Berechenbarkeit und Logik

Prof. Dr. Heribert Vollmer, SS05

Zusammenfassung

Jan Hinzmann

11. Oktober 2005

Inhaltsverzeichnis

0 Einleitung

0.1 Begriffe

Zunächst sollen einige Begriffe und Zeichen rekapituliert werden:

$\mathbb{N}$	$\{0, 1, 2, 3, ...\}$ natürliche Zahlen
$\mathbb{Z}$	$\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$ ganze Zahlen
$A \subseteq B$	„A ist Teilmenge von B“
$B \supseteq A$	„B ist Obermenge von A“

$\rightarrow$	materielle Implikation (wennn ..., dann) $a \rightarrow b$
$\leftrightarrow$	materielle Äquivalenz (genau dann wenn) $a \leftrightarrow b$
$\mathcal{M} \models F$	F wird unter $\mathcal{M}$ wahr
bijektiv	eindeutig, Umkehrfunktion, surjektiv + injektiv
surjektiv	„Jedes Element der Zielmenge wird min. einmal getroffen“
injektiv	eindeutig, keine Umkehrfunktion (Zielbereich größer als Def.-bereich)
$\Gamma,\ \gamma$	„Gamma, gamma“
$\Delta,\ \delta$	„Delta, delta“
$X,\ \chi$	„Chi, chi“
$c_A(x)$	die charakteristische Funktion einer Sprache A, ist sie berechenbar, ist die Sprache A entscheidbar.
$\chi_A(x)$	„Chi von x“, ist sie berechenbar, ist die Sprache A semi-entscheidbar
$A \subseteq \Sigma^*$	Sprache für eine TM
$\overline{A}$	$\overline{A} = \Sigma^* \backslash A$
entscheidbar	rekursiv (Sprachen)
berechenbar	rekursiv (Funktionen)
$\langle x, y \rangle$	$\langle x, y \rangle = c(x, y)$ Skript S.2

Tabelle 1: Begriffe

0.2 Sätze

f ist berechenbar	$\Rightarrow$ f kann von einer TM berechnet werden.
A ist entscheidbar	$\Rightarrow$ $c_A(x)$ ist berechenbar
A ist entscheidbar	$\Rightarrow$ $A, \overline{A}$ sind rekursiv-aufzählbar
A ist semi-entscheidbar	$\Rightarrow$ $\chi_A(x)$ ist berechenbar
A ist rekursiv-aufzählbar	$\Rightarrow$ A ist semi-entscheidbar
A ist rekursiv-aufzählbar	$\Rightarrow$ A ist Wertebereich einer berechenbaren Fkt.
A ist rekursiv-aufzählbar	$\Rightarrow$ $A = \emptyset$ oder es gibt eine totale, berechenbare Funktion, die A aufzählt.
K	$\Rightarrow$ spezielles Haltproblem $K = \{x \mid M_x \text{bei Eingabe } x \text{ hält}\}$, (ist rekursiv-aufzählbar, nicht rekursiv)
$\overline{K}$	$\Rightarrow$ ist nicht rekursiv-aufzählbar
K_0	$\Rightarrow$ allgemeines Halteproblem $K_0 = \{\langle x, y \rangle \mid M_x \text{ bei Eingabe } y \text{ hält}\}$ K_0 ist nicht entscheidbar.
$A \leq B,\ B$ rekursiv	$\Rightarrow$ A ist rekursiv
$A \leq B,\ A$ nicht rekursiv	$\Rightarrow$ B ist nicht rekursiv

Tabelle 3: Sätze

0.3 Turingmaschine

Eine Turingmaschine (TM) ist ein 7-Tupel $M = (Q, \Sigma, \Gamma, \delta, q_0, \square, F)$, wobei

- Q die Menge der Zusände ist, die die Turingmaschine annehmen kann
- Σ das Eingabealphabet ist, welches die TM akzeptiert,
- $\Gamma \supseteq \Sigma$ das Arbeitealphabet ist,
- δ die Überführungsfunktion ist, mit $\delta : Q \times \Gamma \to Q \times \Gamma \times \{L, N, R\}$,
- $q_0 \in Q$ der Startzustand ist
- $\square \in \Gamma$ der Leersymbol ist und
- $F \subseteq Q$ die Endzustände von M sind.

