Rekursions- und Lerntheorie

WiSe 2010/11; Univ. Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

Rekursions- und Lerntheorie Gesamtübersicht

1. Einführung: Grundsätzliche Betrachtungen

2. Berechenbarkeitstheorie: Die Churchsche These (4 VL)

3. Ausblicke auf weitere Ergebnisse der Rekursionstheorie

4. Lerntheorie: Modelle und Aussagen

Der Kleenesche Fixpunktsatz

Satz 1: Zu jeder berechenbaren totalen Funktion f gibt es eine Zahl e, sodass $h_e = h_{f(e)}$.

Grundidee wie aus dem Märchen (Münchhausen zieht sich selbst aus dem Sumpf): Betrachte das Programm:

> Forme dies Programm selbst gemäß f um und wende dieses transformierte Programm auf das Argument x an.

Problem: Selbstbezug, d.h., nicht wohldefiniert.

Gäbe es aber so ein Programm, so hätte es eine Gödelnummer, z.B. e.
Betrachte also:

> Forme das Programm mit Nummer e gemäß f um und wende dieses transformierte Programm auf das Argument x an.

Wenn es e gäbe, hätte auch diese Programm eine Nummer, z.B. $g(e)$ für eine rekursive Funktion $g = h_a$. Damit wäre auch folgendes Programm eine mögliche Lösung:

> Forme das Programm mit Nummer $h_a(e)$ gemäß f um und wende dieses transformierte Programm auf das Argument x an.

Wir könnten nun immer weiter Parameter hinzufügen, aber das ist nicht sinnvoll.
Idee: Diagonalisierung! Betrachte daher $e = a$, d.h.:

> Forme das Programm mit Nummer $h_e(e)$ gemäß f um und wende dieses transformierte Programm auf das Argument x an.

Diese Programm hätte nun wieder eine Gödelnummer, z.B. b.
Diagonalisiere erneut:

> Forme das Programm mit Nummer $h_b(b)$ gemäß f um und wende dieses transformierte Programm auf das Argument x an.

Nach Konstruktion ist die Gödelnummer dieses letzten Programms gerade $h_b(b)$, d.h.: $h_x = h_{f(x)}$ für $x = h_b(b)$.

Der Kleenesche Fixpunktsatz Formaler Beweis:

Erinnerung: (smn-Eigenschaft (für Zahlfunktionen)):
Ist $g : \mathbb{N} \multimap \mathbb{N}$ eine berechenbare Zahlfunktion, so gibt es eine totale berechenbare Zahlfunktion r_g derart, dass für alle $w \in \mathbb{N}$ und alle $x \in \mathbb{N}$ gilt:

$$g(\langle w, x\rangle) = h_{r_g(w)}(x).$$

Betrachte speziell $g(\langle w, x\rangle) = h_{h_w(w)}(x)$.
Für das zugehörige r_g gilt: $h_{r_g(w)} = h_{h_w(w)}$. (Erste Diagonalisierung)
Zu vorgelegtem f betrachte nun Komposition $w \mapsto f(r_g(w))$.
Diese Komposition habe Gödelnummer d. $\rightsquigarrow$ Zweite Diagonalisierung:
(1) $h_{h_d(d)} = h_{r_g(d)}$ für das von uns gewählte g.
(2) $h_{h_d(d)} = h_{f(r_g(d))}$, da d Index der Komposition.
$\rightsquigarrow h_{r_g(d)} = h_{f(r_g(d))}$. Setzt man $e = r_g(d)$ folgt die Beh.

Aufgabe: Bringen Sie diesen Beweis mit der informellen Idee in Einklang!

Bemerkungen zum Kleeneschen Fixpunktsatz

Zu jeder rekursiven Funktion f gibt es eine Zahl e, sodass $h_e = h_{f(e)}$.

(A) Der Beweis liefert sogar mehr, nämlich die Existenz einer rekursiven Funktion s, sodass gilt:
Ist h_a total, so gilt: $h_{s(a)} = h_{h_a(s(a))}$.
D.h.: Der Fixpunkt e lässt sich aus einem Index von f berechnen.

(B) Der Fixpunktsatz ist äquivalent zur smn-Eigenschaft.

(C) Man kann (im Wesentlichen) bei der Def. von berechenbaren Funktionen das μ-Rekursionsschema ersetzen durch Definitionen über Fixpunkte.
Intuitiv ist das nicht verwunderlich: Nullstellensuche und Fixpunktsuche in der Analysis sind sehr verwandte Aufgaben.

Reductionen

Hinweis: Ähnliche Begriffe aus der Komplexitätstheorie und ähnlichen Vorlesungen bekannt.

