GTI

Hannes Diener

ENC B-0123,
diener@math.uni-siegen.de

4.-9. Juli

Entscheidungsprobleme und Halteproblem

In diesem Kapitel wollen wir uns an Stelle von Berechenbarkeit von Funktion, welche bei einem Input eine natürliche Zahl als Output liefern, einfachere Probleme betrachten — die sogenannten Entscheidungsprobleme.
Dies sind Algorithmen von welchen wir nur eine Ja-Nein bzw. 0-1 Antwort erwarten.

Dies ist das Gleiche, wie wenn wir uns auf die Teilmengen der Eingabe konzentrieren, die eine positive Antwort geben:

$$\{\, x \text{ Input } \mid x \text{ liefert Antwort Ja} \,\} .$$

Äquivalent können wir uns ein Entscheidungsproblem auch als das Problem $x \in A$ auffassen, wobei $A \subseteq \mathbb{N}$. An Stelle von Mengen sprechen wir in diesem Sinne auch über Probleme.
Da wir Wörter über einem Alphabet $\{a_1, \ldots, a_n\}$ durch Tupel natürlicher Zahlen $(i_1, \ldots, i_m)$, wobei $i_1, \ldots, i_m \in \{1, \ldots, n\}$ kodieren können, macht es auch Sinn über Entscheidungsprobleme auf Wörtern zu reden.

Formal:

Definition

Eine Menge $A \subseteq \mathbb{N}^k$ heißt entscheidbar, falls ihre charakteristische Funktion $\chi_A : \mathbb{N}^k \to \mathbb{N}$, definiert durch

$$\chi_A(x) = \begin{cases} 1 & \text{falls } x \in A \\ 0 & \text{sonst} \end{cases}$$

berechenbar ist.

Definition

Eine Menge $B \subseteq \mathbb{N}$ heißt (rekursiv) aufzählbar oder semi-entscheidbar, falls sie entweder leer ist oder es eine totale berechenbare Funktion f gibt, so daß $f(\mathbb{N}) = B$; d.h.

$$B = \{f(0), f(1), \ldots\} \ .$$

Wiederholungen in der Aufzählung sind natürlich zugelassen.

Das *Komplement* einer Menge $A \subseteq \mathbb{N}$ ist die Menge
$\overline{A} = \{ n \in \mathbb{N} \mid n \notin A \}$

Satz

1. *Ist $A \subseteq \mathbb{N}$ entscheidbar, so ist A auch rekursiv aufzählbar.*
2. *Ist $A \subseteq \mathbb{N}$ entscheidbar, so auch $\overline{A}$.*
3. *Sind $B \subseteq \mathbb{N}$ und $\overline{B}$ rekursiv aufzählbar, so ist B entscheidbar.*

Man beachte, daß es keinen offensichtlichen Beweis gibt um aus der Aufzählbarkeit einer Menge B auf die von $\overline{B}$ zu schliessen:
Nehmen wir an f zählt A auf. Das heißt

$$B = \{f(0), f(1), \ldots\} \ .$$

Um zu entscheiden, ob ein Element $n \in \mathbb{N}$ ist können wir es nach und nach mit den Werten $f(0), f(1), f(2)$ usw. vergleichen. Kommt es irgendwann vor, wissen wir $n \in B$. Ist allerdings $n \notin B$, so warten wir vergebens. Anderst ausgedrückt wir können nie anfangen uns festzulegen ob ein Element in $\overline{B}$ ist, da ja immer immer noch in der Aufzählung von B vorkommen kann.[1]

[1] Dies ist natürlich kein Beweis, sondern nur eine intuitive Begründung.

Die offensichtliche Frage ist

> *Gibt es rekursiv-aufzählbare Mengen, die nicht entscheidbar sind?*

Dies ist äquivalent zu

> *Gibt es rekursiv-aufzählbare Mengen, deren Komplement nicht rekursiv-aufzählbar ist?*

Bevor wir diese Fragen positiv beantworten, wollen wir uns aber noch ein paar mehr Eigenschaften von entscheidbaren und rekursiv-aufzählbare Mengen betrachten.

Satz

Sind A, B entscheidbar (rekursiv-aufzählbar) so gilt

1. *$A \cup B$ ist entscheidbar (rekursiv-aufzählbar),*
2. *$A \cap B$ ist entscheidbar (rekursiv-aufzählbar).*
3. *Ist A rekursiv-aufzählbar und $f : \mathbb{N} \to \mathbb{N}$, so ist $f(A)$ rekursiv aufzählbar.*

Wie wir gesehen hatten gibt es eine universelle Turingmaschine; d.h. eine Turingmaschine T_u, die bei Eingabe eines Wortes $w_M\$w$, wobei w_M ein Code für die Turingmaschine M ist und w ein Eingabewort, genau dann mit Ausgabe v akzeptiert, wenn M dies tut.
Folgen wir den Ideen des letzten Kapitels können wir damit zeigen, daß es auch ein ähnliches Objekt für die μ-rekursiven Funktionen gibt.

