der Indizes total rekursiver Funktione, die wir in der Vorlesung per Diagonalisierung als nicht r.a. bewiesen hatten. Dieser Beweis liefert eine produktive Funktion.

Satz: *$TR = \{i \varphi_i \in \mathcal{TR}\}$ ist produktiv*

Beweis Es sei $W_x \subseteq TR$ und $f \in \mathcal{TR}$ mit $W_x = range(\varphi_{f(x)})$ für alle x und $\varphi_{f(x)}$ total, falls $W_x \neq \emptyset$. Dann gibt es nach dem smn Theorem eine Funktion $g \in \mathcal{TR}$ mit $\varphi_{g(x)}(n) = \begin{cases} 1 & \Phi_{f(x)}(0) > n \\ \varphi_{\varphi_{f(x)}(n-n_0)}(n)+1 & \Phi_{f(x)}(0) = n_0 \leq n \end{cases}$.

Falls $W_x = \emptyset$ ist, dann ist $\varphi_{f(x)}(0)$ undefiniert, also $\varphi_{g(x)}(n) = 1$ für alle n und damit $g(x) \in TR = TR - W_x$.

Andernfalls ist $\varphi_{f(x)}$ total und gibt es ein n_0 mit $\Phi_{f(x)}(0){=}n_0$. In diesem Fall nimmt $\varphi_{g(x)}$ für alle i an der Stelle $i{+}n_0$ den Wert $\varphi_{\varphi_{f(x)}(i)}(i{+}n_0){+}1$ an. Da $\varphi_{f(x)}(i) \in W_x {\subseteq} TR$ ist, ist $\varphi_{\varphi_{f(x)}(i)}$ total und damit $\varphi_{g(x)}$ an jeder Stelle definiert, also $g(x) \in TR$.

Wir nehmen an $g(x) = z$ für ein $z \in W_x$. Wir wissen, daß $\varphi_{f(x)}(i) = z$ für ein i und daß $\varphi_{\varphi_{f(x)}(i)} = \varphi_z$ total ist. Wir betrachten $\varphi_{g(x)}(i{+}n_0)$. Da $g(x) = z$ ist, folgt $\varphi_{g(x)}(i{+}n_0) = \varphi_z(i{+}n_0) = \varphi_{\varphi_{f(x)}(i)}(i{+}n_0)$. Per Konstruktion ist aber $\varphi_{g(x)}(i{+}n_0) = \varphi_{\varphi_{f(x)}(i)}(i{+}n_0){+}1$. Da φ_z total ist, ist dies ein Widerspruch.

Damit ist $g(x) \notin W_x$ also insgesamt $g(x) \in TR - W_x$. □

Satz: *A produktiv* $\Rightarrow$ *A nicht r.a.*

Dies folgt unmittelbar aus der Definition.

Satz: *A produktiv* $\wedge$ $A{\leq_m}B$ $\Rightarrow$ *B produktiv*

Beweis Sei f die produktive Funktion für A und $A{\leq_m}B$ via g. Da die Abschlußeigenschaften von r.a. Mengen effektiv sind, gibt es ein $h \in \mathcal{TR}$ mit $W_{h(x)} = g^{-1}(W_x)$. Es folgt

$$\begin{aligned} W_x{\subseteq}B \quad &\Rightarrow W_{h(x)} = g^{-1}(W_x){\subseteq}A \\ &\Rightarrow h(x) \in domain(f) \wedge f(h(x)) \in A - W_{h(x)} \\ &\Rightarrow h(x) \in domain(g{\circ}f) \wedge g(f(h(x))) \in B - g(W_{h(x)}) = W_x \end{aligned}$$

Damit ist $g{\circ}f{\circ}h$ die produktive Funktion von B □

Die Tatsache, daß sich Produktivität nach oben vererbt, erleichtert Beweise für Produktivität. Wir hätten statt des Diagonalbeweises nur $\bar{K}{\leq_m}TR$ zeigen müssen, um zu beweisen, daß TR produktiv ist.

Korollar: *A kreativ* $\Rightarrow$ *A unentscheidbar*

Korollar: *A kreativ* $\wedge$ $A{\leq_m}B$ $\Rightarrow$ $\Rightarrow$ $\bar{B}$ *produktiv*

Korollar: *A m-vollständig* $\Rightarrow$ *A kreativ*

Warum dies Korollare sind, läßt sich mit kurzem Resümieren der bisherigen Erkenntnisse herausfinden.

Satz: *Jede produktive Menge hat eine unendliche rekursiv-aufzählbare Teilmenge*

Beweis Sei g die produktive Funktion von A. Da die Abschlußeigenschaften von r.a. Mengen effektiv sind, gibt es ein $f \in \mathcal{TR}$ mit $W_{f\langle i,\, j\rangle} = W_i{\cup}W_j$, ein $h \in \mathcal{TR}$ mit $W_{h(x)} = \{x\}$, und ein x_0 mit $W_{x_0} = \emptyset$. Wir definieren eine Funktion k durch $k(0) = x_0$ und $k(n{+}1) = f\langle h(g(k(n))),\ k(n)\rangle$. Dann ist $k \in \mathcal{TR}$ und $W_{k(0} = \emptyset{\subseteq}A$ und $W_{k(n+1)} = W_{h(g(k(n)))}{\cup}W_{k(n)} = W_{k(n)}{\cup}\{g(k(n))\}{\subseteq}A$, wobei $g(k(n)) \in A - W_{k(n)}$. Damit ist die Funktion g∘k eine injektive Aufzählung einer Teilmenge von A, die r.a. und unendlich ist. □

Korollar: *Jede produktive Menge hat eine unendliche rekursive Teilmenge*

Hier steht noch einiges auf Seite 91ff wozu ich nicht kommen werde. Die Beweise dauern zu lange.