Bekannteste Reduktionsbegriffe:
— *Turing-Reduktion* (s. auch VL Näherungsalg.), kurz T-*Reduktion*
— *Karp-Reduktion* ("der Standard" in KT), auch *many-one Reduktionen* oder kurz $\mathfrak{m}$-*Reduktion*

Bezeichnung Karp-Red. etwas anachronistisch, da schon zuvor in der Rekursionstheorie eingeführt

Weitere Reduktionsbegriffe für RT wichtig, werden hier aber fortgelassen.

m-Reduktion

Eine Menge A heißt *m-reduzierbar* auf die Menge B gdw. es gibt eine rekursive, d.h., berechenbare und totale Funktion f mit $A(x) = B(f(x))$ für alle x, d.h.: $x \in A \Leftrightarrow f(x) \in B$.

Das Elementproblem für A lässt sich also mit Hilfe von der *Reduktionsfunktion* f auf das Elementproblem für B zurückführen.

Schreibweise: $A \leq_m B$: A ist m-reduzierbar auf B.

Schreibweise: $A \equiv_m B$ gdw. $A \leq_m B$ und $B \leq_m A$.

Das Mengensystem $\{B \mid B \equiv_m A\}$ heißt auch *m-Grad* (von A).

Beobachtungen

- $\leq_m$ ist eine *Quasiordnung* auf $\mathbb{N}$ (bzw. E^*), aufgefasst als Gödelnummern, also eine reflexive und transitive Relation.

- Ein Beispiel: $\mathcal{H}$: allgemeines Halteproblem, $\mathcal{K}$: spezielles Halteproblem.
  $x \in \mathcal{K}$ gdw. $f(x) = x\$x \in \mathcal{H}$.
  Also: $\mathcal{K} \leq_m \mathcal{H}$.

- $\equiv_m$ ist eine *Äquivalenzrelation* auf $\mathbb{N}$.
  Die m-Grade sind die Äquivalenzklassen.

Satz 2: A ist m-reduzierbar auf $\mathcal{K}$ gdw. A ist rekursiv aufzählbar.

Beweis: $\mathcal{K}$ ist rekursiv aufzählbar, also der Definitionsber. einer partiell-rekursiven Funktion g.
Falls $A \leq_m \mathcal{K}$ durch (rekursive) Reduktionsfunktion f, so ist A Definitionsbereich der partiell-rekursiven Funktion $x \mapsto g(f(x))$, d.h. A ist rekursiv aufzählbar.
Ist A rekursiv aufzählbar, so definiere die folgende zweistellige partiell-rekursive Funktion f:

$$f(e,x) = \begin{cases} 1 & \text{falls } e \in A; \\ \uparrow & \text{falls } e \notin A. \end{cases}$$

Gemäß smn-Theorem ex. rekursive Funktion g, sodass $h_{g(e)}(x) = f(e,x)$ für alle e, x.

$\rightsquigarrow h_{g(e)}(g(e))$ ist definiert gdw. $e \in A$.

$\rightsquigarrow e \in A \Leftrightarrow g(e) \in \mathcal{K}$ und $A \leq_m \mathcal{K}$ mit Reduktionsfunktion g.

Welche (weiteren) $\mathfrak{m}$-Grade gibt es?

- Soeben (fast) gesehen: Die zu $\mathcal{K}$ äquivalenten Mengen.
- Der (trivialen) m-Grade $\{\emptyset\}$, $\{\mathbb{N}\}$.
- Alle weiteren entscheidbaren Mengen bilden einen weiteren m-Grad:
  Ist nämlich A rekursiv und $a \in A$ sowie $b \in \mathbb{N} \setminus A$ fixiert, so lässt sich jede weitere rekursive Menge auf A m-reduzieren durch $x \mapsto a$, falls $x \in B$, und $x \mapsto b$, falls $x \notin B$.
- $\mathcal{K}$ lässt sich nicht auf eine entscheidbare Menge m-reduzieren.
- Natürliche Fragen: (1) Gibt es weitere m-Grade?
  (2) Lassen sich die zu $\mathcal{K}$ äquivalenten Mengen charakterisieren?

Der Charakterisierungssatz von Myhill für zu $\mathcal{K}$ $\mathfrak{m}$-äquivalente Mengen

Eine rekursiv aufzählbare Menge A, auf welche $\mathcal{K}$ $\mathfrak{m}$-reduzierbar ist, heißt auch $\mathfrak{m}$-*vollständig*.

Eine rekursiv aufzählbare Menge A heißt *kreativ*, wenn es eine rekursive Funktion f (den *Kreativitätszeugen*) gibt, sodass für alle e gilt:
$W_e \subseteq \mathbb{N} \setminus A \Rightarrow f(e) \in \mathbb{N} \setminus (A \cup W_e)$.

