

Berechenbarkeit, Entscheidbarkeit, Aufzählbarkeit

Vorlesungsskript SS 2011

© Christoph Walther

Fachgebiet Programmiermethodik
Fachbereich Informatik
Technische Universität Darmstadt

21. Juni 2011

INHALTSVERZEICHNIS

1	Einleitung	5
2	Rechner, Algorithmen, Programme	10
2.1	Rechner und Programmiersprachen	10
2.2	Die Programmiersprache \mathcal{P}	12
2.3	Semantik von \mathcal{P} -Programmen	21
3	Berechenbare Funktionen	26
3.1	\mathcal{P} -berechenbare Funktionen	26
3.2	Die Churchsche These	27
3.3	Nicht-Konstruktivität und Konstruktivität	29
4	Gödelisierungen	32
4.1	Kodierung von Datentypen	32
4.2	Die Paar-Funktion	34
4.3	Stelligkeit berechenbarer Funktionen	39
4.4	Kodierung von Programmen	41
5	Algorithmisch unlösbare Aufgaben	46
5.1	Abzählbarkeit der \mathcal{P} -berechenbaren Funktionen	46
5.2	Nicht-berechenbare Funktionen	48
5.3	Das Halteproblem	50
6	Universelle Funktion und Interpretierer	52
7	Entscheidbarkeit und Semi-Entscheidbarkeit	54
7.1	Entscheidbare Probleme	54
7.2	Endliche Probleme	56
7.3	Semi-entscheidbare Probleme	57

8	Schrittfunktionen	62
8.1	Die Schrittfunktion eines \mathcal{P} -Programms	62
8.2	Die universelle Schrittfunktion	65
8.3	Schrittweise Abarbeitung von \mathcal{P} -Programmen	67
9	Rekursive Aufzählbarkeit	71
9.1	Aufzählungsverfahren	71
9.2	Abzählbarkeit und rekursive Aufzählbarkeit	77
9.3	Definitions- und Bildbereiche berechenbarer Funktionen	78
10	Unentscheidbare Probleme	81
10.1	Das Totalitätsproblem	81
10.2	Reduzierbarkeit	82
10.3	Das <i>s-m-n</i> -Theorem	84
10.4	Programmäquivalenz	87
10.5	Der Satz von <i>Rice</i>	91
10.6	Weitere Probleme	93
11	Primitiv-rekursive und μ-rekursive Funktionen	96
11.1	Primitiv-rekursive Funktionen	96
11.2	Definitionsprinzipien für primitiv-rekursive Funktionen	99
11.3	Werteverlaufsrekursion	103
11.4	Ein Rechenmodell für primitiv-rekursive Funktionen	106
11.5	loop-berechenbare Funktionen	108
11.6	Die <i>Ackermann</i> -Funktion	118
11.7	μ -rekursive Funktionen	120
12	Turingmaschinen	129
12.1	Definition und Rechenmodell	129
12.2	Turing-berechenbare Funktionen	134
12.3	Berechnungsvollständigkeit von \mathcal{P}	137
13	Begriffe und Schreibweisen	143
	Literaturverzeichnis	144
	Index	145

Vorwort

Dieses Skript ist eine überarbeitete und erweiterte Version des Vorlesungsskripts meiner im SS 2001 erstmalig gehaltenen Vorlesung über Berechenbarkeitstheorie. Da es bei dieser Thematik um fundamentale Grundlagen geht, ist es erforderlich, mit mathematischer Präzision zu arbeiten. Dieser Forderung kann jedoch in einer Vorlesung vom Umfang 2+1 nicht durchgehend nachgekommen werden. Man muß daher an gewissen Stellen an die "Vorstellungskraft" des Auditoriums appellieren, wenn man den Stoff in beschränkter Zeit präsentieren will. Konkret bezieht sich dieser Vorbehalt auf den Nachweis der \mathcal{P} -Berechenbarkeit der universellen Funktion und der universellen Schrittfunktion. Diese Auslassungen sind zugegebenermaßen höchst unbefriedigend, aber aus Zeitgründen unvermeidbar.

Herrn Markus Aderhold – als Hörer der damaligen Vorlesung mit den Schwächen des Originalskripts bestens vertraut – danke ich für sehr sorgfältiges Korrekturlesen, Hinweise auf Fehler und konstruktive Verbesserungsvorschläge.

Bei aller Sorgfalt wird das Skript trotzdem noch Fehler enthalten.¹ Entsprechende Hinweise auf Schreibfehler und inhaltliche Schwächen nehme ich gerne unter Chr.Walther@informatik.tu-darmstadt.de entgegen.

Darmstadt, im Mai 2007

Das Skript wurde für das Sommersemester 2008 überarbeitet. Korrigiert wurden einige Schreibfehler sowie einige Ergänzungen in Definitionen eingefügt (und Beweise dann entsprechend angepaßt). Insbesondere wird jetzt für die Abarbeitung von Programmen unter einer Laufzeitbeschränkung ein einfacheres Kostenmaß verwendet.

Darmstadt, im März 2008

Das Skript wurde für das Sommersemester 2009 überarbeitet. Korrigiert wurden lediglich einige Schreibfehler.

Darmstadt, im April 2009

Das Skript wurde für das Sommersemester 2011 überarbeitet. Neben der Korrektur einiger Schreibfehler, redaktionellen Überarbeitungen und Ergänzungen, wie etwa durch Satz 9.8, wurden die Beweise für Definition durch gegenseitige Rekursion sowie die Modellierung von while-Schleifen mittels μ -rekursiver Funktionen stark vereinfacht.

Darmstadt, im Juni 2011

¹ Einige Indexeinträge vermeiden Umlaute, also 'ae' anstatt 'ä' u.s.w. Dies sind weder Schreibfehler noch Ausdruck einer eigenwilligen Rechtschreibung, sondern vielmehr Notwendigkeiten, um Fehler meiner \TeX -Installation zu umgehen.

1. EINLEITUNG

In der Berechenbarkeitstheorie wird untersucht, welche Aufgaben durch Rechner gelöst werden können und welche Aufgaben prinzipiell nicht durch Rechner lösbar sind. Es geht hier also um die Möglichkeiten und insbesondere um die *prinzipiellen Grenzen* des Problemlösens mittels Rechnern. Die Ergebnisse der Berechenbarkeitstheorie gehören damit zum fundamentalen Grundlagenwissen der Informatik.¹ Daher sollte jeder Informatiker – unabhängig davon, ob er sich für theoretische Fragestellungen interessiert oder nicht – die essentiellen Grundvoraussetzungen seines Berufs kennen. Er sollte beispielsweise wissen,

- warum es keine gängige Programmiersprache gibt, in der nur terminierende Programme geschrieben werden können,
- warum es kein Entwicklungswerkzeug gibt, das feststellen kann, ob die optimierte Version eines Programms (beispielsweise eines Übersetzers für eine Programmiersprache) – abgesehen von verbesserter Laufzeit – das gleiche leistet wie die nicht optimierte Originalversion des Programms,
- warum es kein Testwerkzeug gibt, mit dem festgestellt werden kann, ob die Abarbeitung eines Programms mit bestimmten Eingaben terminiert oder nicht,
- warum jedes Verfahren, mit dem die Terminierung von Programmen bewiesen werden kann, beim Terminierungsnachweis unendlich vieler (terminierender) Programme versagt,
- warum es kein Verifikationswerkzeug gibt, mit dem für jedes Programm festgestellt werden kann, ob das Programm eine bestimmten Aufgabe – etwa das Sortieren von Listen, die Berechnung der Primfaktorzerlegung von natürlichen Zahlen u.s.w. – löst oder nicht löst.

¹ Historisch handelt es sich um Ergebnisse der mathematischen Logik ab den 30er Jahren des letzten Jahrhunderts, also aus einer Zeit, in der die Vorstellung programmierbarer Rechner eine “Vision” ohne jeglichen Realitätsbezug war. Die Informatik, deren “Geburt” als eigenständige Wissenschaft etwa 35 Jahre später datiert, hat diese Ergebnisse als Grundprämissen ihres Fachs übernommen.

Anworten auf diese (und weitere) Fragen findet man in diesem Skript. Dabei werden nur solche Ergebnisse der Berechenbarkeitstheorie vorgestellt, die ein Informatiker mindestens kennen sollte. Es handelt sich hier also nur um eine Einführung in das Gebiet – für Vertiefungen wird auf das Literaturverzeichnis mit einer Auswahl der umfangreichen Literatur zu diesem Thema verwiesen.

Da sich die Berechenbarkeitstheorie aus der mathematischen Logik, also einem Teilgebiet der Mathematik, entwickelt hat, ist offensichtlich, daß man hier um Beweise nicht herumkommt. Diese Beweise sind genaugenommen nicht kompliziert. Verständnisschwierigkeiten resultieren vielmehr daraus, daß die abstrakten Begriffsbildungen nicht verstanden werden. Anders gesagt, viele Studenten haben Schwierigkeiten, die mathematischen Konzepte in Bezug zu ihrer realen Informatikpraxis zu setzen, was zum Verständnis der Inhalte jedoch unabdingbar ist.

Beispielsweise werden Programme “gödelisiert”, d.h. durch natürliche Zahlen kodiert, damit man Programme wie Daten verarbeiten kann. Der Übersetzer einer Programmiersprache, der ja einen Programmtext als Eingabe erwartet, erhält in der Berechenbarkeitstheorie eine natürliche Zahl als Eingabe, die lediglich die Zahldarstellung eines Programmtextes ist. Zum Verständnis von Sätzen und Beweisen muß man deshalb diese Zahlen dann nur als *Repräsentation* von Programmtexten “lesen”. Erkennt man jedoch diesen Bezug nicht, so kann man auch die entsprechenden Sätze und schon gar nicht deren Beweise verstehen.

Um Aussagen über die Berechnungen programmierbarer Rechner zu erhalten, muß ein Maschinenmodell zugrunde gelegt werden. Der überwiegende Teil der Lehrbücher dieses Gebiets verwendet dazu *Turingmaschinen*. Dies hat historische Wurzeln, denn in einer Zeit, in der es keine programmierbaren Rechner (geschweige denn Programmiersprachen) gab, mußte man sich mit dem mathematischen Modell eines Rechners – der Turingmaschine – begnügen. Die Turingmaschine besitzt alle Merkmale eines Rechners (Programm- und Datenspeicher, Rechenwerk), und folglich sind alle Ergebnisse, die man über Turingmaschinen erhält, auf beliebige Rechner mit beliebigen Betriebssystemen und beliebigen Programmiersprachen übertragbar.²

Allerdings ist die Programmierung von Turingmaschinen äußerst aufwendig, und Turingprogramme sind nur mit großer Mühe zu verstehen. Folglich steht man bei Verwendung von Turingmaschinen vor einem Dilemma: Entweder verwendet man in Beweisen andauernd Formulierungen der Form “*wie man sich leicht vorstellen kann, gibt es eine Turingmaschine die Dies-und-Das leistet*”, ersetzt Beweise durch Graphiken und andere Illustrationen u.s.w. und appelliert

² Anstatt ein JAVA Programm unter *Windows XP* auf einem INTEL-Chip auszuführen, kann man also genausogut (die Hardwareimplementierung) einer Turingmaschine verwenden. Aus Effizienzgründen sollte man dies jedoch tunlichst unterlassen.

damit ständig an die Vorstellungskraft der Studenten, oder aber man entwickelt eine Programmiermethodik für Turingmaschinen, mittels derer dann Beweise mathematisch präzise angegeben werden können, d.h. so, wie es in einem Gebiet, in dem es um fundamentale Grundlagen geht, eben erforderlich ist. Mit der zweiten Lösung erhält man zwar die erforderliche mathematische Präzision, allerdings zu einem hohen Preis: Zum einen müssen die Studenten in der Programmierung von Turingmaschinen ausgebildet werden – eine Fähigkeit, die, abgesehen von Bearbeitung der Übungsaufgaben, völlig nutzlos ist. Zum anderen werden die entscheidenden Beweisideen und die Kernaussagen des Gebiets ständig durch die Turingprogrammierung verschleiert und schlimmstenfalls sogar verdeckt. Sätze und deren Beweise werden dadurch genauso “barock” wie die Turingprogramme selbst.

Aber müssen überhaupt Turingmaschinen verwendet werden? Um die zentralen Ergebnisse der Berechenbarkeitstheorie zu erhalten, ist ein Maschinenmodell erforderlich, bei dem Programme Programme verarbeiten können. Dies ist jedoch schon bei Programmierung in irgendeiner Assembler- bzw. Maschinensprache möglich, und folglich verwenden einige Lehrbücher eine sogenannte *Registermaschine* oder *random access machine (RAM)* als Modell eines Rechners. Zwar stellt die Assemblerprogrammierung einen großen Fortschritt gegenüber der Turingprogrammierung dar, sie besitzt im Prinzip jedoch die gleichen Nachteile wie die Turingprogrammierung, allerdings in stark abgeschwächter Form.

Da jedoch auch Programme einer höheren Programmiersprache Programme (dieser Programmiersprache) verarbeiten können (etwa ein in C geschriebener C-Übersetzer oder ein in JAVA geschriebener JAVA-Interpreter), kann man genausogut eine höhere Programmiersprache als Ausgangspunkt wählen. In einigen Programmiersprachen, wie etwa LISP, werden Programme und Daten überhaupt nicht unterschieden, die Verarbeitung von Programmen durch Programme kann dort direkt – also ohne den Umweg über Kodierungen von Programmen – implementiert werden. Einige (wenige) Lehrbücher zur Berechenbarkeitstheorie, wie beispielweise das hier ausdrücklich zur Vertiefung empfohlene [Jones(1997)], verwenden eine solche Programmiersprache als Ausgangspunkt für ihre Präsentation.

Andere Programmiersprachen, wie etwa C oder JAVA, erlauben keine direkte Verarbeitung von Programmen. Dort geht man dann den Umweg über geeignete Datenstrukturen, indem Programme etwa als Texte (*string, array of character*) “kodiert” werden. Auch solche Programmiersprachen werden gelegentlich in Lehrbüchern verwendet, etwa in [Kfoury et al.(1982)Kfoury, Moll, and Arbib] und [Wagner(1994)]. Dies ist genauso akzeptabel wie die Verwendung einer Programmiersprache, in der Programme direkt verarbeitet werden können, denn die Repräsentation von Programmen durch Datenstrukturen der Sprache ist gängige Praxis in der Informatik.

Um das Verständnis der Vorlesungsinhalte nicht unnötig zu erschweren, verwenden wir deshalb in diesem Skript eine einfache (höhere) Programmiersprache – \mathcal{P} genannt – zur Implementierung von Algorithmen. Diese Programmiersprache enthält nur Sprachkonzepte, die man auch in jeder anderen höheren Programmiersprache findet. Damit ist jedermann, der wenigstens mit *einer* höheren Programmiersprache vertraut ist, sofort in der Lage \mathcal{P} -Programme zu verstehen und zu schreiben.

Bei Definition dieser Programmiersprache müssen wir entscheiden, wie ausdrucksstark die Sprache gewählt werden soll. Diese Frage ist deshalb von Bedeutung, da viele Beweise in der Berechenbarkeitstheorie *konstruktiv* geführt werden. Beispielsweise zeigt man, daß ein Problem durch einen Rechner lösbar ist, indem man ein Programm angibt, das die Lösung berechnet. Ebenso kann man die algorithmische Unlösbarkeit von Problemen zeigen: Man führt einen Widerspruchsbeweis und nimmt dafür die Lösbarkeit des Problems an. Damit muß es ein Programm geben, das eine Lösung berechnet. Dieses Programm verwendet man dann zur Konstruktion weiterer Programme, von denen eines offensichtlich Unmögliches leistet, und damit einen Widerspruch offenbar macht.

Kurzum, viele Beweise erfordern hier Programmierung, und je ausdrucksstärker die verwendete Programmiersprache ist, desto einfacher ist es solche Programme zu schreiben. Nur wird es dann auch aufwendiger – und bei Verwendung gängiger Programmiersprachen praktisch unmöglich – Beweise über Berechnungen von Programmen dieser Sprache zu führen.³ Dieses Problem vermeidet man bei Verwendung einer sehr einfachen Programmiersprache. Allerdings ist dann die Programmierung mühselig, und damit werden Beweise aufwendiger. Abhilfe ist hier, die sehr einfache Sprache durch weitere Sprachkonzepte ausdrucksstärker zu gestalten, wobei diese zusätzlichen Sprachkonzepte jedoch nur als abkürzende Schreibweisen für Programmfragmente der Ausgangssprache aufgefaßt werden. Damit wird die Programmierung komfortabler, und bei Beweisen kann dann je nach konkreter Aufgabenstellung frei gewählt werden, ob man die erweiterte Sprache verwendet oder aber nur die Ausdrücke der einfachen Kernsprache betrachtet.

Unter Verwendung von \mathcal{P} -Programmen führen wir nachfolgend diejenigen zentralen Grundbegriffe der Berechenbarkeitstheorie ein und beweisen die Kernaussagen des Gebiets, die jeder Informatiker kennen sollte.

³ Es reicht natürlich nicht, ein Programme nur anzugeben, sondern man muß auch zeigen, daß dieses Programm auch das Gewünschte leistet. D.h., Programme müssen *verifiziert* werden – darin steckt dann der eigentliche Beweis. Ohne Werkzeugunterstützung ist dies bei gängigen Programmiersprachen jedoch ein hoffnungsloses Unterfangen.

Daran anschließend betrachten wir mit den μ -rekursiven Funktionen ein alternatives Berechenbarkeitsmodell, das man als eine Art *funktionale Programmiersprache* auffassen kann. Die Untersuchung des Zusammenhangs zwischen μ -rekursiven Funktionen und (imperativen) \mathcal{P} -Programmen sowie darauf aufbauend der Äquivalenznachweis beider Berechenbarkeitsmodelle bildet den Kern dieses Kapitels.

Abschließend werden Turingmaschinen sowie ihr Zusammenhang mit \mathcal{P} -Programmen betrachtet, denn dieses Berechenbarkeitsmodell ist nach wie vor der de-facto Standard des Gebiets (und verwandter Gebiete, wie etwa der Komplexitätstheorie), und sollte daher jedem Informatiker in seinen Grundzügen geläufig sein.⁴

⁴ Dieses Kapitel steht nicht im Widerspruch zu den zuvor geäußerten Vorbehalten, denn diese beziehen sich ja nicht auf die Turingmaschine an sich, sondern lediglich auf die Didaktik, die die Turingmaschine zum Ausgangspunkt der Einführung in die Grundbegriffe der Berechenbarkeitstheorie macht.

2. RECHNER, ALGORITHMEN, PROGRAMME

2.1. Rechner und Programmiersprachen

Die einfachste Methode nachzuweisen, daß eine Aufgabe mittels eines Rechners lösbar ist, besteht darin, in irgendeiner Programmiersprache ein Programm zu schreiben, das diese Aufgabe löst. Wie soll man aber nun von einer Aufgabe zeigen, daß sie prinzipiell nicht mit Rechnern lösbar ist? Dies zu behaupten bedeutet ja, daß wir nicht nur eine Aussage über alle konkreten Rechner und alle bislang definierten Programmiersprachen treffen, sondern sogar über alle Rechner, die überhaupt noch nicht entworfen wurden und über alle Programmiersprachen, die man sich irgendwann einmal ausdenken kann.

Ausgangspunkt der Untersuchungen ist der Begriff des *Algorithmus*. Darunter soll allgemein ein *Verfahren* verstanden werden, das *automatisch* ausgeführt werden kann. Soll ein Algorithmus auf einem *Rechner* ausgeführt werden, so muß dieser Algorithmus in einer *Programmiersprache* repräsentiert, d.h. aufgeschrieben, werden, deren *Programme* durch den betreffenden Rechner *ausführbar* sind. Ein *Programm* ist also nur eine *Darstellung* eines bestimmten *Algorithmus* in einer bestimmten *Programmiersprache*.

Beispielsweise kann man Felder (“*arrays*”) mit dem *Quicksort*-Algorithmus ordnen. Alternativ können zur Lösung dieser Aufgabe auch andere Algorithmen, wie z.B. *Mergesort*, *Heapsort*, *Bubblesort* u.s.w. verwendet werden. Der Unterschied zwischen diesen Algorithmen besteht darin, daß sie die gestellte Aufgabe (“*ordne ein Feld*”) in unterschiedlicher Art lösen.

Sollen Felder durch einen Rechner geordnet werden, so wählen wir zunächst eine Programmiersprache wie etwa LISP, JAVA, C, C⁺⁺, ... , die auf dem betreffenden Rechner ausführbar ist, und *implementieren* dann den Sortieralgorithmus unserer Wahl, also z.B. *Quicksort*, in der gewählten Programmiersprache. Ergebnis dieser Bemühung ist dann beispielsweise eine *Implementierung* von *Quicksort* in JAVA, die jetzt auf dem gewählten Rechner ausgeführt werden kann.

Mit der Implementierung eines Sortierverfahrens in einer ausführbaren Programmiersprache kann man offensichtlich davon ausgehen, daß das Sortieren von Feldern zu denjenigen Aufgaben gehört, die mittels Rechnern lösbar sind. Jedoch

stellt sich die Frage, was allgemein unter “Ist Aufgabe x durch einen Rechner lösbar?” genau zu verstehen ist.

Mit Definition einer Programmiersprache muß nicht nur deren *Syntax* angegeben werden, sondern auch deren *Semantik*. Mit der Definition der Semantik wird festgelegt, was die Abarbeitung eines Programms der Programmiersprache auf einem Rechner bewirken soll. Dabei wird von konkreten Rechnern abstrahiert: Wird ein Programm auf einem (beliebigen) Rechner ausgeführt, so werden die Speicherinhalte des Rechners verändert. Die “Wirkung” der Abarbeitung eines Programms kann damit abstrakt als Veränderung des initialen Speicherinhalts zu dem Speicherinhalt, der nach Abarbeitung des Programms vorliegt, beschrieben werden. Mit diesem Ansatz müssen wir nicht mehr *alle* Rechner in ihrer Vielseitigkeit und Unterschiedlichkeit betrachten: Jeder Rechner besitzt einen Speicher, der verändert werden kann, und dies reicht uns zur Modellierung *aller* Rechner.

Allerdings haben wir mit Definition der Semantik einer Programmiersprache implizit weitere Annahmen über Rechner getroffen, denn wir fordern ja, daß Rechner auch das *leisten können*, was wir durch die Semantik festgelegt haben. Man muß sich hier also einigen, welche Fähigkeiten von einem Rechner mindestens zu verlangen sind. Dies geschieht dadurch, daß gleichsam eine Art “Standardrechner” definiert wird, dessen Fähigkeiten der Maßstab über alle Aussagen ist, die wir über *beliebige* Rechner treffen. Ein allgemein akzeptierter “Standardrechner” ist die *Turingmaschine*. Kann man nun zeigen, daß eine Programmiersprache (mit gegebener Semantik) diesem Standard genügt, so ist mit dem Nachweis der nicht-Programmierbarkeit (bzw. der Programmierbarkeit) eines Lösungsverfahrens für ein Problem in dieser Programmiersprache zugleich die prinzipielle Unlösbarkeit (bzw. Lösbarkeit) des Problems durch alle Rechner, die dem Turing-Standard genügen, gezeigt. Es bleibt dann nur noch nachzuweisen, daß die Programmiersprache (mit gegebener Semantik) auch tatsächlich dem Turing-Standard genügt. Dies geschieht dadurch, indem man einen Interpreter für eine Turingmaschine in der gegebenen Programmiersprache implementiert. Gelingt dies, so können alle Berechnungen einer Turingmaschine auch durch Programme der gegebenen Programmiersprache durchgeführt werden. Eine Programmiersprache, in der man eine Turingmaschine implementieren kann, wird auch *Turing-vollständig* oder allgemeiner *berechnungsvollständig* genannt.

Hat man nun von einem Problem nachgewiesen, daß kein Programm einer *bestimmten* berechnungsvollständigen Programmiersprache ein Lösungsverfahren für dieses Problem implementiert, so weiß man, daß dieses Problem durch kein Programm *irgendeiner* Programmiersprache gelöst werden kann. In so einem Fall geht man davon aus, daß das Problem prinzipiell nicht mit Rechnern lösbar ist.¹

¹ Bei dieser Schlußfolgerung unterstellt man implizit, daß kein Rechner *mehr* leisten kann

2.2. Die Programmiersprache \mathcal{P}

Mit den Überlegungen des letzten Abschnitts können wir die Frage “Ist Aufgabe x durch einen Rechner lösbar?” mit “nein” beantworten, wenn wir nachweisen können, daß kein Lösungsverfahren für die Aufgabe x als Programm einer berechnungsvollständigen Programmiersprache implementiert werden kann.² Da wir zur Untersuchung der Unlösbarkeit von Aufgaben durch Rechner nur *eine* berechnungsvollständige Programmiersprache betrachten müssen, ist jetzt eine solche Programmiersprache auszuwählen.

In einem ersten Schritt abstrahieren wir von einer konkreten Programmiersprache, denn es ist offenbar für die weiteren Überlegungen unerheblich, ob wir einen Algorithmus in LISP, JAVA, PASCAL, C, C++, ... oder irgendeiner anderen Programmiersprache implementieren. Wir verwenden statt dessen eine einfache Programmiersprache \mathcal{P} , die für unsere Untersuchungen ausreicht. Damit abstrahieren wir von den vielfältigen und reichhaltigen Sprachkonzepten gängiger Programmiersprachen, die für die Programmierung zweifellos nützlich sind, aber unsere Untersuchungen aufwendiger machen würden. Anders gesagt, man kann in den gängigen Programmiersprachen sicher elegantere und “bessere” Programme schreiben als in der von uns verwendeten Programmiersprache \mathcal{P} . Da dieser Aspekt jedoch hier keine Rolle spielt, können wir uns auf eine einfache Programmiersprache beschränken.

Definition 2.1. (Programmiersprache \mathcal{P})

Die Programmiersprache \mathcal{P} ist wie folgt definiert:

- Der einzige Datentyp in \mathcal{P} ist die Menge \mathbb{N} der natürlichen Zahlen. Dabei sind natürliche Zahlen beliebiger Größe erlaubt.
- Ein \mathcal{P} -Programm ist eine \mathcal{P} -Prozedur, die wir in der Form

`procedure PROC(x_1, \dots, x_k) \Leftarrow PROCBODY`

angeben. Dabei sind x_1, \dots, x_k paarweise verschiedene Bezeichner für die formalen Parameter der Prozedur und PROCBODY ist der Rumpf der Prozedur.

als die Turingmaschine. In Abschnitt 3.2 wird die Gültigkeit dieser Annahme diskutiert.

² Um die *Lösbarkeit* einer Aufgabe festzustellen, reicht offenbar die Angabe eines Lösungsverfahrens als Programm *irgendeiner* – also nicht notwendigerweise berechnungsvollständigen – Programmiersprache.

- Der Prozedurrumpf *PROCBODY* einer Prozedur ist ein Block, d.h. ein Ausdruck der Form

`begin var y_1, \dots, y_n ; STA; return(y_i) end`

wobei `var y_1, \dots, y_n` eine nicht-leere Folge von Deklarationen lokaler Variabler gefolgt von einer Programmanweisung `STA` und einer (der deklarierten) lokalen Variablen `y_i` (als Argument von `return`) ist.³ Dabei müssen alle lokalen Variablen einer solchen Deklarationsfolge verschieden bezeichnet sowie verschieden von den formalen Parametern sein. Formale Parameter und lokale Variable werden auch als Programmvariable bezeichnet.

- Als Programmausdrücke `EXPR` sind erlaubt:

- natürliche Zahlen `0, 1, 2, ...`,
- formale Parameter der Prozedur,
- lokale Variable der Prozedur,
- Ausdrücke der Form `SUCC(EXPR')`, sowie
- Ausdrücke der Form `PRED(EXPR')`,

wobei `EXPR'` jeweils ein Programmausdruck ist.⁴

- Als Programmanweisungen verwenden wir

- die Leeranweisung `SKIP`,
- die Zuweisung `y := EXPR`, wobei `EXPR` ein Programmausdruck und `y` eine lokale Variable ist,
- die bedingte Anweisung `if EXPR then STA1 else STA2 end_if`, wobei `EXPR` ein Programmausdruck und `STA1, STA2` Programmanweisungen sind,
- die Hintereinanderausführung von Anweisungen `STA1;STA2`, wobei `STA1` und `STA2` Programmanweisungen sind, sowie

³ Der Ausdruck `return(y_i)` dient lediglich zur Angabe der lokalen Variablen, in der das Ergebnis einer \mathcal{P} -Prozedur abgespeichert ist. Dabei wird `return` nur aus Lesbarkeitsgründen verwendet, man könnte genauso gut eine lokale Variable ohne `return` zu Angabe des Ergebnisses erlauben.

⁴ `SUCC` steht für die Nachfolgerfunktion (engl. *successor*) und `PRED` steht für die Vorgängerfunktion (engl. *predecessor*).

- die Schleifenanweisung `while` *EXPR* `do` *STA* `end_while`, wobei *EXPR* ein Programmausdruck und *STA* eine Programmanweisung ist.

\mathcal{P} ist die Menge aller \mathcal{P} -Programme, und $\mathcal{P}[k] \subseteq \mathcal{P}$ ist die Menge aller \mathcal{P} -Programme mit k formalen Parametern. ■

Abbildung 2.1 zeigt ein \mathcal{P} -Programm, also einen *Text* aus $\mathcal{P}[2]$, der die syntaktischen Forderungen von Definition 2.1 erfüllt.

Da wir die Programmiersprache \mathcal{P} im folgenden häufig verwenden, führen wir einige zusätzliche Programmkonstrukte ein, die die Programmierung vereinfachen und \mathcal{P} -Programme lesbarer gestalten. Dabei stellen diese Erweiterungen lediglich *abkürzende Schreibweisen* dar. Wir geben jeweils an, was genau durch ein zusätzliches Programmkonstrukt abgekürzt wird, und definieren damit die Semantik, d.h. die Bedeutung, dieser neuen Ausdrücke durch Ausdrücke der Originalsprache.

Definition 2.2. (Erweiterung 1 der Programmiersprache \mathcal{P})

1. Wir erlauben Blöcke auf der rechten Seite von Zuweisungen, d.h. wir dürfen auch

```

procedure P'(x1, ..., xk) <=
begin var y1, ..., yn, y;
...
y := begin var y'1, ..., y'm; STA; return(y'j) end;
...
return(...)
end

```

schreiben, wobei *STA* eine Programmanweisung ist, in der die im Block deklarierten lokalen Variablen y'_1, \dots, y'_m sowie Programmvariable des umgebenden Blocks vorkommen dürfen – formale Parameter x_i und lokale Variable y_i von P' sind in *STA* also erlaubt.

Wir fassen solche Prozeduren als Abkürzung für

```

procedure P(x1, ..., xk) <=
begin var y1, ..., yn, y, z1, ..., zm;
...
STA[y'1/z1, ..., y'm/zm];
y := zj;
...
return(...)
end

```

```

procedure EQUAL(x1,x2) <=
begin var n,m,false,res;
  n := x1; m := x2;
  while n do
    n := PRED(n);
    if m then m := PRED(m) else false := 1 end_if
  end_while;
  if false
  then res := 0
  else if m then res := 0 else res := 1 end_if
  end_if;
  return(res)
end

```

Abbildung 2.1: Eine \mathcal{P} -Prozedur zur Berechnung von $x_1 = x_2$

auf, wobei z_1, \dots, z_m Bezeichner für lokale Variable sind, die alle verschieden von den Programmvariablen der Prozedur P' sind und $STA[y'_1/z_1, \dots, y'_m/z_m]$ aus STA entsteht, indem jedes Vorkommen der lokalen Variablen y'_j in STA durch z_j ersetzt wird. Die Umbenennungen stellen sicher, daß bei Namenskonflikten zwischen lokalen Variablen in einem Block und Programmvariablen der Prozedur (durch identische Benennungen) immer die lokalen Variablen des innersten Blocks verwendet werden.⁵

- Wir erlauben Blöcke anstelle von Programmausdrücken auch in bedingten Anweisungen und in Schleifenanweisungen, d.h. wir dürfen sowohl

```

procedure P'(x1, ..., xk) <=
begin var y1, ..., yn;
  ...
  if begin var y'1, ..., y'm; STA; return(y'j) end
  then STA1
  else STA2
  end_if;
  ...
  return(...)
end

```

⁵ In Beispielen werden wir – falls bequem – auf die Umbenennung einer lokalen Variablen y'_j aus dem Rumpf des Blocks zu z_j verzichten, falls y'_j verschieden von allen Programmvariablen der Prozedur ist.

als auch

```
procedure Q'(x1, ..., xk) <=  
begin var y1, ..., yn;  
  ...  
  while begin var y'1, ..., y'm; STA; return(y'j) end  
    do STA1 end_while;  
  ...  
  return(...)  
end
```

schreiben, wobei STA eine Programmanweisung ist, in der die im Block deklarierten lokalen Variablen y'_1, \dots, y'_m sowie Programmvariable des umgebenden Blocks vorkommen dürfen – formale Parameter x_i und lokale Variable y_j von P' bzw. Q' sind in STA also erlaubt.

