

11. Rekursiv aufzählbare Mengen

CHARAKTERISIERUNGEN DER R.A. MENGEN

SATZ. Für eine Menge $A \subseteq \mathbb{N}$ sind folgende Aussagen äquivalent:

- (1) A ist rekursiv aufzählbar.
- (2) Die partielle charakteristische Funktion χ_A von A ist partiell rekursiv.
- (3) A ist die Projektion einer 2-dim. (primitiv) rekursiven Menge B , d.h.

$$x \in A \Leftrightarrow \exists y [(x, y) \in B]$$

(Projektionslemma)

- (4) A ist der Wertebereich einer partiell rekursiven Funktion.
- (5) A ist leer oder der Wertebereich einer total rekursiven Funktion.

Für mehrdimensionales $A \subseteq \mathbb{N}^n$ sind (1), (2) und (3) äquivalent, und A ist genau dann r.a., wenn $\tilde{A} = \{(x_1, \dots, x_n) : (x_1, \dots, x_n) \in A\}$ r.a. ist.

WIEDERHOLUNG

Eine Menge $A \subseteq \mathbb{N}^n$ ist *rekursiv aufzählbar (r.a.)*, wenn sie der Definitionsbereich einer partiell rekursiven Funktion ist.

Wir haben gesehen, dass sich die aufzählbaren Mengen, d.h. die Mengen, die sich durch ein Aufzählungsverfahren beschreiben lassen, entsprechend als Definitionsbereiche partiell berechenbarer Funktionen darstellen lassen.

Nach der Church-Turing-These gilt also:

rekursiv aufzählbar = aufzählbar

Als nächstes werden wir zeigen, dass sich die weiteren anschaulichen Charakterisierungen der aufzählbaren Mengen entsprechend auf die r.a. Mengen übertragen und dort formal nachweisen lassen.

BEWEIS (für 1-dimensionalen Fall).

(1) \Rightarrow (2). Ist A der Definitionsbereich der part. rek. Funktion ψ , so ist χ_A wegen der Darstellung $\chi_A(x) = 1 + 0 \cdot \psi(x)$ ebenfalls part. rek.

(2) \Rightarrow (3). Für einen Index e der part. char. Funktion χ_A von A gilt nach dem Normalformtheorem $\chi_A(x) = U(\mu y T(e, x, y))$. Da A der Definitionsbereich von χ_A ist, folgt hieraus

$$x \in A \Leftrightarrow \exists y T(e, x, y).$$

A ist also die Projektion der primitiv rekursiven Menge $B = \{(x, y) : T(e, x, y)\}$.

(3) \Rightarrow (4), (5). Sei A Projektion der (primitiv) rekursiven Menge B . Dann ist die partielle Funktion $\tilde{\psi}$ mit

$$\tilde{\psi}(x) = \begin{cases} (x)_1 & \text{falls } ((x)_1, (x)_2) \in B \\ \uparrow & \text{sonst} \end{cases}$$

part. rek. und A ist der Wertebereich von $\tilde{\psi}$. Ist A nicht leer, z.B. $x_0 \in A$, so kann man $\tilde{\psi}$ total machen, indem man im 2. Fall der Definition \uparrow durch x_0 ersetzt.

(4), (5) \Rightarrow (1). Ist A leer, so ist A der Definitionsbereich der nirgends definierten part. rek. Funktion $\tilde{\psi}_0$ und daher r.a. O.B.d.A. können wir also im Folgenden annehmen, dass A der Wertebereich der (partiell oder total) rekursiven Funktion $\tilde{\psi}$ ist. Für einen Index e von $\tilde{\psi}$ ist dann A der Definitionsbereich der durch

$$\tilde{\tilde{\psi}}(x) = \mu y [T(e, (y)_1, (y)_2) \& U((y)_2) = x]$$

definierten part. rek. Funktion $\tilde{\tilde{\psi}}$ und daher r.a.

REKURSIVITÄT VS. REKURSIVE AUFZÄHLBARKEIT

SATZ 1. Die Klasse REK der rekursiven Mengen ist echt in der Klasse RA der rekursiv aufzählbaren Mengen enthalten.

BEWEIS:

(1) Jede rekursive Menge ist r.a.: Ist A rekursiv, so auch $B = \{(x, x) : x \in A\}$. Da A die Projektion von B ist, ist A also auch r.a.

(2) Das nichtrekursive Halteproblem $K = \{(e, x) : \varphi(e, x) \downarrow\}$ ist r.a., da K der Definitionsbereich der durch $\hat{\varphi}(x) = \varphi(x)_1, (x)_2$ definierten 1-st. part. rek. Funktion $\hat{\varphi}$ ist.

SATZ 2. Eine Menge A ist genau dann rekursiv, wenn A und das Komplement \bar{A} von A rekursiv aufzählbar sind.

BEWEIS: (\Rightarrow) Ist A rekursiv, so auch \bar{A} . Nach Satz 1 sind also A und \bar{A} r.a.

