

# 10. Unentscheidbare Mengen

## Diagonalisierung und Reduktion

# DAS HALTEPROBLEM

Aus der Existenz universeller partiell rekursiver Funktionen lässt sich leicht mit einem Diagonalargument folgern, dass das Halteproblem für Turingmaschinen nicht rekursiv, also nach der Church-Turing-These unentscheidbar ist. Anschaulich bedeutet dies, dass wir einem Algorithmus i. Allg. nicht ansehen können, ob er für eine gegebene Eingabe terminiert.

Formal ist das Halteproblem wie folgt definiert:

## ALLGEMEINES HALTEPROBLEM:

$$K = \{\langle e, x \rangle : \varphi(e, x) \downarrow\} = \{\langle e, x \rangle : \{e\}(x) \downarrow\}$$

(Hierbei ist hier und im Folgenden  $\varphi$  stets die Gödelnummerierung der 1-stelligen partiell rekursiven Funktionen, die wir durch Gödelisierung der Turingmaschinen erhalten haben.)

## UNENTSCHEIDBARKEIT DES HALTEPROBLEMS

SATZ. Das allgemeine Halteproblem  $K$  ist nicht rekursiv.

BEWEIS (indirekt). Widerspruchsannahme:  $K$  sei rekursiv.

Definiere die Funktion  $g$  durch

$$g(x) = \begin{cases} \varphi(x, x) + 1 = \{x\}(x) + 1 & \text{falls } \langle x, x \rangle \in K \text{ (d.h. } \varphi(x, x) \downarrow) \\ 0 & \text{sonst.} \end{cases}$$

Wegen der angenommenen Rekursivität von  $K$  ist  $g$  rekursiv, besitzt also wegen der 1-Universalität von  $\varphi$  einen Index  $e$ , d.h.  $g = \varphi_e = \{e\}$ . Dies ist aber unmöglich, da  $g$  so definiert wurde, dass es sich an der Stelle  $x$  von der  $x$ -ten p.r. Funktion  $\{x\}$  unterscheidet:

- $\langle e, e \rangle \in K \Rightarrow \{e\}(e) \downarrow \Rightarrow g(e) = \{e\}(e) + 1 \neq \{e\}(e)$
- $\langle e, e \rangle \notin K \Rightarrow \{e\}(e) \uparrow \Rightarrow g(e) = 0 \neq \uparrow = \{e\}(e)$

## BEMERKUNGEN

1. Da eine Menge genau dann rekursiv (entscheidbar) ist, wenn ihre charakteristische Funktion rekursiv (berechenbar) ist, ist die charakteristische Funktion  $c_K$  des Halteproblems ein Beispiel für eine nichtrekursive (nichtberechenbare) Funktion.

2. Der Beweis der Unentscheidbarkeit des Halteproblems ähnelt dem Beweis der Nichtexistenz universeller total rekursiver Funktionen. Dies ist nicht zufällig. Aus letzterem Ergebnis kann man nämlich auf die Unentscheidbarkeit des Halteproblems mit Hilfe des folgenden indirekten Arguments schließen: Wäre  $K$  - und damit der Definitionsbereich von  $\varphi$  - entscheidbar, so könnte man  $\varphi$  zu einer 1-universellen total rekursiven Funktion  $f$  erweitern, indem man  $f(e, x) = 0$  für  $\langle e, x \rangle \notin K$  setzt.

3. Folgende Spezialfälle des Halteproblems sind - wie wir noch zeigen werden - ebenfalls unentscheidbar:

- DIAGONALES HALTEPROBLEM:  $K_d = \{e : \{e\}(e) \downarrow\}$
- INITIALES HALTEPROBLEM:  $K_0 = \{e : \{e\}(0) \downarrow\}$

## REDUKTIONSMETHODE

Der Nachweis der Unentscheidbarkeit eines Problems (d.h. einer Menge)  $B$  mit Hilfe der Diagonalisierungsmethode kann mitunter sehr schwierig sein. Eine Alternative ist die REDUKTIONSMETHODE. Hier zeigt man, dass sich ein bereits als unentscheidbar nachgewiesenes Problem  $A$  so in  $B$  kodieren lässt, dass sich die Unentscheidbarkeit von  $A$  auf  $B$  überträgt.

