
13. Reduktionsmethode und rekursive Reduzierbarkeiten

Der Nachweis der Unentscheidbarkeit einer Menge mit Hilfe der Diagonalisierungsmethode kann mitunter sehr schwierig sein, weshalb man sich andere Methoden ausgedacht hat. Die wichtigste Technik ist hier die Reduktionsmethode: Man zeigt die Unentscheidbarkeit einer Menge A mit Hilfe einer bereits als unentscheidbar nachgewiesenen Menge B , indem man argumentiert, dass ein hypothetisches Entscheidungsverfahren für A in ein (unmögliches) Entscheidungsverfahren für B umgewandelt werden kann. In anderen Worten, man zeigt, dass man B effektiv aus A gewinnen kann, d.h. intuitiv, dass A mindestens genauso schwer wie B und daher ebenfalls unentscheidbar ist.

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

Im einfachsten Fall gilt, dass B so in A kodiert ist, dass sich jede Instanz von B auf eine Instanz von A reduzieren lässt, d.h. dass es eine berechenbare Funktion f gibt mit

$$x \in B \Leftrightarrow f(x) \in A$$

Die hypothetische Entscheidbarkeit von A liefert dann folgendes Entscheidungsverfahren für B : Bei Eingabe x berechne zunächst $f(x)$ und entscheide dann, ob $f(x) \in A$ gilt. Falls dies der Fall ist, gebe JA aus, sonst NEIN. Formalisiert wird dieser einfache Fall einer Reduktion durch die sogenannte many-one-Reduzierbarkeit, die wir hier – wie üblich – nur für 1-stellige Mengen natürlicher Zahlen einführen.

13.1 DEFINITION. Seien $A, B \subseteq \mathbb{N}$. A ist *many-one-(m)-reduzierbar*¹ 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).

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.

13.2 LEMMA. *Es seien $A, B \subseteq \mathbb{N}$ Mengen mit $A \leq_m B$. Dann gilt:*

¹Durch 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.

(i) Falls A nicht rekursiv ist, so ist auch B nicht rekursiv.

(ii) Falls B rekursiv ist, so ist auch A rekursiv.

BEWEIS. Die Aussage (i) folgt logisch aus (ii) (Kontraposition). Es genügt daher (ii) zu zeigen. 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. \square

Teil (i) von Lemma 13.2 formalisiert die oben beschriebenen Reduktionsidee. Wir geben ein Beispiel:

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

BEWEIS. Da das allgemeine Halteproblem K nicht rekursiv ist, genügt es nach Lemma 13.2 $K \leq_m K_d$ und $K \leq_m K_0$ zu zeigen. Wir müssen also eine rekursive Funktion f angeben, mit

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

D.h. intuitiv, dass wir eine Transformation f finden müssen, die ein Programm P und eine Eingabe x für P auf ein Programm $P' = f(P, x)$ abbildet, das auf sich (d.h. seine Kodierung) 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. Terminiert also P bei Eingabe x , so terminiert P' für jede Eingabe (also insbesondere für die geforderten Eingaben) und divergiert P bei Eingabe x , so divergiert P' für jede Eingabe, also wiederum insbesondere für die geforderten Eingaben.

Formal definiert man f mit Hilfe der Tatsache, dass φ mit $\varphi_e = \{e\}$ eine Gödelnummerierung von $F(\text{REK})$ ist: Sei $\Psi^{(2)}$ definiert durch

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

Dann ist Ψ partiell rekursiv, da Ψ explizit über φ und der primitiv rekursiven Projektionsfunktion für kodierte Folgen definiert ist, und es gilt für alle $e, x, y \in \mathbb{N}$, dass

$$\Psi_{(e,x)}(y) = \{e\}(x).$$

Ist also f die rekursive Übersetzungsfunktion von Ψ nach φ , so gilt

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

also

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

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 . \square

Die m -Reduzierbarkeit ist eine Präordnung, erlaubt also eine Klassifizierung von Mengen nach ihrer (relativen) Schwierigkeit:

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

BEWEIS. Es gilt $A \leq_m A$ via $f = U_1^1$. Zum Nachweis der Transitivität, seien $A, B, C \subseteq \mathbb{N}$ und $f, g \in F(\text{REK})$ gegeben, so dass $A \leq_m B$ via f und $B \leq_m C$ via g . Dann gilt $A \leq_m C$ via $g \circ f$. \square

13.5 DEFINITION. 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 Lemma 13.4 folgt, dass die m -Äquivalenz eine Äquivalenzrelation ist, d.h. reflexiv, symmetrisch und transitiv ist.