Satz 3: Eine rekursiv aufzählbare Menge A ist genau dann kreativ, wenn sie $\mathfrak{m}$-vollständig ist.

Nach Satz 2 bedeutet das: $A \equiv_{\mathfrak{m}} \mathcal{K}$.

Die erste Beweisrichtung: m-Vollständigkeit impliziert Kreativität

Betrachte A mit $A \equiv_m \mathcal{K}$. $\leadsto$ Es gibt rek. Reduktionsfunktion g für $\mathcal{K} \leq_m A$; d.h.: $x \in \mathcal{K} \Leftrightarrow g(x) \in A$ für alle x.

Es gibt rek. Funktion h mit $W_{h(x)} = \{y \mid g(y) \in W_x\}$ für alle x:

Man betrachte nämlich das Programm $P_{h(x)}$, das 1 ausgibt, sobald für die Eingabe y für $P_{h(x)}$ das Programm P_x auf $g(y)$ hält. (Formal verwende man utm- und smn-Eigenschaften...)

Unterscheide zwei Fälle:

1. $h(x) \in W_{h(x)}$. Also $h(x) \in \mathcal{K}$, $g(h(x)) \in A$ per def. von g und $g(h(x)) \in W_x$ per def. von h.

2. $h(x) \notin W_{h(x)}$. Damit $h(x) \notin \mathcal{K}$, $g(h(x)) \notin A$ per def. von g und $g(h(x)) \notin W_x$ per def. von h.

Wenn W_x disjunkt von A ist, tritt der erste Fall nicht auf.

Mithin gilt: $g(h(x)) \notin A \cup W_x$. $\leadsto$ A ist kreativ.

Die zweite Beweisrichtung: m-Vollständigkeit folgt aus Kreativität

Sei A kreativ mit Kreativitätszeugen f, d.h. $f(x) \notin W_x \cup A$, falls $W_x \cap A = \emptyset$.
Es gibt rek. Funktion g mit

$$W_{h_{g(e)}(x)} = \begin{cases} \{f(h_e(x))\} & \text{falls } x \in \mathcal{K} \wedge h_e(x)\downarrow; \\ \emptyset & \text{sonst} \end{cases} \tag{1}$$

Wir können g so wählen, dass neben g auch $h_{g(e)}$ total ist:
Betrachte hierzu die folgende partiell-rek. Funktion $h_{e,x}$:
Bei Eingabe von y, simuliere die e-te TM T_e auf Eingabe x.
Hält T_e, prüfe ob $y = f(h_e(x))$. Wenn ja, setze $h_{e,x}(y) = y$; sonst sei $h_{e,x}(y) =\uparrow$.
$h_{e,x}$ selbst ist nicht total, aber $h_{g(e)}(x)$ (smn) liefert einen Index für $h_{e,x}$
$\rightsquigarrow h_{g(e)}$ ist total.
Der Def.-Bereich von $h_{e,x}$ stimmt mit dem von $h_{h_{g(e)}(x)}$ überein, s. (1).

Kleenes Fixpunktsatz liefert ein e mit $h_{g(e)} = h_e$.
Da $h_{g(e)}$ total, ist h_e ebenfalls total. Die Konvergenzbedingung in (1) ist also unnötig.
Zu zeigen bleibt: $x \mapsto f(h_e(x))$ ist eine m-Reduktion von $\mathcal{K}$ auf A.
Betrachte hierzu zwei Fälle:
$x \notin \mathcal{K} \rightsquigarrow W_{h_{g(e)}(x)} = \emptyset \Rightarrow W_{h_e(x)} = \emptyset$ nach der Wahl von e als Fixpunkt von g.
Da f Kreativitätszeuge, folgt $f(h_e(x)) \notin A$.
$x \in \mathcal{K} \rightsquigarrow W_{h_{g(e)}(x)} = W_{h_e(x)} = \{f(h_e(x))\}$, also $f(h_e(x)) \in W_{h_e(x)}$.
$\Rightarrow W_{h_e(x)} \cap A \neq \emptyset$; sonst wäre f kein Kreativitätszeuge; also: $f(h_e(x)) \in A$.

So folgt: $\mathcal{K}(x) = A(f(h_e(x))) \rightsquigarrow m$-Reduktionseigenschaft.
Da A kreativ, ist A rek. aufzählbar (per def.).
Also: A ist m-vollständig.

Der Satz von Rice in alternativer Formulierung:

Eine Klasse $\mathcal{C}$ rek. aufzählbarer Mengen heiße *nicht-trivial* gdw. sie enthält einige aber nicht alle rek. aufzählbaren Mengen. Ihre *Indexmenge* sei $I = \{e : W_e \in \mathcal{C}\}$.

