

---

## 14. Rekursiv aufzählbare Mengen

---

In diesem Abschnitt fassen wir einige Eigenschaften der rekursiv aufzählbaren – d.h. der nach Churchscher These (effektiv) aufzählbaren – Mengen zusammen. In Korollar 11.8 haben wir schon gesehen, dass es „universelle“ rekursiv aufzählbare Mengen gibt. Wir zeigen hier zunächst, dass sich die verschiedenen in Abschnitt 2 erhaltenen Charakterisierungen der aufzählbaren Mengen entsprechend für die rekursiv aufzählbaren Mengen nun streng beweisen lassen. (Man sollte die dort gegebenen Beweise mit den folgenden formalen Beweisen vergleichen.) Im Folgenden bezeichnen REK und RA die Klassen der rekursiven bzw. r.a. Mengen.

14.1 SATZ. (Projektionssatz) Für eine Menge  $A \subseteq \mathbb{N}^n$  sind folgende Aussagen äquivalent:

- (i)  $A$  ist rekursiv aufzählbar.
- (ii)  $A$  ist die Projektion einer (primitiv) rekursiven Menge  $B \subseteq \mathbb{N}^{n+1}$ , d.h.

$$\forall \vec{x} \in \mathbb{N}^n (\vec{x} \in A \Leftrightarrow \exists y \in \mathbb{N} ((\vec{x}, y) \in B)).$$

BEWEIS. Zum Nachweis von „(i)  $\Rightarrow$  (ii)“ sei  $A$  der Definitionsbereich der partiell rekursiven Funktion  $\psi^{(n)}$ . Für einen Index  $e$  von  $\psi$  gilt dann nach dem Normalformsatz

$$\vec{x} \in A \Leftrightarrow \psi(\vec{x}) \downarrow \Leftrightarrow \exists y (T(e, \vec{x}, y)),$$

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

Zum Beweis der Umkehrung „(ii)  $\Rightarrow$  (i)“ sei  $A$  die Projektion der rekursiven Menge  $B$ . Dann ist

$$\psi(\vec{x}) = \mu y (B(\vec{x}, y)) = \mu y (c_{\overline{B}})(\vec{x})$$

partiell rekursiv und  $A = Db(\psi)$ . □

Statt einfacher Projektionen  $(n+1)$ -stelliger rekursiver Mengen kann man im Projektionssatz auch mehrfache Projektionen mehrstelliger rekursiver Mengen betrachten, d.h. die Klasse RA der r.a. Mengen ist gegen den Existenzquantor abgeschlossen:

14.2 KOROLLAR. Ist  $B \subseteq \mathbb{N}^{n+1}$  r.a. und  $A$  die Projektion von  $B$ , so ist  $A$  ebenfalls r.a.

BEWEIS. Nach dem Projektionssatz gibt es eine rekursive Menge  $C \subseteq \mathbb{N}^{n+2}$  mit

$$(\vec{x}, y) \in B \Rightarrow \exists z ((\vec{x}, y, z) \in C)$$

und nach Annahme

$$\vec{x} \in A \Leftrightarrow \exists y ((\vec{x}, y) \in B).$$

Hieraus folgt

$$\begin{aligned} \vec{x} \in A &\Leftrightarrow \exists y \exists z ((\vec{x}, y, z) \in C) \\ &\Leftrightarrow \exists v ((\vec{x}, (v)_1, (v)_2) \in C). \end{aligned}$$

D.h.  $A$  ist die Projektion der rekursiven Menge

$$\tilde{C} = \{(\vec{x}, v) : (\vec{x}, (v)_1, (v)_2) \in C\}$$

und damit nach dem Projektionssatz rekursiv aufzählbar.  $\square$

Mit dem Projektionssatz übertragen sich auch eine Reihe von Abschlusseigenschaften der rekursiven Mengen auf die r.a. Mengen.