1 Rekursive Aufzählbarkeit

1.1 These von Church

Kann eine Funktion mit k Parametern durch eine Turingmaschine berechnet werden, do ist sie *berechenbar* bzw. *rekursiv.*

Dabei gibt die TM das Ergebns aus, wenn die Funktion für die Eingabe definiert ist. Sonst läuft die TM in einer Endlosschleife.

1.2 Gödelisierung

Bei der Gödelisierung werden Turingmaschinen als Wörter über $\{0, 1\}$ kodiert. Die Gödelnummer $e \in \{0, 1\}^\star$ charakterisiert dann eine bestimmte Turingmaschine M_e. Hierzu werden den Buchstaben aus dem Eingabealphabet z.B. Primzahlen zugeordnet. Hierbei wird die Stelle des Vorkommens im Eingabewort berücksichtigt. Die Primzahlen werden anschließend miteinander multipliziert und es ergibt sich die Gödelnummer der Turingmaschine für die bestimmte Eingabe.

Beispiel Das Eingabealphabet sei $\Sigma = \{a, b, c\}$. Die laufenden Primzahlen sind $\{p_0 = 2, p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, ...\}$.

	a	b	c
0	02	03	05
1	07	11	13
2	17	19	23
3	29	31	37
4	41	43	47

Nun wird jedem Buchstaben σ_i aus dem Eingabealphabet der Reihe nach eine Primzahl zugeordnet, wobei der Index i die Stelle des Vorkommens im Eingabewort kennzeichnet. Ein Eingabewort ist also als $\sigma_0\sigma_1\sigma_2...$ zu verstehen.

Das Eingabealphabet in diesem Beipiel wird also durch $a_0 = 2, b_0 = 3, c_0 = 5$ kodiert. Um nun auch die Stelle des Vorkommens in einem Wort zu kennzeichnen, werden jedem Buchstaben weitere Primzahlen zugeordnet, beginnend mit der ersten freien Primzahl. Also $a_1 = 7, b_1 = 11, ...$ (s. Tabelle).

Die Gödelnummer des Eingabewortes *cabba* ergibt sich aus der Multiplikation der einzelnen Primzahlen für die Buchstaben.
Hier also $c_0a_1b_2b_3a_4 = 5 \cdot 7 \cdot 19 \cdot 31 \cdot 41 = 845215$.

1.3 Turingmaschinen als Akzeptoren

Die von einer Turingmaschine M akzeptierte Sprache ist W, unter der Bedingung $\{\omega \mid \text{M hält unter der Eingabe } \omega\}$. Die von M_e akzeptierte Sprache ist W_e.
Eine Sprache heißt *semi-rekursiv* (bzw. *semi-entscheidbar*), wenn sie eine Menge W_e für ein $e \in \mathbb{N}$ ist.
Eine Sprache A heißt *rekursiv* (bzw. *entscheidbar*), falls ihre charakteristische Funktion rekursiv (bzw. berechenbar) ist, wobei gilt:

$$c_A(x) := \begin{cases} 0, & falls\ x \notin A, \\ 1, & falls x \in A. \end{cases}$$

Eine Sprache A heißt *semi-rekursiv* gdw. χ_A rekursiv (bzw. berechenbar) ist, wobei gilt:

$$\chi_A(x) := \begin{cases} 1, & falls\ x \in A, \\ undef., & sonst. \end{cases}$$

Beobachtung: Es gibt nicht berechenbare Funktionen $f : \mathbb{N}^k \to \mathbb{N}$ und somit auch nicht semi-entscheidbare Mengen.