Wir fassen solche Prozeduren als Abkürzung für

```
procedure P(x1, ..., xk) <=  
begin var y1, ..., yn, y;  
  ...  
  y := begin var y'1, ..., y'm; STA; return(y'j) end;  
  if y then STA1 else STA2 end_if;  
  ...  
  return(...)  
end
```

und

```
procedure Q(x1, ..., xk) <=  
begin var y1, ..., yn, y;  
  ...  
  y := begin var y'1, ..., y'm; STA; return(y'j) end;  
  while y do  
    STA1;  
    y := begin var y'1, ..., y'm; STA; return(y'j) end  
  end_while;  
  ...  
  return(...)  
end
```

auf, wobei y ein Bezeichner einer lokalen Variable ist, der verschieden von den Programmvariablen der Prozeduren P' und Q' ist.

3. Wir verwenden Hilfsprozeduren in \mathcal{P} -Programmen, um diese besser zu strukturieren und lesbarer zu gestalten. Dazu erlauben wir Prozeduraufrufe der Form $\text{PROC}(\text{EXPR}_1, \dots, \text{EXPR}_k)$ an allen Stellen in einem Programm bzw. in einer anderen Prozedur, an denen ein Programmausdruck stehen darf. Dabei sind $\text{EXPR}_1, \dots, \text{EXPR}_k$ Programmausdrücke, die keine Prozeduraufrufe enthalten, die zu (direkt oder gegenseitig) rekursiv definierten Programmen führen.⁶ Für eine \mathcal{P} -Prozedur

```
procedure PROC( $x_1, \dots, x_k$ ) <=
begin var  $y_1, \dots, y_n$ ; STA; return( $y_i$ ) end
```

wird ein Prozeduraufruf $\text{PROC}(\text{EXPR}_1, \dots, \text{EXPR}_k)$ in einer \mathcal{P} -Prozedur P als Abkürzung für den Block

```
begin var  $y_1, \dots, y_n$ ;
  STA[ $x_1/\text{EXPR}_1, \dots, x_k/\text{EXPR}_k$ ];
  return( $y_i$ )
end
```

aufgefaßt, wobei $\text{STA}[x_1/\text{EXPR}_1, \dots, x_k/\text{EXPR}_k]$ aus STA entsteht, indem jedes Vorkommen eines formalen Parameters x_i im Rumpf STA von PROC durch den korrespondierenden aktuellen Parameter EXPR_i ersetzt wird. ■

Wir erhalten ein \mathcal{P} -Programm P aus einem Programm P' der erweiterten Sprache wie folgt:

1. Wir eliminieren alle Prozeduraufaufrufe in P', so wie in Definition 2.2(3) angegeben. Dies gelingt immer, da Prozeduraufrufe, die zu (direkt oder gegenseitig) rekursiv definierten Programmen führen, ausgeschlossen sind.
2. In einem zweiten Schritt eliminieren wir alle Blöcke in bedingten und in Schleifenanweisungen, so wie in Definition 2.2(2) angegeben.
3. Nach Schritt 2. erhält man ein Programm der erweiterten Sprache, in dem keine Prozeduraufrufe vorhanden sind und Blöcke nur noch auf der rechten Seite von Zuweisungen vorkommen. Diese werden so wie in Definition 2.2(1) angegeben eliminiert. Resultat ist dann ein \mathcal{P} -Programm P, das den Forderungen von Definition 2.1 genügt.

Um die Programmierung weiter zu vereinfachen, führen wir zusätzliche Schreibweisen ein:

⁶ Mit dieser Forderung erzwingen wir, daß Prozeduraufaufrufe immer ersetzt werden können. Bei einer Prozedur der Form $\text{procedure P}(x) <= \text{begin var } y; y := P(\text{EXPR}); \text{return}(y) \text{ end}$ wäre dies nicht möglich.

```

case EXPR of
  n1: STA1
  n2: STA2
  ⋮
  nk: STAk
  other: STAother
end_case

if EXPR = n1
  then STA1
  else if EXPR = n2
    then STA2
    else ...
      ⋮
      if EXPR = nk
        then STAk
        else STAother
      end_if
    end_if
  ...
end_if

```

Abbildung 2.2: case-Anweisungen als Abkürzungen für bedingte Anweisungen

```

procedure MINUS(y1,y2) <=
begin var n,m;
  n := y1; m := y2;
  while m do
    n := PRED(n); m := PRED(m)
  end_while; return(n)
end

procedure GE(y1,y2) <=
begin var n,m,res;
  n := y1; m := y2;
  while n ^ m do
    n := PRED(n); m := PRED(m)
  end_while;
  if m = 0 then res := 1 end_if;
  return(res)
end

procedure GGT(y1,y2) <=
begin var n,m,res;
  n := y1;
  m := y2;
  while n ^ m do
    if GE(n,m)
      then n := MINUS(n,m)
      else m := MINUS(m,n)
    end_if
  end_while;
  if n
    then res := n
    else res := m
  end_if;
  return(res)
end

```

Abbildung 2.3: Ein \mathcal{P} -Programm mit Hilfsprozeduren zur Berechnung des *ggt*

Definition 2.3. (Erweiterung 2 der Programmiersprache \mathcal{P})

1. Da wir natürliche Zahlen in den bedingten Anweisungen und in den Schleifenanweisungen wie Wahrheitswerte auffassen, ist es praktisch, logische Operatoren auch für natürliche Zahlen zu erlauben. Wir verwenden daher für Programmausdrücke EXPR1 und EXPR2
 - “ $\neg\text{EXPR1}$ ” als Abkürzung für “begin var y; if EXPR1 then y := 0 else y := 1 end_if; return(y) end”,
 - “ $\text{EXPR1} \vee \text{EXPR2}$ ” als Abkürzung für “begin var y; if EXPR1 then y := 1 else y := EXPR2 end_if; return(y) end”, und
 - “ $\text{EXPR1} \wedge \text{EXPR2}$ ” als Abkürzung für “begin var y; if EXPR1 then y := EXPR2 else y := 0 end_if; return(y) end”.
2. Wir erlauben Programmausdrücke der Form $\text{EXPR}' = \text{EXPR}''$, die wir als Abkürzung für den Aufruf $\text{EQUAL}(\text{EXPR}', \text{EXPR}'')$ einer Prozedur EQUAL , definiert wie in Abbildung 2.1, auffassen.
3. Wir erlauben einseitig bedingte Anweisungen und schreiben “if EXPR then STA end_if” als Abkürzung für “if EXPR then STA else SKIP end_if”.
4. Wie erlauben *case*-Anweisungen, d.h. Fallunterscheidungen, die wir als Abkürzung für eine bedingte Anweisung auffassen, siehe Abbildung 2.2. Dabei ist EXPR ein Programmausdruck, n_1, \dots, n_k mit $k \geq 1$ sind natürliche Zahlen und $\text{STA}_1, \dots, \text{STA}_k, \text{STA}_{\text{other}}$ sind Programmanweisungen.
5. Wir erlauben eine zweite Form von Schleifenanweisungen und schreiben “repeat STA until EXPR ” als Abkürzung für “ STA ; while $\neg\text{EXPR}$ do STA end_while”. ■

Mit diesen Erweiterungen unserer Programmiersprache läßt sich jetzt beispielsweise ein GGT-Programm wie in Abbildung 2.3 angeben. Aus diesem Programm entsteht das \mathcal{P} -Programm aus Abbildung 2.4 durch Elimination der Hilfsprozeduren und der logischen Operatoren, so wie in Definitionen 2.2 und 2.3 angegeben.

Um die Lesbarkeit von \mathcal{P} -Programmen weiter zu erhöhen, verwenden wir offensichtliche abkürzende Schreibweisen, also etwa $x \neq y$ anstatt $\neg x = y$. Im folgenden werden wir die Programmiersprache \mathcal{P} sowohl in ihrer ursprünglichen Definition als auch in ihren Erweiterungen verwenden, je nachdem, wie es für den jeweiligen Zweck am bequemsten ist. Dabei dürfen wir jedoch bei Untersuchungen über \mathcal{P} -Programme immer davon ausgehen, daß ein \mathcal{P} -Programm in der ursprünglichen

```

procedure GGT(y1,y2) <=
begin var n,m,res,loop;
  n := y1; m := y2;
  loop := begin var r;
            if n then r := m else r := n end_if;
            return(r)
          end;
  while loop do
    if begin var x,y,res,loop; x := n; y := m; res := 0;
        loop := begin var r;
                  if x then r := y else r := x end_if;
                  return(r)
                end;
        while loop do
          x := PRED(x); y := PRED(y);
          if x then loop := y else loop := x end_if
        end_while;
        if y then SKIP else res := 1 end_if;
        return(res)
      end
    then n := begin var x,y; x := n; y := m;
              while y do
                x := PRED(x); y := PRED(y)
              end_while;
              return(x)
            end; loop := n
    else m := begin var x,y; x := m; y := n;
              while y do
                x := PRED(x); y := PRED(y)
              end_while;
              return(x)
            end; loop := m
    end_if
  end_while;
  if n then res := n else res := m end_if;
  return(res)
end

```

Abbildung 2.4: Ein \mathcal{P} -Programm zur Berechnung des *ggt* von y_1 und y_2

Form nach Definition 2.1 gegeben ist, denn die Programmkonstrukte der erweiterten Sprache können immer – wie in Definitionen 2.2 und 2.3 angegeben – eliminiert werden. Dort, wo es erheblich ist, ob ein \mathcal{P} -Programm in der ursprünglichen oder in der erweiterten Form gegeben ist, werden wir explizit darauf hinweisen.

Da rekursiv definierte Prozeduren verboten sind, dürfen wir insbesondere davon ausgehen, daß jedes Programm aus genau einer Prozedur besteht, denn Prozeduraufrufe können immer durch den instantiierten Rumpf der aufgerufenen Prozedur ersetzt werden. Deshalb verwenden wir im folgenden die Begriffe *Programm* und *Prozedur* auch als Synonyme. Beispielsweise definiert die Prozedur **MINUS** aus Abbildung 2.3 ein Programm, und wir sagen dann z.B. auch, daß das *Programm* **MINUS** aufgerufen wird. Andererseits können wir auch sagen, daß die *Prozedur* **GGT** aufgerufen wird, wobei wir dann stillschweigend voraussetzen, daß die Prozeduren, die bei Definition von **GGT** verwendet wurden, also **MINUS** und **GE**, zusammen mit **GGT** gegeben sind.

2.3. Semantik von \mathcal{P} -Programmen

Die Programme der Programmiersprache \mathcal{P} sind zunächst einmal nur syntaktische Objekte, also Worte über einem bestimmten Alphabet. Da wir mit Programmen Algorithmen beschreiben wollen, müssen wir jetzt definieren, was es bedeuten soll, wenn ein \mathcal{P} -Programm auf einem *Rechner abgearbeitet* wird. Wir müssen also die *Semantik* von \mathcal{P} , d.h. die *Bedeutung* der Ausdrücke und Anweisungen der Programmiersprache \mathcal{P} definieren. Zwar ist in den meisten Fällen intuitiv klar, was die Abarbeitung eines \mathcal{P} -Programms bewirkt. Um aber Mißverständnisse und Fehlinterpretationen zu vermeiden, muß die Semantik von \mathcal{P} -Programmen präzise angegeben werden, etwa um zu klären, was das Ergebnis von **PRED**(0) und was die Bedeutung der Leeranweisung **SKIP** ist, was geschieht, wenn auf eine nicht-initialisierte lokale Variable zugegriffen wird, u.s.w. Die Semantik muß aber vor allem deshalb mathematisch präzise definiert werden, damit wir Aussagen über die Berechnungen, die bei Ausführung von \mathcal{P} -Programmen stattfinden, *formal beweisen* können.

Wir definieren jetzt eine *operationale* Semantik von \mathcal{P} -Programmen, indem wir angeben, wie genau \mathcal{P} -Programme abgearbeitet werden sollen.⁷ Dazu benötigen wir zunächst einen *Speicher* beliebiger Größe. Diesen Speicher modellieren wir durch eine Teilmenge M des kartesischen Produkts $\mathbb{N} \times \mathbb{N}$, wobei $\langle i, n \rangle \in M$ be-

⁷ Man kann die Semantik von Programmen auch nicht-*operational* angeben und diese etwa *axiomatisch* oder *denotational* definieren. Diese verschiedenen Konzepte zur Semantikdefinition besitzen alle Vor- und Nachteile; für unsere Untersuchungen ist die operationale Form zweckmäßig.

deutet, daß in der *Speicherzelle* von M mit *Adresse* i der *Wert* n abgespeichert ist. Den Programmvariablen \mathbf{z} ordnen wir (beginnend mit 0) fortlaufende Adressen $i_{\mathbf{z}}$ aus \mathbb{N} zu, und $M(i_{\mathbf{z}})$ bezeichnet dann den Wert, der in M für eine Programmvariable \mathbf{z} abgespeichert ist.

Definition 2.4. (Speichermodell)

Für die Funktion $cont: 2^{\mathbb{N} \times \mathbb{N}} \times \mathbb{N} \rightarrow \mathbb{N}$ definiert durch

$$cont(M, i) := \begin{cases} n & , \text{ falls } \langle i, n \rangle \in M \text{ und } n < m \\ & \text{für alle } m \in \mathbb{N} \text{ mit } \langle i, m \rangle \in M \\ 0 & , \text{ falls } \langle i, m \rangle \notin M \text{ für alle } m \in \mathbb{N} \end{cases}$$

ist $M(i)$ definiert als $cont(M, i)$.⁸ M^{init} bezeichnet den initialen Speicher mit $M^{init}(i) = 0$ für jedes $i \in \mathbb{N}$.

Durch Ersetzen des Speicherinhalts an der Adresse j durch einen Wert n erhält man den Speicher $M[j \leftarrow n]$, für den $M[j \leftarrow n](i) = n$, falls $i = j$, und andernfalls $M[j \leftarrow n](i) = M(i)$ gilt.

Für eine Programmvariable \mathbf{z} mit Adresse $i_{\mathbf{z}}$ steht $M(\mathbf{z})$ als Abkürzung für $M(i_{\mathbf{z}})$ und $M[\mathbf{z} \leftarrow n]$ als Abkürzung für $M[i_{\mathbf{z}} \leftarrow n]$. ■

Bemerkung 2.5. Zwar ist der Adressraum unseres Speichers endlich (denn \mathcal{P} -Programme sind endliche Texte, und damit gibt es auch nur endliche viele Programmvariable in einem \mathcal{P} -Programm), nicht jedoch der Speicher insgesamt. Da jede natürliche Zahl im Speicher abgelegt werden kann, ist die Größe des Speichers unbegrenzt. Dies wird sofort klar, wenn wir die Programmiersprache \mathcal{P} auf einem konkreten Rechner implementieren, denn dann muß eine Repräsentation für natürliche Zahlen gewählt werden. Stellt man beispielsweise natürliche Zahlen durch Bitworte dar, so sind diese Bitworte zwar immer endlich, sie können jedoch beliebig lang sein (siehe auch Abschnitt 12.2). Damit existiert keine Größenbeschränkung bzgl. des verwendeten realen Speichers. Durch unsere Modellierung als Teilmenge von $\mathbb{N} \times \mathbb{N}$ scheint dagegen ein endlicher Speicherbedarf bei Abarbeitung eines Programms auszureichen. Für unsere Untersuchungen ist dies unerheblich. In der Komplexitätstheorie, in der auch der Speicherbedarf bei Lösung von Problemen untersucht wird, muß dagegen ein Speichermodell gewählt werden, das quantitative Aspekte explizit macht. ■

⁸ Da mit M nur eine *Relation* definiert wird, ist beispielsweise $\langle 2, 7 \rangle \in M$ und $\langle 2, 13 \rangle \in M$ nicht von vornherein ausgeschlossen. Da das Auslesen des Speichers M aber offenbar durch eine *Funktion* (hier: $cont$) modelliert werden muß, ist für solche Fälle eine (willkürliche) Auswahl erforderlich (im Beispiel erhält man $M(2) = 7$). Unsere Verwendung des Speichers M wird jedoch sicherstellen, daß solch willkürliche Auswahl nie erforderlich ist.

Die *Auswertung* von Programmausdrücken und die *Ausführung* von Programm-
anweisungen definieren wir jetzt durch die Funktionen

$$value : 2^{\mathbb{N} \times \mathbb{N}} \times expressions_P \rightarrow \mathbb{N}$$

und

$$eval : 2^{\mathbb{N} \times \mathbb{N}} \times statements_P \mapsto 2^{\mathbb{N} \times \mathbb{N}} .$$

Dabei bezeichnet $expressions_P$ die Menge aller Programmausdrücke und $statements_P$ die Menge aller Programmanweisungen in einem \mathcal{P} -Programm P . Für eine gegebene Speicherbelegung M_P und einen Programmausdruck $EXPR$ gibt $value(M_P, EXPR) \in \mathbb{N}$ den *Wert* von $EXPR$ bezüglich der Speicherbelegung M_P an. Durch Ausführung einer Programmanweisung STA wird aus einer gegebenen Speicherbelegung M_P eine *neue Speicherbelegung* gebildet, d.h. das Ergebnis der Ausführung von STA unter der Speicherbelegung M_P ist die Speicherbelegung $eval(M_P, STA) \subseteq \mathbb{N} \times \mathbb{N}$.

Definition 2.6. (Auswertungsfunktion *value*)

Für ein \mathcal{P} -Programm P definieren wir die Auswertung von Programmausdrücken unter einer endlichen Speicherbelegung $M_P \subseteq \mathbb{N} \times \mathbb{N}$ mittels der Auswertungsfunktion $value : 2^{\mathbb{N} \times \mathbb{N}} \times expressions_P \rightarrow \mathbb{N}$ durch:

$$(v1) \quad value(M_P, n) := n, \text{ falls } n \in \mathbb{N},$$

$$(v2) \quad value(M_P, z) := M_P(z), \text{ falls } z \text{ eine Programmvariable ist,}$$

$$(v3) \quad value(M_P, SUCC(EXPR)) := 1 + value(M_P, EXPR),$$

$$(v4) \quad value(M_P, PRED(EXPR)) := \begin{cases} 0, & \text{falls } value(M_P, EXPR) = 0 \\ value(M_P, EXPR) - 1, & \text{andernfalls.} \end{cases} \quad \blacksquare$$

Definition 2.7. (Ausführungsfunktion *eval*)

Für ein \mathcal{P} -Programm P definieren wir die Ausführung von Programmanweisungen unter einer endlichen Speicherbelegung $M_P \subseteq \mathbb{N} \times \mathbb{N}$ mittels der Ausführungsfunktion $eval : 2^{\mathbb{N} \times \mathbb{N}} \times statements_P \mapsto 2^{\mathbb{N} \times \mathbb{N}}$ durch:

$$(e1) \quad eval(M_P, SKIP) := M_P,$$

$$(e2) \quad eval(M_P, \mathbf{x} := EXPR) := M_P[\mathbf{x} \leftarrow value(M_P, EXPR)],$$

$$(e3) \quad \text{eval}(M_P, \begin{array}{l} \text{if } \text{EXPR} \\ \text{then } \text{STA1} \\ \text{else } \text{STA2} \\ \text{end_if} \end{array}) := \begin{cases} \text{eval}(M_P, \text{STA1}), & \text{falls } \text{value}(M_P, \text{EXPR}) > 0 \\ \text{eval}(M_P, \text{STA2}), & \text{falls } \text{value}(M_P, \text{EXPR}) = 0, \end{cases}$$

$$(e4) \quad \text{eval}(M_P, \text{STA1}; \text{STA2}) := \text{eval}(\text{eval}(M_P, \text{STA1}), \text{STA2}),$$

$$(e5) \quad \text{eval}(M_P, \begin{array}{l} \text{while } \text{EXPR} \\ \text{do } \text{STA} \\ \text{end_while} \end{array}) := \begin{cases} M_P, & \text{falls } \text{value}(M_P, \text{EXPR}) = 0, \text{ und sonst} \\ \text{eval}(\text{eval}(M_P, \text{STA}), \begin{array}{l} \text{while } \text{EXPR} \\ \text{do } \text{STA} \\ \text{end_while} \end{array}) . \quad \blacksquare \end{cases}$$

Die Zuweisung ist also (wenig überraschend) die einzige Programmanweisung, mit der der Speicher verändert wird. Die Ausführung der Leeranweisung **SKIP** hat keine Wirkung, und bei Ausführung der bedingten Anweisung wird lediglich zwischen zwei Anweisungsalternativen ausgewählt. Bei der Hintereinanderausführung **STA1;STA2** von Programmanweisungen wird zunächst **STA1** unter der Speicherbelegung M_P ausgeführt, und anschließend die Programmanweisung **STA2** unter der nach Ausführung von **STA1** gegebenen Speicherbelegung. Die Ausführung der Schleifenanweisung hat keine Wirkung, falls die Schleifenbedingung **EXPR** nicht erfüllt ist. Anderfalls wird der Schleifenrumpf **STA** unter der gegebenen Speicherbelegung einmal ausgeführt, und daran anschließend wieder die gesamte Schleifenanweisung. Damit wird der Schleifenrumpf solange ausgeführt, bis eine Speicherbelegung resultiert, unter der die Schleifenbedingung **EXPR** nicht mehr erfüllt ist.

Offensichtlich bezeichnet *value* eine totale Funktion, d.h. die Auswertung von Programmausdrücken gelingt immer. Dagegen ist die Ausführungsfunktion *eval* im allgemeinen eine *nicht-totale* Funktion, da wir auch *nicht-terminierende* Programme definieren können, etwa durch

```

procedure CYCLEk(x1, ..., xk) <=
begin var y;
  while 1 do SKIP end_while;
  return(y)
end .

```

(2.1)

Mittels *value* und *eval* können wir jetzt die Semantik eines \mathcal{P} -Programms P mathematisch präzise angeben, und zwar als eine *Funktion*, die die *Eingabewerte* von P in das *Ergebnis* der *Abarbeitung* von P abbildet:

Definition 2.8. (Semantik von \mathcal{P} -Programmen)

Sei

```

procedure P( $\mathbf{x}_1, \dots, \mathbf{x}_k$ ) <=
begin var  $y_1, \dots, y_n$ ; STA; return( $y_j$ ) end

```

ein \mathcal{P} -Programm, sei $(n_1, \dots, n_k) \in \mathbb{N}^k$, und sei $M_P^{(n_1, \dots, n_k)}$ eine Teilmenge von $\mathbb{N} \times \mathbb{N}$ mit ⁹

$$\begin{aligned} M_P^{(n_1, \dots, n_k)}(\mathbf{x}_i) &= n_i && \text{für alle } i \in \{1, \dots, k\} \text{ und} \\ M_P^{(n_1, \dots, n_k)}(\mathbf{y}_i) &= 0 && \text{für alle } i \in \{1, \dots, n\} . \end{aligned} \quad (2.2)$$

Dann ist die durch P berechnete Funktion $\llbracket P \rrbracket : \mathbb{N}^k \mapsto \mathbb{N}$ definiert durch

$$\llbracket P \rrbracket(n_1, \dots, n_k) := \text{value}(\text{eval}(M_P^{(n_1, \dots, n_k)}, \text{STA}), \mathbf{y}_j) .$$

Die Semantik $\llbracket P(t_1, \dots, t_k) \rrbracket$ eines Programmaufrufs (bzw. Prozeduraufrufs) $P(t_1, \dots, t_k)$ mit variablenfreien Programmausdrücken t_1, \dots, t_k als aktuelle Parameter definieren wir als $\llbracket P \rrbracket(n_1, \dots, n_k)$ mit $n_i = \text{value}(M_P^{\text{init}}, t_i)$ für alle $i \in \{1, \dots, k\}$. ■

Die *Semantik*, d.h. die *Bedeutung*, eines Programms P ist also die durch P berechnete *Funktion* $\llbracket P \rrbracket$.¹⁰ Für diese Funktion gilt $\llbracket P \rrbracket(n_1, \dots, n_k) = n$ genau dann, wenn P gestartet mit Eingabe n_1, \dots, n_k als Ergebnis n liefert. Anders gesagt, bei Eingabe von $P(t_1, \dots, t_k)$ auf der Tastatur eines Rechners wird $\llbracket P \rrbracket(n_1, \dots, n_k)$ (mit $n_i = \text{value}(M_P^{\text{init}}, t_i)$) als Ergebnis angezeigt, vorausgesetzt natürlich, die Abarbeitung des Programms terminiert. Beispielsweise gilt $\llbracket \text{GGT} \rrbracket(n_1, n_2) = \text{ggt}(n_1, n_2)$ für das Programm **GGT** aus Abbildung 2.4 (und damit auch für das Programm **GGT** aus Abbildung 2.3).

Die Funktion $\llbracket P \rrbracket$ ist genau dann *total*, wenn P für *jede* Eingabe *terminiert*. Dies ist z.B. für das Programm **GGT** der Fall, und somit gilt $\llbracket \text{GGT} \rrbracket : \mathbb{N}^2 \rightarrow \mathbb{N}$. Dagegen terminiert das Programm **CYCLE**₁ $\in \mathcal{P}[1]$ aus (2.1) für keine Eingabe, und folglich gilt $\llbracket \text{CYCLE}_1 \rrbracket = \omega_{\mathbb{N} \rightarrow \mathbb{N}}$.¹¹

⁹ Leere Parameterlisten, also $k = 0$, sind erlaubt.

¹⁰ Da wir die Semantik von \mathcal{P} -Programmen mittels der Funktionen *value* und *eval algorithmisch* definiert haben, haben wir für \mathcal{P} -Programme eine *operationale* Semantik angegeben.

¹¹ $\omega_{\mathbb{N} \rightarrow \mathbb{N}}$ ist die überall undefinierte Funktion von \mathbb{N} nach \mathbb{N} , s. Kapitel 13.

3. BERECHENBARE FUNKTIONEN

3.1. \mathcal{P} -berechenbare Funktionen

Mit der Definition der Semantik von \mathcal{P} -Programmen können wir jetzt die Aussage “Aufgabe x ist lösbar durch einen Rechner” präziser formulieren. Wir definieren eine Funktion $\phi : \mathbb{N}^k \mapsto \mathbb{N}$ und fragen: “Gibt es ein \mathcal{P} -Programm **PROG**, so daß $\phi = \llbracket \text{PROG} \rrbracket$ gilt?”. Beispielsweise formulieren wir die Aufgabe, die n -te Primzahl anzugeben, wie folgt: Sei $\text{prim} : \mathbb{N} \rightarrow \mathbb{N}$ definiert als $\text{prim}(n) = n$ -te Primzahl, also $\text{prim}(0) = 1$, $\text{prim}(1) = 2$, $\text{prim}(2) = 3$, $\text{prim}(3) = 5$, $\text{prim}(4) = 7$ u.s.w.¹ Die Aufgabe “ n -te Primzahl angeben” ist genau dann durch einen Rechner lösbar, wenn $\text{prim} = \llbracket \text{PRIM} \rrbracket$ für ein \mathcal{P} -Programm **PRIM** gilt. Allgemein fragen wir also danach, ob eine Funktion ϕ \mathcal{P} -berechenbar ist.²

Definition 3.1. (\mathcal{P} -berechenbare Funktionen)

Eine Funktion $\phi : \mathbb{N}^k \mapsto \mathbb{N}$ ist \mathcal{P} -berechenbar genau dann, wenn $\phi = \llbracket \text{PROG} \rrbracket$ für ein $\text{PROG} \in \mathcal{P}[k]$ gilt. $\llbracket \mathcal{P} \rrbracket$ mit $\llbracket \mathcal{P} \rrbracket := \{ \llbracket \text{PROG} \rrbracket \mid \text{PROG} \in \mathcal{P} \}$ ist die Menge aller \mathcal{P} -berechenbaren Funktionen. ■

Die Aufgabe “ n -te Primzahl angeben” ist natürlich durch einen Rechner lösbar, da man ein Programm $\text{PRIM} \in \mathcal{P}[1]$ mit $\text{prim} = \llbracket \text{PRIM} \rrbracket$ leicht angeben kann. Ebenso sind alle überall undefinierten arithmetischen Funktionen \mathcal{P} -berechenbar:

Satz 3.2. $\omega_{\mathbb{N}^k \mapsto \mathbb{N}}$ ist \mathcal{P} -berechenbar.

Beweis. Für $\text{CYCLE}_k \in \mathcal{P}[k]$, gegeben wie (2.1), gilt $\llbracket \text{CYCLE}_k \rrbracket(n_1, \dots, n_k) = \perp^3$ für alle $(n_1, \dots, n_k) \in \mathbb{N}^k$, folglich $\omega_{\mathbb{N}^k \mapsto \mathbb{N}} = \llbracket \text{CYCLE}_k \rrbracket$, und damit ist $\omega_{\mathbb{N}^k \mapsto \mathbb{N}}$ \mathcal{P} -berechenbar. ■

¹ Für unsere Zwecke ist es praktisch, auch 1 zu verwenden. Daher definieren wir $\text{prim}(0) = 1$.

² In der englischsprachigen Literatur wird der Begriff “recursive” für “berechenbar” verwendet (“computable” ist dagegen seltener). Es gibt also sowohl “recursive procedures” (dt. “rekursive Prozeduren”) als auch “recursive functions” (dt. “berechenbare Funktionen”). Genaugenommen müßte man von “recursively defined procedures” bzw. “rekursiv definierten Prozeduren” sprechen. Da dies aber oft unterlassen wird, kann es zu Mißverständnissen kommen.

³ \perp steht für “undefiniert”, s. Kapitel 13.

Die Komposition \mathcal{P} -berechenbarer Funktionen liefert wieder eine \mathcal{P} -berechenbare Funktion:

Satz 3.3. Seien $\phi : \mathbb{N}^k \mapsto \mathbb{N}$ und $\psi : \mathbb{N} \mapsto \mathbb{N}$ \mathcal{P} -berechenbare Funktionen. Dann ist auch $\psi \circ \phi : \mathbb{N}^k \mapsto \mathbb{N}$ \mathcal{P} -berechenbar.

Beweis. Seien $\text{PSI} \in \mathcal{P}[1]$ und $\text{PHI} \in \mathcal{P}[k]$ mit $\psi = \llbracket \text{PSI} \rrbracket$ und $\phi = \llbracket \text{PHI} \rrbracket$ gegeben durch

<pre> procedure PSI(x) <= begin var y1, ..., yn; STAψ; return(yψ) end </pre>	und	<pre> procedure PHI(x1, ..., xk) <= begin var y1, ..., ym; STAϕ; return(yϕ) end . </pre>
---	-----	---

Für das \mathcal{P} -Programm $\text{COMPOSE} \in \mathcal{P}[k]$, gegeben durch

```

procedure COMPOSE(x1, ..., xk) <=
begin var y1, ..., yn;
  STA $\psi$ [x/begin var y1, ..., ym; STA $\phi$ ; return(y $\phi$ ) end];
  return(y $\psi$ )
end

```

gilt dann $\llbracket \text{COMPOSE} \rrbracket(n_1, \dots, n_k) = \psi(\phi(n_1, \dots, n_k))$ für alle $(n_1, \dots, n_k) \in \mathbb{N}^k$, und somit ist $\psi \circ \phi$ \mathcal{P} -berechenbar. ■

3.2. Die Churchsche These

Der bislang verwendete Berechenbarkeitsbegriff stützt sich auf die Programmiersprache \mathcal{P} . Wir lösen uns von dieser Einschränkung und definieren allgemeiner:

Eine arithmetische Funktion ϕ ist genau dann *intuitiv berechenbar*, wenn ϕ durch *irgendein algorithmisches Verfahren* berechnet wird.