Dieser Nachweis wird in der allgemeinsten Form dadurch geführt, dass man zeigt, dass man aus einem hypothetischen Entscheidungsverfahren für  $B$  ein Entscheidungsverfahren für  $A$  gewinnen könnte. Da es Letzteres jedoch nicht gibt, kann man folgern, dass es auch kein Entscheidungsverfahren für  $B$  geben kann.

## RELATIVE ENTSCHEIDBARKEIT

$A \leq_{eff} B \Leftrightarrow A$  ist relativ zu  $B$  entscheidbar,  
d.h. aus der Existenz eines (hypothetischen)  
Entscheidungsverfahrens für  $B$  folgt die  
Existenz eines Entscheidungsverfahrens für  $A$

Offensichtlich gilt (mit Church-Turing-These):

- $A \leq_{eff} B$  &  $B$  rekursiv  $\Rightarrow A$  rekursiv

Mit Kontraposition folgt:

- $A \leq_{eff} B$  &  $A$  nicht rekursiv  $\Rightarrow B$  nicht rekursiv

## FORMALISIERUNG DER RELATIVEN ENTSCHEIDBARKEIT

Den Begriff der relativen Entscheidbarkeit und der - analog definierten - relativen Berechenbarkeit kann man mit Hilfe von Turingmaschinen, Registermaschinen oder den partiell rekursiven Funktionen formalisieren, indem man diese formalen Berechnungsmodelle geeignet erweitert.

Im Falle der Turing- bzw. Registermaschinen betrachtet man sog. *Orakelmaschinen* (s. Vorlesung *Berechenbarkeit und Komplexität*).

Im Falle der partiell rekursiven Funktionen definiert man für gegebenes (beliebiges)  $f$  die *f-partiell rekursiven* oder *relativ zu f partiell rekursiven* Funktionen wie die partiell rekursiven Funktionen, nur dass man  $f$  als zusätzliche Ausgangsfunktion hinzunimmt.  $A$  ist dann *rekursiv relativ zu B* (oder wie man auch sagt *auf B Turing-reduzierbar*,  $A \leq_T B$ ), falls die charakteristische Funktion  $c_A$  von  $A$  relativ rekursiv zur charakteristischen Funktion  $c_B$  von  $B$  ist.

Der Äquivalenzsatz lässt sich dann relativieren, d.h. man kann zeigen, dass die formalen relativierten Entscheidbarkeits- (und Berechenbarkeits-)Begriffe äquivalent sind. Die RELATIVIERTE CHURCH-TURING THESE drückt dann die Überzeugung aus, dass diese formalen Begriffe den intuitiven Begriff erfassen, d.h. dass  $\leq_{eff}$  und  $\leq_T$  übereinstimmen (s. Vorlesung *Berechenbarkeit und Komplexität*).

## MANY-ONE REDUZIERBARKEIT

Hier betrachten wir nur einen Spezialfall der relativen Entscheidbarkeit, bei der man  $A$  relativ zu  $B$  dadurch entscheidet, dass man jeder Instanz  $x \in A$ ? des Entscheidungsproblems für  $A$  eine (äquivalente) Instanz  $y \in B$ ? des Entscheidungsproblems für  $B$  effektiv zuordnet. D.h. man gibt eine berechenbare Funktion  $f$  an, sodass  $x \in A \Leftrightarrow f(x) \in B$  gilt. Offensichtlich impliziert dies  $A \leq_{eff} B$ .

**FORMALE DEFINITION.** Seien  $A, B \subseteq \mathbb{N}$ .  $A$  ist *many-one-reduzierbar* (kurz: *m-reduzierbar*) auf  $B$ , wenn es eine 1-stellige total rekursive Funktion  $f$  gibt mit

$$\forall n \in \mathbb{N} (n \in A \Leftrightarrow f(n) \in B).$$

Wir sagen in diesem Fall auch, dass  $A$  auf  $B$  *vermöge* (oder *via*)  $f$  *m-reduzierbar* ist und schreiben  $A \leq_m B$  (via  $f$ ).