**14.3 KOROLLAR.** *Die Klasse RA der r.a. Mengen ist abgeschlossen gegen Vereinigung (Disjunktion), Durchschnitt (Konjunktion), Einsetzen total rekursiver Funktionen und gegen beschränkte Quantoren.*

**BEWEIS.** Man benutzt, dass man die genannten Operatoren mit dem Existenzquantor vertauschen kann. Wir begnügen uns mit einem Beispiel, nämlich dem Abschluss von RA gegen den Durchschnitt. Andere Fälle werden in den Übungen behandelt. Seien  $A_1, A_2 \subseteq \mathbb{N}$  r.a., also nach dem Projektionssatz die Projektionen rekursiver Mengen  $B_1, B_2$ . Für den Durchschnitt  $A_1 \cap A_2$  der Mengen gilt dann

$$\begin{aligned} x \in A_1 \cap A_2 &\Leftrightarrow x \in A_1 \ \& \ x \in A_2 \\ &\Leftrightarrow \exists y_1 ((x, y_1) \in B_1) \ \& \ \exists y_2 ((x, y_2) \in B_2) \\ &\Leftrightarrow \exists y_1 \exists y_2 ((x, y_1) \in B_1 \ \& \ (x, y_2) \in B_2) \end{aligned}$$

wobei die Matrix der letzten Formel rekursiv ist, also  $A_1 \cap A_2$  nach Satz 14.1 und Korollar 14.2 r.a. ist.  $\square$

Wie wir weiter unten sehen werden, ist RA jedoch weder gegen Komplement noch gegen den Allquantor abgeschlossen. Als Nächstes geben wir die (häufig als Definition gewählte) Charakterisierung der r.a. Mengen über Aufzählungsfunktionen an.

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

- (i)  $A$  ist rekursiv aufzählbar.
- (ii)  $A$  ist leer oder  $A$  ist der Wertebereich einer 1-stelligen total rekursiven Funktion über  $\mathbb{N}$ .
- (iii)  $A$  ist der Wertebereich einer 1-stelligen partiell rekursiven Funktion über  $\mathbb{N}$ .

**BEWEIS.** Wir zeigen die Implikationen (i)  $\Rightarrow$  (ii)  $\Rightarrow$  (iii)  $\Rightarrow$  (i).

(i)  $\Rightarrow$  (ii). Sei  $A \neq \emptyset$  r.a. und  $z_0 \in A$ . Nach dem Projektionssatz ist  $A$  Projektion einer rekursiven Menge  $B$ . Die Funktion

$$f(x) = \begin{cases} (x)_1 & \text{falls } ((x)_1, (x)_2) \in B \\ z_0 & \text{sonst} \end{cases}$$

ist dann total rekursiv und  $A = Wb(f)$ .

(ii)  $\Rightarrow$  (iii). Ist  $A \neq \emptyset$ , so ist die Behauptung trivial, und  $A = \emptyset$  ist Wertebereich der

nirgends definierten partiell rekursiven Funktion  $\mu(C_1^2)$ .

(iii)  $\Rightarrow$  (i). Sei  $A = Wb(\psi)$  und sei  $e$  ein Index von  $\psi$ . Dann gilt

$$\begin{aligned} x \in A &\Leftrightarrow \exists y (\psi(y) = x) \\ &\Leftrightarrow \exists y (\{e\}(y) = x) \\ &\Leftrightarrow \exists y \exists z (T(e, y, z) \& U(z) = x) \end{aligned} \quad (14.1)$$

weshalb  $A$  nach Satz 14.1 und Korollar 14.2 r.a. ist.  $\square$

Die Beziehungen zwischen den r.a. und den rekursiven Mengen beschreibt der nächste Satz:

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

**BEWEIS.** Sei zunächst  $A$  rekursiv. Dann gilt

$$\vec{x} \in A \Leftrightarrow \exists y (\vec{x} \in A)$$

weshalb  $A$  Projektion der rekursiven Menge

$$B = \{(\vec{x}, y) : \vec{x} \in A\}$$

und daher r.a. ist. Da die Klasse der rekursiven Mengen gegen Komplement abgeschlossen ist, gilt ebenso, dass  $\bar{A}$  r.a. ist.