Offenbar ist jede \mathcal{P} -berechenbare Funktion auch *intuitiv* berechenbar, denn es gilt dann $\llbracket \text{PROG} \rrbracket = \phi$ für ein \mathcal{P} -Programm PROG , und mit PROG wird offenbar ein algorithmisches Verfahren zur Berechnung von ϕ angegeben. Gilt jedoch $\phi \neq \llbracket \text{PROG} \rrbracket$ für jedes \mathcal{P} -Programm PROG , so können wir keine Aussage darüber treffen, ob ϕ intuitiv berechenbar ist: Entweder ist ϕ nicht intuitiv berechenbar, und

dann kann es natürlich auch kein \mathcal{P} -Programm PROG mit $\llbracket \text{PROG} \rrbracket = \phi$ geben, oder aber ϕ ist nicht \mathcal{P} -berechenbar, da die Programmiersprache \mathcal{P} ungeeignet ist, um einen Algorithmus für ϕ anzugeben. Anders gesagt, mit dem Nachweis, daß eine Funktion ϕ nicht \mathcal{P} -berechenbar ist, wird zunächst nur eine Aussage über die Programmiersprache \mathcal{P} getroffen, nicht jedoch – wie eigentlich erwünscht – über die Funktion ϕ . Dies gilt nicht nur für die Programmiersprache \mathcal{P} , sondern für jeden Formalismus zur Beschreibung von Algorithmen. Man begegnet diesem Dilemma wie folgt:

Zu Beginn des letzten Jahrhunderts wurden verschiedene Berechenbarkeitsbegriffe – also Formalismen zur Beschreibung von Algorithmen – definiert, darunter

- der λ -Kalkül von *A. Church*,
- die *Turingmaschine* von *A. Turing* und
- die *μ -rekursiven Funktionen* von *S. C. Kleene*.⁴

Man konnte zeigen, daß alle diese Formalismen *berechnungsäquivalent* sind, d.h. jede Funktion, die mit einem der Formalismen berechnet werden kann, kann auch mit den jeweils anderen beiden berechnet werden. Da sich diese Formalismen in ihren Definitionen stark unterscheiden, jedoch gleichmächtig sind, liegt es nahe, von einem intuitiven Berechenbarkeitsbegriff auszugehen, der sich nicht auf einen bestimmten Berechnungsformalismus (also etwa eine bestimmte Programmiersprache) stützt. Anders gesagt, man geht davon aus, daß jede *intuitiv* berechenbare Funktion auch durch den λ -Kalkül (die Turingmaschine oder die μ -rekursiven Funktionen) berechnet wird. Diese Vermutung wird ausgedrückt durch die

Churchsche These

Jede *intuitiv berechenbare* Funktion ist durch den λ -Kalkül (die Turingmaschine, die μ -rekursiven Funktionen) berechenbar.

Die Churchsche These ist ein *Postulat*, d.h. kein Satz, den man beweisen kann. Allenfalls könnte man die Churchsche These *widerlegen*, indem man ein Verfahren

⁴ Diese Aufzählung ist nicht erschöpfend. Es gibt noch weitere Berechnungsformalismen, genau genommen beliebig viele, die das gleiche leisten wie die hier genannten.

angibt, von dem übereinstimmend behauptet werden kann, daß es ein *algorithmisches* Verfahren ist, und dann nachweist, daß dieses Verfahren *nicht* durch einen der zuvor genannten Berechnungsformalisten implementiert werden kann.

Bei der Churchschen These handelt es sich damit um eine *empirische* Aussage, mit der von Beobachtungen auf eine allgemeine Gesetzmäßigkeit geschlossen wird. Dies ist auch in anderen Bereichen der Wissenschaft nicht unüblich. Beispielsweise ergibt sich die Unmöglichkeit eines *perpetuum mobile*, also eines Geräts, das (physikalische) Arbeit verrichtet ohne Energie aufzunehmen, aus dem Energieerhaltungssatz der Physik, also einem nicht-beweisbaren Naturgesetz bzw. Postulat, von dessen Wahrheit man aufgrund von Beobachtungen solange ausgeht, bis das Gegenteil nachgewiesen ist.

Mit der Churchschen These emanzipiert man sich von einem konkreten Berechenbarkeitsbegriff: Unter der Voraussetzung dieser These darf man eine Funktion ϕ als *nicht berechenbar* bezeichnen, wenn man gezeigt hat, daß diese Funktion nicht durch den λ -Kalkül (bzw. die Turingmaschine oder die μ -rekursiven Funktionen) berechnet wird. Man kann dabei auch die nicht-Berechenbarkeit durch irgendeinen anderen Formalismus verwenden, vorausgesetzt man hat zuvor gezeigt, daß dieser Formalismus *berechnungsvollständig*, d.h. *berechnungsäquivalent* mit dem λ -Kalkül (bzw. der Turingmaschine oder den μ -rekursiven Funktionen) ist.

In unserem Fall ist also nachzuweisen, daß die Programmiersprache \mathcal{P} berechnungsvollständig ist, siehe Kapitel 11 und 12.⁵ Im Vorgriff auf diesen Beweis dürfen wir – unter Annahme der Churchschen These – im folgenden davon ausgehen, daß jede nicht \mathcal{P} -berechenbare Funktion auch nicht intuitiv berechenbar ist.

3.3. Nicht-Konstruktivität und Konstruktivität

Um zu beweisen, daß eine gegebene Funktion ϕ \mathcal{P} -berechenbar ist, müssen wir die Existenz eines \mathcal{P} -Programms `PROG` mit $\phi = \llbracket \text{PROG} \rrbracket$ nachweisen. Dies kann beispielsweise dadurch geschehen, daß wir ein *konkretes* Programm angeben, etwa ein \mathcal{P} -Programm zur Berechnung der n -ten Primzahl, um nachzuweisen, daß die Funktion, die jedem $n \in \mathbb{N}$ die n -te Primzahl zuordnet, \mathcal{P} -berechenbar ist.

Die Angabe eines konkreten \mathcal{P} -Programms ist zwar *hinreichend* zum Nachweis der \mathcal{P} -Berechenbarkeit einer Funktion, nicht aber *notwendig*. Anders gesagt, man kann die Existenz eines \mathcal{P} -Programms auch nachweisen, *ohne* dieses Programm *konkret anzugeben*. Dies ist in der Mathematik nicht unüblich, denn ein Existenzbeweis erfordert nicht unbedingt, daß das existierende Objekt auch aus

⁵ Präzise formuliert ist bei Verwendung von \mathcal{P} -Programmen mit “Berechnungsformalismus” die *Abarbeitung der Aufrufe* von \mathcal{P} -Programmen gemäß Definition 2.8 gemeint.

dem Beweis rekonstruiert werden kann. In diesem Fall spricht man von einem *unkonstruktiven* Beweis. Dazu zwei einfache Beispiele:

Angenommen, wir wollen die Aussage “ $\forall i \in \mathbb{N} \exists j \in \mathbb{N}. j > i$ ” beweisen. Der Beweis ist offensichtlich – man setzt einfach $j := i + 1$. Dieser Beweis ist *konstruktiv*, denn aus dem Beweis können wir eine “Lösung” für j , nämlich $i + 1$, sofort ablesen.⁶

Als Beispiel für einen *unkonstruktiven* Beweis betrachten wir die Aussage “ $\exists q, r \in \overline{\mathbb{Q}}. q^r \in \mathbb{Q}$ ”, wobei \mathbb{Q} die Menge der rationalen Zahlen und $\overline{\mathbb{Q}}$ die Menge der irrationalen Zahlen bezeichnet. Zum Beweis unterscheiden wir folgende Fälle:

1. *Fall* $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$: Dann gilt die Aussage für $q = r = \sqrt{2}$.
2. *Fall* $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$: Dann gilt $\sqrt{2}^{\sqrt{2}} \in \overline{\mathbb{Q}}$ und die Aussage gilt für $q = \sqrt{2}^{\sqrt{2}}$ und $r = \sqrt{2}$, denn $q^r = \sqrt{2}^{\sqrt{2}\sqrt{2}} = \sqrt{2}^2 = 2$.

Dieser Beweis ist *unkonstruktiv*, denn wir können eine “Lösung” für q und r nicht aus dem Beweis ermitteln.

Genauso wie in diesem Beispiel können wir beweisen, daß eine Funktion \mathcal{P} -berechenbar ist, ohne ein \mathcal{P} -Programm, das diese Funktion berechnet, *konkret* anzugeben.

Betrachten wir als Beispiel die Funktion $\sigma : \mathbb{N} \rightarrow \mathbb{N}$ mit

$$\sigma(n) := \begin{cases} 1 & \text{falls die Dezimalbruchentwicklung von } \pi \text{ mindestens} \\ & \text{\textit{n} aufeinanderfolgende Ziffern 1 enthält} \\ 0 & \text{, andernfalls .} \end{cases}$$

Wir zeigen, daß σ \mathcal{P} -berechenbar ist: Angenommen, in der Dezimalbruchentwicklung von π kommen höchstens k_0 aufeinanderfolgende Ziffern 1 vor. Dann gilt $\sigma = \sigma_1$ mit

$$\sigma_1(n) := \begin{cases} 1 & \text{, falls } n \leq k_0 \\ 0 & \text{, falls } n > k_0 . \end{cases} \quad (3.1)$$

Andernfalls definieren wir $\sigma_2(n) := 1$ und erhalten $\sigma = \sigma_2$. Es ist offensichtlich, daß sowohl σ_1 als auch σ_2 \mathcal{P} -berechenbar sind, etwa durch \mathcal{P} -Programme **PROG1**

⁶ Nicht-triviale Beispiele für konstruktive Beweise findet man z.B. in der Theorie der Formalen Sprachen. Beispielsweise läßt sich aus dem Beweis des Satzes “Für jeden nicht-deterministischen endlichen Automaten *NFA* existiert ein deterministischer endlicher Automat *DFA*, so daß beide Automaten die gleiche Sprache akzeptieren” unmittelbar ein algorithmisches Verfahren ablesen, das aus jedem *NFA* einen äquivalenten *DFA* synthetisiert.

und **PROG2**. Damit ist auch σ \mathcal{P} -berechenbar. Allerdings haben wir auch hier einen *unkonstruktiven* Beweis geführt – die \mathcal{P} -Programme **PROG1** und **PROG2** kann man leicht angeben, nur ist aus dem Beweis nicht ersichtlich, ob wir **PROG1** oder **PROG2** verwenden müssen, um σ zu berechnen.

Generell gilt, daß eine Funktion mit einer Fallunterscheidung, die nicht abhängig von den Parametern der Funktion ist, auch dann berechenbar sein kann, wenn nicht algorithmisch festgestellt werden kann, welcher der Fälle zutrifft.

Beispielsweise gilt für die Funktionen $\phi_1, \phi_2, \phi, \psi : \mathbb{N} \mapsto \mathbb{N}$ mit

$$\phi(n) := \begin{cases} \phi_1(n) & , \text{ falls } \forall m. \psi(m) \neq \perp \\ \phi_2(n) & , \text{ falls } \exists m. \psi(m) = \perp \end{cases}$$

daß ϕ berechenbar ist, falls ϕ_1 und ϕ_2 berechenbar sind: Entweder ist ψ *total*, und dann gilt $\phi(n) = \phi_1(n)$, oder aber ψ ist *nicht total*, und damit gilt dann $\phi(n) = \phi_2(n)$. In Abschnitt 10.1 werden wir zeigen, daß man nicht algorithmisch feststellen kann, ob eine Funktion (wie ψ) total ist oder nicht. Damit kann auch nicht algorithmisch festgestellt werden, ob nun $\phi(n) = \phi_1(n)$ oder $\phi(n) = \phi_2(n)$ gilt. Dies ändert jedoch nichts daran, daß ϕ (wegen ϕ_1 und ϕ_2) berechenbar ist.

Definiert man hingegen eine Funktion $\phi' : \mathbb{N} \mapsto \mathbb{N}$ durch

$$\phi'(n) := \begin{cases} \phi_1(n) & , \text{ falls } \psi(n) \neq \perp \\ \phi_2(n) & , \text{ falls } \psi(n) = \perp \end{cases}$$

so ist ϕ' selbst bei berechenbaren ϕ_1, ϕ_2 und ψ *nicht notwendigerweise* berechenbar, denn um $\phi'(n)$ zu bestimmen muß festgestellt werden, ob $\psi(n) = \perp$ gilt oder nicht. In Abschnitt 5.3 zeigen wir, daß nicht algorithmisch feststellbar ist, ob eine berechenbare Funktion (wie ψ) für eine beliebige Eingabe $n \in \mathbb{N}$ ein Ergebnis $m \in \mathbb{N}$ berechnet. Damit kann ϕ' nicht berechenbar sein.

Der Unterschied zwischen ϕ und ϕ' besteht also darin, daß die Fallunterscheidung in der Definition von ϕ' *abhängig vom Parameter n* der Funktion ϕ' ist. Solch eine Abhängigkeit führt jedoch nicht notwendigerweise zu nicht-Berechenbarkeit: Wenn algorithmisch feststellbar ist, welcher der Fälle zutrifft, so kann eine solchermaßen definierte Funktion durchaus berechenbar sein – die Funktion σ_1 aus (3.1) ist ein Beispiel dafür.

4. GÖDELISIERUNGEN

4.1. Kodierung von Datentypen

Da wir uns bei Definition der Programmiersprache \mathcal{P} auf die natürlichen Zahlen \mathbb{N} als einzigem Datentyp beschränkt haben, stellt sich die Frage, wie die Berechenbarkeit von nicht-arithmetischen Funktionen, also Funktionen, die nicht auf \mathbb{N} definiert sind, untersucht werden kann.

Beispielsweise kann man Listen von natürlichen Zahlen mit dem *Quicksort*-Algorithmus ordnen. Die Funktion $sort : \mathbb{N}^* \rightarrow \mathbb{N}^*$, die jeder Liste l eine geordnete Permutation von l zuordnet, ist also sicher intuitiv berechenbar. Wir können sogar ein konkretes \mathcal{P} -Programm für das Sortieren von Listen angeben, indem wir Listen von natürlichen Zahlen durch natürliche Zahlen *kodieren*. Man nennt solche Kodierungen auch nach K. Gödel *Gödelisierungen*.

Um eine Liste $\langle n_1, \dots, n_k \rangle$ durch eine natürliche Zahl zu kodieren, ordnen wir dieser Liste mit der Funktion $\lambda : \mathbb{N}^* \rightarrow \mathbb{N}$ die natürliche Zahl $\lambda(\langle n_1, \dots, n_k \rangle) :=$

$$prim(1)^{n_k+1} prim(2)^{n_{k-1}+1} \dots prim(k-1)^{n_2+1} prim(k)^{n_1+1}$$

zu, wobei $prim(n)$ die n -te Primzahl bezeichnet. Wir nennen $\lambda(\langle n_1, \dots, n_k \rangle)$ die *Kodierung* von $\langle n_1, \dots, n_k \rangle$. Die leere Liste $\langle \rangle$ wird mit 1 kodiert, d.h. $\lambda(\langle \rangle) = 1$.

Da $prim(n)$, x^y und die Multiplikation natürlicher Zahlen \mathcal{P} -berechenbar sind, ist die Funktion λ *algorithmisch*. Mit "algorithmisch" ist gemeint, daß es ein algorithmisches Verfahren gibt, mit dem $\lambda(\langle n_1, \dots, n_k \rangle)$ aus einer Eingabe $\langle n_1, \dots, n_k \rangle$ ermittelt wird. Wir können λ nicht *\mathcal{P} -berechenbar* nennen, da wir diesen Begriff für die *arithmetischen* Funktionen $\mathbb{N}^k \mapsto \mathbb{N}$ reserviert haben.

Wegen der Eindeutigkeit der Primfaktorzerlegung ist die Funktion λ *injektiv*, und damit werden verschiedenen Listen l_1 und l_2 verschiedene Kodierungen $\lambda(l_1)$ und $\lambda(l_2)$ zugeordnet. Jeder natürlichen Zahl $m \in \text{Bild}(\lambda)$ können wir daher mit der Umkehrfunktion $\lambda^{-1} : \mathbb{N} \mapsto \mathbb{N}^*$ von λ *genau eine* Liste $\langle n_1, \dots, n_k \rangle$ von natürlichen Zahlen zuordnen, d.h. $\lambda^{-1}(m) = \langle n_1, \dots, n_k \rangle$, falls $\lambda(\langle n_1, \dots, n_k \rangle) = m$. Beispielsweise gilt $\lambda(\langle 0, 1, 0, 2 \rangle) = 4200$ und $\lambda^{-1}(4200) = \langle 0, 1, 0, 2 \rangle$, denn $4200 = 2^3 \times 3^1 \times 5^2 \times 7^1$. Dagegen ist $\lambda^{-1}(6600)$ undefiniert, denn $6600 = 2^3 \times 3^1 \times 5^2 \times 11^1$, λ ist also nicht *surjektiv*. Dabei ist offensichtlich sowohl die Umkehrfunktion λ^{-1}

algorithmisch, als auch die Funktion $\lambda^? : \mathbb{N} \rightarrow \{0, 1\}$ mit $\lambda^?(m) = 1$ gdw. $m \in \lambda(\mathbb{N}^*)$.

Allgemein muß eine Kodierung $\gamma : D \rightarrow \mathbb{N}$ einer Menge D folgenden Eigenschaften genügen:¹

Definition 4.1. (Gödelisierung)

Sei D eine Menge und sei $\gamma : D \rightarrow \mathbb{N}$. Dann ist γ eine Gödelisierung von D genau dann, wenn gilt:

1. γ ist injektiv,
2. γ ist algorithmisch,
3. $\gamma^? : \mathbb{N} \rightarrow \{0, 1\}$ mit “ $\gamma^?(m) = 1$ gdw. $m \in \gamma(D)$ ” ist berechenbar, und
4. $\gamma^{-1} : \text{Bild}(\gamma) \rightarrow D$ ist algorithmisch. ■

Es ist offensichtlich, daß λ eine Gödelisierung von \mathbb{N}^* ist. Um jetzt Listen $\langle n_1, \dots, n_k \rangle$ mit einer \mathcal{P} -Prozedur zu sortieren, kodieren wir diese Listen zunächst mit λ durch natürliche Zahlen $\lambda(\langle n_1, \dots, n_k \rangle)$. Diese Kodierung dient dann als Eingabe für einen Sortieralgorithmus $\text{QSORT} \in \mathcal{P}[1]$, der als Ergebnis eine natürliche Zahl m berechnet. Das Ergebnis m des Prozeduraufrufs muß dann mit λ^{-1} in eine Liste von natürlichen Zahlen *dekodiert* werden. Damit kann man das *Quicksort*-Verfahren mittels eines \mathcal{P} -Programms QSORT angeben, für das

$$\lambda^{-1}(\llbracket \text{QSORT} \rrbracket(\lambda(\langle n_1, \dots, n_k \rangle))) = \text{sort}(\langle n_1, \dots, n_k \rangle)$$

gilt. Da λ eine Gödelisierung und $\llbracket \text{QSORT} \rrbracket$ \mathcal{P} -berechenbar ist, ist das Sortieren von Listen mit Angabe von QSORT ebenfalls algorithmisch lösbar.

Die Prozedur QSORT ist dabei sicher umständlich zu schreiben. Beispielsweise muß man die größte Primzahl $p \neq 1$ und eine natürliche Zahl n_1 mit $\lambda(\langle n_1, \dots, n_k \rangle) \bmod p^{n_1+1} = 0$ berechnen, um das erste Element n_1 einer Liste $\langle n_1, n_2, \dots, n_k \rangle$ zu ermitteln. Um die (Kodierung der) Restliste $\langle n_2, \dots, n_k \rangle$ zu berechnen, muß $\lambda(\langle n_1, \dots, n_k \rangle)$ durch p^{n_1+1} dividiert werden. Das zweite Element der Liste erhält man dann als erstes Element dieser Restliste, u.s.w. Dieser umständliche Zugriff auf Listenelemente ist der Preis dafür, daß wir nur \mathbb{N} als Datentyp in \mathcal{P} -Programmen zulassen.

¹ Genau genommen müssen wir von einer Gödelisierungs- bzw. einer Kodierungsfunktion γ sprechen, um γ von den Elementen in $\text{Bild}(\gamma)$ zu unterscheiden. Wir verzichten auf diese sprachliche Feinheit, wenn aus dem Kontext ersichtlich ist, was gerade genau gemeint ist.

$n_1 \setminus n_2$	0	1	2	3	4	...
0	0	1	3	6	10	...
1	2	4	7	11	16	...
2	5	8	12	17	23	...
3	9	13	18	24	31	...
4	14	19	25	32	40	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Abbildung 4.1: Wertetabelle der Paar-Funktion π^2

Allgemein können wir jeden Datentyp durch natürliche Zahlen kodieren. Da jedes Element eines Datentyps im Speicher eines Rechners endlich darstellbar ist, kann man jedes dieser Elemente auch kodieren. Man stelle sich dazu vor, daß jedes Datenobjekt im Speicher eines Rechners durch eine endliche Bitfolge repräsentiert wird. Diese Bitfolge kann man als natürliche Zahl auffassen, wodurch man die Kodierung des Datenobjekts erhält. Die zugehörige Kodierungsfunktion erfüllt dabei offenbar die Forderungen, die mit Definition 4.1 an eine Gödelisierung gestellt werden.

Wesentlich dabei ist, daß Elemente eines Datentyps auch *endlich* darstellbar sind. Beispielsweise kann man keinen Datentyp für die Menge \mathbb{R} der reellen Zahlen definieren, denn reelle Zahlen sind i.A. *unendlich große* Objekte. Man behilft sich deswegen in Programmiersprachen mit einem Datentyp `real` $\subsetneq \mathbb{R}$, der eine *endliche Approximation* der reellen Zahlen darstellt. Damit sind Elemente des Datentyps `real` endliche Objekte und somit auch durch natürliche Zahlen kodierbar.

4.2. Die Paar-Funktion

In diesem Abschnitt betrachten wir eine Gödelisierung von $\mathbb{N} \times \mathbb{N}$, die für weitere Untersuchungen nützlich ist.

Definition 4.2. (Paar-Funktion)

Die Paar-Funktion (engl. pairing function) $\pi^2: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ ist definiert durch

$$\pi^2(n_1, n_2) := \frac{1}{2}(n_1 + n_2)(n_1 + n_2 + 1) + n_1. \quad \blacksquare$$

Abbildung 4.1 gibt einige Funktionswerte der Paar-Funktion an.

n	0	1	2	3	4	5	6	7	8	...
(n_1, n_2)	(0,0)	(0,1)	(1,0)	(0,2)	(1,1)	(2,0)	(0,3)	(1,2)	(2,1)	...

Abbildung 4.2: Wertetabelle der Umkehrfunktion π^{-2} von π^2

Satz 4.3. Die Paar-Funktion π^2 ist

1. \mathcal{P} -berechenbar,
2. eine Gödelisierung von $\mathbb{N} \times \mathbb{N}$,
3. surjektiv.

Beweis. Übung. ■

Mit Satz 4.3(1) dürfen wir im folgenden also die Existenz einer \mathcal{P} -Prozedur PAIR^2 mit $[[\text{PAIR}^2]] = \pi^2$ voraussetzen. Mit Satz 4.3(2,3) ist π^2 *bijektiv*, und damit kommt jede natürliche Zahl n in Abbildung 4.1 *genau* einmal vor. Damit können wir jeder natürlichen Zahl n ein Paar (n_1, n_2) von natürlichen Zahlen *eindeutig* zuordnen, nämlich dasjenige Paar (n_1, n_2) , für das $\pi^2(n_1, n_2) = n$ gilt. Daraus folgt, daß die Umkehrfunktion $\pi^{-2} : \mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}$ von π^2 , s. Abbildung 4.2, ebenfalls *bijektiv* ist.² Mit Satz 4.3(2) ist π^{-2} auch algorithmisch, und folglich sind die Funktionen $\pi_1^2 : \mathbb{N} \rightarrow \mathbb{N}$ und $\pi_2^2 : \mathbb{N} \rightarrow \mathbb{N}$ mit

$$\pi_1^2(\pi^2(n_1, n_2)) = n_1, \quad \pi_2^2(\pi^2(n_1, n_2)) = n_2 \quad \text{und} \quad \pi^2(\pi_1^2(n), \pi_2^2(n)) = n \quad (4.1)$$

berechenbar. Abbildung 4.3 gibt einige Funktionswerte von π_1^2 und π_2^2 an. Wir zeigen, daß auch π_1^2 und π_2^2 \mathcal{P} -berechenbar sind:

Satz 4.4. $\pi_1^2 : \mathbb{N} \rightarrow \mathbb{N}$ und $\pi_2^2 : \mathbb{N} \rightarrow \mathbb{N}$ mit (4.1) sind \mathcal{P} -berechenbar.

Beweis. Mit Satz 4.3(1) ist π^2 \mathcal{P} -berechenbar und damit existiert ein Programm $\text{PAIR}^2 \in \mathcal{P}[2]$ mit $[[\text{PAIR}^2]] = \pi^2$. Sei $\text{PAIR}_1^2 \in \mathcal{P}[1]$ definiert wie in Abbildung 4.4. Dieses Programm erzeugt systematisch eine Folge $(0, 0); (1, 0), (1, 1); (2, 0), (2, 1), (2, 2); (3, 0), \dots$ von Paaren (n_1, n_2) natürlicher Zahlen mit $n_1 \geq n_2$. Jedes Paar wird mit dem Programm PAIR^2 daraufhin überprüft, ob $\pi^2(n_1, n_2) = n$ gilt. Verläuft der Test positiv, so gilt $\pi_1^2(n) = n_1$. Andernfalls wird $\pi^2(n_2, n_1) = n$

² Aus Gründen der Lesbarkeit schreiben wir π^{-2} anstatt des formal korrekten $(\pi^2)^{-1}$.

überprüft, denn dann gilt $\pi_1^2(n) = n_2$. Mit $\text{stop} := 1$ wird für beide Schleifen der Abbruch erzwungen, wenn einer der Tests positiv verläuft, und PAIR_1^2 hält mit Ergebnis n_1 bzw. n_2 , also mit $\pi_1^2(n)$. Da (1) mit der **repeat**-Schleife alle Paare $(n_1, n_2) \in \mathbb{N} \times \mathbb{N}$ mit $n_1 \geq n_2$ erzeugt werden, (2) für alle Paare $(n_1, n_2) \in \mathbb{N} \times \mathbb{N}$ entweder $n_1 \geq n_2$ oder $n_2 \geq n_1$ gilt und (3) π^2 surjektiv ist, wird entweder der Test $\text{PAIR}^2(\mathbf{n1}, \mathbf{n2}) = \mathbf{n}$ oder der Test $\text{PAIR}^2(\mathbf{n2}, \mathbf{n1}) = \mathbf{n}$ nach endlich vielen Schritten positiv beantwortet, und damit hält PAIR_1^2 für jede Eingabe n . Folglich gilt $\llbracket \text{PAIR}_1^2 \rrbracket = \pi_1^2$, und damit ist π_1^2 \mathcal{P} -berechenbar.

Man erhält ein Programm $\text{PAIR}_2^2 \in \mathcal{P}[1]$ mit $\llbracket \text{PAIR}_2^2 \rrbracket = \pi_2^2$ aus dem Programm PAIR_1^2 , indem man lediglich die Zuweisungen $\text{res} := \mathbf{n1}$ und $\text{res} := \mathbf{n2}$ im Rumpf von PAIR_1^2 vertauscht. ■

Mit der Paar-Funktion können wir auch endliche Listen (beliebiger Länge) von natürlichen Zahlen und damit dann insbesondere (in Abschnitt 4.3) die Listen der aktuellen Parameter von Prozeduraufrufen gödelisieren.

Bemerkung 4.5. Allgemein definiert man den abstrakten Datentyp $\text{list}[\mathbb{N}]$ durch die Funktionssignatur

$$\begin{array}{ll} \varepsilon : \rightarrow \text{list}[\mathbb{N}] & \text{hd} : \text{list}[\mathbb{N}] \rightarrow \mathbb{N} \\ \text{add} : \mathbb{N} \times \text{list}[\mathbb{N}] \rightarrow \text{list}[\mathbb{N}] & \text{tl} : \text{list}[\mathbb{N}] \rightarrow \text{list}[\mathbb{N}] \end{array}$$

sowie die Gleichungen

$$\begin{array}{ll} \text{hd}(\varepsilon) = 0 & \text{hd}(\text{add}(n, k)) = n \\ \text{tl}(\varepsilon) = \varepsilon & \text{tl}(\text{add}(n, k)) = k \end{array} \quad (4.2)$$

Dabei steht ε für die leere Liste, mit add wird aus einer natürlichen Zahl und einer Liste eine neue Liste gebildet, mit hd (für head) erhält man das erste Element einer nicht-leeren Liste, und mit tl (für tail) die Liste ohne das erste Listenelement. Die Liste $\langle 0, 1, 0 \rangle$ wird beispielsweise als $\text{add}(0, \text{add}(1, \text{add}(0, \varepsilon)))$ geschrieben.

Mit der Paar-Funktion kodieren wir Listen durch natürliche Zahlen. Dabei übernimmt π^2 die Rolle von add , 0 kodiert ε , π_1^2 entspricht hd und π_2^2 steht für tl . Da in \mathcal{P} nur die natürlichen Zahlen als Datentyp zur Verfügung stehen, repräsentiert eine natürliche Zahl sowohl eine natürliche Zahl als auch eine Liste (von natürlichen Zahlen). Mit $\pi^2(0, 0) = 0$ darf 0 jedoch keine natürliche Zahl repräsentieren, denn man erhielte sonst 0 sowohl als Kodierung von ε als auch als Kodierung von $\text{add}(0, \varepsilon)$, also der Liste $\langle 0 \rangle$. Anders gesagt, man kann bei Kodierung einer Liste $\langle n_1, n_2, \dots, n_k \rangle$ durch $\pi^2(n_1, \pi^2(n_2, \pi^2(\dots, \pi^2(n_{k-1}, n_k) \dots)))$ nicht das Listenende erkennen. Um dieses Problem zu umgehen, werden Listen $\langle n_1, n_2, \dots, n_k \rangle$ durch $\pi^2(n_1 + 1, \pi^2(n_2 + 1, \pi^2(\dots, \pi^2(n_k + 1, 0) \dots)))$ kodiert. Bei dieser Kodierung von Listen ist unmittelbar einsichtig, daß mit (4.1) die Gleichungen (4.2) für die kodierten Listen auch tatsächlich gelten.

n	0	1	2	3	4	5	6	7	8	...
$\pi_1^2(n)$	0	0	1	0	1	2	0	1	2	...
$\pi_2^2(n)$	0	1	0	2	1	0	3	2	1	...

Abbildung 4.3: Wertetabelle der Funktionen π_1^2 und π_2^2

```

procedure PAIR12(n) <=
begin var n1,n2,stop,res;
repeat
n2 := 0;
while GE(n1,n2) ∧ ¬stop do
if PAIR2(n1,n2) = n
then res := n1;
stop := 1
else if PAIR2(n2,n1) = n
then res := n2;
stop := 1
else n2 := SUCC(n2)
end_if
end_if
end_while;
n1 := SUCC(n1)
until stop;
return(res)
end

```

Abbildung 4.4: Ein \mathcal{P} -Programm für π_1^2

Definition 4.6. (Verallgemeinerte Paar-Funktion)

Die verallgemeinerte Paar-Funktion $\pi^k: \mathbb{N}^k \rightarrow \mathbb{N}$ ist für jedes $k \geq 1$ definiert durch

- $\pi^1(n_1) := n_1$,
- $\pi^2(n_1, n_2) := \frac{1}{2}(n_1 + n_2)(n_1 + n_2 + 1) + n_1$, und
- $\pi^{k+2}(n_1, \dots, n_{k+2}) := \pi^2(n_1, \pi^{k+1}(n_2, \dots, n_{k+2}))$. ■

Satz 4.7. Für jedes $k \geq 1$ ist die verallgemeinerte Paar-Funktion $\pi^k: \mathbb{N}^k \rightarrow \mathbb{N}$

1. \mathcal{P} -berechenbar,
2. eine Gödelisierung von \mathbb{N}^k
3. surjektiv.