Definition Eine Sprache heißt

1.4 Satz von Rice

Sei $\mathcal{F} \neq \emptyset$ ein Menge von berechenbaren Funktionen, die aber nicht alle berechenbaren Funktionen enthält. Dann ist $C(\mathcal{F}) = \{x|\phi_x \in \mathcal{F}\}$ nicht rekursiv und nicht entscheidbar.
Beispiele nicht entscheidbarer Mengen sind:

$$\begin{aligned}
K_1 &= \{x \mid W_x \neq \emptyset\} = \{x \mid \delta_x \text{ hat nicht-leeren Definitionsbereich}\} \\
\text{Fin} &= \{x \mid W_x \text{ ist endlich}\} \\
\text{Inf} &= \{x \mid W_x \text{ ist unendlich}\} \\
\text{Tot} &= \{x \mid \delta_x \text{ ist total}\} \\
\text{Con} &= \{x \mid \delta_x \text{ ist total und konstant}\} \\
\text{Rec} &= \{x \mid W_x \text{ ist entscheidbar}\} \\
\text{Cof} &= \{x \mid \overline{W_x} \text{ ist endlich}\}
\end{aligned}$$

Es gilt $K_0 \equiv K1 \equiv K$, Inf $\equiv$ Tot $\equiv$ Con und Rec $\equiv$ Cof.

2 PL1 – Prädikatenlogik erster Stufe

2.1 Syntax

Die folgende Tabelle gibt eine Übersicht über die Syntax der prädikaten Logik erster Stufe.

Syntax

Logische Symbole	$\neg, \vee, \wedge, \rightarrow, \leftarrow, \forall, \exists, =$
Syntaktische Symbole	`(`, `)` und `,`
Variablen	x, y, z
Nichtlogische Symbole	f, g, h, ... (Funktionen) R, ... (Relationen) a, b, c, ... (Konstanten)
Terme	a Konstantensymbol $\Rightarrow a$ ist ein Term x Variable $\Rightarrow x$ ist ein Term $t_1, \ldots, t_n$ Terme, f n-stelliges Funktionensymbol $\Rightarrow f(t_1, \ldots, t_n)$ ist ein Term
Atomare Formeln	Gleichungen von Termen $(t_1 = t_2)$ und Relationen $(R(t_1, \cdots, t_n))$ sind atomare Formeln.
Formeln	
Sätze	Eine Formel ist ein Satz, wenn in ihr keine freien Variablen vorkommen

Beispiele für Terme: $f(x, y)$, a, $g(x)$ sind Terme.

Atomare Formeln Seien t_1, t_2 Terme, dann ist $t_1 = t_2$ eine atomare Formel. Ebenso gilt: Sind $t_1, ..., t_n$ Terme und R ein n-stelliges Relationssymbol, dann ist $R(t_1, ...t_n)$ eine atomare Formel.

Beispiele für atomare Formeln: $f(x, y) = a$, $R(x, y)$, $R(x, g(x))$ sind atomare Formeln.

Formeln F_1, F_2 Formeln $\Rightarrow \neg F_1,\ F_1 \wedge F_2,\ F_1 \vee F_2,\ F_1 \rightarrow F_2,\ F_1 \leftrightarrow F_2$ sind Formeln.
F Formel, x Variable $\Rightarrow \exists xF$, $\forall yF$ sind Formeln.

Symbolmenge Man fasst die nichtlogischen Symbole in der Menge L zusammen. Dies ist die „Symbolmenge“. Die Symbolmenge der Arithmetik heißt L^* und umfasst die Symbole:

Konstantensymbol	0	
einstelliges Funktionensymbol	$'$	*Schreibweise:* postfix: $0', x'$
zweistelliges Funktionensymbol	$+, \cdot$	*Schreibweise:* infix: $x + y$, $x \cdot y$
zweistelliges Funktionensymbol	$<$	*Schreibweise:* infix: $x < y$

Beispiele für Formeln über L^*

$$\forall x \forall y(x \cdot y = 0 \rightarrow (x = 0 \vee y = 0))$$
$$\forall x(x < x' \wedge \neg \exists z(x < z \wedge z < x'))$$

Sätze In Formeln gibt es *gebundene Variablen* und *freie Variablen*. In der Formel $\forall x(a+x = b)$ ist x eine gebundene Variable und a und b sind freie Variablen. Eine Formel ist ein Satz, wenn in ihr keine freien Variablen vorkommen.