Sind umgekehrt  $A$  und  $\bar{A}$  r.a., so wählt man rekursive Mengen  $B_1$  und  $B_2$ , deren Projektionen  $A$  und  $\bar{A}$  sind. Es gilt dann

$$\vec{x} \in A \Leftrightarrow (\vec{x}, y_x) \in B_1 \text{ für } y_x = \mu y((\vec{x}, y) \in B_1 \cup B_2)$$

d.h.

$$c_A(\vec{x}) = c_{B_1}(\vec{x}, \mu y((\vec{x}, y) \in B_1 \cup B_2))$$

woraus die Rekursivität von  $A$  aufgrund der Abschlusseigenschaften von F(REK) folgt.  $\square$

Satz 14.5 zeigt insbesondere, dass jede rekursive Menge auch rekursiv aufzählbar ist. Dass die Umkehrung nicht gilt, ergibt sich aus der Nichtrekursivität des Halteproblems.

**14.6 KOROLLAR.** *Die Klasse REK der rekursiven Mengen ist echt enthalten in der Klasse RA der rekursiv aufzählbaren Mengen. Das Halteproblem  $K$  ist ein Beispiel für eine r.a. Menge, die nicht rekursiv ist.*

**BEWEIS.** Nach den obigen Bemerkungen genügt es zu zeigen, dass  $K$  r.a. ist, was wegen

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

nach dem Projektionssatz gilt.  $\square$

Dies zeigt auch, dass  $\bar{K}$  nicht r.a. ist. Hieraus folgt, dass RA weder gegen Komplement noch gegen Allquantor abgeschlossen ist. Ebenfalls sieht man hiermit, dass REK weder gegen den Existenz- noch gegen den Allquantor abgeschlossen ist.

14.7 KOROLLAR. (a) Die Klasse der r.a. Mengen ist weder gegen Komplement noch gegen den Allquantor abgeschlossen.

(b) Die Klasse der rekursiven Mengen ist weder gegen den Existenzquantor noch gegen den Allquantor abgeschlossen.

BEWEIS. (a) Nach Korollar 14.6 und Satz 14.5 ist das Komplement  $\bar{K}$  des r.a. Halteproblems  $K$  nicht r.a. Da

$$\langle e, x \rangle \in \bar{K} \Leftrightarrow \{e\}(x) \uparrow \Leftrightarrow \neg \exists y T(e, x, y) \Leftrightarrow \forall y (\neg T(e, x, y))$$

gilt und da  $\neg T(e, x, y)$  wegen des Abschlusses von REK gegen Komplement rekursiv ist, folgt hieraus auch der 2. Teil der Behauptung.

(b) Da nach dem Projektionssatz jede r.a. Menge durch Existenzquantifizierung aus einer rekursiven Menge entsteht, ist REK nach Korollar 14.6 nicht gegen  $\exists$  abgeschlossen. Da der Existenzquantor  $\exists$  vermöge  $\neg \forall \neg$  durch Allquantor und Negation darstellbar ist, kann wegen des Abschlusses gegen  $\neg$  die Klasse REK dann auch nicht gegen den Allquantor abgeschlossen sein.  $\square$

Weiter impliziert dies, dass  $\bar{K} \not\leq_m K$  gilt, da die Klasse der r.a. Mengen nach unten gegen die  $m$ -Reduktion (aber – wie das Beispiel von  $\bar{K}$  auch zeigt – nicht gegen die  $T$ -Reduktion) abgeschlossen ist.

14.8 LEMMA. Die Klasse RA der r.a. Mengen ist gegen  $\leq_m$  abgeschlossen. D.h. ist  $B$  r.a. und gilt  $A \leq_m B$ , dann ist auch  $A$  r.a.