Beweis. Für $k = 1$ ist die Aussagen trivial. Für $k = 2$ ist die Behauptung bereits mit Satz 4.3 gezeigt. Für $k = k' + 2$ zeigt man die Behauptung durch Induktion über k' . ■

Mit Satz 4.7 dürfen wir im folgenden also für jedes $k \geq 1$ die Existenz einer \mathcal{P} -Prozedur PAIR^k mit $[[\text{PAIR}^k]] = \pi^k$ voraussetzen.

Satz 4.8. Für $k \geq 1$ und $h \in \{1, \dots, k\}$ existieren \mathcal{P} -berechenbare Funktionen $\pi_h^k: \mathbb{N} \rightarrow \mathbb{N}$ mit

1. $\pi_h^k(\pi^k(n_1, \dots, n_k)) = n_h$, und
2. $\pi^k(\pi_1^k(n), \dots, \pi_h^k(n), \dots, \pi_k^k(n)) = n$.

Beweis. Für $k = 1$ ist die Aussage trivial. Für $k = 2$ ist die Behauptung bereits mit Satz 4.4 gezeigt. Für $k = k' + 2$ zeigt man die Behauptung durch Induktion über k' . ■

Mit Satz 4.8 dürfen wir im folgenden also für jedes $k \geq 1$ und jedes $h \in \{1, \dots, k\}$ die Existenz einer \mathcal{P} -Prozedur PAIR_h^k mit $[[\text{PAIR}_h^k]] = \pi_h^k$ voraussetzen.

Bemerkung 4.9. Mit der verallgemeinerten Paar-Funktion π^k können wir Listen $\langle n_1, \dots, n_k \rangle$ durch $\pi^k(n_1, \dots, n_k)$ – anstatt durch $\pi^2(n_1+1, \pi^2(n_2+1, \pi^2(\dots, \pi^2(n_k+1, 0) \dots)))$, vgl. Bemerkung 4.5 – kodieren, denn für $\pi_h^k(n) = 0$ kann n nur die Kodierung einer Liste $\langle n_1, n_2, \dots, n_k \rangle$ mit $n_h = 0$ sein. Das Listenende muß hier nicht gesondert durch 0 gekennzeichnet werden, da mit π^k nur Listen einer festen Länge k kodiert werden.

4.3. Stelligkeit berechenbarer Funktionen

Mit der verallgemeinerten Paar-Funktion π^k kann man jedes k -Tupel (n_1, \dots, n_k) natürlicher Zahlen eindeutig durch eine natürliche Zahl kodieren und jede Komponente n_h dieses k -Tupels mit π_h^k zurückgewinnen, vgl. Bemerkung 4.9. Damit können wir jede \mathcal{P} -berechenbare Funktion $\phi : \mathbb{N}^k \mapsto \mathbb{N}$ durch eine *einstellige* \mathcal{P} -berechenbare Funktion $\phi' : \mathbb{N} \mapsto \mathbb{N}$ darstellen:³

Satz 4.10. *Für jede \mathcal{P} -berechenbare Funktion $\phi : \mathbb{N}^k \mapsto \mathbb{N}$ existiert eine \mathcal{P} -berechenbare Funktion $\phi' : \mathbb{N} \mapsto \mathbb{N}$, so daß gilt:*

1. $\phi'(n) = \phi(\pi_1^k(n), \dots, \pi_h^k(n), \dots, \pi_k^k(n))$ und
2. $\phi(n_1, \dots, n_k) = \phi'(\pi^k(n_1, \dots, n_k))$.⁴

Beweis. (1) Mit Satz 4.8 gibt es Prozeduren $\text{PAIR}_1^k, \dots, \text{PAIR}_k^k \in \mathcal{P}[1]$ so daß $\pi_h^k = \llbracket \text{PAIR}_h^k \rrbracket$ für jedes $h \in \{1, \dots, k\}$ gilt. Sei $\text{PHI} \in \mathcal{P}[k]$ mit $\llbracket \text{PHI} \rrbracket = \phi$ gegeben durch

```

procedure PHI(x1, ..., xk) <=
begin var y1, ..., yn;
  STA $\phi$ ;
  return(y $\phi$ )
end .

```

Für die Prozedur $\text{PHI}' \in \mathcal{P}[1]$, gegeben durch

```

procedure PHI'(x) <=
begin var y;
  y := PHI(PAIR $_1^k$ (x), ..., PAIR $_k^k$ (x));
  return(y)
end

```

gilt dann $\llbracket \text{PHI}' \rrbracket(n) = \llbracket \text{PHI} \rrbracket(\llbracket \text{PAIR}_1^k \rrbracket(n), \dots, \llbracket \text{PAIR}_k^k \rrbracket(n))$ für alle $n \in \mathbb{N}$, also $\llbracket \text{PHI}' \rrbracket(n) = \phi(\pi_1^k(n), \dots, \pi_k^k(n))$. Folglich gilt $\llbracket \text{PHI}' \rrbracket = \phi'$, und damit ist ϕ' \mathcal{P} -berechenbar.

(2) Folgt unmittelbar aus (1) und Satz 4.8(1). ■

³ Dies ist insbesondere deshalb relevant, da man so einen Interpretierer für \mathcal{P} -Programme durch ein \mathcal{P} -Programm `APPLY` angeben kann, s. Kapitel 6. Der Interpretierer erwartet den Code eines auszuführenden \mathcal{P} -Programms P sowie die Parameter für die Ausführung von P als Eingabe. Da die *Anzahl* dieser Parameter von P abhängt, die Anzahl der Parameter jedes \mathcal{P} -Programms (also insbesondere auch von `APPLY`) ein fester Wert ist, werden die Parameter von P in einen einem einzigen Wert, der *Parameterliste*, zusammengefaßt. Damit erhält `APPLY` dann neben dem Programmkode die Parameterliste als einziges weiteres Argument.

⁴ Im Fall $k = 0$ liest man 1. $\phi'(n) = \phi$ sowie 2. $\phi = \phi'(n)$.

Als Konsequenz von Satz 4.10 können wir immer davon ausgehen, daß jede \mathcal{P} -berechenbare Funktion ϕ *einstellig* ist, also durch ein Programm aus $\mathcal{P}[1]$ berechnet werden kann. Dies kann man sich folgendermaßen veranschaulichen:

Ein Programm $\text{PROG} \in \mathcal{P}[k]$ erwartet eine Liste (n_1, \dots, n_k) aktueller Parameter mit k Elementen als Eingabe. Diese Liste können wir mit der verallgemeinerten Paar-Funktion π^k kodieren.⁵ Wir erhalten so eine $\mathcal{P}[1]$ -Prozedur PROG' , in deren Rumpf dann mittels der $\mathcal{P}[1]$ -Prozeduren PAIR_h^k auf die aktuellen Parameter n_h der kodierten Parameterliste zugegriffen werden kann, vgl. die Prozedur PHI' in Satz 4.10.

Für die $\mathcal{P}[2]$ -Prozedur MINUS aus Abbildung 2.3 erhält man beispielsweise die $\mathcal{P}[1]$ -Prozedur

```

procedure MINUS'(x) <=
begin var n,m;
  n := PAIR12(x); m := PAIR22(x);
  while m do
    n := PRED(n); m := PRED(m)
  end_while;
  return(n)
end .

```

Um jetzt etwa $3-2$ zu berechnen, wird – anstatt die Prozedur MINUS mit den aktuellen Parametern 3 und 2 aufzurufen – die Prozedur MINUS' mit dem aktuellen Parameter 18 aufgerufen, denn $\pi^2(3, 2) = 18$. In der ersten Zuweisung der Prozedur MINUS' erhält n dann den Wert 3 ($= \pi_1^2(18)$), und in der zweiten Zuweisung erhält m den Wert 2 ($= \pi_2^2(18)$). Jetzt wird 2 in der *while*-Schleife von 3 subtrahiert, und das Ergebnis des Prozeduraufrufs $\text{MINUS}'(18)$ ist 1.

Verwendet man nur $\mathcal{P}[1]$ -Programme, so stellt sich die Frage, wie denn im Beispiel der aktuelle Parameter 18 als Kodierung der Parameterliste $(3, 2)$ berechnet werden soll. Bei Aufruf einer $\mathcal{P}[k]$ -Prozedur $\text{PROG}(n_1, \dots, n_k)$ im Rumpf eines \mathcal{P} -Programms P geschieht dies mittels der \mathcal{P} -Prozedur PAIR^k , d.h. der Prozeduraufruf wird im Rumpf von P durch $\text{PROG}'(\text{PAIR}^k(n_1, \dots, n_k))$ ersetzt. Im Rumpf der Prozedur GGT aus Abbildung 2.3 würden daher die Prozeduraufrufe $\text{MINUS}(n, m)$ und $\text{MINUS}(m, n)$ durch $\text{MINUS}'(\text{PAIR}^2(n, m))$ bzw. $\text{MINUS}'(\text{PAIR}^2(m, n))$ ersetzt. Da wir Prozeduraufrufe immer eliminieren können, vgl. Definition 2.2, ist die Verwendung der $\mathcal{P}[k]$ -Prozedur PAIR^k hier unkritisch.

Bei einem $\mathcal{P}[k]$ -Programm als “*Hauptprogramm*”, etwa dem $\mathcal{P}[2]$ -Programm GGT aus Abbildung 2.4 oder dem $\mathcal{P}[2]$ -Programm MINUS (als “*Hauptprogramm*”

⁵ Dies gilt natürlich nur für den Fall $k \geq 1$, denn π^0 ist nicht definiert. Die Anpassung der nachfolgenden Diskussion auf den Fall $k = 0$ ist jedoch trivial, so daß wir darauf verzichten.

und nicht als Hilfsprozedur aufgefaßt) können wir jedoch nicht so vorgehen, denn für diese Programme kennen wir ja keine Aufrufe, die wir modifizieren könnten. Anders gesagt, diese Programme werden *außerhalb* unserer \mathcal{P} -Programme aufgerufen, also muß *dort* die Kodierung der aktuellen Parameter $\mathbf{n1}$ und $\mathbf{n2}$ zu $\pi^2(\mathbf{n1}, \mathbf{n2})$ vorgenommen werden. Für uns ist daher belanglos, wie die Kodierung der Parameterliste $(3, 2)$ mittels π^2 zu 18 berechnet wird, wenn etwa $ggt(3, 2)$ oder $3-2$ mittels der $\mathcal{P}[1]$ -Programme \mathbf{GGT}' bzw. \mathbf{MINUS}' berechnet werden sollen. Diese beiden $\mathcal{P}[1]$ -Programme *interpretieren* 18 als Kodierung der Liste $(3, 2)$, denn die Programme aus $\mathcal{P}[1]$ arbeiten anstatt direkt auf natürlichen Zahlen auf kodierten Listen von natürlichen Zahlen (die selbst wieder natürliche Zahlen sind). Wie diese Kodierungen genau berechnet werden ist für unsere Untersuchungen genauso unerheblich wie die Frage, wie die Gödelisierung irgendeines Datentyps D nun genau berechnet wird. Wesentlich ist nur, daß die Kodierungsfunktion π^k für \mathbb{N}^k den Forderungen von Definition 4.1 für eine Gödelisierung genügt, und dies ist mit Satz 4.7 der Fall.

Damit bleibt nur noch die Frage, wie denn ein $\mathcal{P}[1]$ -Programm $\mathbf{PAIR}^{2'}$ für \mathbf{PAIR}^2 aussehen könnte. Da wir behaupten, daß jede k -stellige berechenbare Funktion als 1-stellige berechenbare Funktion dargestellt werden kann, so muß es ja ein $\mathcal{P}[1]$ -Programm $\mathbf{PAIR}^{2'}$ mit $(*) \llbracket \mathbf{PAIR}^2 \rrbracket(n_1, n_2) = \pi^2(n_1, n_2) = \llbracket \mathbf{PAIR}^{2'} \rrbracket(\pi^2(n_1, n_2))$ geben. Dies gilt offenbar, falls $\llbracket \mathbf{PAIR}^{2'} \rrbracket$ die Identitätsfunktion ist, also definieren wir

```

procedure PAIR2'(x) <=
begin var y; y := x; return(y) end .

```

Wir werden daher im folgenden arithmetische Funktionen $\phi : \mathbb{N}^k \mapsto \mathbb{N}$ in vielen Fällen anstatt in der Form $\phi(n_1, \dots, n_k) := \mathcal{DEF}[n_1, \dots, n_k]$ in der Form $\phi : \mathbb{N} \mapsto \mathbb{N}$ mit $\phi(\pi^k(n_1, \dots, n_k)) := \mathcal{DEF}[n_1, \dots, n_k]$ definieren, wobei dann mit Satz 4.8 $\phi(n) = \mathcal{DEF}[\pi_1^k(n), \dots, \pi_k^k(n)]$ gilt.

4.4. Kodierung von Programmen

Mit Programmen irgendeiner Programmiersprache PS können auch Programme (dieser Programmiersprache) verarbeitet werden. Beispielsweise können wir einen Übersetzer in der Programmiersprache PS schreiben, der PS -Programme als Eingabe erhält und diese dann in eine Zielsprache übersetzt. Mit einem in PS geschriebenen Editor können wir PS -Programme editieren, mit einem in PS geschriebenen Datenkompressionsprogramm können wir PS -Programme platzsparend abspeichern, mit einem in PS geschriebenen Interpretierer können wir PS -Programme ausführen, u.s.w.

In einigen Programmiersprachen, wie z.B. Assemblersprachen oder LISP, werden Programme und Daten überhaupt nicht unterschieden, so daß die Verarbeitung von Programmen durch Programme direkt implementiert werden kann. In anderen Sprachen, wie z.B. JAVA oder C, werden Programme und Daten unterschiedlich behandelt. Hier müssen dann Programme durch einen bestimmten Datentyp, wie z.B. den Datentyp *string* oder als Feld von Zeichen (*array integer of character*), kodiert werden, um Programme durch Programme zu verarbeiten.

Die Fähigkeit von Programmen, Programme zu verarbeiten, ist wesentlich für die Ergebnisse der Berechenbarkeitstheorie. Wir kodieren daher (wie schon zuvor Datentypen) \mathcal{P} -Programme durch natürliche Zahlen, um \mathcal{P} -Programme mit \mathcal{P} -Programmen verarbeiten zu können:

\mathcal{P} -Programme sind endliche Worte über einem endlichen Alphabet $A_{\mathcal{P}}$, die den syntaktischen Konventionen von Definition 2.1 genügen. Es gilt also $\mathcal{P} \subseteq A_{\mathcal{P}}^+$. Das Alphabet $A_{\mathcal{P}}$ enthält alle Buchstaben in Groß- und Kleinschreibung, die Ziffern $0, \dots, 9$ und Sonderzeichen wie “<”, “=”, “,”, “:”, “;”, “)”, “(”, \dots . Damit können wir die Elemente von $A_{\mathcal{P}}$ durch Bitworte über $\{0, 1\}$ mit einer festen Länge $\ell > 0$ kodieren, wobei 0^ℓ als Kodierung für kein Zeichen aus $A_{\mathcal{P}}$ erlaubt ist. Für $\ell = 8$ können wir beispielsweise 255 verschiedene Zeichen in $A_{\mathcal{P}}$ darstellen – das sollte reichen, um \mathcal{P} -Programme zu schreiben. Die Zuordnung von ℓ -Bit Worten zu den Symbolen von $A_{\mathcal{P}}$ legen wir durch eine endliche *Kodetabelle* fest. Diese Tabelle repräsentiert den Graphen einer Funktion $code : A_{\mathcal{P}} \rightarrow \{0, 1\}^\ell \setminus \{0^\ell\}$. Da wir verschiedenen Symbolen in $A_{\mathcal{P}}$ verschiedene ℓ -Bit Worte zuordnen, ist $code$ injektiv. Damit können wir jetzt jedes Wort $a_1 \dots a_k \in A_{\mathcal{P}}^+$ (und damit insbesondere jedes \mathcal{P} -Programm) durch eine natürliche Zahl $\natural(a_1 \dots a_k) := dual^{-1}(code(a_1) \oplus \dots \oplus code(a_k))$ gödelisieren, wobei $dual^{-1} : \{0, 1\}^+ \rightarrow \mathbb{N}$ eine natürliche Zahl aus deren Dualzahldarstellung berechnet (und damit z.B. $dual^{-1}(11010) = 26$ gilt).

Definition 4.11. (Programmkode $\natural P$) Sei

- $A_{\mathcal{P}} \neq \emptyset$ das endliche Alphabet von \mathcal{P} , d.h. $\mathcal{P} \subseteq A_{\mathcal{P}}^+$,
- $code: A_{\mathcal{P}} \rightarrow \{0, 1\}^\ell \setminus \{0^\ell\}$ mit $\ell = \lceil \log_2(|A_{\mathcal{P}}| + 1) \rceil$ eine injektive Funktion, die jedes Symbol aus $A_{\mathcal{P}}$ in ein ℓ -Bit Wort abbildet,⁶
- $dual: \mathbb{N} \rightarrow \{0, 1\}^\ell$ diejenige Funktion, die jede natürliche Zahl n in ihre Dualzahldarstellung $dual(n)$ abbildet, d.h. in eine Zeichenreihe minimaler Länge von Bits 0 und 1,

⁶ $\lceil \log_2(n) \rceil \in \mathbb{N}$ ist der nach oben gerundete Logarithmus von n zur Basis 2.

- $dual_\ell: \mathbb{N} \rightarrow \{\{0,1\}^\ell\}^+$ diejenige Funktion, die jede natürliche Zahl n in ihre in Bit-Blöcke der Länge ℓ eingeteilte Dualzahldarstellung $dual_\ell(n)$ abbildet, d.h. in eine Zeichenreihe minimaler Länge von Bits 0 und 1, deren Länge ein Vielfaches von ℓ ist,⁷
- $dual^{-1}: \{0,1\}^+ \rightarrow \mathbb{N}$ diejenige Funktion mit
 1. $dual^{-1}(\alpha) = 0$ für alle $\alpha \in \{0\}^+$ sowie
 2. $dual^{-1}(\beta \oplus dual(n)) = n$ für alle $\beta \in \{0\}^*$ und alle $n \in \mathbb{N} \setminus \{0\}$,
 3. $dual(dual^{-1}(0)) = 0$, sowie
 4. $dual(dual^{-1}(1\gamma)) = 1\gamma$ für alle $\gamma \in \{0,1\}^*$, und sei
- $\oplus: \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$ diejenige Funktion, die zwei Bitworte α und β in ihre Konkatenation $\alpha\beta$ abbildet.

Dann ist die Programmkodierungsfunktion $\natural: \mathcal{P} \rightarrow \mathbb{N}$ von \mathcal{P} gegeben durch

$$\natural(a_1 \dots a_k) := dual^{-1}(code(a_1) \oplus \dots \oplus code(a_k)) . \quad (4.3)$$

Für $P \in \mathcal{P}$ schreiben wir $\natural P$ anstatt $\natural(P)$ und nennen $\natural P$ den Kode von P . Die Menge $\natural\mathcal{P}$ aller Kodes der Programmiersprache \mathcal{P} ist definiert durch $\natural\mathcal{P} := \{\natural P \in \mathbb{N} \mid P \in \mathcal{P}\}$.⁸ ■

Lemma 4.12. Mit den Begriffen aus Definition 4.11 gilt:

1. $dual^{-1}(dual_\ell(n)) = n$ für alle $n \in \mathbb{N}$.
2. $dual_\ell(dual^{-1}(\alpha_1 \oplus \dots \oplus \alpha_k)) = \alpha_1 \oplus \dots \oplus \alpha_k$ für alle $\alpha_1, \dots, \alpha_k \in \{0,1\}^\ell \setminus \{0^\ell\}$.

Beweis. (1) Für $n = 0$ gilt $dual_\ell(n) = 0^\ell$ und damit $dual^{-1}(dual_\ell(n)) = 0$. Andernfalls erhält man $dual_\ell(n) = 0^i \oplus dual(n)$ für ein $i \in \mathbb{N}$ mit $0 \leq i < \ell$ und folglich $dual^{-1}(dual_\ell(n)) = dual^{-1}(0^i \oplus dual(n)) = dual^{-1}(dual(n)) = n$.

(2) Mit $\alpha_1 \in \{0,1\}^\ell \setminus \{0^\ell\}$ gilt $\alpha_1 = 0^i 1\gamma$ für ein $i \in \mathbb{N}$ mit $0 \leq i < \ell$ sowie ein $\gamma \in \{0,1\}^{\ell-i-1}$. Man erhält so $dual^{-1}(\alpha_1 \oplus \dots \oplus \alpha_k) = dual^{-1}(1\gamma \oplus \alpha_2 \oplus \dots \oplus \alpha_k)$ und damit $dual_\ell(dual^{-1}(\alpha_1 \oplus \dots \oplus \alpha_k)) = dual_\ell(dual^{-1}(1\gamma \oplus \alpha_2 \oplus \dots \oplus \alpha_k)) = 0^i \oplus dual(dual^{-1}(1\gamma \oplus \alpha_2 \oplus \dots \oplus \alpha_k)) = 0^i \oplus 1\gamma \oplus \alpha_2 \oplus \dots \oplus \alpha_k = \alpha_1 \oplus \dots \oplus \alpha_k$.⁹ ■

⁷ Dieser Forderung kann immer durch Voranstellen von 0-Bits genügt werden und wird benötigt, um die Aussage von Lemma 4.12(2.) zu sichern. Mit $dual$ anstatt $dual_\ell$ erhielte man sonst für $\ell = 2$ beispielsweise $dual(dual^{-1}(01)) = dual(1) = 1 \neq 01$, während $dual_\ell(1) = 01$ gilt.

⁸ Bei der Definition von $\natural\mathcal{P}$ gehen wir davon aus, daß \mathcal{P} nach Definition 2.1 gegeben ist, also insbesondere keine Prozeduraufrufe enthält.

⁹ Das Verbot von 0^ℓ als Kode ist erforderlich, denn man erhielte sonst für $\ell = 2$ beispielsweise $dual_\ell(dual^{-1}(0000)) = dual_\ell(0) = 00 \neq 0000$.

Satz 4.13. Die Programmkodierungsfunktion \natural ist eine Gödelisierung von \mathcal{P} .

Beweis. (1) “ $\natural : \mathcal{P} \rightarrow \mathbb{N}$ ist injektiv”: Da alle Elemente von $\text{Bild}(\text{code})$ Bitworte der Länge ℓ und code nach Voraussetzung injektiv ist, gilt $\text{code}(a_1) \oplus \dots \oplus \text{code}(a_k) \neq \text{code}(a'_1) \oplus \dots \oplus \text{code}(a'_{k'})$ falls $a_1 \dots a_k \neq a'_1 \dots a'_{k'}$. Für $k = k'$ gilt dann (*) $\text{dual}^{-1}(\text{code}(a_1) \oplus \dots \oplus \text{code}(a_k)) \neq \text{dual}^{-1}(\text{code}(a'_1) \oplus \dots \oplus \text{code}(a'_{k'}))$, denn verschiedene Bitworte gleicher Länge werden mit dual^{-1} in verschiedene natürliche Zahlen abgebildet. Für $k \neq k'$ gilt (*) ebenfalls, denn Bitworte unterschiedlicher Länge werden mit dual^{-1} in verschiedene natürliche Zahlen abgebildet, da 0^ℓ als Kodierung verboten ist.¹⁰

(2) “ \natural ist algorithmisch”: Um $\natural(a_1 \dots a_k)$ für ein Wort $a_1 \dots a_k \in \mathcal{P}$ zu berechnen, bearbeitet man $a_1 \dots a_k$ Zeichen für Zeichen von links nach rechts und ersetzt dabei jedes Symbol a_i durch $\text{code}(a_i)$, so wie in der Kodetabelle angegeben. Dieses Verfahren ist offenbar algorithmisch. Die ℓ -Bit Worte $\text{code}(a_i)$ werden mit \oplus zu einem Bitwort $\text{code}(a_1) \oplus \dots \oplus \text{code}(a_k)$ konkateniert, was auch algorithmisch bewerkstelligt werden kann. Schließlich wird $\text{code}(a_1) \oplus \dots \oplus \text{code}(a_k)$ in die natürliche Zahl $\text{dual}^{-1}(\text{code}(a_1) \oplus \dots \oplus \text{code}(a_k))$ umgewandelt. Auch diese Umwandlung ist algorithmisch, und damit ist auch \natural algorithmisch.

(3) “ $\natural? : \mathbb{N} \rightarrow \{0, 1\}$ mit ‘ $\natural?(n) = 1$ gdw. $n \in \natural\mathcal{P}$ ’ ist berechenbar”: Die Programmiersprache \mathcal{P} ist eine sehr einfache Programmiersprache, die nur Konstrukte enthält, die wir (mitunter in syntaktischen Abwandlungen) bereits aus implementierten Programmiersprachen kennen. Damit dürfen wir davon ausgehen, daß man (in \mathcal{P}) einen Syntaxanalysator (engl. Parser) $\text{parse} : \{\{0, 1\}^\ell\}^+ \rightarrow \{0, 1\}$ für \mathcal{P} implementieren kann, für den $\text{parse}(\text{code}(a_1) \oplus \dots \oplus \text{code}(a_k)) = 1$ für alle $a_1 \dots a_k \in \mathcal{P}$ sowie $\text{parse}(\alpha_1 \oplus \dots \oplus \alpha_k) = 0$ für alle $\alpha_1, \dots, \alpha_k \in \{\{0, 1\}^\ell\}^+$ mit $\text{code}^{-1}(\alpha_1) \dots \text{code}^{-1}(\alpha_k) \in A_{\mathcal{P}}^+ \setminus \mathcal{P}$ oder $\alpha_i \notin \text{Bild}(\text{code})$ für ein $i \in \{1, \dots, k\}$ gilt. Damit erhält man $\natural?(n) := \text{parse}(\text{dual}_\ell(n))$ und folglich ist $\natural?$ berechenbar, denn dual_ℓ und parse sind algorithmisch.

Für $\natural?(n) = 1$ gilt $\text{dual}_\ell(n) = \alpha_1 \oplus \dots \oplus \alpha_k$ mit $\alpha_i \in \text{Bild}(\text{code})$ für jedes α_i sowie $\text{parse}(\alpha_1 \oplus \dots \oplus \alpha_k) = 1$. Mit der Definition von parse gilt $\text{code}^{-1}(\alpha_1) \dots \text{code}^{-1}(\alpha_k) \in \mathcal{P}$, und folglich $\natural(\text{code}^{-1}(\alpha_1) \dots \text{code}^{-1}(\alpha_k)) \in \natural\mathcal{P}$. Mit der Definition von \natural erhält man dann $n \in \natural\mathcal{P}$, denn

¹⁰ Die Funktion \natural ist nicht *injektiv*, falls 0^ℓ als Kodierung für ein Zeichen aus $A_{\mathcal{P}}$ erlaubt wird. Für $\ell = 2$ und $\text{code}(;) = 00$ erhielte man beispielsweise $\natural(;) = \text{dual}^{-1}(\text{code}(;)) = \text{dual}^{-1}(00) = 0 = \text{dual}^{-1}(0000) = \text{dual}^{-1}(\text{code}(;) \text{code}(;)) = \natural(;;)$.

$$\begin{aligned}
& \natural(\text{code}^{-1}(\alpha_1) \dots \text{code}^{-1}(\alpha_k)) \\
&= \text{dual}^{-1}(\text{code}(\text{code}^{-1}(\alpha_1)) \oplus \dots \oplus \text{code}(\text{code}^{-1}(\alpha_k))) \quad (\text{mit (4.3)}) \\
&= \text{dual}^{-1}(\alpha_1 \oplus \dots \oplus \alpha_k) \\
&= \text{dual}^{-1}(\text{dual}_\ell(n)) \\
&= n \quad (\text{mit Lemma 4.12(1.)}) .
\end{aligned} \tag{4.4}$$

Für $\natural(n) \neq 1$ gilt $\text{parse}(\alpha_1 \oplus \dots \oplus \alpha_k) = 0$, wobei $\alpha_1 \oplus \dots \oplus \alpha_k = \text{dual}_\ell(n)$ und $\alpha_i \in \{0,1\}^\ell$ für jedes α_i gilt. Falls $\alpha_i \notin \text{Bild}(\text{code})$ für ein $i \in \{1, \dots, k\}$, so gilt $n \notin \natural\mathcal{P}$ wegen (4.3). Andernfalls gilt $\text{code}^{-1}(\alpha_1) \dots \text{code}^{-1}(\alpha_k) \notin \mathcal{P}$ mit der Definition von parse , und folglich $n \notin \natural\mathcal{P}$ mit (4.4). Damit sind die Forderungen erfüllt, die an \natural ? gestellt werden.

(4) “ $\natural^{-1} : \text{Bild}(\natural) \rightarrow \mathcal{P}$ ist algorithmisch”: Mit dual_ℓ kann jede natürliche Zahl n algorithmisch in ihre Dualzahldarstellung $\alpha_1 \oplus \dots \oplus \alpha_k$ überführt werden. Das Bitwort $\alpha_1 \oplus \dots \oplus \alpha_k$ bearbeitet man jetzt in ℓ -Bit Abständen von links nach rechts und ersetzt dabei mittels der Kodetabelle jedes ℓ -Bit Wort α_i durch $\text{code}^{-1}(\alpha_i)$. Dies gelingt, denn mit $n \in \natural\mathcal{P}$ gilt $\alpha_i \in \text{Bild}(\text{code})$ für jedes α_i . Auch dieses Verfahren ist algorithmisch, und damit ist \natural^{-1} mit $\natural^{-1}(n) := \text{code}^{-1}(\alpha_1) \dots \text{code}^{-1}(\alpha_k)$ auch algorithmisch. ■

Da die Programmkodierungsfunktion \natural injektiv ist, gilt $P = P'$ falls $\natural P = \natural P'$ für je zwei Programme $P, P' \in \mathcal{P}$. Damit werden *verschiedenen Programmen* durch \natural *verschiedene Codes* zugeordnet. Die Programmkodierungsfunktion \natural ist jedoch nicht *surjektiv*, d.h. es gibt natürliche Zahlen n mit $\natural P \neq n$ für alle $P \in \mathcal{P}$, und damit gilt $\natural\mathcal{P} \subsetneq \mathbb{N}$. Dies ist einleuchtend, denn andernfalls würde ja *jedes* Bitwort ein Programm repräsentieren.¹¹ Für eine beliebige natürliche Zahl n können wir jedoch mit \natural ? feststellen, ob n der Code eines Programms ist, d.h. ob $n = \natural P$ für ein $P \in \mathcal{P}$ gilt.

¹¹ Insbesondere wäre dann jedes ℓ -Bitwort die Kodierung eines Zeichens aus $A_{\mathcal{P}}$, und damit wäre jedes Wort aus $A_{\mathcal{P}}^+$ ein syntaktisch korrektes \mathcal{P} -Programm.

5. ALGORITHMISCH UNLÖSBARE AUFGABEN

5.1. Abzählbarkeit der \mathcal{P} -berechenbaren Funktionen

Mit Hilfe der Codes von \mathcal{P} -Programmen können wir eine wichtige Eigenschaft der \mathcal{P} -berechenbaren Funktionen beweisen, nämlich die *Abzählbarkeit* der Menge $[[\mathcal{P}]]$ aller \mathcal{P} -berechenbaren Funktionen. Zum Nachweis definieren wir zunächst:

Definition 5.1.