## BEMERKUNGEN

1. Durch den Begriff *many-one* soll der funktionale Charakter der Reduktion ausgedrückt werden. Da  $f$  nicht injektiv sein muss, können hierbei *viele* Instanzen  $x$  von  $A$  auf *eine* Instanz  $f(x)$  von  $B$  abgebildet werden. Verlangt man zusätzlich, dass  $f$  injektiv ist, so erhält man eine *one-one*-Reduktion.

2. Man beachte, dass  $A \leq_m B$  via  $f$  impliziert, dass

$$A = f^{-1}(B) = \{x : f(x) \in B\},$$

weshalb  $A$  durch  $B$  und  $f$  eindeutig bestimmt ist. (Umgekehrt lässt sich eine Menge  $A$  i.a. jedoch via  $f$  auf verschiedene Mengen  $B$  reduzieren.)

3. Nicht jede effektive Reduktion lässt sich in eine *many-one*-Reduktion überführen, d.h. es gibt Mengen  $A$  und  $B$  mit  $A \leq_T B$  aber  $A \not\leq_m B$ .

Z.B. gibt es Mengen  $A$  mit  $A \not\leq_m \bar{A}$  wogegen  $A \leq_T \bar{A}$  stets gilt. (Die Reduktion stellt nur eine Frage, die Auswertung ist aber nicht positiv.) Ähnlich gilt stets  $A_2 := \{x : x \in A \ \& \ x + 1 \in A\} \leq_T A$  aber es gibt Beispiele  $A$  für  $A_2 \not\leq_m A$ . (Die Reduktion stellt zwei Fragen.)

Bei der Untersuchung natürlicher Probleme kommt man aber in der Regel mit der  $m$ -Reduzierbarkeit aus.

## DAS REDUKTIONSLEMMA

REDUKTIONSLEMMA. Seien  $A, B \subseteq \mathbb{N}$  Mengen mit  $A \leq_m B$ .  
Dann gilt:

(\*) Falls  $A$  nicht rekursiv ist, so ist auch  $B$  nicht rekursiv.

BEWEIS. Der Beweis ist durch Kontraposition: Wir zeigen, dass für rekursives  $B$  auch  $A$  rekursiv ist. Es gelte also  $A \leq_m B$  via  $f$  und  $B$  sei rekursiv. Dann gilt  $c_A(x) = c_B(f(x))$ , d.h.  $c_A = c_B \circ f$ . Da  $c_B$  und  $f$  rekursiv sind, ist daher auch  $c_A$  und damit  $A$  ebenfalls rekursiv.

## EIN ERSTES ANWENDUNGSBEISPIEL

SATZ. Das diagonale Halteproblem  $K_d$  und das initiale Halteproblem  $K_0$  sind nicht rekursiv.

BEWEIS. Wegen der Nichtrekursivität des allgemeinen Halteproblems  $K$ , genügt es  $K \leq_m K_d$  und  $K \leq_m K_0$  zu zeigen, d.h. eine rekursive Funktion  $f$  anzugeben, mit

$$\{e\}(x) \downarrow \Leftrightarrow \{f(\langle e, x \rangle)\}(f(\langle e, x \rangle)) \downarrow \quad \text{bzw.} \quad \{e\}(x) \downarrow \Leftrightarrow \{f(\langle e, x \rangle)\}(0) \downarrow$$

Intuitiv bedeutet dies, dass wir eine effektive Transformation  $f$  finden müssen, die ein Programm  $P$  und eine Eingabe  $x$  für  $P$  auf ein Programm  $P' = f(P, x)$  abbildet, das auf seine Kodierung  $gn(P')$  bzw. auf die 0 angesetzt genau dann terminiert, wenn  $P$  bei Eingabe  $x$  terminiert. Hierfür geeignet ist das Programm  $P'$ , das – *unabhängig von seiner Eingabe* – das Programm  $P$  bei Eingabe  $x$  simuliert.