BEWEIS. Gilt  $A \leq_m B$  via  $f$ , so entsteht  $A$  aus  $B$  durch Einsetzen der rekursiven Funktion  $f$ , nämlich

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

weshalb die Behauptung aus Korollar 14.3 folgt.  $\square$

Man kann zeigen, dass  $K$  zu den schwierigsten Problemen unter den r.a. Mengen gehört, nämlich dass sich jedes andere r.a. Problem effektiv auf  $K$  reduzieren lässt. Man sagt,  $K$  ist vollständig für die Klasse der r.a. Mengen.

14.9 DEFINITION. Sei  $C$  eine Klasse von Teilmengen von  $\mathbb{N}$ . Eine Menge  $A$  heißt  $m$ -hart für  $C$ , falls

$$\forall B \in C (B \leq_m A).$$

Gilt zusätzlich  $A \in C$ , so heißt  $A$   $m$ -vollständig für  $C$ . (Entsprechend definiert man  $T$ -Härte und  $T$ -Vollständigkeit.)  $\square$

Spricht man nur von vollständigen oder harten Mengen, ohne die Klasse anzugeben, für die die Menge vollständig bzw. hart ist, so meint man stets die Klasse der r.a. Mengen. Weiter sagt man statt  $m$ -vollständig für  $C$  häufig einfach  $C$ -vollständig.

Im nächsten Lemma fassen wir einfache, aber wichtige, Beobachtungen über vollständige und harte Mengen zusammen.

14.10 LEMMA. (a) Ist  $A$   $m$ -hart (vollständig) für  $C$ , so ist  $A$  auch  $T$ -hart (vollständig) für  $C$ .

- (b) Ist  $A$   $r$ -hart für  $C$  und gilt  $A \leq_r B$ , so ist auch  $B$   $r$ -hart für  $C$  ( $r = m, T$ ).
- (c) Enthält  $C$  eine nichtrekursive Menge, so ist jede  $r$ -harte (und daher jede  $r$ -vollständige) Menge für  $C$  nicht rekursiv ( $r = m, T$ ).
- (d) Ist  $C$  gegen  $r$ -Äquivalenz abgeschlossen, so ist jede Menge, die zu einer  $r$ -vollständigen Menge für  $C$   $r$ -äquivalent ist, ebenfalls  $r$ -vollständig für  $C$  ( $r = m, T$ ).

BEWEIS. Diese Aussagen folgen direkt aus den elementaren algebraischen Eigenschaften der Reduzierbarkeiten und der Tatsache, dass  $A \leq_m B$  auch  $A \leq_T B$  impliziert.  $\square$

14.11 SATZ. Die Halteprobleme  $K, K_d, K_0$  sind  $m$ -vollständig (und daher  $T$ -vollständig).

BEWEIS. Wegen  $K =_m K_d =_m K_0$  und wegen des Abschlusses von RA gegen  $=_m$  genügt es  $K$  zu betrachten. Dass  $K$  r.a. ist, wurde bereits gezeigt. Es genügt also die  $m$ -Härte von  $K$  zu zeigen.

Sei also  $A$  eine r.a. Menge. Wir haben  $A \leq_m K$  zu zeigen. Hierzu wählen wir  $\psi \in F(\text{REK})$  mit  $A = Db(\psi)$  und einen Index  $e$  für  $\psi$ . Es gilt dann

$$x \in A \Leftrightarrow \psi(x) \downarrow \Leftrightarrow \{e\}(x) \downarrow \Leftrightarrow \langle e, x \rangle \in K$$