Satz

Es gibt eine universelle Funktion $u : \mathbb{N}^2 \to \mathbb{N}$, *d.h. eine* μ*-rekursive Funktion* u, *so daß für jede* μ*-rekursive Funktion* f *eine Zahl* e *mit*

$$u(e, n) = f(n)$$

für alle $n \in \mathbb{N}$ *existiert.*

Beweis.

Die Funktion u ist prinzipiell nichts anderes, als die von der universellen Turingmaschine berechnete zweistellige Funktion. Da letztere offensichtlich Turingberechenbar ist, ist u μ-rekursiv. □

Die Zahl e sollte man sich also als Code einer Turingmaschine vorstellen, die f berechnet.

Kurzer Einschub: Funktionen mehrerer Variablen.

Satz

Ist $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ *eine Funktion, so gibt es eine Funktion* $g : \mathbb{N} \rightharpoonup \mathbb{N}$ *mit* $g(\langle x_1, \ldots, x_k \rangle^k) = f(x_1, \ldots, x_k)$. *Ausserdem ist* g *primitiv rekursiv (*μ*-rekursiv) genau dann wenn* f *es ist.*

D.h. für uns: es reicht unsere Betrachtungen auf einstellige Funktionen zu beschränken.

Dies führt uns zu folgenden Entscheidungsproblemen:

Definition

1. $H = \left\{ \langle e, x \rangle^2 \in \mathbb{N} \,\middle|\, u(e, x) \textit{ ist definiert} \right\}$ *(das Halteproblem)*
2. $H_d = \{ x \in \mathbb{N} \mid u(x, x) \textit{ ist definiert} \}$
3. $H_0 = \{ x \in \mathbb{N} \mid u(x, 0) \textit{ ist definiert} \}$

Satz (Unentscheidbarkeit des Halteproblems)

1. *Die Mengen H, H_d und H_0 semi-entscheidbar*
2. *Das Problem H_d ist nicht entscheidbar.*
3. *Das Problem H ist nicht entscheidbar.*

Bevor wir uns den Beweis ansehen benötigen wir noch eine interessante Definition.

Definition

Ein Problem $A \subseteq \mathbb{N}$ heißt reduzierbar auf ein Problem B via f, falls es eine μ-rekursive Funktion f gibt, so daß

$$x \in A \iff f(x) \in B \ .$$

In diesem Falle schreiben wir $A \leqslant B$.

Satz

Die Relation $\leqslant$ ist reflexiv und transitiv. D.h., $A \leqslant A$ und wenn $A \leqslant B$ und $B \leqslant C$, dann ist auch $A \leqslant C$.

Satz

Seien $A, B \subseteq \mathbb{N}$ mit $A \leqslant B$. Ist B entscheidbar, so auch A.

Beweis der Unentscheidbarkeit des Halteproblems.

1. Technisch, Idee in der Vorlesung.
2. Nehmen wir an H_d wäre entscheidbar. Sei $f : \mathbb{N} \to \mathbb{N}$ nun definiert durch

$$f(x) = \begin{cases} u(x,x) & \text{falls } \chi_{H_d}(x) = 1 \\ 0 & \text{sonst .} \end{cases}$$

Man beachte, daß f aus den μ-rekursiven Funktionen $\lambda x.u(x,x)$, $\lambda x.0$ und χ_{H_d} durch Fallunterscheidung hervorgeht, also μ-rekursiv ist.
Also existiert ein Index e, so daß $u(e,x) = f(x)$ für alle x.

... Beweis.

Wir unterscheiden nun zwei Fälle, die aber beide zu einem Widerspruch führen.

- Fall 1: $e \in H_d$. Dann ist $\chi_{H_d}(e) = 1$, also $f(e) = u(e, e) + 1$ nach Definition von f. Andererseits ist $f(e) = u(e, e)$, und wir haben einen Widerspruch.
- Fall 2: $e \notin H_d$. Dann ist $\chi_{H_d}(e) = 0$, also $f(e) = 0$ nach Definition von f. Andererseits ist $f(e) = u(e, e) = \bot$; ebenfalls ein Widerspruch.

Insgesamt kann H_d also nicht entscheidbar sein, da wir sonst auf alle Fälle einen Widerspruch finden können. □

Als nächstes wollen wir uns noch drei technische Sätze über die Berechenbarkeit ansehen:

- Das s-m-n–Theorem.
- Den Rekursionssatz.
- Den Fixpunktsatz.