Für jedes $i \in \mathbb{N}$ ist die Funktion $\varphi_i : \mathbb{N} \mapsto \mathbb{N}$ definiert durch

$$\varphi_i := \begin{cases} [[P]] & , \text{ falls } i = \natural P \text{ für ein } P \in \mathcal{P} \\ \omega & , \text{ falls } i \notin \natural \mathcal{P} . \quad \blacksquare \end{cases}$$

Für $i \in \natural \mathcal{P}$ ist φ_i also diejenige Funktion, die von dem \mathcal{P} -Programm mit Kode i berechnet wird. Also gilt $\varphi_{\natural P} = [[P]]$ für jedes Programm $P \in \mathcal{P}$. Falls $i \notin \natural \mathcal{P}$, so ordnen wir i die überall undefinierte Funktion zu, d.h. es gilt dann $\varphi_i = \omega$. Man beachte, daß φ_i *wohldefiniert* ist, denn mit der Injektivität von \natural (vgl. Satz 4.13) gibt es *höchstens* ein Programm P mit $\natural P = i$, und mit Satz 4.10 dürfen wir annehmen, daß $[[P]] : \mathbb{N} \mapsto \mathbb{N}$ für jedes Programm $P \in \mathcal{P}$ gilt.

Nun können wir die Abzählbarkeit aller \mathcal{P} -berechenbaren Funktionen einfach beweisen:

Satz 5.2. $[[\mathcal{P}]] = \{\varphi_i \mid i \in \mathbb{N}\}$, d.h. $[[\mathcal{P}]]$ ist abzählbar.

Beweis. “ \subseteq ” Sei $\phi \in [[\mathcal{P}]]$. Dann gilt $\phi = [[P]]$ für ein $P \in \mathcal{P}$ und damit $\phi = \varphi_{\natural P}$. Also gilt $\phi \in \{\varphi_i \mid i \in \mathbb{N}\}$, denn $\natural P \in \mathbb{N}$.

“ \supseteq ” Falls $i \notin \natural \mathcal{P}$, so gilt $\varphi_i = \omega = [[\text{CYCLE}_1]]$ mit Satz 3.2, und mit $\text{CYCLE}_1 \in \mathcal{P}$ dann $\varphi_i \in [[\mathcal{P}]]$. Andernfalls gilt $i = \natural P$ für ein Programm $P \in \mathcal{P}$ und damit $\varphi_{\natural P} = [[P]]$, also ebenfalls $\varphi_i \in [[\mathcal{P}]]$. ■

Wesentlich im Beweis von Satz 5.2 ist, daß den \mathcal{P} -berechenbaren Funktionen ein Programm zugeordnet werden kann und Programme in natürliche Zahlen *kodiert* werden können, woraus dann die Abzählbarkeit von \mathcal{P} folgt. Die folgenden Sätze zeigen, daß der Beweis von Satz 5.2 ohne diese Voraussetzungen nicht gelingt:

Satz 5.3. Sei N eine abzählbare Menge, d.h. $N = \{n_i \mid i \in \mathbb{N}\}$, und sei $M \subseteq N$. Dann ist M abzählbar.

Beweis. Für $M = \emptyset$ gilt die Aussage trivialerweise. Für $M \neq \emptyset$ sei $m' \in M$ fest gewählt. Wir definieren für jedes $i \in \mathbb{N}$

$$m_i := \begin{cases} n_i & , \text{ falls } n_i \in M \\ m' & , \text{ falls } n_i \notin M . \end{cases}$$

Mit $M \subseteq N$ gibt es für jedes $m \in M$ ein $i \in \mathbb{N}$ mit $m = n_i$, und damit gilt $m_i = m$, d.h. $M = \{m_i \mid i \in \mathbb{N}\}$. ■

Mit Satz 5.3 ist also jede Teilmenge einer abzählbaren Menge auch abzählbar. Umgekehrt bedeutet dies, daß jede Obermenge einer nicht-abzählbaren Menge auch nicht abzählbar ist. Wir geben jetzt eine nicht-abzählbare Menge von Funktionen an.

Satz 5.4. Sei \mathcal{F}_{tot} die Menge aller totalen Funktionen $\mathbb{N} \rightarrow \mathbb{N}$. Dann ist \mathcal{F}_{tot} nicht abzählbar.

Beweis. Wir nehmen an, daß \mathcal{F}_{tot} abzählbar ist, und leiten daraus mit einem sogenannten Diagonalisierungsbeweis einen Widerspruch her: Mit der Annahme gilt $\mathcal{F}_{tot} = \{\phi_i \mid i \in \mathbb{N}\}$ und $\gamma \in \mathcal{F}_{tot}$ für die Funktion $\gamma : \mathbb{N} \rightarrow \mathbb{N}$ mit $\gamma(n) := \phi_n(n) + 1$. Mit $\gamma \in \mathcal{F}_{tot}$ gilt $\gamma = \phi_k$ für ein $k \in \mathbb{N}$, und man erhält $\phi_k(k) = \gamma(k) = \phi_k(k) + 1$. Also muß $\phi_k(k) = \perp$ gelten, d.h. $\phi_k \notin \mathcal{F}_{tot}$. ▼ Damit kann \mathcal{F}_{tot} nicht abzählbar sein. ■

Mit Satz 5.4 können wir jetzt zeigen, daß die Menge *aller* arithmetischen Funktionen auch nicht abzählbar ist:

Satz 5.5. Sei \mathcal{F} die Menge aller Funktionen $\mathbb{N} \mapsto \mathbb{N}$. Dann ist \mathcal{F} nicht abzählbar.

Beweis. Wir führen einen Widerspruchsbeweis und nehmen an, daß \mathcal{F} abzählbar ist. Mit Satz 5.3 und $\mathcal{F}_{tot} \subseteq \mathcal{F}$ gilt dann, daß \mathcal{F}_{tot} abzählbar ist, also ein Widerspruch zu Satz 5.4. Damit kann \mathcal{F} nicht abzählbar sein. ■

Man beachte, daß Satz 5.5 nicht im Widerspruch zu Satz 5.2 steht, denn Satz 5.2 macht nur eine Aussage über *berechenbare* Funktionen, während Satz 5.5 eine Aussage über *alle* (arithmetischen) Funktionen macht. Entscheidend ist hier also die Forderung nach *Berechenbarkeit*.

5.2. Nicht-berechenbare Funktionen

Mit der Abzählbarkeit der \mathcal{P} -berechenbaren Funktionen können wir jetzt ein zentrales Ergebnis der Berechenbarkeitstheorie beweisen, nämlich daß es Aufgaben gibt, die prinzipiell *nicht algorithmisch lösbar* sind. D.h. es gibt Aufgaben, deren Lösung nicht durch einen Rechner berechnet werden kann. Formal heißt das, daß es *nicht-berechenbare Funktionen* gibt:

Korollar 5.6. *Es gibt eine Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$ mit $\phi \notin \llbracket \mathcal{P} \rrbracket$.*

Beweis. *Es gilt $\llbracket \mathcal{P} \rrbracket \subseteq \mathcal{F}$ für die Menge \mathcal{F} aller Funktionen $\phi : \mathbb{N} \mapsto \mathbb{N}$, mit Satz 5.2 ist $\llbracket \mathcal{P} \rrbracket$ abzählbar und mit Satz 5.5 ist \mathcal{F} nicht abzählbar. Damit gilt $\mathcal{F} \setminus \llbracket \mathcal{P} \rrbracket \neq \emptyset$. ■*

Der Beweis von Korollar 5.6 ist unkonstruktiv, vgl. Abschnitt 3.3, d.h. eine konkrete nicht-berechenbare Funktion wird in dem Beweis nicht angegeben. Dies holen wir jetzt nach:

Definition 5.7. (Selbstanwendungsfunktion)

Die Selbstanwendungsfunktion $self : \mathbb{N} \rightarrow \mathbb{N}$ ist definiert durch

$$self(n) := \begin{cases} 0 & , \text{ falls } \varphi_n(n) = \perp \\ 1 & , \text{ falls } \varphi_n(n) \neq \perp . \quad \blacksquare \end{cases}$$

Untersuchen wir zunächst, welche Ergebnisse die Funktion $self$ liefert: Für $n \notin \natural\mathcal{P}$ gilt $\varphi_n = \omega$, folglich $\varphi_n(n) = \perp$, und damit $self(n) = 0$. Andernfalls gilt $\varphi_n = \llbracket P \rrbracket$ für ein $P \in \mathcal{P}$, wobei $n = \natural P$. Um $self(n)$ zu bestimmen, führen wir das Programm P mit der Eingabe $\natural P$ aus, d.h. wir wenden P auf seinen eigenen Programmcode $\natural P$ an. Hält P mit dieser Eingabe, so gilt $\varphi_n(n) \neq \perp$ und damit $self(n) = 1$. Andernfalls erhalten wir $self(n) = 0$. Es gilt also

$$self(\natural P) = \begin{cases} 0 & , \text{ falls } \llbracket P \rrbracket(\natural P) = \perp \\ 1 & , \text{ falls } \llbracket P \rrbracket(\natural P) \neq \perp . \end{cases}$$

Wir zeigen jetzt, daß die Selbstanwendungsfunktion nicht berechenbar ist. Dazu führen wir einen Widerspruchsbeweis, d.h. wir nehmen an, $self$ sei berechenbar, und leiten daraus dann einen Widerspruch her.

Satz 5.8. Die Selbstanwendungsfunktion $self : \mathbb{N} \rightarrow \mathbb{N}$ ist nicht berechenbar.

Beweis. Angenommen, $self$ sei berechenbar. Dann gibt es eine \mathcal{P} -Prozedur $SELF$ mit $self = \llbracket SELF \rrbracket$. Mit $SELF$ konstruieren wir jetzt eine weitere \mathcal{P} -Prozedur $KURIOS$:

```

procedure KURIOS(n) <=
begin var x, res;
  if SELF(n) then x := CYCLE1(x) end_if;
  res := 1;
  return(res)
end .

```

Es gilt

$$\llbracket KURIOS \rrbracket(n) = \begin{cases} 1 & , \text{ falls } self(n) = 0 \\ \perp & , \text{ falls } self(n) \neq 0 , \end{cases}$$

und mit der Definition von $self$ erhält man

$$\llbracket KURIOS \rrbracket(n) = \begin{cases} 1 & , \text{ falls } \varphi_n(n) = \perp \\ \perp & , \text{ falls } \varphi_n(n) \neq \perp . \end{cases}$$

Für $n = \natural KURIOS$ erhalten wir insbesondere

$$\llbracket KURIOS \rrbracket(\natural KURIOS) = \begin{cases} 1 & , \text{ falls } \llbracket KURIOS \rrbracket(\natural KURIOS) = \perp \\ \perp & , \text{ falls } \llbracket KURIOS \rrbracket(\natural KURIOS) \neq \perp . \end{cases}$$

Damit haben wir einen Widerspruch hergeleitet, denn es gilt $\llbracket KURIOS \rrbracket(\natural KURIOS) = \perp$ gdw. $\llbracket KURIOS \rrbracket(\natural KURIOS) \neq \perp$. Die Anwendung der Prozedur $KURIOS$ auf ihre eigene Kodierung $\natural KURIOS$ führt also zu einem Widerspruch, und damit kann $self$ keine berechenbare Funktion sein. ■

Der Nachweis, daß $self$ nicht berechenbar ist, erscheint zunächst wie ein mathematisches “Kunststück”. Die Schritte der Herleitung sind einfach nachvollziehbar, weniger einleuchtend ist jedoch, wie man auf die gewählte Konstruktion eigentlich kommt, und *warum* sich daraus ein Widerspruch ergibt. Es ist daher zum Verständnis wichtig, daß man sich die Argumentationsweise und die dabei verwendeten Fakten noch einmal genau vor Augen führt:

1. Mit der Behauptung, daß $self$ berechenbar sei, dürfen wir die Existenz des Programms $SELF$ voraussetzen.

2. Unter Verwendung von `SELF` und dem Programm `CYCLE1` können wir ein weiteres Programm, nämlich `KURIOS`, angeben.
3. Mit der Definition von `KURIOS` erhalten wir eine berechenbare Funktion, nämlich $\llbracket \text{KURIOS} \rrbracket$.
4. $\llbracket \text{KURIOS} \rrbracket(n)$ ist insbesondere dann definiert, wenn n der Kode eines Programms P ist, also $n = \natural P$, und P aufgerufen mit $\natural P$ nicht terminiert.
5. Damit terminiert `KURIOS` insbesondere dann, wenn `KURIOS` mit dem Kode $\natural P$ eines Programms P aufgerufen wird, und P aufgerufen mit $\natural P$ *nicht* terminiert.
6. Folglich terminiert `KURIOS` aufgerufen mit $\natural \text{KURIOS}$ insbesondere dann, wenn `KURIOS` aufgerufen mit $\natural \text{KURIOS}$ *nicht* terminiert. ▼
7. Der Widerspruch entsteht also dadurch, daß wir die Existenz des Programms `SELF` annehmen, $\varphi_n(n) = \perp$ jedoch (für beliebige n) nicht durch einen Algorithmus festgestellt werden kann.

5.3. Das Halteproblem

Die nicht berechenbare Selbstanwendungsfunktion *self* mutet zunächst wenig nützlich an, und man fragt sich unwillkürlich, ob es auch "sinnvolle" Funktionen gibt, die nicht berechenbar sind.

Jeder Programmierer hat schon die leidvolle Erfahrung gemacht, daß sein Programm nicht terminiert. Üblicherweise wird ein Programm mit gewissen Eingaben getestet. Erhält man ein Resultat, so ist der Terminierungstest bestanden. Andernfalls gibt es zwei Möglichkeiten: Entweder terminiert das Programm mit der Eingabe nicht, oder aber es dauert nur etwas länger, bis ein Ergebnis berechnet ist. Es ist daher wünschenswert, ein Testwerkzeug `HALT` zu entwickeln, das als Eingabe den Kode $\natural P$ eines Programms P sowie eine Eingabe $m \in \mathbb{N}$ für dieses Programm erhält. Bei Ausführung von `HALT` soll nach endlicher Zeit 0 ausgegeben werden, wenn die Ausführung von P mit m nicht terminiert. Andernfalls soll `HALT` das Ergebnis 1 ausgeben.

Bevor wir `HALT` entwickeln, betrachten wir vorsichtshalber die von `HALT` berechnete Funktion. Dabei müssen wir feststellen, daß es kein Programm `HALT` mit den gewünschten Eigenschaften geben kann:

Satz 5.9. Die Haltefunktion $halt : \mathbb{N} \rightarrow \mathbb{N}$, gegeben durch

$$halt(\pi^2(i, n)) := \begin{cases} 0 & , \text{ falls } \varphi_i(n) = \perp \\ 1 & , \text{ falls } \varphi_i(n) \neq \perp , \end{cases}$$

ist nicht berechenbar.¹

Beweis. Wir führen einen Widerspruchsbeweis und nehmen an, daß es ein \mathcal{P} -Programm $HALT$ mit $\llbracket HALT \rrbracket = halt$ gibt. Mit $HALT$ können wir auch das \mathcal{P} -Programm

```

procedure PROG(x) <=
begin var y;
  y := HALT(PAIR2(x, x));
  return(y)
end

```

definieren. Es gilt $\llbracket PROG \rrbracket(n) = \llbracket HALT \rrbracket(\pi^2(n, n))$, und mit der Definition von $halt$ erhält man

$$\llbracket PROG \rrbracket(n) = \begin{cases} 0 & , \text{ falls } \varphi_n(n) = \perp \\ 1 & , \text{ falls } \varphi_n(n) \neq \perp , \end{cases}$$

also $\llbracket PROG \rrbracket = self$, vgl. Definition 5.7. Mit Satz 5.8 ist $\llbracket PROG \rrbracket$ nicht berechenbar, und damit kann es kein \mathcal{P} -Programm $HALT$ mit $\llbracket HALT \rrbracket = halt$ geben. ■

Mit Satz 5.9 ist es also prinzipiell unmöglich, das gewünschte Testwerkzeug $HALT$ zu implementieren. Ursache ist, daß man für ein beliebiges Programm P und beliebige Eingaben m für dieses Programm nicht algorithmisch feststellen kann, ob P ausgeführt mit m nicht hält.²

¹ Siehe Abschnitt 4.3 zur Bedeutung der Schreibweise $halt(\pi^2(i, n)) := \dots$.

² Ob ein Programm P mit Eingabe m hält kann dagegen offenbar algorithmisch ermittelt werden – man läßt P einfach “laufen” und falls P hält, ist das ja feststellbar (etwa durch Anzeige eines Ergebnisses). Genau dieser Idee werden wir später – etwa im Beweis von Satz 7.11 – folgen.

6. UNIVERSELLE FUNKTION UND INTERPRETIERER

In Abschnitt 5.1 wurde mit Satz 5.2 gezeigt, daß die Menge aller \mathcal{P} -berechenbaren Funktionen abzählbar ist, d.h. $\llbracket \mathcal{P} \rrbracket = \{\varphi_i \mid i \in \mathbb{N}\}$. Damit können wir definieren:

Definition 6.1. (Universelle Funktion)

Die universelle Funktion $u_{\mathcal{P}} : \mathbb{N} \mapsto \mathbb{N}$ ist gegeben durch

$$u_{\mathcal{P}}(\pi^2(i, n)) := \varphi_i(n). \quad \blacksquare$$

Die Funktion $u_{\mathcal{P}}$ wird *universell* genannt, da mit $u_{\mathcal{P}}$ jede Funktion $\varphi_i \in \llbracket \mathcal{P} \rrbracket$ dargestellt werden kann. Mit $\varphi_{\natural P} = \llbracket P \rrbracket$, vgl. Definition 5.1, erhält man

$$u_{\mathcal{P}}(\pi^2(\natural P, n)) = \llbracket P \rrbracket(n) \quad (6.1)$$

und für die Prozedur

```
procedure P(x) <=
begin var y1, ..., yn; STA; return(yi) end
```

mit Definition 2.8 dann

$$u_{\mathcal{P}}(\pi^2(\natural P, n)) = \text{value}(\text{eval}(M_P^{(n)}, \text{STA}), y_i) . \quad (6.2)$$

Wegen (6.2) wird $u_{\mathcal{P}}$ auch der *Interpreter* der Programmiersprache \mathcal{P} genannt.

Wir überlegen jetzt, ob die Funktion $u_{\mathcal{P}}$ \mathcal{P} -berechenbar ist: Um $u_{\mathcal{P}}(\pi^2(i, n))$ zu berechnen, muß zuerst festgestellt werden, ob $i \in \natural \mathcal{P}$ gilt. Dies gelingt mit der \mathcal{P} -berechenbaren Funktion $\natural?$, vgl. Satz 4.13. Mit $i = \natural P$ für ein $P \in \mathcal{P}$ erhält man $u_{\mathcal{P}}(\pi^2(\natural P, n))$, indem man aus $\natural P$ das \mathcal{P} -Programm P bildet, also den Programmcode $\natural P$ mittels \natural^{-1} in das \mathcal{P} -Programm P *dekodiert*, und dann P auf n anwendet, vgl. (6.1). Andernfalls gilt $\varphi_i = \omega$ und damit $u_{\mathcal{P}}(\pi^2(i, n)) = \llbracket \text{CYCLE}_1 \rrbracket(n)$.

Damit ist $u_{\mathcal{P}}$ \mathcal{P} -berechenbar und folglich dürfen wir die Existenz eines $\mathcal{P}[1]$ -Programms `APPLY` mit

$$u_{\mathcal{P}}(m) = \llbracket \text{APPLY} \rrbracket(m) \quad (6.3)$$

annehmen, für das $\llbracket \text{APPLY} \rrbracket(\pi^2(\natural P, n)) = \llbracket P \rrbracket(n)$ gilt. Das \mathcal{P} -Programm `APPLY` überprüft bei Eingabe m mittels $\natural?$, ob $\pi_1^2(m)$ der Kode eines \mathcal{P} -Programms P ist. Im positiven Fall wird dann P mit $\pi_2^2(m)$ als Eingabe ausgeführt. Für $\pi_1^2(m) \notin \natural\mathcal{P}$ ruft `APPLY` die \mathcal{P} -Prozedur `CYCLE1` auf, d.h. der Aufruf `APPLY(m)` terminiert in diesem Fall nicht. Damit *implementiert* `APPLY` den Interpretierer der Programmiersprache \mathcal{P} . Mit dem Interpretierer `APPLY` können wir \mathcal{P} -Programme P , die als Daten $\natural P$ repräsentiert werden, *durch ein \mathcal{P} -Programm* ausführen.

Bemerkung 6.2. Den Nachweis, daß $u_{\mathcal{P}}$ \mathcal{P} -berechenbar ist, haben wir hier nur informell geführt. Eigentlich müßte diese Behauptung mit einem streng formalen Beweis nachgewiesen werden, und zwar indem `APPLY` konkret angegeben und damit dann (6.3) bewiesen wird. Wir verzichten darauf, da dies hier einen zu großen beweistechnischen Aufwand erfordert.

Bemerkung 6.3. Als `APPLY` kann man sich genauso gut ein Programm vorstellen, das als Eingabe eine endliche Folge $a_1 \dots a_n$ von ASCII Zeichen erhält, feststellt, ob $a_1 \dots a_n$ ein \mathcal{P} -Programm P nach Definition 2.1 ist, im positiven Fall P ausführt, und im negativen Fall nicht terminiert. Dies ist natürlich unpraktisch, denn man erwartet sinnvollerweise bei Ausführungsversuch eines vermeintlichen \mathcal{P} -Programms mit syntaktischen Fehlern, wie etwa falsche Klammerung, nicht-deklarierte lokale Variable u.s.w., einen Hinweis des Rechners anstatt eine Endlosberechnung. Sinnvoller wäre also ein $\mathcal{P}[1]$ -Programm `APPLY'` mit

$$\llbracket \text{APPLY}' \rrbracket(m) = \begin{cases} 0 & , \text{ falls } \pi_1^2(m) \notin \natural\mathcal{P} \\ 1 + \llbracket P \rrbracket(\pi_2^2(m)) & , \text{ falls } \pi_1^2(m) = \natural P \end{cases}$$

d.h. `APPLY'` hält bei Eingabe “fehlerhafter” \mathcal{P} -Programme immer mit Ergebnis 0 und bei Eingabe “korrekter” \mathcal{P} -Programme P mit $\llbracket P \rrbracket(\pi_2^2(m)) + 1$, falls die Ausführung von P terminiert. Da solch “praktische” Erwägungen für unsere Untersuchungen jedoch belanglos sind, reicht uns die Definition von `APPLY` so wie in (6.3) angegeben.

7. ENTSCHEIDBARKEIT UND SEMI-ENTSCHEIDBARKEIT

7.1. Entscheidbare Probleme

Die Frage aus Abschnitt 5.3, ob ein beliebiges Programm P ausgeführt mit einer beliebigen Eingabe $m \in \mathbb{N}$ anhält oder nicht, wird das *Halteproblem* genannt. Allgemein formulieren wir Probleme, die durch einen Rechner gelöst werden sollen, wie folgt:

Sei $M \subseteq \mathbb{N}$ und sei $m \in \mathbb{N}$. Das gestellte Problem besteht dann darin festzustellen, ob “ $m \in M$ ” wahr oder falsch ist. Das Halteproblem H kann man jetzt durch

$$H := \{\pi^2(n, m) \in \mathbb{N} \mid \varphi_n(m) \neq \perp\}$$

formulieren. Für beliebige $n, m \in \mathbb{N}$ soll hier festgestellt werden, ob “ $\pi^2(n, m) \in H$ ” wahr oder falsch ist.

Die Aufgabe $\varphi_n(n) \neq \perp$ festzustellen, vgl. Abschnitt 5.2, nennt man auch das *Selbstanwendbarkeitsproblem* (oder das *spezielle Halteproblem*) S , das man durch

$$S := \{n \in \mathbb{N} \mid \varphi_n(n) \neq \perp\}$$

formulieren kann. Für beliebige $n \in \mathbb{N}$ soll dabei festgestellt werden, ob “ $n \in S$ ” wahr oder falsch ist.

Die Antwort auf die Frage “ $m \in M$?” wollen wir natürlich berechnen lassen, und allgemein untersuchen wir Probleme daraufhin, ob sie durch einen Rechner gelöst werden können oder nicht. Ein Problem, wie z.B. das Halteproblem, nennen wir im folgenden *entscheidbar*, wenn ein Rechner immer – also in endlicher Zeit – eine korrekte Antwort liefern kann. Wir definieren daher:

Definition 7.1. (Entscheidbare Menge, charakteristische Funktion)

Sei $M \subseteq \mathbb{N}$ und sei $\chi_M : \mathbb{N} \rightarrow \{0, 1\}$ mit

$$\chi_M(m) := \begin{cases} 0 & , \text{ falls } m \notin M \\ 1 & , \text{ falls } m \in M . \end{cases}$$

Dann ist M entscheidbar genau dann, wenn χ_M berechenbar ist. Die Funktion χ_M wird die charakteristische Funktion von M genannt. Ein \mathcal{P} -Programm PROG mit $\chi_M = \llbracket \text{PROG} \rrbracket$ wird ein Entscheidungsverfahren für M genannt.¹ ■

Das Halteproblem ist genau dann entscheidbar, wenn die charakteristische Funktion $\chi_H : \mathbb{N} \rightarrow \{0, 1\}$ berechenbar ist. Mit der Definition von H erhalten wir

$$\chi_H(\pi^2(n, m)) = \begin{cases} 0 & , \text{ falls } \varphi_n(m) = \perp \\ 1 & , \text{ falls } \varphi_n(m) \neq \perp . \end{cases}$$

Da $\chi_H = \text{halt}$ für die nicht-berechenbare Funktion halt aus Satz 5.9 gilt, ist H nicht entscheidbar. Man erhält also:

Korollar 7.2. *Das Halteproblem H ist nicht entscheidbar.*

Mit Satz 5.8 ist auch die Selbstanwendungsfunktion self nicht berechenbar, und damit gilt:

Korollar 7.3. *Das Selbstanwendbarkeitsproblem S ist nicht entscheidbar.*

Betrachten wir ein weiteres Problem: Ist entscheidbar, ob eine natürliche Zahl eine Primzahl ist? Um dies zu beantworten, betrachten wir die charakteristische Funktion $\chi_{\mathbb{P}} : \mathbb{N} \rightarrow \{0, 1\}$ für die Menge \mathbb{P} aller Primzahlen

$$\chi_{\mathbb{P}}(n) = \begin{cases} 0 & , \text{ falls } n \notin \mathbb{P} \\ 1 & , \text{ falls } n \in \mathbb{P} . \end{cases}$$

Da wir offensichtlich ein Programm $\text{PRIM} \in \mathcal{P}[1]$ mit $\chi_{\mathbb{P}} = \llbracket \text{PRIM} \rrbracket$ angeben können, ist die Menge aller Primzahlen entscheidbar.

Die Entscheidbarkeit von Problemen überträgt sich auf deren Vereinigung und Schnitt:

Satz 7.4. *Für $M_1, M_2 \subseteq \mathbb{N}$ sind $M_1 \cup M_2$ und $M_1 \cap M_2$ entscheidbar, falls M_1 und M_2 entscheidbar sind.*

¹ In der englischsprachigen Literatur wird neben “decidable” auch der Begriff “recursive” für “entscheidbar” verwendet. Es gibt also sowohl “recursive functions” als auch “recursive problems” (s. auch die Fußnote auf Seite 26).

Beweis. Seien DECIDE_M_1 , DECIDE_M_2 \mathcal{P} -Prozeduren mit $\llbracket \text{DECIDE_M}_1 \rrbracket = \chi_{M_1}$ und $\llbracket \text{DECIDE_M}_2 \rrbracket = \chi_{M_2}$, und seien die Prozeduren $\text{DECIDE_M}_1 \cup \text{M}_2$, $\text{DECIDE_M}_1 \cap \text{M}_2 \in \mathcal{P}$ gegeben durch

```

procedure DECIDE_M1 ∪ M2(x) <=
begin var res;
  if DECIDE_M1(x) then res := 1 else res := DECIDE_M2(x) end_if;
  return(res)
end

```

und

```

procedure DECIDE_M1 ∩ M2(x) <=
begin var res;
  if DECIDE_M1(x) then res := DECIDE_M2(x) else res := 0 end_if;
  return(res)
end .

```

Dann gilt offensichtlich $\llbracket \text{DECIDE_M}_1 \cup \text{M}_2 \rrbracket = \chi_{M_1 \cup M_2}$ sowie $\llbracket \text{DECIDE_M}_1 \cap \text{M}_2 \rrbracket = \chi_{M_1 \cap M_2}$, und damit sind sowohl $M_1 \cup M_2$ als auch $M_1 \cap M_2$ entscheidbar. ■

7.2. Endliche Probleme

Eine Konsequenz von Definition 7.1 ist, daß *endliche* Probleme immer entscheidbar sind:

Satz 7.5. $M \subseteq \mathbb{N}$ mit $|M| < \infty$ ist entscheidbar.

Beweis. Für $M = \emptyset$ ist $\chi_M : \mathbb{N} \rightarrow \{0, 1\}$ mit $\chi_M(m) := 0$ für alle $m \in \mathbb{N}$ die charakteristische Funktion von M , und offenbar ist χ_M berechenbar.

Andernfalls gilt $M = \{m_0, \dots, m_n\}$ für gewisse $m_0, \dots, m_n \in \mathbb{N}$ und damit gilt $\llbracket \text{DECIDE_M} \rrbracket = \chi_M$ für die \mathcal{P} -Prozedur DECIDE_M aus Abbildung 7.1. Folglich ist M entscheidbar. ■

Der Beweis von Satz 7.5 ist *nicht konstruktiv*, vgl. Abschnitt 3.3, denn die Elemente m_0, \dots, m_n von M müssen ja nicht bekannt sein. Beispielsweise folgt aus Satz 7.5, daß das Problem

$$H_{<10^{10}} := \{\pi^2(n, m) \in \mathbb{N} \mid n, m < 10^{10} \text{ und } \varphi_n(m) \neq \perp\}$$

entscheidbar ist, denn $H_{<10^{10}} \subseteq H$ ist endlich. Wie folgende Überlegung zeigt, ist $H_{<10^{10}}$ entscheidbar, auch wenn wir die Elemente von $H_{<10^{10}}$ nicht kennen:

```

procedure DECIDE_M(x) <=
begin var res;
  case x of
    m0: res := 1
    m2: res := 1
    ...
    mn: res := 1
  other: res := 0
end_case;
return(res)
end .

```

Abbildung 7.1: Ein Entscheidungsverfahren für eine endliche Menge

Allgemein gibt es für jedes $k \in \mathbb{N}$ 2^{k^2} Teilmengen N von \mathbb{N} , so daß $\pi_1^2(j), \pi_2^2(j) < k$ für jedes $j \in N$ gilt, und es gilt $N = H_{<k}$ für genau eine dieser Teilmengen. Jede dieser Teilmengen N ist endlich, wobei wir alle Elemente von N *kennen*, und wir können daher wie im Beweis von Satz 7.5 für jedes N ein Programm `DECIDE_M` schreiben, das die charakteristische Funktion χ_N von N berechnet. Unter den endlich vielen, nämlich 2^{k^2} Programmen, befindet sich dann auch das Programm, das die charakteristische Funktion von $H_{<k}$ berechnet. Wir können also tatsächlich ein Programm angeben, mit dem $H_{<k}$ entschieden werden kann, wir wissen nur nicht, welches der 2^{k^2} Programme das Gewünschte leistet, vgl. Abschnitt 3.3.

7.3. Semi-entscheidbare Probleme

Da *Probleme* in unserem Zusammenhang mittels *Mengen* definiert werden, können wir auch das Komplement solcher Mengen betrachten. Für das Halteproblem erhalten wir beispielsweise das komplementäre Problem

$$\overline{H} = \{ \pi^2(n, m) \in \mathbb{N} \mid \varphi_n(m) = \perp \} .$$

Offensichtlich ist auch \overline{H} nicht entscheidbar, denn $\pi^2(n, m) \in \overline{H}$ gdw. $\pi^2(n, m) \notin H$. Da wir die charakteristische Funktion χ_H mit Hilfe der charakteristischen Funktion $\chi_{\overline{H}}$ bilden können, d.h.

$$\chi_H(\pi^2(n, m)) = \begin{cases} 0 & , \text{ falls } \chi_{\overline{H}}(\pi^2(n, m)) = 1 \\ 1 & , \text{ falls } \chi_{\overline{H}}(\pi^2(n, m)) = 0 , \end{cases}$$

folgt aus der Unentscheidbarkeit von H sofort, daß auch \overline{H} nicht entscheidbar ist. Allgemein gilt:

Satz 7.6. $M \subseteq \mathbb{N}$ ist genau dann entscheidbar, wenn das komplementäre Problem \overline{M} entscheidbar ist.