13.6 LEMMA. Die m -Äquivalenz $=_m$ ist eine Äquivalenzrelation. \square

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 deg kommt von dem Englischen degree.) Beispiele für äquivalente Mengen sind zum einen die Halteprobleme (s.u.), zum anderen die rekursiven Mengen $\neq \mathbb{N}, \emptyset$ (s. Übungen).

13.7 SATZ. $K =_m K_d =_m K_0$.

BEWEIS. Da wir im Beweis von Satz 13.3 bereits $K \leq_m K_d$ und $K \leq_m K_0$ gezeigt haben, genügt es zu zeigen, dass $K_d \leq_m K$ und $K_0 \leq_m K$ gilt. Dies gilt aber vermöge der Reduktionsfunktionen $f(e) = \langle e, e \rangle$ bzw. $g(e) = \langle e, 0 \rangle$. \square

Für die meisten Anwendungen reicht die many-one-Reduzierbarkeit aus, obwohl sie die folgenden beiden Einschränkungen besitzt: Gilt $A \leq_m B$ via f , so geschieht die Beantwortung der Frage, ob $x \in A$, über den Zugriff auf B mit Hilfe nur *einer* Frage an B (nämlich „ $f(x) \in B$?“) und zudem wird diese Frage *positiv* ausgewertet (d.h. ist $f(x) \in B$ ($f(x) \notin B$), so gilt auch $x \in A$ ($x \notin A$)). In einer allgemeinen effektiven Reduktion von A auf B genügt es jedoch, dass durch endlich viele effektiv ausgewählte Fragen an B , die beliebig effektiv ausgewertet werden können, die Frage, ob $x \in A$ gilt, beantwortet werden kann. (Dabei darf sogar eine Frage an B von der Antwort auf die vorhergehenden Fragen an B abhängen, d.h. die Fragen dürfen *adaptiv* gestellt werden.) Diese allgemeinste Form einer effektiven Reduktion wird durch die im folgenden definierte Turing-Reduzierbarkeit formalisiert. Diese basiert auf der *relativen Berechenbarkeit*, formalisiert durch die *relative Rekursivität*:

13.8 DEFINITION. Sei f eine beliebige totale Funktion über \mathbb{N} . Die Klasse $F(\text{REK}^f)$ der *partiell f -rekursiven Funktionen* ist induktiv definiert wie die Klasse $F(\text{REK})$ der partiell rekursiven Funktionen, jedoch mit f als zusätzlicher Ausgangsfunktion. Eine partielle Funktion $\varphi \in F(\text{REK}^f)$ heißt auch *partiell rekursiv in* oder *relativ zu f* . Ist φ total, so heißt φ *f -rekursiv* (oder *rekursiv in f* oder *rekursiv relativ zu f*).

Ist $f = c_A$ die charakteristische Funktion einer Menge A , so schreiben wir auch $F(\text{REK}^A)$ statt $F(\text{REK}^{c_A})$ und sagen φ ist partiell A -rekursiv statt φ ist partiell c_A -rekursiv (etc.). Ähnlich sagen wir, dass eine Menge B A -rekursiv ist, falls ihre charakteristische Funktion c_B A -rekursiv ist.

Die Hinzunahme von f zu den Ausgangsfunktionen entspricht intuitiv der hypothetischen Annahme, dass f berechenbar ist. Insbesondere bedeutet also die A -Rekursivität einer Menge B , dass B entscheidbar ist relativ zu (einem hypothetischen Entscheidungsverfahren für) A , also dass B effektiv auf A reduzierbar ist. Die Annahme, dass auch hier die intuitiven Konzepte mit den formalen übereinstimmen, bezeichnet man auch als *relativierte Church-Turing-These*. Der Begriff einer effektiven Reduktion in seiner allgemeinsten Form, d.h. die eingangs definierte Relation \leq_{eff} , wird also durch die folgende Turing-Reduzierbarkeit formalisiert.