Satz 4. Sei $\mathcal{C}$ eine nicht-triviale Klasse rek. aufz. Mengen mit Indexmenge I.
Entsprechend ist $J = \mathbb{N} \setminus I$ die Indexmenge des Komplements von $\mathcal{C}$.
Dann gilt $\mathcal{K} \leq_m I$ oder $\mathcal{K} \leq_m J$.

Beweis: Falls $\emptyset \notin \mathcal{C}$, gibt es eine andere Menge $A \in \mathcal{C}$. Definiere eine Nummerierung $L_0, L_1, L_2, \ldots$ vermöge

$$L_x = \begin{cases} \emptyset & \text{falls } x \notin \mathcal{K}; \\ A & \text{falls } x \in \mathcal{K}. \end{cases}$$

Da $W_0, W_1, W_2, \ldots$ eine akzeptable Nummerierung ist, gibt es rekursive Funktion f mit $W_{f(x)} = L_x$. Also gilt: $W_{f(x)} \in \mathcal{C} \Leftrightarrow x \in \mathcal{K}$. M.a.W.: f ist eine m-Reduktionsfunktion von $\mathcal{K}$ auf I.

Falls $\emptyset \in \mathcal{C}$, wähle eine Menge $A \notin \mathcal{C}$.

Entsprechend zeigt man: Es gibt eine m-Reduktionsfunktion von $\mathcal{K}$ auf J.

Eine wichtige Eigenschaft m-vollständiger Mengen

Satz 5. Ist A m-vollständig, so gibt es eine unendliche rekursiv aufzählbare von A disjunkte Menge B.

Beweis: Wegen der Myhill-Charakt. ist A kreativ mit Zeugen f.
smn-Eigenschaft $\leadsto$ Es gibt rek. Fkt. r mit $W_{r(x)} = W_x \cup \{f(x)\}$.
Sei e_0 ein Index für die leere Menge, $e_{n+1} = r(e_n)$.
$B := \bigcup_n W_{e_n} = \{f(e_n) \mid n \in \mathbb{N}\}$.
Per Ind.: $|W_{e_n}| = n$ und $W_{e_n} \cap A = \emptyset$.
Im IS Ann.: $|W_{e_n}| = n$ und $W_{e_n} \cap A = \emptyset$; $W_{e,n+1}$ enthält zusätzlich das Element $f(e_n) \notin A$.
$\leadsto$ B hat die geforderten Eigenschaften.

Diese Konstruktion motivierte Post zu folgender Definition:
Eine rekursiv aufzählbare Menge A heiße *simpel*, wenn $\mathbb{N} \setminus A$ unendlich ist und jede unendliche rek. aufzählbare Menge schneidet.
Klar: Simple Mengen sind nicht m-vollständig.

Zur Existenz weiterer rek. aufzählbarer $\mathfrak{m}$-Grade; Post konnte zeigen:

Satz 6. Es gibt eine simple Menge.

Beweis: Sei $I_n = \{2^n - 1, 2^n, \ldots, 2^{n+1} - 2\}$.
Definiere $\psi(\langle e, n\rangle)$ durch folgenden Algorithmus:
1. Falls $e < n$, so suche das erste s mit $W_{e,s} \cap I_n \neq \emptyset$ und setze $\psi(\langle e, n\rangle) = \min(W_{e,s} \cap I_n)$.
2. Falls $e \geq n$ (oder falls die Suche in 1. nicht terminiert), so ist $\psi(\langle e, n\rangle)$ undefiniert.
Für jedes n ist $\psi(\langle e, n\rangle)$ höchstens für n Zahlen e definiert, die kleiner als n sind und für die $\psi(\langle e, n\rangle) \in I_n$ gilt (sofern $\psi(\langle e, n\rangle)$ def.)
Sei A der Wertebereich von ψ. Eigenschaften von A:

- A ist rek. aufzählbar als Werteber. einer part.-rek. Fkt.;
- A is co-unendlich: für jedes n gilt: $|A \cap I_n| \leq n < |I_n|$;
- A besitzt mit jeder Menge W_e einen unendlichen Schnitt, denn jede Menge I_n mit $n > e$ erfüllt entweder $W_e \cap I_n = \emptyset$ oder $\psi(\langle e, n\rangle)\downarrow \in A \cap W_e \cap I_n$.

Einordnung und Ausblick

Post hat $\mathfrak{m}$-Reduktionen und simple Mengen als Hilfsmittel eingeführt.
Eigentlich war er an den *Turing-Graden* interessiert.
Damit beschäftigen wir uns in der nächsten Stunde.

Auf dem langen Weg zur Lösung dieser Fragestellung wurden viele weitere Reduktionsbegriffe eingeführt.

Ganz analoge Überlegungen finden sich auch in der Komplexitätstheorie.