Satz: *Jede produktive Menge hat eine total-rekursive produktive Funktion*

Beweis Erweiterung der obigen Methode, siehe Seite 92 □

Definition: A ist *vollständig produktiv*, wenn es ein $f \in \mathcal{TR}$ gibt so daß für alle x gilt $f(x) \in W_x - A$ oder $f(x) \in A - W_x A$.

$\bar{K}$ ist vollständig produktiv mit $\lambda x.x$

Definition: A ist *semi-produktiv*, wenn es ein $f \in \mathcal{R}$ gibt mit $\forall x\ W_x{\subseteq}A \Rightarrow x \in domain(f) \wedge W_x{\subset}W_{f(x)}{\subseteq}A$.

Definition: A und B sind *rekursiv trennbar*, wenn es eine entscheidbare Menge C gibt mit $A{\subseteq}C \wedge B{\subseteq}\bar{C}$

B sind *effektiv untrennbar*, wenn es ein $f \in \mathcal{R}$ gibt mit
$(A{\subseteq}W_i \wedge B{\subseteq}W_j \wedge W_i{\cap}W_j{=}\emptyset) \Rightarrow \langle i,j\rangle \in domain(f) \wedge W_{f\langle i,\, j\rangle} \in \bar{W}_i{\cap}\bar{W}_j$

Satz:

1. *Wenn A und B effektiv untrennbar sind, dann sind sie nicht rekursiv trennbar.*
2. *Sind A und B effektiv untrennbar, disjunkt und r.a., dann sind beide Mengen kreativ*
3. *Es gibt A und B, die effektiv untrennbar, disjunkte und r.a. sind.*

Beweis

1. Übung
2. Übung
3. Wähle $A = \{i \mid \varphi_i(i) = 0\}$ und $B = \{i \mid \varphi_i(i) = 1\}$ ... Rest auf Seite 94 $\square$

7.3 1-Äquivalenz und Rekursive Isomorphie

Es hat sich herausgestellt, daß 1-Äquivalenz und Rekursive Isomorphie (Äquivalenz unter rekursiven Bijektionen) dasselbe sind. Dieser Satz, der 1955 von Myhill gezeigt wurde, hat einen sehr technischen Beweis, den ich vorerst auslasse.

Satz: $A \equiv B \;\Leftrightarrow\; A \equiv_1 B$

7.4 Zylinder

Zylinder dienen dazu, die 1-Unterstruktur von m-Graden aufzufächern.

Definition: A ist ein Zylinder, wenn $A \equiv B \times \mathbb{N} = \{\langle i, j\rangle \mid i \in B, j \in \mathbb{N}\}$

Man beachte, daß Rekursive Isomorphie anstelle von Gleichheit gewählt wurde, um rekursive Invarianz des Begriffs zu erreichen

Satz:

1. $A \leq_1 A \times \mathbb{N}$
2. $A \times \mathbb{N} \leq_m A$
3. A *Zylinder* $\Leftrightarrow (\forall B\; B \leq_m A \Rightarrow B \leq_1 A)$
4. $A \leq_m B \Leftrightarrow A \times \mathbb{N} \leq_1 B \times \mathbb{N}$
5. A *Zylinder* $\Leftrightarrow\; A \times \mathbb{N} \leq_1 A \;\Leftrightarrow\; A \equiv A \times \mathbb{N}$

Beweis

1. $A \leq_1 A \times \mathbb{N}$ via $\lambda x.\langle x, 0\rangle$
2. $A \times \mathbb{N} \leq_m A$ via π_1
3. $\Rightarrow$: Sei $A \equiv C \times \mathbb{N}$ und $B \leq_m A$. Dann $B \leq_m C$ via f, also $B \leq_m C \times \mathbb{N}$ via $\lambda x.\langle f(x), x\rangle$, d.h. $B \leq_1 A$.
   $\Leftarrow$: Sei $(\forall B\; B \leq_m A \Rightarrow B \leq_1 A)$. Wegen $A \times \mathbb{N} \leq_m A$ gilt $A \times \mathbb{N} \leq_1 A$ also $A \equiv_1 A \times \mathbb{N}$.
   Nach dem Satz von Myhill ist $A \equiv A \times \mathbb{N}$ Zylinder.
4. $\Rightarrow$: Sei $A \leq_m B$, dann $A \times \mathbb{N} \leq_m A \leq_m B \leq_1 B \times \mathbb{N}$ und mit (3) $A \times \mathbb{N} \leq_1 B \times \mathbb{N}$
   $\Leftarrow$: Sei $A \times \mathbb{N} \leq_1 B \times \mathbb{N}$, dann $A \leq_1 A \times \mathbb{N} \leq_1 B \times \mathbb{N} \leq_m B$
5. Folgt direkt aus (1) – (4) $\square$

Eine wichtige Konsequenz aus (3) ist, daß K ein Zylinder ist (steht so nicht in Rogers), da K 1-vollständig ist und aus $B \leq_m K$ folgt, daß B r.a. ist.

Satz: A *Zylinder* $\Leftrightarrow$ *es gibt ein* $g \in \mathcal{TR}$ *mit* $g(x) \in \begin{cases} A - D_x & \emptyset \neq D_x \subseteq A \\ \bar{A} - D_x & \emptyset \neq D_x \subseteq \bar{A} \end{cases}$.

Beweis Analog zum Beweis des entsprechenden Lemmas für K $\square$

7.5 Logikanwendungen

Dieser Abschnitt diskutiert den Zusammenhang zwischen Gödel's Unvollständigkeitstheorem und Produktivität. Er gibt eine Einführung – die eigentlichen Aussagen kommen später im Buch