Für die formale Definition von  $f$  benutzen wir die Tatsache, dass  $\varphi$  mit  $\varphi_e = \{e\}$  eine Gödelnummerierung von  $F(\text{REK})$  ist: Wir definieren zunächst die partiell rekursive Funktion  $\psi^{(2)}$  durch

$$\psi(z, y) = \{(z)_1\}((z)_2) = \varphi((z)_1, (z)_2).$$

Es gilt dann

$$\psi_{\langle e, x \rangle}(y) = \{e\}(x)$$

und damit für die rekursive Übersetzungsfunktion  $f$  von  $\psi$  nach  $\varphi$

$$\{f(\langle e, x \rangle)\}(y) = \varphi_{f(\langle e, x \rangle)}(y) = \psi_{\langle e, x \rangle}(y) = \{e\}(x),$$

also insbesondere

$$\{f(\langle e, x \rangle)\}(y) \downarrow \Leftrightarrow \{e\}(x) \downarrow \Leftrightarrow \langle e, x \rangle \in K$$

für alle  $y \in \mathbb{N}$ . Wählt man  $y = f(\langle e, x \rangle)$  bzw.  $y = 0$ , so zeigt dies, dass

$$f(\langle e, x \rangle) \in K_d \Leftrightarrow f(\langle e, x \rangle) \in K_0 \Leftrightarrow \langle e, x \rangle \in K$$

weshalb  $K \leq_m K_d$  via  $f$  und  $K \leq_m K_0$  via  $f$ . *q.e.d.*

## $m$ -ÄQUIVALENZ und $m$ -UNLÖSBARKEITSGRADE

Die Relation  $\leq_m \subseteq \mathbb{N} \times \mathbb{N}$  ist eine Präordnung, d.h. reflexiv und transitiv:

Reflexivität:  $A \leq_m A$  via  $f(x) = x$ , d.h.  $f = U_1^1$ .

Transitivität:  $A \leq_m B$  via  $f$  &  $B \leq_m C$  via  $g \Rightarrow A \leq_m C$  via  $g(f)$ .

Zwei Mengen  $A, B \subseteq \mathbb{N}$  heißen *many-one* ( $m$ -) äquivalent ( $A =_m B$ ), falls  $A \leq_m B$  und  $B \leq_m A$  gilt.

Aus Reflexivität und Transitivität von  $\leq_m$  folgt, dass die  $m$ -Äquivalenz eine Äquivalenzrelation ist, d.h. reflexiv, symmetrisch und transitiv ist.

$m$ -äquivalente Mengen sind, grob gesprochen, gleichschwer. Man nennt die  $m$ -Äquivalenzklassen daher auch die ( $m$ -)Unlösbarkeitsgrade, d.h.

$$\text{deg}_m(A) = \{B : B =_m A\}$$

ist der  $m$ -Grad von  $A$ . (Die Bezeichnung  $\text{deg}$  kommt von dem Englischen  $\text{degree}$ .)

Beispiele für äquivalente Mengen sind zum einen die rekursiven Mengen  $\neq \mathbb{N}, \emptyset$ , zum anderen die Halteprobleme:  $K =_m K_d =_m K_0$  (Übung!).

## WEITERE UNENTSCHEIDBARE PROBLEME

Durch Reduktion des Halteproblems (oder dessen Komplements) lässt sich die Unentscheidbarkeit von praktisch allen allgemeinen semantischen Fragen über Turingmaschinen  $M$  (d.h. intuitiv: Algorithmen) zeigen. So sind insbesondere folgende Fragen unentscheidbar:

- TOTALITÄTSPROBLEM: Terminiert  $M$  für alle Eingaben?
- KOMPLEXITÄTSPROBLEM: Ist die von  $M$  berechnete Funktion primitiv rekursiv?
- KORREKTHEITSPROBLEM: Berechnet  $M$  die gewünschte Funktion  $f$ ?
- ÄQUIVALENZPROBLEM: Sind  $M$  und  $M'$  äquivalent?
- LEERHEITS- (ENDLICHKEITS-, UNENDLICHKEITS-) PROBLEM: Ist der Definitionsbereich der von  $M$  berechneten partiellen Funktion leer (endlich, unendlich)?

Um dies zu zeigen, beweisen wir einen allgemeinen Satz über die Unentscheidbarkeit von Indexmengen.