Beweis. “ \Rightarrow ” Wenn M entscheidbar ist, so gilt $\chi_M = \llbracket \text{DECIDE_M} \rrbracket$ für eine \mathcal{P} -Prozedur DECIDE_M . Für die \mathcal{P} -Prozedur $\text{DECIDE_}\overline{M}$ mit

```

procedure DECIDE_ $\overline{M}$ (x) <=
begin var res;
  if DECIDE_M(x) then res := 0 else res := 1 end_if;
  return(res)
end

```

gilt $\chi_{\overline{M}} = \llbracket \text{DECIDE_}\overline{M} \rrbracket$, und damit ist \overline{M} entscheidbar.

“ \Leftarrow ” Offensichtlich, denn $\overline{\overline{M}} = M$. ■

Mit Satz 7.5 und Satz 7.6 folgt sofort die Entscheidbarkeit kofiniter Mengen:

Korollar 7.7. $M \subseteq \mathbb{N}$ mit $|\overline{M}| < \infty$ ist entscheidbar.

Bezüglich Entscheidbarkeit gibt es also keinen Unterschied zwischen einem Problem und seinem Komplementärproblem. Begnügen wir uns jedoch mit einer schwächeren Forderung, so können wir doch einen Unterschied feststellen.

Für das Halteproblem H erhalten wir immer eine positive Antwort, falls es eine positive Antwort gibt: Für $n, m \in \mathbb{N}$ gibt es ja (mindestens) ein Programm $\text{PROG}_n \in \mathcal{P}$ mit $\varphi_n = \llbracket \text{PROG}_n \rrbracket$. Wir können daher PROG_n mit Eingabe m ausführen. Falls $\pi^2(n, m) \in H$, so gilt $\varphi_n(m) \neq \perp$, d.h. PROG_n ausgeführt mit Eingabe m hält auf jeden Fall mit irgendeinem Ergebnis. Umgekehrt gilt $\pi^2(n, m) \in H$, falls PROG_n ausgeführt mit Eingabe m irgendein Ergebnis liefert.

Anders gesagt, für $n, m \in \mathbb{N}$ starten wir PROG_n mit m und erhalten immer eine korrekte Antwort, falls $\pi^2(n, m) \in H$ gilt. Gilt jedoch $\pi^2(n, m) \notin H$, so erhalten wir i.A. nie eine Antwort. Das ist zugegebenermaßen unbefriedigend, aber mehr kann man nicht erreichen, da H nicht entscheidbar ist.

Probleme, für die zumindest immer eine positive Antwort berechnet werden kann, nennt man *semi-entscheidbar*:

Definition 7.8. (Semi-entscheidbare Menge, semi-charakteristische Funktion)
Für eine Menge $M \subseteq \mathbb{N}$ definieren wir die Funktion $\tilde{\chi}_M : \mathbb{N} \mapsto \{1\}$ durch

$$\tilde{\chi}_M(m) := \begin{cases} \perp & , \text{ falls } m \notin M \\ 1 & , \text{ falls } m \in M . \end{cases}$$

Für eine Funktion $\psi : \mathbb{N} \mapsto \{0, 1\}$ schreiben wir $\psi \cong_M \tilde{\chi}_M$, falls $\psi(m) \neq 1$ für $m \notin M$ und $\psi(m) = 1$ für $m \in M$.

Eine Menge M ist semi-entscheidbar genau dann, wenn eine berechenbare Funktion ψ mit $\psi \cong_M \tilde{\chi}_M$ existiert. Jede solche Funktion ψ wird eine semi-charakteristische Funktion von M genannt. Ein \mathcal{P} -Programm **PROG** mit $\tilde{\chi}_M \cong_M \llbracket \text{PROG} \rrbracket$ wird ein semi-Entscheidungsverfahren für M genannt. ■

Die charakteristische Funktion χ_M eines Problems M erfüllt offenbar die Forderung, die wir an eine *semi*-charakteristische Funktion stellen, und folglich ist jedes entscheidbare Problem auch semi-entscheidbar:

Satz 7.9. Wenn M entscheidbar ist, so ist M auch semi-entscheidbar.

Beweis. Offensichtlich, denn $\chi_M \cong_M \tilde{\chi}_M$ und χ_M ist nach Voraussetzung berechenbar. ■

Im Unterschied zu charakteristischen Funktionen sind semi-charakteristische Funktionen nicht eindeutig bestimmt. Für eine Funktion ψ mit $\psi \cong_M \tilde{\chi}_M$ ist $\psi(m)$ im Fall $m \notin M$ *unterspezifiziert*, d.h. nicht eindeutig festgelegt. Allgemein gilt für $m \notin M$ immer $\psi(m) = 0$ oder $\psi(m) = \perp$ für eine semi-charakteristische Funktion ψ . Mit Satz 7.5 folgt sofort, daß $\psi(m) = \perp$ für unendlich viele $m \in \mathbb{N}$ gelten muß, falls M nicht entscheidbar ist.² Mit der Existenz *irgendeiner* berechenbaren semi-charakteristischen Funktion ist *die* semi-charakteristische Funktion $\tilde{\chi}_M$ jedoch immer berechenbar:

Satz 7.10. $\tilde{\chi}_M$ ist berechenbar, falls M semi-entscheidbar ist.

Beweis. Wenn M semi-entscheidbar ist, so existiert ein semi-Entscheidungsverfahren $\text{PROG} \in \mathcal{P}$, d.h. $\tilde{\chi}_M \cong_M \llbracket \text{PROG} \rrbracket$. Für die \mathcal{P} -Prozedur **SEMI_DECIDE_M** gegeben durch

```

procedure SEMI_DECIDE_M(x) <=
begin var res;
  if PROG(x) then res := 1 else res := CYCLE1(x) end_if;
  return(res)
end

```

² Damit ist natürlich nicht ausgeschlossen, daß bei unentscheidbarem M auch $\psi(m) = 0$ für unendlich viele $m \in \mathbb{N}$ gelten *kann*.

gilt dann

$$\llbracket \text{SEMI_DECIDE_M} \rrbracket(m) = \begin{cases} 1, & \text{falls } \llbracket \text{PROG} \rrbracket(m) = 1 \\ \perp, & \text{falls } \llbracket \text{PROG} \rrbracket(m) = 0 \\ \perp, & \text{falls } \llbracket \text{PROG} \rrbracket(m) = \perp . \end{cases}$$

und damit

$$\llbracket \text{SEMI_DECIDE_M} \rrbracket(m) = \begin{cases} 1 & , \text{ falls } m \in M \\ \perp & , \text{ falls } m \notin M , \end{cases}$$

also $\llbracket \text{SEMI_DECIDE_M} \rrbracket = \tilde{\chi}_M$. ■

Wir können jetzt beweisen, daß das Halteproblem semi-entscheidbar ist:

Satz 7.11. *Das Halteproblem H ist semi-entscheidbar.*

Beweis. Sei $\text{SEMI_DECIDE_H} \in \mathcal{P}$ definiert durch

```

procedure SEMI_DECIDE_H(x) <=
begin var y,z;
  y := 1;
  z := APPLY(x);
  return(y)
end .

```

Dann gilt

$$\llbracket \text{SEMI_DECIDE_H} \rrbracket(\pi^2(n, m)) = \begin{cases} \perp & , \text{ falls } \llbracket \text{APPLY} \rrbracket(\pi^2(n, m)) = \perp \\ 1 & , \text{ falls } \llbracket \text{APPLY} \rrbracket(\pi^2(n, m)) \neq \perp \end{cases}$$

und mit $\llbracket \text{APPLY} \rrbracket(\pi^2(n, m)) = \varphi_n(m)$ dann

$$\llbracket \text{SEMI_DECIDE_H} \rrbracket(\pi^2(n, m)) = \begin{cases} \perp & , \text{ falls } \varphi_n(m) = \perp \\ 1 & , \text{ falls } \varphi_n(m) \neq \perp . \end{cases}$$

Also gilt $\tilde{\chi}_H = \llbracket \text{SEMI_DECIDE_H} \rrbracket$, und damit ist H semi-entscheidbar. ■

Korollar 7.12. *Das Selbstanwendungsproblem S ist semi-entscheidbar.*

Beweis. *Für die \mathcal{P} -Prozedur*

```

procedure SEMI_DECIDE_S(x) <=
begin var y;
  y := SEMI_DECIDE_H(PAIR2(x, x));
  return(y)
end

```

zeigt man leicht $\tilde{\chi}_S = \llbracket \text{SEMI_DECIDE_S} \rrbracket$. ■

Betrachten wir nun das Komplementärproblem \overline{H} : Hier gilt $\varphi_n(m) = \perp$, falls $\pi^2(n, m) \in \overline{H}$, d.h. `APPLY` ausgeführt mit Eingabe $\pi^2(n, m)$ hält *nie* mit einem Ergebnis. Offenbar können wir nicht analog der Konstruktion im Beweis von Satz 7.11 vorgehen, um ein Programm $\text{SEMI_DECIDE_}\overline{H} \in \mathcal{P}$ anzugeben, für das $\tilde{\chi}_{\overline{H}} \cong_{\overline{H}} \llbracket \text{SEMI_DECIDE_}\overline{H} \rrbracket$ gilt.

Damit ist natürlich noch nicht bewiesen, daß \overline{H} nicht semi-entscheidbar ist. Es könnte ja gelingen, ein Programm $\text{SEMI_DECIDE_}\overline{H}$ mit $\llbracket \text{SEMI_DECIDE_}\overline{H} \rrbracket \cong_{\overline{H}} \tilde{\chi}_{\overline{H}}$ auf andere Weise zu definieren. Nehmen wir einmal an, dies gelingt uns tatsächlich. Dann können wir das folgende Experiment durchführen:

Wir besorgen uns 2 Rechner und installieren auf dem einen Rechner das Programm `SEMI_DECIDE_H`, und auf dem anderen Rechner wird `SEMI_DECIDE_}\overline{H}` installiert. Für beliebige $n, m \in \mathbb{N}$ starten wir dann `SEMI_DECIDE_H` mit Eingabe $\pi^2(n, m)$ auf Rechner 1 und `SEMI_DECIDE_}\overline{H}` mit der gleichen Eingabe auf Rechner 2. Gilt $\pi^2(n, m) \in H$, so hält Rechner 1 nach endlicher Zeit mit Ergebnis 1. Gilt jedoch $\pi^2(n, m) \notin H$, so hält Rechner 2 nach endlicher Zeit mit Ergebnis 1. Wir bekommen so immer in endlicher Zeit eine korrekte Antwort für das Halteproblem und haben damit doch noch ein Entscheidungsverfahren für das Halteproblem gefunden. Da dies im Widerspruch zu Satz 7.2 steht, gibt es entweder kein Programm `SEMI_DECIDE_H` (als semi-Entscheidungsverfahren für H) oder kein Programm `SEMI_DECIDE_}\overline{H}` (als semi-Entscheidungsverfahren für \overline{H}). Da wir jedoch mit Satz 7.11 die Existenz von `SEMI_DECIDE_H` nachgewiesen haben, kann es kein Programm `SEMI_DECIDE_}\overline{H}` als semi-Entscheidungsverfahren für \overline{H} geben, und folglich ist \overline{H} nicht semi-entscheidbar.

Nun kann man an der Argumentationsweise kritisieren, daß wir bislang immer nur *einen* Rechner betrachtet haben, wenn wir die Berechenbarkeit einer Funktion bzw. die Entscheidbarkeit eines Problems untersucht haben. In Abschnitt 8.3 werden wir daher ohne Rückgriff auf mehrere Rechner beweisen, daß \overline{H} nicht semi-entscheidbar ist.

8. SCHRITTFUNKTIONEN

8.1. Die Schrittfunktion eines \mathcal{P} -Programms

Das Experiment vom Ende des letzten Abschnitts kann man auch mit einem einzigen Rechner durchführen. Wenn dieser Rechner ein Betriebssystem besitzt, mit dem mehrere Prozesse verwaltet werden können, so starten wir `SEMI_DECIDE_H` und `SEMI_DECIDE_H̄` jeweils als einen eigenen Prozeß. Das Betriebssystem konfigurieren wir so, daß jedem der beiden Prozesse immer abwechselnd eine feste Prozessorzeit zugeordnet wird. Mit dieser Vorgehensweise erhalten wir dann das gleiche Resultat wie zuvor.

Die Grundidee ist hier also, daß die Programme `SEMI_DECIDE_H̄` und `SEMI_DECIDE_H` Schritt für Schritt “verzahnt” abgearbeitet werden. Dies ist erforderlich, denn wir können ja nicht die Programme hintereinander ausführen, also etwa zuerst `SEMI_DECIDE_H̄` und dann `SEMI_DECIDE_H`. Gilt bei dieser Programmreihenfolge $\pi^2(n, m) \in H$, so hält `SEMI_DECIDE_H̄` nicht, und `SEMI_DECIDE_H` wird nie aufgerufen, um $\pi^2(n, m) \in H$ festzustellen.

Die Prozessorzeit, die wir im Beispiel jedem der beiden Prozesse abwechselnd zugeordnet haben, modellieren wir formal mit der *Anzahl der Schritte*, die bei Abarbeitung eines Programms erlaubt sind. Jedes Programm wird ja von einem Rechner “Schritt für Schritt” abgearbeitet. Auf der untersten Maschinenebene besteht ein “Schritt” aus dem *fetch&execute*-Zyklus des Prozessors, bei dem dasjenige Bitwort, auf das der Befehlszähler verweist, aus dem Speicher gelesen, ein Maschinenbefehl gemäß dem gelesenen Bitwort ausgeführt und abschließend der Befehlszähler verändert wird, bevor der nächste *fetch&execute*-Zyklus beginnt.

Man kann einen Abarbeitungsschritt auch auf der Ebene einer höheren Programmiersprache – wie etwa \mathcal{P} – definieren, indem man abstrakt die *Interpretationskosten* eines Programms definiert. Damit kann man dann die Abarbeitung eines Programms durch Angabe einer *Laufzeitbeschränkung*, d.h. durch Angabe einer maximal erlaubten Schrittzahl *kontrollieren*, und so eine *beschränkte Ausführung* von *Programmanweisungen* implementieren. Dabei ist ein realistisches Kostenmaß für unsere Zwecke unerheblich: Da lediglich die Terminierung von Programmausführungen sichergestellt werden muß und nicht-Terminierung nur

bei Ausführung von **while**-Schleifen auftreten kann, reicht es hier die Anzahl der Ausführungen von Schleifenrumpfen zu begrenzen.

Wir realisieren diese Idee durch Angabe einer *totalen* Funktion

$$step : \mathbb{N} \times 2^{\mathbb{N} \times \mathbb{N}} \times statements_P \rightarrow \mathbb{N}$$

mit der die Kosten bei Ausführung von Programmanweisungen bestimmt werden: Für $step(b, M_P, STA)$ erhält man 0 als Ergebnis, falls die initial vorgegebene Laufzeitbeschränkung b nicht ausreicht, um die Programmanweisung STA unter der Speicherbelegung M_P durch *eval* auszuwerten. Andernfalls ist die nach Abarbeitung von STA verbleibende Restschrittzahl das Ergebnis von $step(b, M_P, STA)$, und es gilt dann $b \geq step(b, M_P, STA) > 0$. Da in diesem Fall garantiert ist, daß die gegebene Laufzeitbeschränkung b ausreicht um die Programmanweisung STA durch *eval* auszuführen, ist diese Programmausführung unkritisch, denn eine nicht-terminierende Abarbeitung von STA ist dann ausgeschlossen.

Definition 8.1. (Schrittzählfunktion *step*)

Die Schrittzählfunktion

$$step : \mathbb{N} \times 2^{\mathbb{N} \times \mathbb{N}} \times statements_P \rightarrow \mathbb{N}$$

für Programmanweisungen in \mathcal{P} unter einer Laufzeitbeschränkung $b \in \mathbb{N}$ und einer Speicherbelegung $M_P \subseteq \mathbb{N} \times \mathbb{N}$ ist definiert durch:

- (s1) $step(0, M_P, STA) := 0$,
- (s2) $step(b + 1, M_P, SKIP) := b + 1$,
- (s3) $step(b + 1, M_P, x := EXPR) := b + 1$,
- (s4) $step(b + 1, M_P, \text{if } EXPR \text{ then } STA1 \text{ else } STA2 \text{ end_if})$
 $:= \begin{cases} step(b + 1, M_P, STA1), & \text{falls } value(M_P, EXPR) > 0 \\ step(b + 1, M_P, STA2), & \text{falls } value(M_P, EXPR) = 0, \end{cases}$
- (s5) $step(b + 1, M_P, STA1; STA2) :=$
 $:= step(step(b + 1, M_P, STA1), eval(M_P, STA1), STA2),$
- (s6) $step(b + 1, M_P, \text{while } EXPR \text{ do } STA \text{ end_while})$
 $:= \begin{cases} b + 1, & \text{falls } value(M_P, EXPR) = 0, \\ step(step(b, M_P, STA), & \\ \quad eval(M_P, STA), & \text{, andernfalls} \\ \quad \text{while } EXPR \text{ do } STA \text{ end_while}) . & \end{cases}$ ■

Die beschränkte Ausführung von Programmanweisungen unterscheidet sich von der unbeschränkten Form also lediglich darin, daß die Verarbeitung durch (s1) abbricht, da dann die vorgegebene Schrittzahl erschöpft ist. Der folgende Satz illustriert den Zusammenhang zwischen beschränkter und unbeschränkter Abarbeitung von \mathcal{P} -Programmen:

Satz 8.2. Für alle $P \in \mathcal{P}$, $\text{STA} \in \text{statements}_P$, $M_P \in 2^{\mathbb{N} \times \mathbb{N}}$ und alle $b \in \mathbb{N}$ gilt:

1. $\text{eval}(M_P, \text{STA}) \neq \perp \Leftrightarrow \exists b_0 \in \mathbb{N} \forall b \geq b_0. \text{step}(b, M_P, \text{STA}) > 0$
2. $\text{step}(b, M_P, \text{STA}) > 0 \Leftrightarrow \text{eval}(M_P, \text{STA}) \neq \perp$.

Beweis. Durch strukturelle Induktion über STA. ■

Mit Satz 8.2(1) gibt es für jede unbeschränkte Ausführung einer Programmanweisung STA mit Ergebnis $M'_P \neq \perp$ eine Laufzeitbeschränkung b_0 , so daß $\text{step}(b, M_P, \text{STA})$ mit jeder Laufzeitbeschränkung $\geq b_0$ erfolgreich ist. Umgekehrt gilt mit (2), daß mit $\text{step}(b, M_P, \text{STA}) > 0$ die Abarbeitung von STA durch *eval* gelingt.

Mit Satz 8.2(1) folgt insbesondere, daß *step* monoton ist:

Korollar 8.3. (Monotonie von *step*)

Für alle $P \in \mathcal{P}$, $\text{STA} \in \text{statements}_P$, $M_P \in 2^{\mathbb{N} \times \mathbb{N}}$ und alle $b, b' \in \mathbb{N}$ mit $b \geq b'$ gilt

$$\text{step}(b, M_P, \text{STA}) \geq \text{step}(b', M_P, \text{STA}). \quad \blacksquare$$

Mit Hilfe der beschränkten Abarbeitung können wir jetzt für jedes Programm $P \in \mathcal{P}[k]$ eine Funktion definieren, die für beliebige Argumente n_1, \dots, n_k und eine Laufzeitbeschränkung b angibt, ob die Berechnung von $\llbracket P \rrbracket(n_1, \dots, n_k)$ mit weniger als b Schritten gelingt:

Definition 8.4. (Schrittfunktion eines \mathcal{P} -Programms)

Für ein \mathcal{P} -Programm

```

procedure P( $x_1, \dots, x_k$ ) <=
begin var  $y_1, \dots, y_n$ ; STA; return( $y$ ) end

```

ist die durch P berechnete Schrittfunktion $\llbracket P^{STEP} \rrbracket : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ definiert durch

$$\llbracket P^{STEP} \rrbracket(b, n_1, \dots, n_k) := \text{step}(b, M_P^{(n_1, \dots, n_k)}, \text{STA}) . \quad \blacksquare$$

Satz 8.5. Für alle $n_1, \dots, n_k \in \mathbb{N}$ gilt:

1. $(\forall b \in \mathbb{N}. \llbracket P^{STEP} \rrbracket(b, n_1, \dots, n_k) = 0) \curvearrowright \llbracket P \rrbracket(n_1, \dots, n_k) = \perp$, und
2. $\llbracket P \rrbracket(n_1, \dots, n_k) = \perp \curvearrowright (\forall b \in \mathbb{N}. \llbracket P^{STEP} \rrbracket(b, n_1, \dots, n_k) = 0)$.

Beweis. Mit Satz 8.2. ■

Mit Satz 8.5(1) scheitert die Berechnung von $\llbracket P \rrbracket(n_1, \dots, n_k)$, falls die Schrittfunktion für jede Laufzeitbeschränkung als Ergebnis 0 liefert. Umgekehrt gilt mit (2), daß die Schrittfunktion für jede Laufzeitbeschränkung 0 berechnet, falls die Berechnung von $\llbracket P \rrbracket(n_1, \dots, n_k)$ erfolglos ist. Als Kontraposition von Satz 8.5 erhält man

- 1'. $\llbracket P \rrbracket(n_1, \dots, n_k) \neq \perp \curvearrowright \exists b \in \mathbb{N}. \llbracket P^{STEP} \rrbracket(b, n_1, \dots, n_k) > 0$, und
- 2'. $(\exists b \in \mathbb{N}. \llbracket P^{STEP} \rrbracket(b, n_1, \dots, n_k) > 0) \curvearrowright \llbracket P \rrbracket(n_1, \dots, n_k) \neq \perp$.

Mit (1') findet man für jede erfolgreiche Berechnung von $\llbracket P \rrbracket(n_1, \dots, n_k)$ eine Laufzeitbeschränkung b , so daß die Schrittfunktion ein Ergebnis > 0 liefert. Umgekehrt gilt mit (2'), daß die Berechnung von $\llbracket P \rrbracket(n_1, \dots, n_k)$ erfolgreich ist, falls die Schrittfunktion für irgendeine Laufzeitbeschränkung ein Ergebnis > 0 berechnet.

In Abschnitt 11.7 werden wir zeigen, daß $\llbracket P^{STEP} \rrbracket$ allein durch ein `loop-Programm` – das ist ein \mathcal{P} -Programm in dem `while`-Anweisungen nur in der Art von `for`-Schleifen verwendet werden – implementiert werden kann.

8.2. Die universelle Schrittfunktion

Genauso, wie wir für jedes \mathcal{P} -Programm P die Funktion $\llbracket P \rrbracket$ mittels der universellen Funktion $\mathbf{u}_{\mathcal{P}}$ berechnen können, vgl. Kapitel 6, können wir die Schrittfunktion $\llbracket P^{STEP} \rrbracket$ von P universell berechnen. Wir definieren daher:

Definition 8.6. (Universelle Schrittfunktion)

Die universelle Schrittfunktion $\mathbf{s}_{\mathcal{P}} : \mathbb{N} \rightarrow \mathbb{N}$ ist gegeben durch

$$\mathbf{s}_{\mathcal{P}}(\pi^3(i, b, n)) = \begin{cases} 0, & \text{falls } i \notin \mathfrak{b}P \\ \llbracket P^{STEP} \rrbracket(b, n), & \text{falls } i = \mathfrak{b}P. \quad \blacksquare \end{cases}$$

Mit der Funktion $s_{\mathcal{P}}$ kann die Schrittfunktion eines jeden Programms P dargestellt werden. Man erhält

$$s_{\mathcal{P}}(\pi^3(\natural P, b, n)) = \llbracket P^{STEP} \rrbracket(b, n) \quad (8.1)$$

und für die Prozedur

```
procedure P(x) <=
begin var y1, ..., yn; STA; return(y) end
```

mit Definition 8.4 dann

$$s_{\mathcal{P}}(\pi^3(\natural P, b, n)) = step(b, M_P^{(n)}, STA) . \quad (8.2)$$

Um $s_{\mathcal{P}}(\pi^3(i, b, n))$ zu berechnen, muß zuerst festgestellt werden, ob $i \in \natural \mathcal{P}$ gilt.¹ Dies gelingt mit der \mathcal{P} -berechenbaren Funktion $\natural?$ vgl. Satz 4.13. Für $i \notin \natural \mathcal{P}$ ist 0 das Ergebnis der Berechnung. Andernfalls gilt $i = \natural P$ für ein $P \in \mathcal{P}$ und man erhält $s_{\mathcal{P}}(\pi^3(i, b, n))$, indem aus $\natural P$ das \mathcal{P} -Programm P gebildet, also der Programmcode $\natural P$ mittels \natural^{-1} in das \mathcal{P} -Programm P *dekodiert*, und dann P auf n angewendet wird. Bei der Abarbeitung von P wird jedoch (im Unterschied zur Interpretation mit der universellen Funktion $u_{\mathcal{P}}$) die Laufzeitbeschränkung b berücksichtigt. Ist die Berechnung beendet – was aufgrund der Laufzeitbeschränkung immer eintritt – wird abschließend überprüft, ob der Abbruch der Berechnung aufgrund der Laufzeitbeschränkung erfolgte. In diesem Fall ist das Ergebnis 0, und andernfalls $b' > 0$, vgl. (8.2).

Damit ist $s_{\mathcal{P}}$ \mathcal{P} -berechenbar und folglich dürfen wir die Existenz eines $\mathcal{P}[1]$ -Programms **STEP** mit

$$s_{\mathcal{P}}(m) = \llbracket \mathbf{STEP} \rrbracket(m) \quad (8.3)$$

annehmen, für das $\llbracket \mathbf{STEP} \rrbracket(\pi^3(\natural P, b, n)) = \llbracket P^{STEP} \rrbracket(b, n)$ gilt. Das \mathcal{P} -Programm **STEP** überprüft bei Eingabe m mittels $\natural?$, ob $\pi_1^3(m)$ der Kode eines \mathcal{P} -Programms P ist. Im positiven Fall wird dann P mit $\pi_3^3(m)$ als Eingabe unter der Laufzeitbeschränkung $\pi_2^3(m)$ ausgeführt. Für $\pi_1^3(m) \notin \natural \mathcal{P}$ hält **STEP** sofort mit 0 als Ergebnis.

¹ Den Nachweis, daß $s_{\mathcal{P}}$ \mathcal{P} -berechenbar ist, führen wir – wie schon zuvor bei der universellen Funktion u – nur *informell*. Wir verzichten auf einen streng *formalen* Beweis, da dies hier einen zu großen beweistechnischen Aufwand erfordert.

```

procedure DECIDE_M(x) <=
begin var b, continue, res;
  b := 1; continue := 1;
  while continue do
    if STEP(PAIR3(⊥SEMI_DECIDE_M, b, x))
    then res := SEMI_DECIDE_M(x);
      continue := 0
    else if STEP(PAIR3(⊥SEMI_DECIDE_M̄, b, x))
    then res := ¬SEMI_DECIDE_M̄(x);
      continue := 0
    else b := SUCC(b)
    end_if
  end_if
end_while;
return(res)
end

```

Abbildung 8.1: Zum Beweis von Satz 8.7 – Ein Entscheidungsverfahren für M

8.3. Schrittweise Abarbeitung von \mathcal{P} -Programmen

Mit der Prozedur STEP können wir die “verzahnte” Abarbeitung mehrerer \mathcal{P} -Programme P_1, \dots, P_j , die in Form von Daten $\perp P_1, \dots, \perp P_j$ vorliegen, *kontrollieren*, indem wir diese Programme *schrittweise* abarbeiten. Damit steht uns jetzt eine Beweistechnik zur Verfügung, mit der wir – ohne Rückgriff auf mehrere Rechner oder die Vorstellung eines Betriebssystems mit *time sharing* – nachweisen können, daß das Komplement \overline{H} des Halteproblems H nicht semi-entscheidbar ist.

Um dies zu beweisen zeigen wir zunächst, daß jedes semi-entscheidbare Problem genau dann entscheidbar ist, wenn dessen Komplementärproblem ebenfalls semi-entscheidbar ist:

Satz 8.7. *M ist genau dann entscheidbar, wenn M und \overline{M} semi-entscheidbar sind.*

Beweis. “ \Rightarrow ” Folgt mit Satz 7.6 und Satz 7.9.

“ \Leftarrow ” Seien SEMI_DECIDE_M und SEMI_DECIDE_M̄ semi-Entscheidungsverfahren für M und \overline{M} . Für die Prozedur DECIDE_M $\in \mathcal{P}$ aus Abbildung 8.1 muß einer der beiden Prozeduraufrufe SEMI_DECIDE_M(m) oder SEMI_DECIDE_M̄(m) auf jeden Fall halten da, entweder $m \in M$ oder $m \in \overline{M}$ gilt. Zur Berechnung von SEMI_DECIDE_M(m) oder SEMI_DECIDE_M̄(m) werden b_m Schritte benötigt, wobei

b_m nicht von vornherein bekannt ist. Da die Laufzeitbeschränkung b in der Schleife nach b_m Schleifendurchläufen den Wert $b_m + 1$ erhält, verläuft einer der beiden Tests $\text{STEP}(\text{PAIR}^3(\text{SEMIDECIDE}_M, b, m)) = 1$ und $\text{STEP}(\text{PAIR}^3(\text{SEMIDECIDE}_{\bar{M}}, b, m)) = 1$ im $b_m + 1$ -ten Schleifendurchlauf positiv. Damit wird die Schleife beendet, und für $\text{DECIDE}_M(m)$ erhält man damit

$$\llbracket \text{DECIDE}_M \rrbracket(m) = \begin{cases} \llbracket \text{SEMIDECIDE}_M \rrbracket(m) & , \text{ falls } \llbracket \text{SEMIDECIDE}_M \rrbracket(m) \neq \perp \\ \neg \llbracket \text{SEMIDECIDE}_{\bar{M}} \rrbracket(m) & , \text{ falls } \llbracket \text{SEMIDECIDE}_{\bar{M}} \rrbracket(m) \neq \perp . \end{cases}$$

Für $m \in M$ gilt $\llbracket \text{SEMIDECIDE}_M \rrbracket(m) = 1$ und damit $\llbracket \text{DECIDE}_M \rrbracket(m) = 1$. Für $m \notin M$ gilt $\llbracket \text{SEMIDECIDE}_{\bar{M}} \rrbracket(m) = 1$ und damit $\llbracket \text{DECIDE}_M \rrbracket(m) = 0$. Also gilt

$$\llbracket \text{DECIDE}_M \rrbracket(m) = \begin{cases} 1 & , \text{ falls } m \in M \\ 0 & , \text{ falls } m \notin M , \end{cases}$$

d.h. DECIDE_M ist ein Entscheidungsverfahren für M .² ■

Entscheidend im Beweis von Satz 8.7 ist die Verwendung der Prozedur STEP .³ Da weder für SEMIDECIDE_M noch für $\text{SEMIDECIDE}_{\bar{M}}$ garantiert ist, daß diese Prozeduren halten, müssen wir die Ausführung dieser Prozeduren geeignet kontrollieren: Gilt $\text{STEP}(\text{PAIR}^3(\text{SEMIDECIDE}_M, b, m)) = 1$ so hält $\text{SEMIDECIDE}_M(m)$ mit Satz 8.5(2), und wir können das Ergebnis für $\text{DECIDE}_M(m)$ aus dem Ergebnis von $\text{SEMIDECIDE}_M(m)$ bilden. Andernfalls testen wir, ob $\text{STEP}(\text{PAIR}^3(\text{SEMIDECIDE}_{\bar{M}}, b, m)) = 1$ gilt. Im positiven Fall hält dann $\text{SEMIDECIDE}_{\bar{M}}(m)$, und wir bilden das Ergebnis für $\text{DECIDE}_M(m)$ aus dem Ergebnis von $\text{SEMIDECIDE}_{\bar{M}}(m)$. Gilt jedoch weder $\text{STEP}(\text{PAIR}^3(\text{SEMIDECIDE}_M, b, m)) = 1$ noch $\text{STEP}(\text{PAIR}^3(\text{SEMIDECIDE}_{\bar{M}}, b, m)) = 1$, so erhöhen wir die erlaubte Laufzeitbeschränkung b , um dann anschließend die Tests mit dem erhöhten Schrittzähler durchzuführen.