(\Leftarrow) Sind umgekehrt A und \bar{A} r.a. und B_+ und B_- rekursive Mengen, deren Projektionen A und \bar{A} sind, so lässt sich die charakteristische Funktion von A durch

$$c_A(x) = (\mu y [(y)_1 = 1 \ \& \ (x, (y)_2) \in B_+] \vee [(y)_1 = 0 \ \& \ (x, (y)_2) \in B_-])_1$$

beschreiben und ist daher rekursiv.

ABSCHLUSSEIGENSCHAFTEN DER R. A. MENGEN

SATZ. Die Klasse der rekursiv aufzählbaren Mengen ist abgeschlossen gegen

- Einsetzung total rekursiver Funktionen
- Vereinigung und Durchschnitt
- Existenzquantor
- m -Reduzierbarkeit nach unten (D.h.: $A \leq_m B$ & B r.a. $\Rightarrow A$ r.a.)

aber *nicht* abgeschlossen gegen

- Komplement
- Allquantor.

BEWEISIDEE. Die positiven Abschlusseigenschaften ergeben sich leicht aus dem Projektionslemma und aus Abschlusseigenschaften der rekursiven Mengen. Unsere Ergebnisse über den Zusammenhang von Rekursivität und rekursiver Aufzählbarkeit zeigen, dass das Komplement einer nicht-rekursiven r.a. Menge nicht r.a. ist. Wegen $\neg \exists x (\dots) \Leftrightarrow \forall x \neg (\dots)$ folgt hieraus auch der fehlende Abschluss gegen den Allquantor mit Hilfe des Projektionslemmas und des Abschlusses der rekursiven Mengen gegen Komplement.

PART. REKURSIVITÄT VS. REKURSIVE AUFZÄHLBARKEIT

Wir haben den Begriff der Rekursiven Aufzählbarkeit über den Begriff der partiell rekursiven Funktion definiert. Umgekehrt lassen sich die partiell rekursiven Funktionen mit Hilfe der rekursiven Aufzählbarkeit wie folgt definieren:

GRAPHENLEMMA. Für eine partielle Funktion $\psi : \mathbb{N}^m \rightarrow \mathbb{N}$ sind folgende Aussagen äquivalent:

- (1) ψ ist partiell rekursiv.
- (2) Der Graph G_ψ von ψ ist r.a.

BEWEIS. (1) \Rightarrow (2): Für einen Index e von ψ lässt sich G_ψ beschreiben durch

$$(\vec{x}, y) \in G_\psi \Leftrightarrow \exists z (T(e, \vec{x}, z) \ \& \ U(z) = y),$$

weshalb G_ψ nach dem Projektionslemma r.a. ist.

(2) \Rightarrow (1): Für r.a. G_ψ wähle B rekursiv, so dass G_ψ Projektion von B ist. Es gilt dann

$$\psi(\vec{x}) = (\mu y B(\vec{x}, (y)_1, (y)_2))_1,$$

woraus ψ part. rek. folgt.

UNIVERSELLE R.A. MENGEN (Wiederholung)

SATZ. Die Klasse RA der r.a. Mengen besitzt n -universelle Mengen W (für jedes $n \geq 1$), d.h.

- W ist eine $(n+1)$ -st. r.a. Menge
- $\{W_e : e \geq 0\}$ ist die Klasse aller n -st. r.a. Mengen (Hierbei ist $W_e = \{\vec{x} : (e, \vec{x}) \in W\}$ der e -te Zweig von W .)

BEWEIS. Es genügt W als Definitionsbereich der n -universellen part. rek. Funktion φ zu wählen.

Ist W 1-universell für RA, so ist jede 1-st. r.a. Menge unmittelbar in $\hat{W} = \{(x_1, x_2) : (x_1, x_2) \in W\}$ kodiert. D.h. \hat{W} ist eine *schwerste* 1-st. r.a. Menge. Schwerste Mengen in einem allgemeineren Sinn sind die vollständigen Mengen.

VOLLSTÄNDIGKEIT

Allgemein definiert man *Härte* und *Vollständigkeit* bezüglich einer Klasse C von Teilmengen von \mathbb{N} wie folgt:

DEFINITION. Sei $C \subseteq \mathcal{P}(\mathbb{N})$ und $A \subseteq \mathbb{N}$.

- A ist *C-hart*, falls $C \leq_m A$ für jedes $C \in C$ gilt.
- Gilt zusätzlich $A \in C$, so ist A *C-vollständig*.

Ist A *C-hart*, so ist A also mindestens genauso schwer, wie jede Menge in C , und ist A *C-vollständig*, so gehört A zu den schwersten Mengen in C .

Für die Klasse RA der r.a. Mengen sagen wir kurz *hart* und *vollständig* statt *RA-hart* und *RA-vollständig*.

