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

Mehr zu Turing-Graden

Eine Menge A heißt *T-reduzierbar* auf die Menge B gdw. A ist rekursiv bzgl. B.

Schreibweise: $A \leq_T B$: A ist T-reduzierbar auf B.

Schreibweise: $A \equiv_T B$ gdw. $A \leq_T B$ und $B \leq_T A$.

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

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

Heute studieren wir die Menge $\mathbf{D}$ der T-Grade, zusammen mit der von $\leq$ geerbten Halbordnung $\leq$. Bsp.: $\mathbf{0} \leq \mathbf{0}'$ (hier strikt!)
Das gestattet sogar eine befriedigende Antwort auf Posts Problem!

Kleinste obere Schranken und größte untere Schranken

Diese (bekannten) Begriffe machen für jede Halbordnung Sinn.
Schreibweise: $\mathbf{a} \cup \mathbf{b}$ bzw. $\mathbf{a} \cap \mathbf{b}$ für Grade $\mathbf{a}, \mathbf{b}$.
Die *disjunkte Vereinigung* zweier Zahlenmengen lässt sich wie folgt realisieren:
$A \oplus B \iff \{2x \mid x \in A\} \cup \{2x+1 \mid x \in B\}$,

Satz 1: Für bel. T-Grade $\mathbf{a}, \mathbf{b}$ und bel. Mengen $A \in \mathbf{a}$, $B \in \mathbf{b}$ gilt: $\mathbf{a} \cup \mathbf{b}$ ist der T-Grad von $A \oplus B$.

Beweis: Wegen $x \in A \iff 2x \in A \oplus B$ und $x \in B \iff 2x+1 \in A \oplus B$ gilt $A, B \leq_T A \oplus B$.
Betrachte C mit $A, B \leq_T C$. Zu zeigen bleibt: $A \oplus B \leq_T C$.
Seien $\chi_A = h_a^C$ und $\chi_B = h_b^C$ (Gödelnummern bzgl. Orakel C).
Berechne $\phi = \chi_{A \oplus B}$ wie folgt mit Hilfe von C:
$\phi(z) = h_a^C(x)$, falls $z = 2x$.
$\phi(z) = h_b^C(x)$, falls $z = 2x+1$.
Also ist $A \oplus B \in \mathbf{a} \cup \mathbf{b}$.

Der Sprungoperator

Der *Sprung* einer Menge A, kurz A', ist die Relativierung von $\mathcal{K}$ auf A, d.h.:

$$x \in A' \iff x \in W_x^A \iff h_x^A(x) \downarrow .$$

Bsp.: Mit $A = \emptyset$ folgt: $\emptyset' = \mathcal{K}$.
Das erklärt auch die Schreibweisen für T-Grade.

Durch Relativierung des bekannten Ergebnisses über das spezielle Halteproblem $\mathcal{K}$ folgt:

Lemma: A' ist nicht rekursiv in A.

Weitere Eigenschaften des Sprungoperators

Man kann zeigen: Gilt $A \equiv_T B$ und ist $\mathbf{a}$ der Turing-Grad von A, so gilt: $A' \equiv_T B'$, und $\mathbf{a}'$ ist der Turing-Grad von A'.

$\leadsto$ Der Sprungoperator ist ein Operator auf T-Graden.

In diesem Sinne gilt: $\mathbf{a} \leq \mathbf{b} \implies \mathbf{a}' \leq \mathbf{b}'$.

Daraus folgt: $\mathbf{a}' \cup \mathbf{b}' \leq (\mathbf{a} \cup \mathbf{b})'$.

Man sieht nämlich so, dass $(\mathbf{a} \cup \mathbf{b})'$ eine obere Schranke von $\mathbf{a}'$ und von $\mathbf{b}'$ ist, die natürlich nicht kleiner sein kann als die kleinste obere Schranke.

Die Halbordnungsperspektive legt Fragen nahe wie:
Ist diese Grad-Ordnung linear? Oder gibt es unvergleichbare Grade?
Gäbe es solche sogar unterhalb von $\mathbf{0}'$, so wäre das eine weitere Lösung für das Postsche Problem.

Die endliche Erweiterungsmethode

Satz 2. Es gibt zwei unvergleichbare T-Grade.