weshalb  $A \leq_m K$  via  $f(x) = \langle e, x \rangle$ .  $\square$

Es gibt viele interessante Probleme auch außerhalb der Berechenbarkeitstheorie, die rekursiv aufzählbar aber nicht rekursiv sind. Bei diesen Problemen handelt es sich um *unbeschränkte Suchprobleme*, d.h. Probleme  $P$ , für die die Mitgliedschaft einer Eingabe  $x$  in  $P$  durch einen Zeugen  $y$  gesichert wird, dessen Größe man nicht effektiv beschränken kann, man aber für jeden Kandidaten  $y$  effektiv überprüfen kann, ob er ein Zeuge für  $x \in P$  ist. D.h. das Problem  $P$  ist die Projektion der entscheidbaren Menge

$$ZP = \{(x, y) : y \text{ ist Zeuge für } x \in P\}$$

und damit (nach Churchscher These und dem Projektionssatz) r.a. Den Nachweis, dass man die Suche nicht effektiv beschränken kann, führt man meist durch  $m$ -Reduktion des Halteproblems auf  $P$ , womit sich dann nicht nur die Unentscheidbarkeit von  $P$ , sondern zugleich die  $m$ -Vollständigkeit von  $P$  ergibt.

Ein Beispiel für ein solches unbeschränktes Suchproblem in der Mathematischen Logik ist die Menge  $B$  der in einer (hinreichend starken) Theorie beweisbaren Sätze. Ein Zeuge  $y$  für  $x \in B$  ist hier ein Beweis  $y$  von  $x$ . Die Korrektheit eines Beweises lässt sich effektiv überprüfen, d.h. wir können entscheiden, ob  $y$  bezeugt, dass  $x \in B$  gilt. Für hinreichend starke Theorien kann man aber die Beweislängen nicht effektiv beschränken.

Im Vorlesungsteil über Formale Sprachen werden wir weitere Beispiele für unbeschränkte Suchprobleme kennenlernen, nämlich die Menge der Wörter, die in einer (hinreichend komplexen) Grammatik eine Herleitung besitzen.

Obwohl man bei „natürlichen“ r.a. Problemen in der Regel die Erfahrung macht, dass sie entweder rekursiv oder  $m$ -vollständig sind, so kann man dennoch zeigen, dass es rekursiv aufzählbare Mengen gibt, die weder rekursiv noch vollständig sind. In der Tat gibt es unendlich viele Unlösbarkeitsgrade von r.a. Mengen, d.h. unendlich viele zueinander nicht  $r$ -äquivalente r.a. Mengen ( $r = m, T$ ). Die Untersuchung dieser Unlösbarkeitsgrade ist ein zentrales Forschungsgebiet in der Berechenbarkeitstheorie.

Der Projektionssatz lässt sich wie folgt verschärfen:

14.12 SATZ. (SATZ VON MATIJASEVIČ) 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

$$\vec{x} \in A \Leftrightarrow \exists \vec{y} \in \mathbb{N}^k (p_1(\vec{x}, \vec{y}) = p_2(\vec{x}, \vec{y})) \quad (14.2)$$

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

Da die Relation  $p_1(\vec{x}, \vec{y}) = p_2(\vec{x}, \vec{y})$  primitiv rekursiv ist, ist nach dem Projektionssatz jede gemäß (14.2) definierte Menge  $A$  r.a. Die Umkehrung ist sehr viel schwieriger zu zeigen und wir wollen hier auf den Beweis verzichten. 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?

(Ursprünglich betrachtete Hilbert sog. *Diophantische* Gleichungssysteme, d.h. endliche Systeme von Polynomgleichungen wie oben, wobei jedoch die Koeffizienten aus  $\mathbb{Z}$  sein dürfen. Jedes solche System kann jedoch in eine Gleichung w.o. effektiv übersetzt werden, ohne die Lösbarkeit zu verändern.)