Mit Satz 8.7 können wir jetzt beweisen, daß \bar{H} tatsächlich nicht semi-entscheidbar ist:

Korollar 8.8. \bar{H} ist nicht semi-entscheidbar.

Beweis. Angenommen, \bar{H} sei semi-entscheidbar. Da H semi-entscheidbar ist, vgl. Satz 7.11, folgt mit Satz 8.7, daß H entscheidbar ist, also ein Widerspruch zu Satz 7.2. Folglich ist \bar{H} nicht semi-entscheidbar. ■

² Die Initialisierung “ $\mathbf{b} := 1$ ” der Laufzeitbeschränkung \mathbf{b} und deren Erhöhung “ $\mathbf{b} := \text{SUCC}(\mathbf{b})$ ” in der Prozedur DECIDE_M aus Abbildung 8.1 sind willkürlich. Man kann genausogut “ $\mathbf{b} := n_1$ ” und “ $\mathbf{b} := \mathbf{b} + n_2$ ” für beliebige $n_1, n_2 > 0$ verwenden.

³ In der englischsprachigen Literatur wird die Beweistechnik der “verzahnten” Abarbeitung von Programmen auch als “dovetailing” bezeichnet.

```

procedure PSI(x) <=
begin var b, continue, res, y, z;
  b := 1; continue := 1;
  y := PAIR12(x); z := PAIR22(x)
  while continue do
    if STEP(PAIR3(⊥SIGMA, b, z))
      then res := SIGMA(z);
           continue := 0
    else if STEP(PAIR3(y, b, y))
      then res := THETA(z);
           continue := 0
    else b := SUCC(b)
    end_if
  end_if
end_while;
return(res)
end .

```

Abbildung 8.2: Die Prozedur PSI für Beispiel 8.10

Genauso zeigt man:

Korollar 8.9. \overline{S} ist nicht semi-entscheidbar.

Wir illustrieren die Verwendung von STEP mit einem weiteren Beispiel:

Beispiel 8.10. Seien $\theta, \sigma : \mathbb{N} \mapsto \mathbb{N}$ beliebige berechenbare Funktionen und sei $\psi : \mathbb{N} \mapsto \mathbb{N}$ definiert durch

$$\psi(\pi^2(y, z)) = \begin{cases} \theta(z) & , \text{ falls } \varphi_y(y) \neq \perp \\ \sigma(z) & , \text{ falls } \varphi_y(y) = \perp . \end{cases}$$

Dann ist ψ i.A. nicht berechenbar, denn für $\theta(z) = 1$ und $\sigma(z) = 0$ (für alle $z \in \mathbb{N}$) würde beispielsweise $\chi_S(y) = \psi(\pi^2(y, z))$ für alle $y, z \in \mathbb{N}$ gelten, und mit der Berechenbarkeit von ψ wäre das Selbstanwendbarkeitsproblem S dann im Widerspruch zu Satz 7.3 entscheidbar. Das Problem besteht offensichtlich darin, daß mit der Unentscheidbarkeit von $\varphi_y(y) = \perp$ bei Berechnung von $\psi(\pi^2(y, z))$ nicht zwischen $\theta(z)$ und $\sigma(z)$ ausgewählt werden kann.

Angenommen, θ ist eine Erweiterung von σ , d.h. es gilt $\sigma(z) = \perp$ oder $\sigma(z) = \theta(z)$ für alle $z \in \mathbb{N}$. Obwohl $\varphi_y(y) = \perp$ nicht entscheidbar ist, können wir jetzt

$\psi(\pi^2(y, z))$ doch berechnen: Seien SIGMA, THETA, PSI $\in \mathcal{P}$ -Prozeduren mit $\llbracket \text{SIGMA} \rrbracket = \sigma$, $\llbracket \text{THETA} \rrbracket = \theta$ und PSI definiert wie in Abbildung 8.2. Wir zeigen, daß $\llbracket \text{PSI} \rrbracket = \psi$ gilt, und damit, daß ψ berechenbar ist:

Angenommen, es gilt $\varphi_y(y) \neq \perp$: Dann gilt $\text{STEP}(\text{PAIR}^3(\mathbf{y}, \mathbf{k}, \mathbf{y})) = 1$ für ein $k \in \mathbb{N}$. Nehmen wir weiter an, daß $\text{STEP}(\text{PAIR}^3(\natural\text{SIGMA}, \mathbf{h}, \mathbf{z})) = 1$ für ein $h \leq k$ gilt. Man erhält $\llbracket \text{PSI} \rrbracket(\pi^2(y, z)) = \sigma(z)$ und $\sigma(z) = \theta(z)$, also $\llbracket \text{PSI} \rrbracket(\pi^2(y, z)) = \theta(z)$, denn mit $\text{STEP}(\text{PAIR}^3(\natural\text{SIGMA}, \mathbf{h}, \mathbf{z})) = 1$ gilt $\sigma(z) \neq \perp$. Also gilt $\llbracket \text{PSI} \rrbracket(\pi^2(y, z)) = \psi(\pi^2(y, z))$. Andernfalls gilt $\text{STEP}(\text{PAIR}^3(\natural\text{SIGMA}, \mathbf{h}, \mathbf{z})) = 0$ für alle $h \leq k$, und man erhält $\llbracket \text{PSI} \rrbracket(\pi^2(y, z)) = \theta(z) = \psi(\pi^2(y, z))$.

Nehmen wir jetzt an, daß $\varphi_y(y) = \perp$ gilt. Dann gilt auch $\text{STEP}(\text{PAIR}^3(\mathbf{y}, \mathbf{k}, \mathbf{y})) = 0$ für alle $k \in \mathbb{N}$. Nehmen wir weiter an, daß $\text{STEP}(\text{PAIR}^3(\natural\text{SIGMA}, \mathbf{h}, \mathbf{z})) = 1$ für ein $h \in \mathbb{N}$ gilt. Man erhält $\llbracket \text{PSI} \rrbracket(\pi^2(y, z)) = \sigma(z) = \psi(\pi^2(y, z))$. Andernfalls gilt $\text{STEP}(\text{PAIR}^3(\natural\text{SIGMA}, \mathbf{h}, \mathbf{z})) = 0$ für alle $h \in \mathbb{N}$, und man erhält $\llbracket \text{PSI} \rrbracket(\pi^2(y, z)) = \perp = \sigma(z) = \psi(\pi^2(y, z))$, denn mit $\text{STEP}(\text{PAIR}^3(\natural\text{SIGMA}, \mathbf{h}, \mathbf{z})) = 0$ (für alle $h \in \mathbb{N}$) gilt $\sigma(z) = \perp$. ■

9. REKURSIVE AUFZÄHLBARKEIT

9.1. Aufzählungsverfahren

Ein semi-Entscheidungsverfahren $\text{SEMI_DECIDE_M} \in \mathcal{P}$ implementiert ein *akzeptierendes* Erkennungsprinzip für eine Menge $M \subseteq \mathbb{N}$: Für $m \in \mathbb{N}$ erhalten wir *immer* eine positive Antwort, d.h. 1, falls $m \in M$, und (vielleicht) *manchmal* auch eine negative Antwort, also 0, falls $m \notin M$. Diesem Erkennungsprinzip stellen wir ein *generatives* Prinzip gegenüber: Wenn man die Elemente einer Menge M *systematisch erzeugen* kann, so kann man aus solch einem Erzeugungsverfahren in einfacher Weise ein semi-Entscheidungsverfahren bilden. Den Begriff “*systematisch erzeugen*” erfassen wir formal mit dem Begriff der *rekursiven Aufzählbarkeit*:

Definition 9.1. (Rekursive Aufzählbarkeit)

Eine Menge $M \subseteq \mathbb{N}$ ist genau dann rekursiv aufzählbar, falls $M = \emptyset$ oder andernfalls eine totale Funktion $\alpha_M : \mathbb{N} \rightarrow M$ existiert, so daß gilt:

1. $\alpha_M(\mathbb{N}) = M$, d.h. α_M ist surjektiv, und
2. α_M ist berechenbar.

Eine Funktion $\alpha_M : \mathbb{N} \rightarrow \mathbb{N}$, für die (1) und (2) gilt, wird eine Aufzählungsfunktion von M genannt. Ein \mathcal{P} -Programm PROG mit $\alpha_M = \llbracket \text{PROG} \rrbracket$ heißt ein Aufzählungsverfahren für M . ■

Jede rekursiv aufzählbare Menge ist auch semi-entscheidbar: Für ein $m \in \mathbb{N}$ muß man nur alle Elemente von M Schritt für Schritt erzeugen, also M *aufzählen*, und nach jedem Aufzählungsschritt überprüfen, ob das zuletzt erzeugte Element identisch m ist. Verläuft der Test positiv, so hält man mit positiver Antwort (also 1) an, denn dann gilt ja $m \in M$. Für $m \in M$ muß das Verfahren in jedem Fall halten, denn mit der Surjektivität der Aufzählungsfunktion wird m nach endlich vielen Schritten erzeugt.

Satz 9.2. Wenn $M \subseteq \mathbb{N}$ rekursiv aufzählbar ist, so ist M semi-entscheidbar.

Beweis. Wenn $M = \emptyset$, so gilt $\tilde{\chi}_M = \llbracket \text{CYCLE}_1 \rrbracket$, d.h. $\text{CYCLE}_1 \in \mathcal{P}$ ist ein semi-Entscheidungsverfahren für M .¹ Andernfalls gibt es ein Aufzählungsverfahren $\text{ENUMERATE}_M \in \mathcal{P}$ für M . Für das Programm $\text{SEMI_DECIDE}_M \in \mathcal{P}$ mit

```

procedure SEMI_DECIDE_M(x) <=
begin var i, res;
  while ENUMERATE_M(i) ≠ x do i := SUCC(i) end_while;
  res := 1;
  return(res)
end

```

gilt

$$\llbracket \text{SEMI_DECIDE}_M \rrbracket(m) = \begin{cases} \perp & , \text{ falls } \llbracket \text{ENUMERATE}_M \rrbracket(i) \neq m \text{ für alle } i \in \mathbb{N} \\ 1 & , \text{ falls } \llbracket \text{ENUMERATE}_M \rrbracket(i) = m \text{ für ein } i \in \mathbb{N} . \end{cases}$$

Da ENUMERATE_M ein Aufzählungsverfahren für M ist, gilt $\llbracket \text{ENUMERATE}_M \rrbracket(\mathbb{N}) = M$, und damit gibt es für jedes $m \in M$ ein (kleinstes) $i \in \mathbb{N}$ mit $\text{ENUMERATE}_M(i) = m$. Für $m \in M$ bricht die Schleife in SEMI_DECIDE_M also nach i Schleifendurchläufen ab, und man erhält das Ergebnis 1. Gilt dagegen $m \notin M$, so bricht die Schleife nie ab und $\text{SEMI_DECIDE}_M(m)$ hält nicht. Damit gilt

$$\llbracket \text{SEMI_DECIDE}_M \rrbracket(m) = \begin{cases} \perp & , \text{ falls } m \notin M \\ 1 & , \text{ falls } m \in M , \end{cases}$$

und folglich $\tilde{\chi}_M = \llbracket \text{SEMI_DECIDE}_M \rrbracket$. Damit ist M semi-entscheidbar. ■

Rekursive Aufzählbarkeit ist nicht nur *hinreichend* für semi-Entscheidbarkeit, sondern auch *notwendig*, d.h. aus der semi-Entscheidbarkeit einer Menge M folgt auch deren rekursive Aufzählbarkeit. Zum Beweis konstruieren wir aus einem semi-Entscheidungsverfahren SEMI_DECIDE_M für M eine Prozedur ENUMERATE_M für M , die eine Aufzählungsfunktion α_M für M implementiert. Zur Konstruktion benötigen wir die Paar-Funktion sowie die universelle Schrittfunktion:

Mittels der Paar-Funktion interpretieren wir ein $i \in \mathbb{N}$ als ein Paar $(b, m) \in \mathbb{N} \times \mathbb{N}$, d.h. $i = \pi^2(b, m)$, und überprüfen mittels SEMI_DECIDE_M unter der Laufzeitbeschränkung b , ob $m \in M$ gilt. Im positiven Fall definieren wir $\alpha_M(i) := m$. Andernfalls wurde entweder $m \notin M$ durch SEMI_DECIDE_M festgestellt oder aber die

¹ Anstatt CYCLE_1 kann man natürlich auch eine \mathcal{P} -Prozedur wie `procedure ZERO(x) <= begin var y; y := 0; return(y) end` verwenden, für die dann $\tilde{\chi}_M \cong_M \llbracket \text{ZERO} \rrbracket$ gilt.

```

procedure ENUMERATE_M(i) <=
begin var b, element, res;
  b := PAIR12(i);
  element := PAIR22(i);
  res := m0;
  if STEP(PAIR3(⊥SEMI_DECIDE_M,b,element))
    then if SEMI_DECIDE_M(element) then res := element end_if
  end_if;
  return(res)
end

```

Abbildung 9.1: Die Prozedur ENUMERATE_M zum Beweis von Satz 9.3

Ausführung von SEMI_DECIDE_M mit Eingabe m scheiterte an der Laufzeitbeschränkung b . In diesen Fällen definieren wir $\alpha_M(i) := m_0$, wobei $m_0 \in M$ beliebig aber fest gewählt ist. Damit gilt $\alpha_M(i) \in M$ in jedem Fall, d.h. das implementierte Verfahren ENUMERATE_M ist *korrekt*.

Da für jedes $m \in M$ ein $b_m \in \mathbb{N}$ existiert, so daß SEMI_DECIDE_M in b_m Schritten “ $m \in M$ ” feststellen kann, gilt $m = \alpha_M(\pi^2(b_m + 1, m))$. Damit ist α_M surjektiv, und folglich ist das implementierte Verfahren ENUMERATE_M auch *vollständig*.

Satz 9.3. Wenn $M \subseteq \mathbb{N}$ semi-entscheidbar ist, so ist M rekursiv aufzählbar.

Beweis. Für $M = \emptyset$ ist die Behauptung trivialerweise wahr. Andernfalls können wir ein beliebiges Element $m_0 \in M$ wählen. Da M semi-entscheidbar ist, gibt es ein semi-Entscheidungsverfahren SEMI_DECIDE_M $\in \mathcal{P}[1]$ für M . Für die Prozedur ENUMERATE_M $\in \mathcal{P}[1]$ aus Abbildung 9.1 hält die Ausführung von ENUMERATE_M(i) für beliebiges $i \in \mathbb{N}$, denn die Ausführung von STEP(PAIR³(⊥SEMI_DECIDE_M,b,element)) hält immer und SEMI_DECIDE_M(element) wird nur dann ausgeführt, wenn ein Ergebnis in weniger als b Schritten berechnet werden kann.

Weiter gilt $\llbracket \text{ENUMERATE_M} \rrbracket(i) \in M$, denn für $\llbracket \text{ENUMERATE_M} \rrbracket(i) = m$ gilt entweder $m = m_0 \in M$ oder $\llbracket \text{SEMI_DECIDE_M} \rrbracket(m) = 1$, und damit ebenfalls $m \in M$. Also ist $\llbracket \text{ENUMERATE_M} \rrbracket : \mathbb{N} \rightarrow \mathbb{N}$ eine totale berechenbare Funktion mit $\llbracket \text{ENUMERATE_M} \rrbracket(\mathbb{N}) \subseteq M$.

Es ist jetzt noch zu zeigen, daß $\llbracket \text{ENUMERATE_M} \rrbracket(\mathbb{N}) = M$ gilt. D.h. wir zeigen, daß für jedes $m \in M$ ein $i \in \mathbb{N}$ mit $\llbracket \text{ENUMERATE_M} \rrbracket(i) = m$ existiert: Für jedes $m \in M$ gilt $\llbracket \text{SEMI_DECIDE_M} \rrbracket(m) = 1$, und folglich liefert SEMI_DECIDE_M(m) nach endlich vielen, also etwa b_m Schritten, das Ergebnis 1. Für $i := \pi^2(b_m + 1, m)$ erhält man $\llbracket \text{ENUMERATE_M} \rrbracket(i) = m$, denn mit $\llbracket \text{PAIR}_1^2 \rrbracket = \pi_1^2$ und $\llbracket \text{PAIR}_2^2 \rrbracket = \pi_2^2$ gilt $b = b_m + 1$ und $\text{element} = m$.

Folglich gilt $\llbracket \text{STEP} \rrbracket(\text{PAIR}^3(\natural \text{SEMI_DECIDE_M}, b_m + 1, m)) = \llbracket \text{SEMI_DECIDE_M} \rrbracket(m) = 1$ und damit $\llbracket \text{ENUMERATE_M} \rrbracket(i) = \pi_2^2(i) = \pi_2^2(\pi^2(b_m + 1, m)) = m$. Also ist ENUMERATE_M ein Aufzählungsverfahren für M , d.h. M ist rekursiv aufzählbar. ■

Korollar 9.4. $M \subseteq \mathbb{N}$ ist genau dann semi-entscheidbar, wenn M rekursiv aufzählbar ist.

Beweis. Offensichtlich mit Satz 9.2 und Satz 9.3. ■

Semi-Entscheidbarkeit und rekursive Aufzählbarkeit sind also äquivalente Begriffe, die lediglich unterschiedlich definiert sind. Wir machen uns dies zunutze, indem wir bei den weiteren Untersuchungen jeweils denjenigen Begriff wählen, dessen Definition für uns am bequemsten ist.

Bemerkung 9.5. Mit der Beweisidee von Satz 9.2 überlegt man sich leicht, daß jede Menge M , deren Elemente durch Herleitung mittels eines endlichen Regelsystems definiert sind, semi-entscheidbar ist.² Man erzeugt dazu die Elemente von M in systematischer Weise, etwa indem die Regelanwendungen durch eine Breitensuche organisiert werden, und vergleicht die erzeugten Elemente jeweils mit demjenigen m , für daß “ $m \in M$?” überprüft werden soll. Gilt $m \in M$, so wird m auf diese Weise nach endlicher Zeit erzeugt, so daß man ein positives Ergebnis erhält. Für $m \notin M$ muß das Erzeugungsverfahren dagegen nicht terminieren. Beispielsweise folgt so, daß die Menge der allgemeingültigen prädikatenlogischen Formeln semi-entscheidbar ist, denn aufgrund der Vollständigkeit der Prädikatenlogik 1. Stufe, ist jede allgemeingültige Formel durch einen prädikatenlogischen Kalkül herleitbar. Weitere Beispiele sind Wortmengen, die durch generative Grammatiken (Chomsky-Grammatiken) definiert werden.

Mittels rekursiver Aufzählbarkeit kann man zeigen, daß jede unendliche, rekursiv aufzählbare Menge eine unendliche, entscheidbare Teilmenge enthält. Zum Beweis benötigen wir den Begriff *aufsteigend rekursiv aufzählbar*. Damit ist gemeint, daß die Aufzählungsfunktion α_M einer Menge M *monoton* ist, also $i < j \curvearrowright \alpha_M(i) < \alpha_M(j)$ für alle $i, j \in \mathbb{N}$ gilt. Folgende Überlegung zeigt, daß aufsteigend rekursiv aufzählbare Mengen entscheidbar sind: Wie in Satz 9.2 erzeugen wir mittels der Aufzählungsfunktion α_M systematisch die Elemente von M und vergleichen diese mit $x \in \mathbb{N}$. Für $\alpha_M(i) = x$ gilt $x \in M$, die Suche kann also mit positivem Ergebnis beendet werden. Andernfalls prüfen wir, ob $\alpha_M(i) > x$ gilt.

² Die Endlichkeit eines Regelsystems, oder präziser die *lokale Endlichkeit* (engl. *locally finite*), garantiert, daß auf jedes erzeugte Element nur endlich viele Regelanwendungen möglich sind. Damit erhält man einen Suchbaum mit *endlichem Verzweigungsgrad*. Andernfalls könnte Breitensuche nicht erfolgreich sein.

Ist dies der Fall, so kann x nicht in $\alpha_M(\mathbb{N})$ enthalten sein, denn aufgrund der Monotonie von α_M gilt dann $\alpha_M(j) > x$ für alle $j > i$. Die Suche kann also mit negativem Ergebnis abgebrochen werden. Ansonsten muß weiter gesucht werden. Die Suche endet jedoch nach endlich vielen Schritten, denn wegen der Monotonie von α_M gilt nach endlich vielen Schritten $\alpha_M(i) \geq x$.

Satz 9.6. $M \subseteq \mathbb{N}$ ist entscheidbar, falls M aufsteigend rekursiv aufzählbar ist.

Beweis. Für $M = \emptyset$ gilt $\chi_M(n) = 0$ für alle $n \in \mathbb{N}$. Damit ist M entscheidbar, denn χ_M ist trivialerweise berechenbar. Andernfalls gibt es ein monotones Aufzählungsverfahren $\text{ENUMERATE_M} \in \mathcal{P}$ für M . Für das Programm $\text{DECIDE_M} \in \mathcal{P}$ mit

```

procedure DECIDE_M(x) <=
begin var i, res;
  while ENUMERATE_M(i) < x do i := SUCC(i) end_while;
  if ENUMERATE_M(i) = x then res := 1 end_if;
  return(res)
end

```

gilt

$$\llbracket \text{DECIDE_M} \rrbracket(m) = \begin{cases} 0 & , \text{ falls } \llbracket \text{ENUMERATE_M} \rrbracket(i) \neq m \text{ für alle } i \in \mathbb{N} \\ 1 & , \text{ falls } \llbracket \text{ENUMERATE_M} \rrbracket(i) = m \text{ für ein } i \in \mathbb{N} . \end{cases}$$

Da ENUMERATE_M ein Aufzählungsverfahren für M ist, gilt $\llbracket \text{ENUMERATE_M} \rrbracket(\mathbb{N}) = M$, und damit gibt es für jedes $m \in M$ ein (kleinstes) $i \in \mathbb{N}$ mit $\text{ENUMERATE_M}(i) = m$. Für $m \in M$ bricht die Schleife in DECIDE_M also nach i Schleifendurchläufen ab, und man erhält das Ergebnis 1. Für $m \notin M$ gilt $\llbracket \text{ENUMERATE_M} \rrbracket(j) > m$ für ein (kleinstes) $j \in \mathbb{N}$ aufgrund der Monotonie von $\llbracket \text{ENUMERATE_M} \rrbracket$. Also bricht die Schleife dann nach j Schritten ab, und man erhält das Ergebnis 0. Damit gilt

$$\llbracket \text{DECIDE_M} \rrbracket(m) = \begin{cases} 0 & , \text{ falls } m \notin M \\ 1 & , \text{ falls } m \in M , \end{cases}$$

und folglich $\chi_M = \llbracket \text{DECIDE_M} \rrbracket$. Damit ist M entscheidbar. ■

Bemerkung 9.7. Ein praktisches Beispiel für die Anwendung von Satz 9.6 ist der Nachweis der Entscheidbarkeit von kontext-sensitiven Sprachen (= Typ-1 Sprachen). Hier gilt, daß ein Wort aufgrund der Längenbeschränkung der Grammatikregeln innerhalb einer (durch das Wort gegebenen) Suchtiefe herleitbar sein muß. Wird also ein Wort m nicht innerhalb dieser Suchtiefe gefunden, so ist $m \in \overline{M}$ (für die Typ-1 Sprache M) nachgewiesen.

Die Existenz einer unendlichen, entscheidbaren Teilmenge einer unendlichen, rekursiv aufzählbaren Menge M zeigen wir jetzt folgendermaßen: Aus einem Aufzählungsverfahren α_M von M bilden wir eine berechenbare Funktion $\beta : \mathbb{N} \rightarrow M$, so daß β *monoton* ist. Damit ist $\beta(\mathbb{N})$ sowohl unendlich als auch aufsteigend rekursiv aufzählbar, also mit Satz 9.6 auch entscheidbar.

Satz 9.8. *Sei $M \subseteq \mathbb{N}$ unendlich und rekursiv aufzählbar. Dann enthält M eine unendliche entscheidbare Menge.*

Beweis. *Sei α_M eine Aufzählungsfunktion für M und sei $\text{ALPHA_M} \in \mathcal{P}$ mit $\llbracket \text{ALPHA_M} \rrbracket = \alpha_M$. Wie definieren das \mathcal{P} -Programm **BETA** durch*

```

procedure BETA(i) <=
begin var j, k, b;
  b := ALPHA_M(0);
  while k < i
    do if b < ALPHA_M(j)
      then k := k + 1;
         b := ALPHA_M(j);
      end_if;
      j := j + 1
    end_while;
  return(b)
end

```

Angenommen, es gibt ein $i \in \mathbb{N}$ so daß $i < j \curvearrowright \alpha_M(i) \geq \alpha_M(j)$ für alle $j \in \mathbb{N}$. Dann enthält M höchstens $i + (\alpha_M(i) - 1)$ Elemente und ist somit endlich. \blacktriangledown Also gibt es für jedes $i \in \mathbb{N}$ ein $j \in \mathbb{N}$, so daß (*) $i < j \wedge \alpha_M(i) < \alpha_M(j)$ gilt. Sei $n_0 := 0$ sowie $n_{k+1} := \min \{j \in \mathbb{N} \mid n_k < j \wedge \alpha_M(n_k) < \alpha_M(j)\}$. Wegen (*) ist n_k wohldefiniert, und es gilt $\alpha_M(n_k) < \alpha_M(n_{k+1})$ für alle $k \in \mathbb{N}$. Folglich ist $\beta : \mathbb{N} \rightarrow M$ definiert durch $\beta(i) := \alpha_M(n_i)$ *monoton*. Für die **while**-Anweisung der Prozedur **BETA** gilt die Schleifeninvariante

$$\begin{array}{l}
\{b := \alpha_M(n_k)\} \\
\text{while } k < i \text{ do } \dots \text{ end_while} \\
\{b := \alpha_M(n_k)\}
\end{array} \tag{9.1}$$

denn für $k = h$ und $b = \alpha_M(n_h)$ vor Ausführung des Schleifenrumpfs erhält man nach dessen Ausführung $k = h + 1$ und $b = \alpha_M(n_{h+1})$, falls $b < \text{ALPHA_M}(j)$, und $k = h$ und $b = \alpha_M(n_h)$ andernfalls. Da der Wert der Programmvariablen j bei jeder Ausführung des Schleifenrumpfs erhöht wird, terminiert die **while**-Schleife

wegen (*). Dann gilt $\mathbf{k} = i$ und folglich $\mathbf{b} = \alpha_M(n_{\mathbf{k}}) = \alpha_M(n_i) = \beta(i)$. Also gilt $\beta = \llbracket \text{BETA} \rrbracket$, somit ist $\beta(\mathbb{N})$ mittels β aufsteigend rekursiv aufzählbar und mit Satz 9.6 entscheidbar. Schließlich ist $\beta(\mathbb{N})$ unendlich, denn β ist monoton. ■

Beispiel 9.9. (Entscheidbare Teilmengen rekursiv aufzählbarer Mengen)

1. Sei \mathcal{P}_0 die Menge aller \mathcal{P} -Programme, in denen keine Schleifenanweisungen vorkommen. Für $S_0 := \llbracket \mathcal{P}_0 \rrbracket$ gilt $S_0 \subset S$ für das rekursiv aufzählbare Selbstanwendungsproblem S sowie $|S_0| = \infty$, denn es gibt unendlich viele schleifenlose \mathcal{P} -Programme. Da algorithmisch festgestellt werden kann, ob ein \mathcal{P} -Programm while-Schleifen enthält, ist S_0 entscheidbar.
2. Die Menge AG der allgemeingültigen Formeln der Prädikatenlogik erster Stufe ist unendlich und rekursiv aufzählbar. Ein Beispiel für eine unendliche, entscheidbare Teilmenge von AG ist die Menge TAU der Tautologien, also der wahren aussagenlogischen Formeln, s.a. Abschnitt 10.6.

9.2. Abzählbarkeit und rekursive Aufzählbarkeit

Es ist wichtig, zwischen den Begriffen der *Abzählbarkeit* und der *rekursiven Aufzählbarkeit* einer Menge M zu unterscheiden.³ In beiden Fällen kann $M \neq \emptyset$ als Bild einer totalen und surjektiven Aufzählungsfunktion $\alpha : \mathbb{N} \rightarrow M$ dargestellt werden, d.h. $M = \alpha(\mathbb{N})$. Für die *rekursive Aufzählbarkeit* wird zusätzlich gefordert, daß α eine *berechenbare* Funktion ist. Daraus folgt, daß jede rekursiv aufzählbare Menge auch abzählbar ist. Umgekehrt gilt das jedoch nicht. Insbesondere können wir Satz 5.3 nicht für rekursive Aufzählbarkeit formulieren. Anders gesagt, eine Teilmenge einer rekursiv aufzählbaren Menge ist nicht notwendigerweise auch rekursiv aufzählbar, wie man leicht zeigt:

Die Menge \mathbb{N} ist trivialerweise rekursiv aufzählbar, denn die Identitätsfunktion ist offenbar berechenbar. Damit ist \mathbb{N} natürlich ebenso trivialerweise abzählbar. Mit $\overline{H} \subseteq \mathbb{N}$ ist dann auch das Komplement \overline{H} des Halteproblems abzählbar, vgl. Satz 5.3. \overline{H} ist jedoch nicht rekursiv aufzählbar, denn \overline{H} ist nicht semi-entscheidbar, vgl. Satz 8.8 und Satz 9.2. Wir haben also mit \overline{H} eine abzählbare, aber nicht rekursiv aufzählbare Teilmenge einer rekursiv aufzählbaren Menge, nämlich \mathbb{N} , angegeben.

³ Wir folgen hier dem allgemeinen Sprachgebrauch. Man könnte genauso von *Aufzählbarkeit* oder von *rekursiver Abzählbarkeit* sprechen. Anders gesagt, mit “auf” und “ab” wird keine weitere Unterscheidung ausgedrückt.

```

procedure SEMI_DECIDE_M(m) <=
begin var y,z;
  y := PHI(m);
  z := 1;
  return(z)
end

```

Abbildung 9.2: Ein semi-Entscheidungsverfahren für $Def(\phi)$

9.3. Definitions- und Bildbereiche berechenbarer Funktionen

Semi-Entscheidbarkeit bzw. rekursive Aufzählbarkeit kann durch die Definitions- und Bildbereiche berechenbarer Funktionen charakterisiert werden:

Satz 9.10. $M \subseteq \mathbb{N}$ ist genau dann semi-entscheidbar, wenn $M = Def(\phi)$ für eine berechenbare Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$.

Beweis. “ \Rightarrow ” Mit $\phi := \tilde{\chi}_M$.

“ \Leftarrow ” Sei $M = Def(\phi)$ für eine berechenbare Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$, und sei $\text{PHI} \in \mathcal{P}[1]$ mit $\llbracket \text{PHI} \rrbracket = \phi$. Dann gilt $\llbracket \text{SEMI_DECIDE_M} \rrbracket = \tilde{\chi}_M$ für die Prozedur $\text{SEMI_DECIDE_M} \in \mathcal{P}[1]$ aus Abbildung 9.2, denn $\text{PHI}(m)$ terminiert genau dann, wenn $m \in Def(\phi)$, d.h. wenn $m \in M$. ■

Satz 9.11. $M \subseteq \mathbb{N}$ ist genau dann semi-entscheidbar, wenn $M = Bild(\phi)$ für eine berechenbare Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$.

Beweis. “ \Rightarrow ” Mit Satz 9.3 gibt es eine berechenbare Aufzählungsfunktion $\alpha_M : \mathbb{N} \rightarrow \mathbb{N}$ mit $\alpha_M(\mathbb{N}) = M$, d.h. $M = Bild(\alpha_M)$.