Interpretationen Um nun Sätzen Wahrheitswerte zuzuordnen werden Interpretationen der nichtlogischen Symbole benötigt. Ist L die Symbolmenge, dann ist $\mathcal{M}$ eine Interpretation von L, bestehend aus:

- Einer Grundmenge $M \neq \emptyset$ ($M = |\mathcal{M}|$), („Universum")
- Für jedes n-stellige Funktionensymbol f aus L enthält $\mathcal{M}$ eine n-stellige Funktion $f^{\mathcal{M}} : M^n \rightarrow M$.
- Für jedes n-stellige Relationensymbol R aus L enthält $\mathcal{M}$ eine n-stellige Relation $R^{\mathcal{M}} \subseteq M^n$.
- Für jedes Konstantensymbol $a \in L$ enthält $\mathcal{M}$ eine Konstante $a^{\mathcal{M}} \in M$.

Beispiel: Die Standardinterpretation $\mathcal{N}^*$ der Symbolmenge L^* der Arithmetik ist gegeben durch

- $|\mathcal{N}^*| = \mathbb{N}$ (Menge der natürlichen Zahlen $\{1,2,3, ...\}$)
- $0^{\mathcal{N}^*} = 0$
- $+^{\mathcal{N}^*}$ ist die Addition, $\cdot^{\mathcal{N}^*}$ die Multiplikation und $'^{\mathcal{N}^*}$ die Nachfolgerfunktion $\big((n)'^{\mathcal{N}^*} = (n+1)\big)$ auf $\mathbb{N}$
- $<^{\mathcal{N}^*}$ ist die Kleiner-Relation auf $\mathbb{N}$, $<^{\mathcal{N}^*} = \{(m, n) | m < n\}$

2.2 Semantik

s. Skript, S.8

Extrakt: $\mathcal{M} \models F$, falls F unter $\mathcal{M}$ wahr wird. Zum Beispiel

- Sei $F : t_1 = t_2$, dann ist $\mathcal{M} \models F$ gdw. $t_1^{\mathcal{M}} = t_2^{\mathcal{M}}$.
- $\mathcal{M} \models \neg F$, falls nicht $\mathcal{M} \models F$
- ...

3 Die Unentscheidbarkeit der Prädikatenlogik erster Stufe

Satz von Church Das Entscheidungsproblem für logische Implikationen ist unentscheidbar.

4 Beweise in der Prädikatenlogik erster Stufe

$\Gamma \vdash F$ soll heißen: „F ist ableitbar aus Γ“ bzw. „F ist beweisbar aus Γ“. Es gilt: $\Gamma \vdash F$ gdw. $\Gamma \models F$.

Theorie Eine Theorie ist eine Menge von Sätzen, die aus der Theorie ableitbar und in ihr enthalten sind. Es gilt also $T \vdash F$; $F \in T$.

Sei $\mathcal{M}$ eine L-Struktur, dan ist

$$Th(\mathcal{M}) = \{F | F \text{ ist Satz über } L, \Gamma \models F\}$$

eine Theorie (L Symbolmenge, $\mathcal{M}$ Interpretation).

Eine Theorie über der (Standard-)Interpretation der Arithmethik $Th(\mathcal{N}^*)$ heißt elementare Arithmetik.

Eine Theorie ist *vollständig*, wenn für jeden Satz F über der Symbolmenge L der Theorie gilt: $F \in T \vee \neg F \in T$.

Eine Theorie ist *axiomatisierbar*, wenn es eine entscheidbare Menge Γ von Sätzen F über der Symbolmenge L gibt, sodass $T = \Gamma^{\vdash} = \{F | F \text{ Satz über } L,\ \Gamma \models F\}$.

Eine axiomatisierbare Theorie ist rekursiv-aufzählbar.

Eine axiomatisierbare, vollständige Theorie ist entscheidbar.

5 Arithmetische Definierbarkeit

Es sei L^* die Symbolmenge der Arithmetik und $\mathcal{N}^*$ die Standardinterpretation der Arithmetik.

6 Zusammenfassung

In diesem Kaptitel werden die wichtigsten Begriffe und Sätze zusammengefasst.