## INDEXMENGEN

DEFINITION. Eine Menge  $I \subseteq \mathbb{N}$  heisst *Indexmenge*, falls  $I$  gegen äquivalente Indices abgeschlossen ist, d.h. falls für alle Zahlen (=Indices)  $e$  und  $e'$  gilt:

$$e \in I \ \& \ \{e\} = \{e'\} \Rightarrow e' \in I.$$

Die Indexmenge  $I$  ist *nichttrivial*, falls  $I \neq \emptyset, \mathbb{N}$  gilt.

Anschaulich sind Indexmengen Klassen von Maschinen, die mit einer Maschine auch alle äquivalenten Maschinen enthalten.

BEISPIELE. 1. Für jede 1-st. part. rek. Funktion  $\psi$  ist die Menge

$$\text{Ind}(\psi) = \{e : \{e\} = \psi\}$$

aller Indizes von  $\psi$  eine nichttriviale Indexmenge.

2. Die auf der letzten Folie genannten Probleme sind mit Ausnahme des Äquivalenzproblems nichttriviale Indexmengen. Z.B. wird das Totalitätsproblem durch die Indexmenge

$$\text{TOT} = \{e : \{e\} \text{ total}\}$$

beschrieben.

## DER SATZ VON RICE

SATZ. Jede nichttriviale Indexmenge  $I$  ist nichtrekursiv.

KOROLLAR 1. Die folgenden Mengen sind nichtrekursiv:

TOT =  $\{e : \{e\} \text{ total}\}$  Totalitätsproblem

PRIM =  $\{e : \{e\} \text{ primitiv rekursiv}\}$  Komplexitätsproblem

Ind( $\psi$ ) =  $\{e : \{e\} = \psi\}$  Korrektheitsproblem für  $\psi \in F(REK)$

EMPTY =  $\{e : Db(\{e\}) = \emptyset\}$  Leerheitsproblem

FIN =  $\{e : Db(\{e\}) \text{ endlich}\}$  Endlichkeitsproblem

INF =  $\{e : Db(\{e\}) \text{ unendlich}\}$  Unendlichkeitsproblem

KOROLLAR 2. Das Äquivalenzproblem  $EQ = \{\langle e, e' \rangle : \{e\} = \{e'\}\}$  ist nichtrekursiv. (Beweis: Es gilt  $\text{Ind}(\varphi_0) \leq_m EQ$  via  $f(x) = \langle x, 0 \rangle$ .)

## BEWEIS DES SATZES VON RICE

Sei  $I$  eine nichttriviale Indexmenge. Um zu zeigen, dass  $I$  nicht rekursiv ist, unterscheiden wir die beiden folgende Fälle, wobei  $\psi_\emptyset$  die nirgends definierte 1-st. part. rek. Funktion ist:

1. Fall:  $I \cap \text{Ind}(\psi_\emptyset) = \emptyset$ .

Es genügt  $K_0 \leq_m I$  zu zeigen. Hierzu wähle  $\psi^{(1)}$  part. rek. mit  $\text{Ind}(\psi) \subseteq I$ , definiere die part. rek. Funktion  $\theta^{(2)}$  durch

$$\theta(e, x) = (0 \cdot \varphi(e, 0)) + \psi(x),$$

und betrachte eine rekursive Übersetzungsfunktion  $f$  von  $\theta$  nach  $\varphi$ . Nach Definition von  $\theta$  gilt dann  $e \in K_0 \Leftrightarrow f(e) \in I$ , d.h.  $K_0 \leq_m I$  via  $f$  da

$$\varphi_{f(e)} = \theta_e = \begin{cases} \psi & \text{falls } e \in K_0 \\ \psi_\emptyset & \text{sonst.} \end{cases}$$

2. Fall: Sonst.

Da  $I$  eine Indexmenge ist, gilt dann  $\text{Ind}(\psi_\emptyset) \subseteq I$  und daher  $\bar{I} \cap \text{Ind}(\psi_\emptyset) = \emptyset$ . Da mit  $I$  auch  $\bar{I}$  eine nichttriviale Indexmenge ist, ist also  $\bar{I}$  nach Fall 1 nicht rekursiv. Da die rekursiven Mengen gegen Komplement abgeschlossen sind, folgt hieraus aber die Nichtrekursivität von  $I$ .