Beweis: Aufgabe: Konstruktion zweier Mengen A, B, sodass weder $A \leq_T B$ noch $B \leq_T A$ gilt.
$A \leq_T B$ bedeutet: $\chi_A = h_e^B$.
Als Bedingungen formulieren wir:
$R_{2e}: \chi_A \neq h_e^B$.
$R_{2e+1}: \chi_B \neq h_e^A$.
Mengen $M \subseteq \mathbb{N}$ lassen sich als “Bitvektoren” $M : \mathbb{N} \to \{0, 1\}$ interpretieren und so als unendliche Zeichenkette aufschreiben.
Endliche Anfangsstücke hiervon entsprechen wiederum Approximationen an M.
Wir werden die Mengen A und B induktiv definieren, wobei jeweils endliche Anfangsstücke σ_s bzw. τ_s auf Stufe s angegeben werden.
Schließlich setze: $A = \bigcup_{s\in\mathbb{N}} \sigma_s$ und $B = \bigcup_{s\in\mathbb{N}} \tau_s$.

Forts. des Beweises

Anfang: $\sigma_0 = \tau_0 = \emptyset$.

Auf Stufe $s+1$ nehmen wir an, σ_s und τ_s seien definiert.
Falls $s = 2e$, so erfüllen wir R_{2e} wie folgt:
Wir setzen zunächst $\tau_{s+1} = \tau_s$ und kümmern uns nun um σ_{s+1}.
Sei x das kleinste Element, für das $\sigma_s(x)$ nicht def. ist.
Wir wollen erreichen, dass $\chi_A(x) \neq h_e^B(x)$ ist.
Da wir von B evtl. noch nicht genügend kennen, suchen wir nach einer Erweiterung τ von τ_s (Breitensuche), sodass $h_e^\tau(x) \downarrow$.
Ist diese Suche erfolgreich, so setzen wir $\tau_{s+1} = \tau$.
Ist $h_e^B(x) \uparrow$ (d.h., der beschriebene Suchprozess war nicht erfolgreich) oder $h_e^B(x) \notin \{0, 1\}$, so können wir σ_{s+1} bel. festlegen, z.B. als lexikographisch kleinste Erweiterung von σ_s, sodass σ_{s+1} auf x def. ist.
Andernfalls diagonalisiere: $\sigma_{s+1}(x) = 1 - h_e^B(x) = 1 - h_e^{\tau_{s+1}}(x)$.

Falls $s = 2e+1$, so erfüllen wir R_{2e+1} entsprechend.

Doch noch eine Lösung für Posts Frage

Hinweis: Man kann den Induktionsschritt effektivisieren, indem man die Suche nach einer geeigneten Erweiterung τ von τ_s genauer beschreibt. Wenn $A, B \leq_T \mathbf{0}'$, kann man dies mit der Schwalbenschwanzmethode durchführen und jeweils mit einem Orakelaufruf an $\mathcal{K}$ die Konvergenzfrage von $h_e^\tau(x)$ klären. Dies ist möglich, denn ein endliches Orakel (wie τ) kann in eine "normale TM" fest eingebaut werden als endliche Zusatzinformation in der Überführungstafel.

Folgerung: Es gibt zwei unvergleichbare T-Grade unterhalb von $\mathbf{0}'$.

Sacks konnte einen viel stärkeren Satz zeigen:

Mitteilung: Jede abzählbare Halbordnung lässt sich in die Grade unterhalb von $\mathbf{0}'$ einbetten.

Die Arithmetische Hierarchie

Was bedeutet überhaupt “Wahrheit” für eine arithmetische Aussage, also eine Aussage “über Zahlen”?

Um dies formal beschreiben zu können, ordnen wir den uns bekannten Zahlen Zahlensymbole zu durch Einführung eines Überstrichs.
Entsprechend verfahren wir mit den Operationen Plus und Mal.
Wir betrachten für die Definition der Wahrheit in der Arithmetik außerdem die Sprache der Logik erster Stufe, die Quantifizierungen nur für Zahlen (und nicht für Mengen) zulässt.