Der Satz von Matijasevič zeigt (mit Churchscher These), dass es solch einen Algorithmus nicht geben kann. Hierzu wählt man eine nichtrekursive r.a. Menge  $A \subseteq \mathbb{N}$  (z.B.  $K_d$ ) und eine Darstellung von  $A$  gemäß (14.2). Für jede Zahl  $m$  kann man dann effektiv die Polynome  $p_{1,m}$  und  $p_{2,m}$  angeben, die man aus  $p_1$  und  $p_2$  erhält, wenn man dort die Variable  $x$  durch  $m$  ersetzt. Es gilt dann aber, dass  $m$  genau dann in  $A$  ist, wenn die Gleichung  $p_{1,m}(\vec{y}) = p_{2,m}(\vec{y})$  eine Lösung besitzt. Der von Hilbert gesuchte Algorithmus würde daher ein Entscheidungsverfahren für  $A$  liefern, das es aber nach Wahl von  $A$  nicht geben kann.

Zum Abschluss dieses Abschnitts gehen wir noch kurz auf die *arithmetische Hierarchie* ein. Wir haben gesehen, dass die Klasse der r.a. Mengen gegen die Junktoren  $\vee$  und  $\&$ , nicht aber gegen die Negation  $\neg$  abgeschlossen ist. Weiter gilt der Abschluss gegen den Existenzquantor, aber nicht gegen den Allquantor. Schließt man die Klasse der r.a. Mengen nun zusätzlich gegen Negation und Allquantor ab, so erhält man die Klasse der sogenannten *arithmetischen Mengen*. Durch logische Operationen lässt sich jede arithmetische Menge  $A$  in Pränexnormalform darstellen, d.h.

$$\vec{x} \in A \Leftrightarrow \exists y_1 \forall y_2 \dots Q y_n ((\vec{x}, \vec{y}) \in B) \quad (14.3)$$

wobei die Quantoren in dem Präfix alternieren und  $B$  eine rekursive Menge ist. Hat  $A$  eine Darstellung (14.3) mit  $n$  Quantoren, so sagt man, dass  $A$  eine  $\Sigma_n$ -Menge ist. Besitzt  $A$  eine duale mit einem Allquantor beginnende Darstellung, so ist  $A$  eine  $\Pi_n$ -Menge. (Wie man sich leicht überlegt, ist  $A$  genau dann eine  $\Sigma_n$ -Menge, wenn  $\bar{A}$  eine  $\Pi_n$ -Menge ist.) Man kann dann zeigen, dass man hierdurch eine echte Hierarchie der arithmetischen Mengen erhält:

$$\Sigma_1 \subset \Sigma_1 \cup \Pi_1 \subset \Sigma_2 \subset \Sigma_2 \cup \Pi_2 \subset \Sigma_3 \dots$$

Diese wird die arithmetische Hierarchie genannt. Wegen des Projektionssatzes besteht  $\Sigma_1$  gerade aus den r.a. Mengen. Jede Klasse  $\Sigma_n$  besitzt eine vollständige Menge, nämlich den weiter oben definierten  $n$ -ten Jump  $0^{[n]}$ . (Wir verzichten hier auf den Beweis.)

Die Arithmetische Hierarchie ist ein wichtiges Hilfsmittel zur Klassifikation unentscheidbarer Mengen. „Natürliche“ unentscheidbare Probleme sind in der Regel vollständig für eine (meist niedrige) Stufe dieser Hierarchie. Beispiele für  $\Sigma_1$ -vollständige (d.h. RA-vollständige) Mengen haben wir oben schon kennengelernt. Das Totalitätsproblem

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

ist z.B.  $\Pi_2$ -vollständig, während das Rekursivitätsproblem

$$\text{REK} = \{e : W_e \text{ rekursiv}\}$$

$\Sigma_3$ -vollständig ist. Wir verzichten hier auf die Härtebeweise und zeigen lediglich  $\text{TOT} \in \Pi_2$  und  $\text{REK} \in \Sigma_3$ . Hierzu beschreiben wir diese Mengen formal (wobei wir im Fall von REK Satz 14.5 benutzen) und formen in Pränormalform um:

$$\begin{aligned} e \in \text{TOT} &\Leftrightarrow \{e\} \text{ total} \\ &\Leftrightarrow \forall x(\{e\}(x) \downarrow) \\ &\Leftrightarrow \forall x \exists y(T(e, x, y)) \end{aligned}$$