13.9 DEFINITION. Seien $A, B \subseteq \mathbb{N}$. A ist *Turing-(T-)reduzierbar* auf B ($A \leq_T B$), falls A B -rekursiv ist, d.h. falls $c_A \in F(\text{REK}^{c_B})$ gilt. A und B sind *Turing-(T-)äquivalent* ($A =_T B$), falls $A \leq_T B$ und $B \leq_T A$ gilt.

Die oben für die m -Reduzierbarkeit gezeigten Eigenschaften lassen sich auch für die T -Reduzierbarkeit zeigen.

13.10 LEMMA. Es seien $A, B \subseteq \mathbb{N}$ Mengen mit $A \leq_T B$. Dann gilt:

- (i) Falls A nicht rekursiv ist, so ist auch B nicht rekursiv.
- (ii) Falls B rekursiv ist, so ist auch A rekursiv.

BEWEIS. Es genügt wiederum (ii) zu zeigen. Dies folgt aber aus der folgenden einfachen Beobachtung.

13.11 LEMMA. Für total rekursives f gilt $F(\text{REK}) = F(\text{REK}^f)$.

BEWEIS. $F(\text{REK}) \subseteq F(\text{REK}^f)$ gilt nach Definition, während $F(\text{REK}^f) \subseteq F(\text{REK})$ durch triviale Induktion (nach dem Aufbau der Funktionen in $F(\text{REK}^f)$) gezeigt wird. \square

13.12 LEMMA. Die Relation \leq_T ist eine Präordnung und damit $=_T$ eine Äquivalenzrelation.

BEWEIS. Zum Nachweis der Reflexivität beobachtet man, dass $c_A \in F(\text{REK}^{c_A})$ nach Definition und damit $A \leq_T A$ nach Definition von \leq_T . Zum Nachweis der Transitivität seien A, B, C gegeben mit $A \leq_T B$ und $B \leq_T C$. Wir haben $A \leq_T C$ zu zeigen. Nach Annahme gilt $c_A \in F(\text{REK}^{c_B})$ und $c_B \in F(\text{REK}^{c_C})$. Dass $c_A \in F(\text{REK}^{c_C})$, sieht man wie folgt: Wegen $c_A \in F(\text{REK}^{c_B})$ gibt es eine B -rekursive Darstellung von c_A , d.h. eine bis auf mögliche Vorkommen von c_B partiell rekursive Darstellung von c_A und entsprechend gibt es eine C -rekursive Darstellung von c_B . Ersetzt man nun in der Darstellung von c_A alle Vorkommen von c_B durch die C -rekursive Darstellung von c_B , so erhält man eine C -rekursive Darstellung von c_A . (Formal zeigt man dies durch Induktion nach dem Aufbau der B -rekursiven Darstellung von c_A .) \square

Aus der Transitivität von \leq_T folgt, dass

$$A \leq_T B \Leftrightarrow F(\text{REK}^A) \subseteq F(\text{REK}^B)$$

also

$$A =_T B \Leftrightarrow F(\text{REK}^A) = F(\text{REK}^B).$$

Nach Lemma 13.11 gilt hiermit, dass die rekursiven Mengen eine Turing-Äquivalenzklasse bilden, und dass

$$A \text{ rekursiv} \Leftrightarrow A \text{ ist auf alle Mengen } T\text{-reduzierbar}$$

gilt. Wir vergleichen als Nächstes die m - und die T -Reduzierbarkeit:

13.13 LEMMA. Für beliebige Mengen $A, B \subseteq \mathbb{N}$ mit $A \leq_m B$ gilt auch $A \leq_T B$.

BEWEIS. Gelte $A \leq_m B$ via f . Dann gilt $f \in F(\text{REK})$ und $c_A(x) = c_B(f(x))$, d.h. $c_A = c_B \circ f \in F(\text{REK}^B)$ und damit $A \leq_T B$. \square

13.14 LEMMA. Jede Menge A ist auf ihr Komplement \bar{A} Turing-reduzierbar, d.h. $A \leq_T \bar{A}$.

BEWEIS. Es gilt $c_A = \overline{c_{\bar{A}}} \in F(\text{REK}^{\bar{A}})$. \square

Ein triviales Beispiel einer Menge A , für die $A \leq_m \bar{A}$ nicht gilt ist die Menge $A = \mathbb{N}$. Würde nämlich hier $A \leq_m \bar{A}$ via f – d.h. $\mathbb{N} \leq_m \emptyset$ via f – gelten, so müsste z.B. $f(0) \in \emptyset$ gelten, was aber unmöglich ist. Mit Lemma 13.14 folgt:

13.15 LEMMA. Es gibt Mengen A, B mit $A \leq_T B$, aber $A \not\leq_m B$.

\square

Später werden wir zeigen, dass auch $K \not\leq_m \bar{K}$ gilt, sodass sich \leq_m und \leq_T auch nicht-trivial, d.h. auf den nichtrekursiven Mengen unterscheiden.