VOLLSTÄNDIGE MENGEN

Für jede 1-universelle r.a. Menge W ist die Menge $\bar{W} = \{(x_1, x_2) : (x_1, x_2) \in W\}$ vollständig. Da das allgemeine Halteproblem K gerade die Menge \bar{W} für die 1-universelle r.a. Menge $W = DB(\varphi)$ ist, ist also K vollständig.

Da $K \leq_m K_0$ und $K \leq_m K_d$ sind die Varianten des Halteproblems ebenfalls vollständig.

Weiter haben wir gesehen, dass $K \leq_m I$ für jede Indexmenge I gilt, die die Indizes der nirgends definierten Funktion nicht enthält. Jede solche Indexmenge ist also hart (Z.B. $I = INF$ und $I = TOT$). Diese Indexmengen sind i.a. jedoch nicht vollständig, da sie i.a. nicht r.a. sind.

BEMERKUNGEN

Eine Klasse C besitzt genau dann *C-harte* Mengen, wenn C abzählbar ist. Es gibt aber abzählbare Klassen C , die keine *C-vollständigen* Mengen besitzen. (Übung!)

Ist A *C-hart* (oder *C-vollständig*) für eine Klasse C , die nichtrekursive Probleme enthält, so ist A nicht rekursiv! **Insbesondere sind harte (und vollständige) Mengen nicht rekursiv.**

NACHWEIS DER HÄRTE: Ist A *C-hart* und gilt $A \leq_m B$, so ist (wegen der Transitivität von \leq_m) B ebenfalls *C-hart*.

BEDEUTUNG DER VOLLSTÄNDIGKEIT

Praktisch alle natürlichen nichtrekursiven r.a. Mengen sind vollständig. Da die r.a. Mengen nach der Church-Turing-These gerade die unbeschränkten effektiven Suchprobleme sind und viele dieser Probleme unentscheidbar sind, gibt es zahlreiche interessante vollständige Mengen in vielen Bereichen der Mathematik und Informatik. So weist man in der Regel für ein Suchproblem S dessen Unentscheidbarkeit dadurch nach, dass man das Halteproblem (oder ein anderes vollständiges Problem) auf S m -reduziert, also zeigt, dass S vollständig ist.

Im Folgenden geben wir zwei weitere Beispiele vollständiger Mengen.

DAS POSTSCHE KORRESPONDENZPROBLEM

Ein *Korrespondenzproblem* P über dem Alphabet Σ

$$P = \langle (v_0, w_0), \dots, (v_n, w_n) \rangle$$

besteht aus einer endlichen Folge von Wortpaaren über Σ .

Eine *Lösung* von P ist eine endliche Folge i_1, \dots, i_m von Zahlen $\leq n$ mit

$$v_{i_1} \dots v_{i_m} = w_{i_1} \dots w_{i_m}.$$

Besitzt P eine Lösung, so heisst P *lösbar*.

BEISPIEL.

$$P = \langle (\lambda, 200), (0, 011), (0, 200), (007, 7), (02, 03), (06, 0), (062, 606),$$

$$(08, 15), (06, 6), (1, 19), (3, 33), (47, 11), (69, 120) \rangle$$

ist lösbar. Eine Lösung ist ???

Für das unäre Alphabet $\Sigma = \Sigma_1$ ist die Frage, ob ein Korrespondenz-Problem eine Lösung besitzt entscheidbar. Für mehrbuchstabile Alphabete ist das Problem dagegen unentscheidbar und -geeignet kodiert- vollständig.

Letzteres zeigt man (z.B.) durch Reduktion des initialen Halteproblems: Gegeben e , beschreibt man die Arbeitsweise der e -ten Turingmaschine M_e so durch ein Korrespondenzproblem P_e , dass P_e genau dann eine Lösung besitzt, wenn M_e bei Eingabe 0 stoppt.

DER SATZ VON MATIJASEVIČ

SATZ. Eine Menge $A \subseteq \mathbb{N}^n$ ist genau dann rekursiv aufzählbar, wenn es ein $k \geq 1$ und Polynome p_1 und p_2 in $n + k$ Variablen mit Koeffizienten in \mathbb{N} gibt, sodass

$$\vec{x} \in A \Leftrightarrow \exists \vec{y} \in \mathbb{N}^k (p_1(\vec{x}, \vec{y}) = p_2(\vec{x}, \vec{y}))$$

für alle $\vec{x} \in \mathbb{N}^n$ gilt.

Der Satz von Matijasevič ist berühmt als negative Lösung zu dem *Zehnten Hilbertschen Problem*, das man wie folgt formulieren kann:

Gibt es einen Algorithmus, der für beliebige Polynomen $p_1(\vec{x})$ und $p_2(\vec{x})$ in $k \geq 1$ Variablen mit Koeffizienten aus \mathbb{N} feststellt, ob die Gleichung $p_1(\vec{x}) = p_2(\vec{x})$ eine Lösung $\vec{x} \in \mathbb{N}^k$ besitzt?