$$\begin{aligned} e \in \text{REK} &\Leftrightarrow W_e \text{ rekursiv} \\ &\Leftrightarrow \exists x(W_e = \overline{W_x}) \\ &\Leftrightarrow \exists x \forall y(y \in W_e \Leftrightarrow y \notin W_x) \\ &\Leftrightarrow \exists x \forall y([y \in W_e \vee y \in W_x] \& \neg[y \in W_e \& y \in W_x]) \\ &\Leftrightarrow \exists x \forall y([\exists u_1 T(e, y, u_1) \vee \exists u_2 T(x, y, u_2)] \\ &\quad \& \neg[\exists v_1 T(e, y, v_1) \& \exists v_2 T(x, y, v_2)]) \\ &\Leftrightarrow \exists x \forall y(\exists u[T(e, y, u) \vee T(x, y, u)] \\ &\quad \& \neg \exists v[T(e, y, (v)_1) \& T(x, y, (v)_2)]) \\ &\Leftrightarrow \exists x \forall y(\exists u[T(e, y, u) \vee T(x, y, u)] \\ &\quad \& \forall v[\neg T(e, y, (v)_1) \vee \neg T(x, y, (v)_2)]) \\ &\Leftrightarrow \exists x \forall y \forall v \exists u([T(e, y, u) \vee T(x, y, u)] \\ &\quad \& [\neg T(e, y, (v)_1) \vee \neg T(x, y, (v)_2)]) \\ &\Leftrightarrow \exists x \forall z \exists u([T(e, (z)_1, u) \vee T(x, (z)_1, u)] \\ &\quad \& [\neg T(e, (z)_1, (z)_{2,1}) \vee \neg T(x, (z)_1, (z)_{2,2})]) \end{aligned}$$

Der Name der Klasse der Arithmetischen Mengen stammt aus der Mathematischen Logik: Die arithmetischen Mengen sind genau diejenigen, die man in einem formalen System der Arithmetik definieren kann, wobei solch ein System auf der Prädikatenlogik erster Stufe basiert und zusätzlich mathematische Axiome zur Beschreibung der natürlichen Zahlen enthält. (Dies folgt unmittelbar aus dem Satz von Matijasevič, war aber schon viel früher bekannt.) Das von Hilbert am Anfang des Jahrhunderts begründete *Hilbertsche Programm* hatte zum Ziel, die Mathematik zu formalisieren, um diese auf eine sichere Basis zu stellen. Gödel mit seinem berühmten *Unvollständigkeitssatz* hat jedoch gezeigt, dass dies nicht vollständig gelingen kann: Es gibt kein widerspruchsfreies formales System der Arithmetik, in dem alle wahren Sätze der Arithmetik herleitbar, d.h. beweisbar, sind. Gödel gelang dies durch Gödelisierung des Systems zu zeigen. Hierdurch werden Sätzen Zahlen zugeordnet, weshalb die Aussage,

dass ein Satz wahr oder beweisbar ist, in ein zahlentheoretisches Prädikat übergeht. Daher kann man Aussagen *über* das System durch Aussagen *in* dem System ausdrücken und damit die logischen Ebenen verschmelzen. Gödel benutzte dies, um einen Satz zu definieren, der (zu Recht) seine eigene Unbeweisbarkeit im System behauptet, und der damit wahr aber unbeweisbar ist. Berechenbarkeitstheoretisch kann man das Unvollständigkeitsphänomen durch die Analyse der Komplexität der beweisbaren und der wahren Sätze (d.h. genauer deren Gödelnummern) nachweisen: Für jedes System bildet die Klasse der beweisbaren Sätze (wie schon oben bemerkt) eine r.a. Menge, während – wie von Tarski gezeigt wurde – die Menge der wahren Sätze der Arithmetik noch nicht einmal eine arithmetische Menge ist.