Den Begriff der relativen Berechenbarkeit hätten wir statt über die relative Rekursivität auch über die relativierte Turing- oder Registermaschinen-Berechenbarkeit einführen können. Wir skizzieren hier die relativierte Turing-Berechenbarkeit, wobei wir uns auf den Fall von Mengen beschränken. Um die Klasse der relativ zu einer Menge A (partiell) Turing-berechenbaren Funktionen zu definieren, benötigen wir eine Verallgemeinerung des Turingmaschinenmodells, nämlich die *Orakel (-Turing)maschine* (OTM). Die Arbeitsweise einer OTM M hängt nicht nur von der Eingabe \vec{x} ab sondern auch von der Menge A , relativ zu der M die Rechnung ausführen soll. Während der Rechnung kann M Information über A der Form „ $y \in A?$ “ abfragen. Die Bezeichnung Orakelmaschine rührt daher, dass man sich vorstellen kann, dass M ein *Orakel* befragt, das diese Fragen beantwortet. (Die Menge A muss ja i. Allg. nicht entscheidbar sein, weshalb es i. Allg. eines nicht effektiven Mediums bedarf, die Fragen zu beantworten.) Entsprechend nennt man die Menge A auch die *Orakelmenge*.

Implementiert werden die Orakelfragen mit Hilfe eines zusätzlichen Bandes (*Orakelband*), auf das die Maschine schreibend zugreifen kann. Will M wissen, ob y ein Element von A ist, so schreibt M (die Unärdarstellung von) y auf das Orakelband und geht anschließend in einen ausgezeichneten Fragezustand „?“ . Die Frage wird dann im nächsten Schritt von dem Orakel durch den Nachfolgezustand „+“ bzw. „-“ beantwortet. (In diesem einen Schritt wird auch das Orakelband wieder vollständig gelöscht, so dass Platz für eine eventuelle weitere Frage ist.)

Wir überlassen die formale Definition der Orakelmaschinen als Übung. Wie im unrelativierten Fall lässt sich ein *relativierter Äquivalenzsatz* zeigen, d.h. zeigen, dass eine (partielle) Funktion genau dann (partiell) A -rekursiv ist, wenn sie Turing-berechenbar relativ zu A ist. In der Tat lassen sich alle Begriffe und Grundergebnisse der Berechenbarkeitstheorie relativieren, indem man in den Definitionen „rekursiv“ durch „rekursiv in“ ersetzt und die entsprechenden Änderungen in Sätzen und Beweisen vornimmt. So könnten wir zum Beispiel eine Entsprechung des Kleeneschen Normalformatsatzes für die partiell A -rekursiven Funktionen für jede Menge A zeigen. Das *relativierte Halteproblem*

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

wobei $\{e\}^A$ die e -te partiell A -rekursive Funktion ist, ist wiederum nicht A -rekursiv, d.h. $A <_T K^A$. Man bezeichnet K^A auch mit A' und nennt den Operator, der A auf A' abbildet, den *Jump-(Sprung-)Operator*, da er einen Sprung in der Komplexität bewirkt. Insbesondere erhält man so eine aufsteigende Kette

$$\emptyset <_T \emptyset' <_T \emptyset'' <_T \emptyset''' <_T \dots \emptyset^{[n]} <_T \emptyset^{[n+1]} < \dots$$

von Mengen wachsender Komplexität (wobei $n > 3$ und $A^{[n]}$ den n -fach iterierten Jump von A bezeichnet), beginnend mit der rekursiven Menge \emptyset , gefolgt von $\emptyset' = K^{\emptyset} = {}_m K$, $\emptyset'' = K^{K^{\emptyset}} = {}_m K^K$, etc.