## DAS REKURSIONSTHEOREM

Neben Diagonalisierung und Reduktionsmethode ist das Rekursionstheorem ein alternatives Werkzeug zum Nachweis der Nichtrekursivität von Problemen. Wir stellen dieses Theorem hier in zwei Versionen ohne Beweis vor (Beweise: s. Skript oder Vorlesung *Berechenbarkeit und Komplexität*).

REKURSIONSTHEOREM (1.Version) Zu jeder  $(n + 1)$ -stelligen partiell rekursiven Funktion  $\psi$  gibt es eine Zahl  $k \in \mathbb{N}$  mit

$$\psi_k = \{k\} (= \varphi_k)$$

REKURSIONSTHEOREM (2.Version = FIXPUNKTSATZ) Zu jeder 1-stelligen total rekursiven Funktion  $f$  und zu jedem  $n \geq 1$  gibt es eine Zahl  $k \in \mathbb{N}$  mit

$$\{f(k)\}^{(n)} = \{k\}^{(n)}.$$

*Anschaulich: Jede effektive Programmtransformation bildet zumindest ein Programm auf ein äquivalentes Programm ab!*

Das Rekursionstheorem in seinen beiden Formen ist ein elegantes Hilfsmittel in der Rekursionstheorie (wie die Berechenbarkeitstheorie auch genannt wird). Man kann damit sowohl die Rekursivität wie die Nichtrekursivität von Funktionen und Mengen zeigen. Wir demonstrieren dies an zwei Beispielen:

- einem alternativen Beweis des Satzes von Rice
- dem Nachweis, dass die Ackermann-Funktion rekursiv ist

## ALTERNATIVER BEWEIS DES SATZES VON RICE

Sei  $I$  eine nichttriviale Indexmenge. Um die Nichtrekursivität von  $I$  zu zeigen, gehen wir von der Widerspruchsansnahme aus, dass  $I$  rekursiv ist. Für fest gewählte Zahlen  $y \in I$  und  $z \notin I$  (die wegen der Nichttrivialität von  $I$  existieren) ist dann die durch

$$f(x) = \begin{cases} z & \text{falls } x \in I \\ y & \text{falls } x \notin I \end{cases}$$

definierte Funktion  $f$  total rekursiv. Da nach Definition von  $f$

$$x \in I \Leftrightarrow f(x) \notin I,$$

folgt mit der Tatsache, dass  $I$  eine Indexmenge ist, dass  $\{f(x)\} \neq \{x\}$  für alle  $x$  gilt. Dies widerspricht jedoch dem Fixpunktsatz.

## REKURSIVITÄT DER ACKERMANN-FUNKTION

Um die Rekursivität der Ackermann-Funktion zu zeigen, transformieren wir deren implizite Definition

$$\begin{aligned}\alpha(0, y) &= y + 1 \\ \alpha(x + 1, 0) &= \alpha(x, 1) \\ \alpha(x + 1, y + 1) &= \alpha(x, \alpha(x + 1, y))\end{aligned}$$

zunächst in die explizite Definition einer 3-stelligen partiell rekursiven Funktion

$$\psi(e, x, y) = \begin{cases} y + 1 & \text{falls } x = 0 \\ \{e\}(x - 1, 1) & \text{falls } x > 0 \text{ und } y = 0 \\ \{e\}(x - 1, \{e\}(x, y - 1)) & \text{falls } x, y > 0. \end{cases}$$

Hierbei wird jeder Zweig  $\psi_e$  von  $\psi$  wie  $\alpha$  definiert, nur dass man auf der rechten Seite  $\alpha$  durch  $\{e\}$ , d.h. den entsprechenden Zweig  $\varphi_e$  der universellen Funktion  $\varphi$  ersetzt, und damit die Definition explizit macht. Für das nach dem Rekursionstheorem existierende  $k$  mit  $\psi_k = \{k\}$  gilt dann  $\alpha = \psi_k = \{k\}$ .

NB. Man kann dieses Vorgehen intuitiv so interpretieren, dass man bei der Definition einer partiell rekursiven Funktion annehmen darf, einen ihrer Indizes *a priori* zu kennen, auf diesen also in der Definition Bezug nehmen darf!