Satz (*s-m-n*–Theorem)

Es gibt eine totale, μ-rekursive Funktion $s : \mathbb{N}^3 \to \mathbb{N}$, so daß für alle $i, m \in \mathbb{N}$ und $x_1, \ldots, x_m, y_1, \ldots, y_n \in \mathbb{N}$ gilt:

$$u(i, \langle x_1, \ldots, x_m, y_1, \ldots, y_n \rangle) = u(s(i, m, \langle x_1, \ldots, x_m \rangle), \langle y_1, \ldots, y_n \rangle)$$

Beweis.

Ausgelassen. □

Satz (Rekursionssatz)

Sei $h : \mathbb{N}^2 \to \mathbb{N}$ eine μ-rekursive Funktion. Dann gibt es einen Index r, so daß

$$u(r, \cdot) = h(r, \cdot)$$

Beweis.

- Sei $s' : \mathbb{N}^2 \to \mathbb{N}$ definiert durch $s'(i, x) = s(i, 1, x)$.
- Sei nun j, so daß $u(j, \langle i, x \rangle^2) = h(s'(i, i), x)$.
- Jetzt ist $h(s'(j, j), x) = u(j, \langle j, x \rangle^2) = u(s'(j, j), x)$.
- Also ist $r = (s'(j, j)$ ist der gesuchte Index. □

Satz (Fixpunktsatz)

Sei f eine totale μ-rekursive Funktion. Dann gibt es einen Index e, so daß

$$u(e, \cdot) = u(f(e), \cdot)$$

Beweis.

Sei $h : \mathbb{N}^2 \to \mathbb{N}$ definiert durch $h(i, x) = u(f(i), x)$. Offensichtlich ist h μ-rekursiv. Also existiert nach dem Rekursionssatz ein Index r, so daß $u(r, x) = h(r, x) = u(f(r), x) = u(f(r), x)$. □

Der Fixpunktsatz hat zwei nette Folgerungen:

- Es gibt keinen perfekten Virus
- Es gibt keinen schlechten Compiler

Aus dem *s-m-n*–Theorem können wir jetzt auch folgern, daß H_d auf H_0 reduzierbar ist und damit H_0 nicht entscheidbar ist.

Beweis.

Sei $f : \mathbb{N} \to \mathbb{N}$ definiert durch $f(\langle x, y \rangle^2) = u(x, x)$. Da f μ-rekursiv ist können wir einen Index r finden, so daß $u(r, \cdot) = f(\cdot)$. Dann ist mit dem *s-m-n*–Theorem

$$u(s(r, 1, x), y) = u(r, \langle x, y \rangle^2) = f(\langle x, y \rangle^2) = u(x, x) \ .$$

Insbesondere für $y = 0$ gilt also $u(s(r, 1, x), 0) = u(x, x)$. Also ist $H_d \leqslant H_0$ via $\lambda x.s(r, 1, x)$. □

Es gibt noch eine Vielzahl an natürlichen Problemen, die nicht entscheidbar sind. Allen gemeinsam ist, daß sie ähnlich dem Halteproblem Aussagen über alle berechenbaren Funktionen machen.

1. $\{ e \in \mathbb{N} \mid u(e, \cdot) \text{ ist total} \}$ (Totalitätsproblem)
2. $\{ e \in \mathbb{N} \mid u(e, \cdot) \text{ ist nirgends definiert} \}$ (Leerheitsproblem)
3. $\{ e \in \mathbb{N} \mid u(e, \cdot) = f \}$ (Korrektheitsproblem für eine Funktion f)

Definition (Indexmenge)

Eine Menge $I \subseteq \mathbb{N}$ heißt Indexmenge falls für alle $i, j \in \mathbb{N}$ gilt:

$$i \in I \wedge u(i, \cdot) = u(j, \cdot) \implies j \in I \ .$$

Satz (Satz von Rice)

Jede nicht-triviale Indexmenge ist nicht entscheidbar.

Beweis.

Wenn I nicht-trivial ist, also $\varnothing \neq I \neq \mathbb{N}$ gibt es i, j so daß $i \in I$ und $j \notin I$. Nehmen wir nun an, daß I entscheidbar ist, so ist $f : \mathbb{N} \to \mathbb{N}$ definiert durch

$$f(x) = \begin{cases} j, & \text{falls } x \in I \\ i, & \text{falls } x \notin I \end{cases}$$

total und μ-rekursiv. Nach dem Fixpunktsatz gibt es $r \in \mathbb{N}$ so daß $u(r, \cdot) = u(f(r), \cdot)$.

... Beweis.

- Ist $r \in I$, so ist dann, da I Indexmenge ist, auch $f(r) \in I$. Andererseits ist $f(r) = j \notin I$ ein Widerspruch.
- Ist $r \notin I$, so ist $f(r) = i \in I$ nach Definition von f. Also ist, da I Indexmenge ist auch $r \in I$; ebenfalls ein Widerspruch.

Insgesamt kann I also nicht entscheidbar sein. □