Wahrheit in der Arithmetik (gemäß Tarski)

Es sei $\mathcal{A}$ die intendierte Struktur, also hier die natürlichen Zahlen.

Die Logiksprache $\mathcal{L}$ wird im Folgenden beschrieben.

$\mathcal{A} \models \overline{m \mathbin{\overline{+}} n} = \overline{p}$ gdw. $m + n = p$.

$\mathcal{A} \models \overline{m} \mathbin{\bar{\cdot}} \overline{n} = \overline{p}$ gdw. $m \cdot n = p$.

$\mathcal{A} \models \neg\psi$ gdw. $\mathcal{A} \models \psi$ ist falsch.

$\mathcal{A} \models \psi_0 \wedge \psi_1$ gdw. $\mathcal{A} \models \psi_0$ und $\mathcal{A} \models \psi_1$.

$\mathcal{A} \models \psi_0 \vee \psi_1$ gdw. $\mathcal{A} \models \psi_0$ oder auch $\mathcal{A} \models \psi_1$.

$\mathcal{A} \models \exists x \psi(x)$ gdw. $\mathcal{A} \models \psi(\overline{n})$ für eine nat. Zahl n.

$\mathcal{A} \models \forall x \psi(x)$ gdw. $\mathcal{A} \models \psi(\overline{n})$ für alle nat. Zahlen n.

Eine n-stellige Relation P heißt *definierbar in Logik erster Ordnung* oder kurz *arithmetisch* gdw. für eine Formel ϕ mit n freien Variablen gilt:

$P(x_1, \ldots, x_n) \iff \mathcal{A} \models \phi(\overline{x_1}, \ldots, \overline{x_n})$

Man kann die obige Definition noch etwas verallgemeinern, indem für jede rekursive n-stellige Relation R ein atomares Symbol h_R in die Logik eingeführt wird.
Zur Unterscheidung werde die intendierte Struktur jetzt mit $\mathcal{A}^*$ bezeichnet.
Die Logiksprache heiße nun $\mathcal{L}^*$. Es gilt also:
$\mathcal{A}^* \models h_R(\overline{x_1}, \ldots, \overline{x_n})$ gdw. $R(x_1, \ldots, x_n)$.
Eine n-stellige Relation P liegt in der *arithmetischen Hierarchie* gdw. für eine Formel ϕ mit n freien Variablen gilt:
$P(x_1, \ldots, x_n) \iff \mathcal{A}^* \models \phi(\overline{x_1}, \ldots, \overline{x_n})$.

Gödel konnte zeigen:
Mitteilung: Die arithmetische Hierarchie enthält genau die arithmetischen Relationen.

Normalformen

Satz 3. Jede Relation in der arithmetischen Hierachie lässt sich in eine Form bringen, in der zunächst alternierend Quantoren aufgelistet sind und dann eine rekursive Relation beschrieben wird.
Solch eine *pränexe Normalform* ist aus der Logik bekannt.
Wesentliche Hilfsmittel:
—de Morgan für das Vorziehen von Quantoren,
—Cantorsche Paarfunktion für das Zusammenziehen gleichartiger Quantoren.
"Alternierend" soll nämlich bedeuten: Auf einen Allquantor folgt ein Existenzquantor und darauf wieder ein Allquantor usf.

Die Schichten der Arithmetischen Hierarchie

Σ_n: Die Klasse der Relationen, die über $\mathcal{A}^*$ definierbar sind durch eine Formel in $\mathcal{L}^*$ in pränexer Form (mit rekursiver Relation am Ende) mit n alternierenden Quantoren im Präfix, dessen äußerster (also erster) ein Existenzquantor ist.
Π_n: wie eben, nur dass der äußerste Quantor ein Allquantor ist.
$\Delta_n = \Sigma_n \cap \Pi_n$.

Speziell:
$\Sigma_0 = \Pi_0 = \Delta_0 = \Delta_1$ sind die rekursiven Relationen.
Σ_1 sind die aufzählbaren Relationen.
Π_1 sind die Komplemente aufzählbarer Relationen.

Beispiele

Die Menge FIN der Indizes endlicher Mengen liegt in Σ_2:
W_x ist endlich gdw. $\exists s \forall t [t \leq s \vee W_{x,s} = W_{x,t}]$.

Die Menge $\{\langle x, y \rangle \mid W_x \subseteq W_y\}$ liegt in Π_2:

$$\begin{aligned} W_x \subseteq W_y &\iff \forall z [z \in W_x \to z \in W_y] \\ &\iff \forall z [z \notin W_x \vee z \in W_y] \\ &\iff \forall z [\forall s \exists t (z \notin W_{x,s} \vee (t > s \wedge z \in W_{y,t}))] \\ &\iff \forall q = \langle z, s \rangle \exists t (z \notin W_{x,s} \vee (t > s \wedge z \in W_{y,t})) \end{aligned}$$

Übungen: (1) Die Menge aller Indizes der Menge $\mathbb{N}$ liegt in Π_2,
(2) Die Menge REC aller Indizes aller rekursiven Mengen liegt in Σ_3.

Elementare Eigenschaften

Satz 4. Es gelten die folgenden Eigenschaften:

(1) $A \in \Sigma_n$ gdw. $\bar{A} \in \Pi_n$.

(2a) $A, B \in \Sigma_n$ impliziert $A \cup B, A \cap B \in \Sigma_n$.

(2b) $A, B \in \Pi_n$ impliziert $A \cup B, A \cap B \in \Pi_n$.

(3) $(R \in \Sigma_n, n > 0, A = \{x \mid \exists y R(x, y)\}) \implies A \in \Sigma_n$.

(4) $(B \leq_m A, A \in \Sigma_n) \implies B \in \Sigma_n$.

(5a) Die universelle Quantifizierung einer Σ_n-Relation ist in Π_{n+1}, und

(5b) die existentielle Quantifizierung einer Π_n-Relation ist in Σ_{n+1}.

Eine wichtige Relativierung: Der Satz von Post

Satz von Post (bekannt): Eine Menge A ist rekursiv gdw. $A \in \Sigma_1$ und $\bar{A} \in \Sigma_1$ (also $A \in \Pi_1$), d.h., A liegt in Δ_1.

Allgemeiner gilt:

Satz 5. Eine Menge A ist rekursiv in einer Menge $B \in \Sigma_n$ gdw. A ist rek. aufzählbar in B und $\bar{A}$ ist rek. aufzählbar in B, d.h., A liegt in Δ_{n+1}.

Speziell liegt eine Menge in Δ_2 gdw. sie rekursiv in $\mathcal{K}$ ist.

Shoenfields Limit-Lemma

Satz 6. $A \in \Delta_2$ gdw. $\forall x[\chi_A(x) = \lim_{s\to\infty} g(x,s)]$ für eine rekursive Fkt. g.

Beweis: Ist g gegeben, so gilt: $x \in A$ gdw. $\forall s \exists t[t \geq s \wedge g(x,t) = 1]$ gdw. $\exists s \forall t[t < s \vee g(x,t) = 1]$-
D.h.: $A \in \Delta_2 = \Sigma_2 \cap \Pi_2$.
Falls $A \in \Delta_2$, so $A \leq_T \mathcal{K}$. Sei e ein Index mit $\chi_a \simeq h_e^{\mathcal{K}}$. Setze nun $g(x,s) = h_e^{\mathcal{K},s}(x)$.

Der Schluss-Sprung

Der Begriff der m-Vollständigkeit lässt sich auch für die Schichten der Arithmetischen Hierarchie anwenden.
Man kann zeigen (wieder durch Relativierung):
Satz 7. $\emptyset^{(n)}$ ist m-vollständig für Σ_n.

Konkrete m-vollständige Probleme liefern gerade die Beispiele von oben:
FIN ist Σ_2-(m)-vollständig.
REC ist Σ_3-(m)-vollständig.

Einordnung und Ausblick

Wir werden hier den Einstieg in die Rekursionstheorie abbrechen.

In der nächsten Vorlesung beginnen wir mit der Lerntheorie.

Wir werden dort einigen Techniken wieder begegnen, was nicht verwundern sollte, denn Lerntheorie will in ihrer rekursionstheoretischen Ausprägung untersuchen, inwieweit künstliche Systeme (Computer) lernen können.

Wieder geht es also um die Grenzen dessen, was mit Rechnern möglich ist.