“ \Leftarrow ” Sei $M = Bild(\phi)$ für eine berechenbare Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$, und sei $\text{PHI} \in \mathcal{P}[1]$ mit $\llbracket \text{PHI} \rrbracket = \phi$. Für die \mathcal{P} -Prozedur SEMI_DECIDE_M aus Abbildung 9.3 gilt dann

$$\llbracket \text{SEMI_DECIDE_M} \rrbracket(m) = \begin{cases} 1 & , \text{ falls } m = \phi(n) \text{ für ein } n \in \mathbb{N} \\ \perp & , \text{ falls } m \neq \phi(n) \text{ für alle } n \in \mathbb{N} \end{cases}$$

und mit $M = Bild(\phi)$ folglich

$$\llbracket \llbracket \text{SEMI_DECIDE_M} \rrbracket \rrbracket(m) = \begin{cases} 1 & , \text{ falls } m \in M \\ \perp & , \text{ falls } m \notin M \end{cases}$$

also $\llbracket \llbracket \text{SEMI_DECIDE_M} \rrbracket \rrbracket = \tilde{\chi}_M$. ■

```

procedure SEMI_DECIDE_M(m) <=
begin var b,n,i,res;
  while res = 0 do
    n := PAIR12(i);
    b := PAIR22(i);
    if STEP(PAIR3( $\downarrow$ PHI,b,n))
      then if m = PHI(n) then res := 1 else i := SUCC(i) end_if
      else i := SUCC(i)
    end_if
  end_while;
return(res)
end

```

Abbildung 9.3: Ein semi-Entscheidungsverfahren für $Bild(\phi)$

Mit Satz 9.10 ist der Definitionsbereich einer berechenbaren Funktion mindestens semi-entscheidbar. Für Programme, die partielle Funktionen mit *entscheidbarem* Definitionsbereich berechnen, kann man die nicht-Terminierung einfach ausschließen, indem man vor Programmausführung entscheidet, ob die Eingabe Element des Definitionsbereichs ist. Beispielsweise resultiert ein Prozeduraufruf $QUOT(EXPR, 0)$ zur Division in gängigen Programmiersprachen in einem Laufzeitfehler und nicht in einem unendlichen Programmablauf, denn es ist natürlich entscheidbar, ob der Divisor identisch 0 ist oder nicht.

Formal kann man den Unterschied zwischen “harmlosen” partiellen berechenbaren Funktionen, wie z.B. $[[QUOT]]$, und “inhärent” partiellen berechenbaren Funktionen, wie z.B. $\tilde{\chi}_H$, wie folgt charakterisieren:

Definition 9.12. Seien $\phi, \psi : \mathbb{N} \mapsto \mathbb{N}$. Dann ist ϕ weniger definiert oder gleich ψ , kurz $\phi \sqsubseteq \psi$, gdw. $\phi(n) = \perp$ oder $\phi(n) = \psi(n)$ für alle $n \in \mathbb{N}$ gilt.

Satz 9.13. Sei $\phi : \mathbb{N} \mapsto \mathbb{N}$ berechenbar, so daß $Def(\phi)$ entscheidbar ist. Dann gibt es eine totale berechenbare Funktion $\psi : \mathbb{N} \rightarrow \mathbb{N}$ mit $\phi \sqsubseteq \psi$.

Beweis. Sei $m_0 \in \mathbb{N}$ beliebig aber fest gewählt, sei PHI eine \mathcal{P} -Prozedur mit $[[PHI]] = \phi$ und sei $DECIDE_DEF_PHI \in \mathcal{P}[1]$ ein Entscheidungsverfahren für $Def(\phi)$. Für die \mathcal{P} -Prozedur PSI mit

```

procedure PSI(n) <=
begin var res;
  if DECIDE_DEF_PHI(n) then res := PHI(n) else res := m0 end_if;
  return(res)
end

```

gilt dann

$$\llbracket \text{PSI} \rrbracket(n) = \begin{cases} \phi(n) & , \text{ falls } n \in \text{Def}(\phi) \\ m_0 & , \text{ falls } n \notin \text{Def}(\phi) . \end{cases}$$

*Die Prozedur PSI terminiert, denn DECIDE_DEF_PHI terminiert und PHI(**n**) terminiert, wenn DECIDE_DEF_PHI(**n**) gilt. Für $\psi := \llbracket \text{PSI} \rrbracket$ gilt dann $\phi \sqsubseteq \psi$, ψ ist berechenbar und ψ ist total. ■*

Mit Satz 9.13 kann also jede partielle berechenbare Funktion ϕ mit entscheidbarem Definitionsbereich zu einer totalen berechenbaren Funktion ψ *erweitert* werden, die auf $\text{Def}(\phi)$ das gleiche leistet wie ϕ . In der Praxis macht man sich dies zunutze, indem man Programme, die partielle Funktionen berechnen, anstatt in eine Endlosschleife zu geraten mit Laufzeitfehlern terminieren läßt, wenn die Eingabe außerhalb des Definitionsbereichs einer solchen Funktion liegt.

10. UNENTSCHEIDBARE PROBLEME

10.1. Das Totalitätsproblem

Da wir das Halteproblem nicht entscheiden können, probieren wir einen anderen Ansatz, um nicht-terminierende Programme zu vermeiden. Man könnte ja versuchen eine Programmiersprache zu entwerfen, mit deren Programmen genau die totalen (berechenbaren) Funktionen implementiert werden können. Damit würde ein nicht-terminierendes Programm schon durch einen Übersetzer ausgeschlossen. Ein Gelingen dieses Ansatzes setzt jedoch voraus, daß das *Totalitätsproblem*

$$TOT = \{i \in \mathbb{N} \mid \varphi_i(x) \neq \perp \text{ für alle } x \in \mathbb{N}\}$$

entscheidbar ist. Das Totalitätsproblem ist jedoch noch nicht einmal rekursiv aufzählbar:

Satz 10.1. *TOT ist nicht rekursiv aufzählbar.*

Beweis. Wir führen einen Widerspruchsbeweis und nehmen an, daß *TOT* rekursiv aufzählbar sei. Dann gibt es eine totale und berechenbare Aufzählungsfunktion $\alpha : \mathbb{N} \rightarrow \mathbb{N}$ mit $\alpha(\mathbb{N}) = TOT$. Folglich gibt es eine \mathcal{P} -Prozedur ALPHA mit $\llbracket \text{ALPHA} \rrbracket = \alpha$, und mit der \mathcal{P} -Prozedur PSI, definiert durch

```
procedure PSI(x) <=
begin var y;
  y := SUCC(APPLY(PAIR2(ALPHA(x), x)));
  return(y)
end
```

erhält man eine berechenbare Funktion $\llbracket \text{PSI} \rrbracket$, für die $\llbracket \text{PSI} \rrbracket(j) = 1 + \mathbf{u}_{\mathcal{P}}(\pi^2(\alpha(j), j)) = 1 + \varphi_{\alpha(j)}(j)$ gilt. Mit $\alpha(j) \in TOT$ ist $\varphi_{\alpha(j)}$ total. Damit ist auch $\llbracket \text{PSI} \rrbracket$ total, und folglich gilt $\natural\text{PSI} \in TOT$. Mit der Surjektivität von α gibt es ein $i \in \mathbb{N}$, so daß $\alpha(i) = \natural\text{PSI}$. Damit gilt $\llbracket \text{PSI} \rrbracket = \varphi_{\alpha(i)}$ und man erhält $\llbracket \text{PSI} \rrbracket(i) = 1 + \varphi_{\alpha(i)}(i) = 1 + \llbracket \text{PSI} \rrbracket(i)$. Dies ist aber unmöglich, denn $\llbracket \text{PSI} \rrbracket$ ist total, also gilt $\llbracket \text{PSI} \rrbracket(i) \in \mathbb{N}$ und damit $\llbracket \text{PSI} \rrbracket(i) \neq 1 + \llbracket \text{PSI} \rrbracket(i)$. \blacktriangledown Also ist *TOT* nicht rekursiv aufzählbar. \blacksquare

Bemerkung 10.2. *Im Beweis von Satz 10.1 wird die gleiche Argumentationsweise, nämlich die Diagonalisierung, verwendet wie im Beweis von Satz 5.4. Trotzdem folgt Satz 10.1 nicht aus Satz 5.4, da dieser eine Aussage über die Menge aller totalen Funktionen macht und aus der nicht-Abzählbarkeit einer Menge – hier $\mathcal{F}_{tot} = \{\phi : \mathbb{N} \rightarrow \mathbb{N}\}$ – nicht folgt, daß eine Teilmenge – hier $\{\varphi_i : \mathbb{N} \rightarrow \mathbb{N} \mid i \in TOT\}$ – auch nicht abzählbar ist. Umgekehrt folgt auch Satz 5.4 nicht aus Satz 10.1, denn TOT ist abzählbar, und so kann nicht mit Satz 5.3 auf die nicht-Abzählbarkeit von \mathcal{F}_{tot} geschlossen werden.*

Eine Konsequenz von Satz 10.1 ist, daß es für jede Programmiersprache, in der *nur* terminierende Programme geschrieben werden können – wir werden solch eine Programmiersprache in Kapitel 11 definieren –, eine totale berechenbare Funktion gibt, die durch kein Programm dieser Programmiersprache berechnet werden kann. Verwendet man dagegen eine Programmiersprache, in der *alle* totalen berechenbaren Funktionen programmiert werden können – was für \mathcal{P} und für alle gängigen Programmiersprachen gilt –, so muß man in Kauf nehmen, daß auch nicht-terminierende Programme in dieser Programmiersprache geschrieben werden können.

Eine weitere Konsequenz von Satz 10.1 ist, daß jedes *Terminierungsbeweisverfahren*, also ein Verfahren, das für *terminierende* Prozeduren als Eingabe einen Terminierungsbeweis für diese Prozedur berechnet, *unvollständig* ist. Anders gesagt, für jedes (korrekte) Terminierungsbeweisverfahren kann man eine terminierende Prozedur angeben, für die das Verfahren *keinen* Beweis berechnen kann. Dabei ist natürlich nicht ausgeschlossen, daß man die Totalität von berechenbaren Funktionen nicht doch beweisen oder widerlegen kann. Mit Satz 10.1 ist es nur unmöglich, ein Verfahren anzugeben, mit dem die Totalität *jeder* totalen berechenbaren Funktion bewiesen wird.

10.2. Reduzierbarkeit

In den Abschnitten 3.3 und 7.2 wurde schon gezeigt, daß man die Berechenbarkeit einer Funktion nachweisen kann, ohne konkret ein Programm anzugeben, das diese Funktion berechnet. Ursache war dort, daß man für eine berechenbare Funktion ϕ eine Menge von Programmen angeben kann, so daß eines dieser Programme die Funktion auch tatsächlich berechnet, jedoch unbekannt ist, *welches* dieser Programme konkret das Gewünschte leistet.

In diesem Abschnitt betrachten wir eine andere Vorgehensweise, um die Berechenbarkeit einer Funktion nachzuweisen, ohne dabei ein konkretes Programm anzugeben. Seien beispielsweise $\phi : \mathbb{N} \rightarrow \mathbb{N}$ und $\psi : \mathbb{N} \rightarrow \mathbb{N}$ Funktionen mit

$\psi(n) = \phi(\pi^2(n, n))$ für alle $n \in \mathbb{N}$. Um zu zeigen, daß ψ \mathcal{P} -berechenbar ist, reicht es offensichtlich nachzuweisen, daß ϕ berechenbar ist. Wir müssen dann für ψ kein konkretes Programm $P \in \mathcal{P}$ mit $\psi = \llbracket P \rrbracket$ angeben. Wir haben hier die Aufgabe, die Berechenbarkeit von ψ zu beweisen, auf die Aufgabe, die Berechenbarkeit von ϕ nachzuweisen, *reduziert*.

Man kann natürlich einwenden, daß wir hier ja nur eine Aufgabe durch eine andere Aufgabe ersetzt haben, und somit nichts gewonnen ist. Daher versucht man, ein Problem auf ein *gelöstes* Problem zu *reduzieren*. Beispielsweise können wir die Frage, ob die Quadratfunktion x^2 berechenbar ist, auf die Frage reduzieren, ob die Multiplikationsfunktion $x \times y$ berechenbar ist, denn $x^2 = x \times x$. Da wir wissen, daß $x \times y$ berechenbar ist, ist die Berechenbarkeit von x^2 ohne Angabe eines konkreten Programms bewiesen.

Wir präzisieren jetzt den Begriff “reduzierbar” und definieren:

Definition 10.3. Ein Problem $M \subseteq \mathbb{N}$ ist genau dann auf ein Problem $N \subseteq \mathbb{N}$ reduzierbar, wenn es eine totale und berechenbare Funktion $\varrho : \mathbb{N} \rightarrow \mathbb{N}$ gibt, so daß $m \in M \Leftrightarrow \varrho(m) \in N$ für alle $m \in \mathbb{N}$ gilt. In diesem Fall schreiben wir kurz $M \preceq_{\varrho} N$. ■

Die Reduzierbarkeit von M auf N bedeutet also, M in *berechenbarer* Weise, nämlich mittels ϱ , als *Spezialfall* von N darzustellen. Dies kann dann ausgenutzt werden, um von der (semi-)Entscheidbarkeit von N auf die (semi-)Entscheidbarkeit von M zu schließen:

Satz 10.4. Für $M \subseteq \mathbb{N}$ und $N \subseteq \mathbb{N}$ mit $M \preceq_{\varrho} N$ gilt:

1. Wenn N entscheidbar ist, so ist auch M entscheidbar.
2. Wenn N semi-entscheidbar ist, so ist auch M semi-entscheidbar.

Beweis. (1) Mit Satz 3.3 ist $\chi_N \circ \varrho$ berechenbar, denn χ_N und ϱ sind nach Voraussetzung berechenbar. Wenn $m \in M$, so gilt $\varrho(m) \in N$ mit der Definition von ϱ , und mit der Definition von χ_N gilt dann $\chi_N(\varrho(m)) = 1$. Für $m \notin M$ gilt $\varrho(m) \notin N$ mit der Definition von ϱ , und mit der Definition von χ_N gilt dann $\chi_N(\varrho(m)) = 0$. Also gilt $\chi_N \circ \varrho = \chi_M$.

(2) Wie in (1) zeigt man $\tilde{\chi}_N \circ \varrho \cong_M \tilde{\chi}_M$. ■

Beispielsweise können wir so einfach zeigen, daß das Selbstanwendbarkeitsproblem S semi-entscheidbar ist, indem S auf das Halteproblem H reduziert wird (vgl. den Beweis von Korollar 7.12): Wir definieren einfach $\varrho : \mathbb{N} \rightarrow \mathbb{N}$ durch

$\varrho(n) := \pi^2(n, n)$, und offensichtlich ist ϱ berechenbar. Es gilt $n \in S \Leftrightarrow \varrho(n) \in H$ für alle $n \in \mathbb{N}$, und da H semi-entscheidbar ist, ist mit Satz 10.4(2) auch S semi-entscheidbar.

Anstatt Satz 10.4 direkt in einem Beweis zu verwenden, wird häufig die Kontraposition von Satz 10.4 angewandt:

Korollar 10.5. *Für $M \subseteq \mathbb{N}$ und $N \subseteq \mathbb{N}$ mit $M \preceq_{\varrho} N$ gilt:*

1. *Wenn M nicht entscheidbar ist, so ist auch N nicht entscheidbar.*
2. *Wenn M nicht semi-entscheidbar ist, so ist auch N nicht semi-entscheidbar.*

Beispielsweise können wir mit Korollar 10.5 einfach zeigen, daß das Halteproblem H unentscheidbar ist, indem das Selbstanwendbarkeitsproblem S mit $\varrho(n) := \pi^2(n, n)$ auf H reduziert wird (vgl. den Beweis von Satz 5.9). Da S nicht entscheidbar ist, ist mit Korollar 10.5(1) auch H nicht entscheidbar (siehe auch Bemerkung 10.10).

10.3. Das *s-m-n*-Theorem

Sei `procedure EXP(y, z) <= BODY_EXP` eine \mathcal{P} -Prozedur mit $\llbracket \text{EXP} \rrbracket(y, z) = z^y$.¹ Dann können wir mit

$$\text{procedure SQUARE}(z) \text{ <= BODY_EXP}[y/2]$$

eine Prozedur zur Berechnung der Quadratfunktion angeben. Dabei entsteht der Prozedurrumpf `BODY_EXP[y/2]` von `SQUARE` aus dem Prozedurrumpf `BODY_EXP` von `EXP`, indem in `BODY_EXP` jedes Vorkommen des formalen Parameters `y` durch die Konstante 2 ersetzt wird. Damit gilt $\llbracket \text{SQUARE} \rrbracket(z) = \llbracket \text{EXP} \rrbracket(2, z) = z^2$, d.h. wir haben aus einer 2-stelligen Funktion eine 1-stellige Funktion gewonnen, indem wir für einen formalen Parameter, nämlich `y`, einen festen Wert, nämlich 2, eingesetzt haben. Man sagt auch, die Prozedur `EXP` wurde *parametrisiert*.

Um allgemein parametrisierte Prozeduren zu erhalten, erlauben wir jetzt in einem \mathcal{P} -Programm für eine gegebene Prozedur

$$\text{procedure PROC}(y_1, \dots, y_m, z_1, \dots, z_n) \text{ <= BODY_PROC}$$

¹ In diesem und in den folgenden Abschnitten verwenden wir Prozeduren mit *mehreren* Parametern und arithmetische Funktionen $\phi : \mathbb{N} \times \dots \times \mathbb{N} \mapsto \mathbb{N}$ mit *mehreren* Argumenten. Dies geschieht allein aus Gründen der Lesbarkeit und bedeutet keine Abänderung unseres formalen Rahmens, vgl. Abschnitt 4.3.

Prozeduraufrufe der Form

$$\text{PROC}[k_1, \dots, k_m](\text{EXPR1}, \dots, \text{EXPRn})$$

mit $k_1, \dots, k_m \in \mathbb{N}$, wobei wir uns jede *parametrisierte Prozedur* $\text{PROC}[k_1, \dots, k_m]$ durch

$$\begin{aligned} \text{procedure } \text{PROC}[k_1, \dots, k_m](z_1, \dots, z_n) &<= \\ \text{BODY_PROC}[y_1/k_1, \dots, y_m/k_m] \end{aligned} \quad (10.1)$$

definiert vorstellen. Damit stehen uns im Beispiel beliebig viele Prozeduren

$$\begin{aligned} \text{procedure } \text{EXP}[0](z) &<= \text{BODY_EXP}[y/0] \\ \text{procedure } \text{EXP}[1](z) &<= \text{BODY_EXP}[y/1] \\ \text{procedure } \text{EXP}[2](z) &<= \text{BODY_EXP}[y/2] \\ \text{procedure } \text{EXP}[3](z) &<= \text{BODY_EXP}[y/3] \\ &\dots \end{aligned}$$

zur Verfügung, für die $\llbracket \text{EXP}[k] \rrbracket(z) = \llbracket \text{EXP} \rrbracket(k, z) = z^k$ gilt, wobei k eine beliebige, aber *feste* natürliche Zahl ist.

Es stellt sich natürlich sofort die Frage, warum wir in einem Programm Aufrufe parametrisierter Prozeduren, wie z.B. $\text{EXP}[2](\text{EXPR})$, verwenden sollen, anstatt einfach die Originalprozedur mit den entsprechenden aktuellen Parametern, also etwa $\text{EXP}(2, \text{EXPR})$, aufzurufen. Der Grund ist, daß wir mittels Parametrisierung den Code eines Programms in Abhängigkeit von aktuellen Parametern berechnen können: Für jedes Programm $P \in \mathcal{P}$ gilt $\llbracket P \rrbracket = \varphi_{\natural P}$, also beispielsweise $\llbracket \text{EXP} \rrbracket = \varphi_{\natural \text{EXP}}$ und $\llbracket \text{EXP}[k] \rrbracket = \varphi_{\natural \text{EXP}[k]}$ für jedes $k \in \mathbb{N}$. Mit (10.1) erhält man offenbar $\natural \text{EXP}[k]$ allein aus $\natural \text{EXP}$ und k , denn $\text{EXP}[k]$ wird allein aus EXP und k gebildet. Anders gesagt, es gilt $\natural \text{EXP}[k] = s(\natural \text{EXP}, k)$ für eine Funktion $s : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, und man erhält damit $\llbracket \text{EXP}[k] \rrbracket = \varphi_{s(\natural \text{EXP}, k)}$.²

Diese Konstruktion kann man natürlich mit beliebigen Programmen und beliebigen Parametern durchführen.³ Wir zeigen, daß die Funktion s , mit der der

² Dabei gehen wir davon aus, daß EXP selbst keine Prozeduraufrufe enthält. Dies kann immer durch "Einkopieren" der aufgerufenen Prozedur erreicht werden, denn rekursiv definierte Prozeduren sind verboten, vgl. Definition 2.2. Diese Forderung ist notwendig, da EXP sonst von weiteren Prozeduren P_1, \dots, P_j abhängt und wir folglich $\natural \text{EXP}[k] = s(\natural \text{EXP}, k, \natural P_1, \dots, \natural P_j)$ definieren müßten.

³ Unsere Notation zur Parametrisierung von Prozeduren hat allerdings die Schwäche, daß nur formale Parameter *vom Anfang* der Parameterliste durch Konstanten aus \mathbb{N} ersetzt werden können. Beispielsweise gilt auch $\llbracket \text{EXP} \rrbracket(y, 2) = 2^y$, die 2er Potenz kann aber in unserer Notation nicht durch Parametrisierung von EXP gewonnen werden. Um dieser Schwäche abzuweichen, müßte unsere Notation entsprechend erweitert werden. Wir verzichten darauf, da die verwendete Notation für unsere Zwecke ausreicht.

Kode eines parametrisierten Programms aus dem Ursprungsprogramm und den Parametern gewonnen wird, berechenbar und total ist:

Satz 10.6. (*s-m-n-Theorem*) Sei $i \in \mathbb{N}$ mit $\varphi_i : \mathbb{N}^{m+n} \mapsto \mathbb{N}$. Dann gibt es eine berechenbare und totale Funktion $s_n^m : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$ mit

$$\varphi_{s_n^m(i, y_1, \dots, y_m)}(z_1, \dots, z_n) = \varphi_i(y_1, \dots, y_m, z_1, \dots, z_n) \quad (10.2)$$

für alle $(y_1, \dots, y_m, z_1, \dots, z_n) \in \mathbb{N}^{m+n}$.

Beweis. Sei

procedure PROC($y_1, \dots, y_m, z_1, \dots, z_n$) <= BODY_PROC

eine Prozedur mit $\natural\text{PROC} = i$. Dann berechnen wir $s_n^m(i, y_1, \dots, y_m)$ wie folgt: Jedem m -Tupel $(y_1, \dots, y_m) \in \mathbb{N}^m$ ordnen wir die Prozedur

$$\begin{aligned} \text{procedure PROC}[y_1, \dots, y_m](z_1, \dots, z_n) <= \\ \text{BODY_PROC}[y_1/y_1, \dots, y_m/y_m] \end{aligned} \quad (10.3)$$

zu, und damit gilt

$$\llbracket \text{PROC}[y_1, \dots, y_m] \rrbracket(z_1, \dots, z_n) = \llbracket \text{PROC} \rrbracket(y_1, \dots, y_m, z_1, \dots, z_n). \quad (10.4)$$

Mit $\text{PROC}[y_1, \dots, y_m]$ definieren jetzt

$$s_n^m(\natural\text{PROC}, y_1, \dots, y_m) := \natural\text{PROC}[y_1, \dots, y_m]. \quad (10.5)$$

Da wir $\text{PROC}[y_1, \dots, y_m]$ mit (10.3) allein aus $\natural\text{PROC}$ und y_1, \dots, y_m bilden, ist s_n^m berechenbar: Wir dekodieren $\natural\text{PROC}$ mit \natural^{-1} zu der Prozedur PROC , ersetzen dann die formalen Parameter y_i im Rumpf von PROC durch y_i und berechnen schließlich mit \natural den Kode $\natural\text{PROC}[y_1, \dots, y_m]$ der so erhaltenen Prozedur $\text{PROC}[y_1, \dots, y_m]$. Da die Funktionen \natural und \natural^{-1} total und algorithmisch sind, ist s_n^m total und berechenbar. Es gilt

$$\begin{aligned} & \varphi_{s_n^m(\natural\text{PROC}, y_1, \dots, y_m)}(z_1, \dots, z_n) \\ &= \varphi_{\natural\text{PROC}[y_1, \dots, y_m]}(z_1, \dots, z_n) \quad , \text{ mit (10.5),} \\ &= \llbracket \text{PROC}[y_1, \dots, y_m] \rrbracket(z_1, \dots, z_n) \quad , \text{ denn } \varphi_{\natural\text{PROC}[y_1, \dots, y_m]} = \llbracket \text{PROC}[y_1, \dots, y_m] \rrbracket, \\ &= \llbracket \text{PROC} \rrbracket(y_1, \dots, y_m, z_1, \dots, z_n) \quad , \text{ mit (10.4),} \\ &= \varphi_{\natural\text{PROC}}(y_1, \dots, y_m, z_1, \dots, z_n) \quad , \text{ denn } \llbracket \text{PROC} \rrbracket = \varphi_{\natural\text{PROC}}, \end{aligned}$$

und damit ist (10.2) bewiesen. ■

Wir illustrieren die Anwendung des *s-m-n*-Theorems mit dem Beweis des folgenden Satzes:

Satz 10.7. *Es gibt eine berechenbare und totale Funktion $h : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$, so daß für alle Funktionen $\varphi_j : \mathbb{N}^n \mapsto \mathbb{N}$ und $\varphi_i : \mathbb{N} \mapsto \mathbb{N}$ gilt:*

$$\varphi_{h(i,j)} = \varphi_i \circ \varphi_j. \quad (10.6)$$

Beweis. Sei $\theta : \mathbb{N}^{n+2} \mapsto \mathbb{N}$ definiert durch $\theta(i, j, x_1, \dots, x_n) := \varphi_i(\varphi_j(x_1, \dots, x_n))$. Für die \mathcal{P} -Prozedur

```

procedure THETA(i, j, x1, ..., xn) <=
begin var y;
  y := APPLY(PAIR2(i, APPLY(PAIRn+1(j, x1, ..., xn))));
  return(y)
end

```

gilt dann $\llbracket \text{THETA} \rrbracket = \theta$, damit ist θ berechenbar, und man erhält $\theta = \varphi_{\llbracket \text{THETA} \rrbracket}$. Mit dem *s-m-n*-Theorem 10.6 ist dann $h : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ mit $h(i, j) := s_n^2(\llbracket \text{THETA} \rrbracket, i, j)$ total und berechenbar, und mit

$$\begin{aligned}
\varphi_{h(i,j)}(x_1, \dots, x_n) &= \varphi_{s_n^2(\llbracket \text{THETA} \rrbracket, i, j)}(x_1, \dots, x_n) && \text{, mit Definition } h, \\
&= \varphi_{\llbracket \text{THETA} \rrbracket}(i, j, x_1, \dots, x_n) && \text{, mit dem s-m-n-Theorem 10.6,} \\
&= \theta(i, j, x_1, \dots, x_n) && \text{, mit Definition THETA,} \\
&= \varphi_i(\varphi_j(x_1, \dots, x_n)) && \text{, mit Definition } \theta .
\end{aligned}$$

ist (10.6) bewiesen. ■

10.4. Programmäquivalenz

Wenn wir ein Programm schreiben, um eine bestimmte Aufgabe mittels eines Rechners zu lösen, müssen wir uns vergewissern, daß das Programm auch das Geforderte leistet. Wir müssen also unsere Programme *verifizieren*. Dabei stellt sich natürlich die Frage, wie wir angeben, was genau das Programm leisten soll, d.h. wie man ein Programm *spezifiziert*.

Ein Ansatz dazu besteht darin, daß wir ein alternatives Programm angeben und dann zeigen, daß beide Programme die gleiche Funktion berechnen, d.h. daß beide Programme *äquivalent* sind. Natürlich ist dieser Ansatz nicht für jedes Programm praktikabel – es ergibt offenbar keinen Sinn etwa einen Übersetzer zu spezifizieren, indem man einen zweiten Übersetzer schreibt und dann zeigt, daß

beide Programme das gleiche leisten. Für bestimmte Aufgaben ist dieser Ansatz jedoch trotzdem nützlich:

In der Informatik sind wir auch an *effizienten* Programmen interessiert, d.h. an Programmen, die möglichst wenig Speicher bzw. Rechenzeit benötigen. Nun kommt es oft vor, daß für eine Aufgabe sowohl ein effizienter, jedoch komplizierter Algorithmus als auch ein einfacher, aber ineffizienter Algorithmus existiert. Beispielsweise ist *InsertionSort*, also “Sortieren durch Einfügen”, einfach aber ineffizient, während *Heapsort* ein effizientes Sortierverfahren ist, das jedoch eine wesentlich kompliziertere Programmstruktur als *InsertionSort* aufweist. Damit ist auch die Verifikation von *Heapsort* wesentlich aufwendiger als die Verifikation von *InsertionSort*. Man kann jedoch *Heapsort* auch dadurch verifizieren, indem man zunächst die Korrektheit von *InsertionSort* direkt zeigt, und dann in einem zweiten Schritt nachweist, daß *InsertionSort* und *Heapsort* äquivalent sind, also die gleichen Funktionen berechnen. Bei diesem Verifikationsansatz verwenden wir also *InsertionSort*, um *Heapsort* zu *spezifizieren*. Genauso könnten wir einen Übersetzer als Spezifikation für die *optimierte Version* des Übersetzers verwenden. Mit dem Nachweis der Äquivalenz beider Programme wäre dann gezeigt, daß beide Übersetzer (abgesehen von der Laufzeit) das Gleiche leisten.

Den Nachweis der Programmäquivalenz wollen wir natürlich einem Rechner überlassen. Anders gesagt, wir wollen ein Werkzeug entwickeln, mit dem für beliebige Programme P_1 und P_2 entschieden werden kann, ob $\llbracket P_1 \rrbracket = \llbracket P_2 \rrbracket$ gilt. Bevor wir beginnen dieses Werkzeug zu entwickeln, untersuchen wir natürlich, ob diese Aufgabe überhaupt lösbar ist. Formal heißt das, wir untersuchen, ob das *Äquivalenzproblem*

$$EQV := \{ \pi^2(i, j) \in \mathbb{N} \mid \varphi_i = \varphi_j \}$$

entscheidbar ist.

Wir beginnen dazu mit einem einfacheren Problem: Wir wollen feststellen, ob ein beliebiges Programm P die Identitätsfunktion berechnet, d.h. ob $\llbracket P \rrbracket(n) = n$ für alle $n \in \mathbb{N}$ gilt. Formal heißt das, wir untersuchen die Entscheidbarkeit des *Identitätsproblems*

$$ID := \{ i \in \mathbb{N} \mid \varphi_i(n) = n \text{ für alle } n \in \mathbb{N} \}.$$

Folgender Satz zeigt jedoch, daß ID noch nicht einmal semi-entscheidbar ist:

Satz 10.8. *ID ist nicht semi-entscheidbar.*

Beweis. Sei $\psi : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ definiert durch

$$\psi(i, j) := \begin{cases} j & , \text{ falls } \varphi_i(j) \neq \perp, \\ \perp & , \text{ falls } \varphi_i(j) = \perp. \end{cases}$$

Für das Programm $\text{PSI} \in \mathcal{P}$ mit

```

procedure PSI(i, j) <=
begin var y, z;
  y := j;
  z := APPLY(PAIR2(i, j));
  return(y)
end

```

gilt $\psi = \llbracket \text{PSI} \rrbracket$, d.h. ψ ist mit PSI berechenbar und folglich gilt $\psi = \varphi_{\text{PSI}}$. Mit dem s-m-n-Theorem 10.6 gilt dann

$$\varphi_{\text{PSI}}(i, j) = \varphi_{s_1^1(\text{PSI}, i)}(j) . \quad (10.7)$$

Wir zeigen jetzt, daß das Totalitätsproblem TOT mittels der (totalen und berechenbaren) Funktion $s_1^1(\text{PSI}, i)$ auf ID reduzierbar ist, d.h. es gilt:

$$i \in TOT \Leftrightarrow s_1^1(\text{PSI}, i) \in ID . \quad (10.8)$$

“ \Rightarrow ” Für $i \in TOT$ gilt $\varphi_i(j) \neq \perp$ für alle $j \in \mathbb{N}$, also $\varphi_{\text{PSI}}(i, j) = j$ mit Definition von ψ . Mit (10.7) erhält man $\varphi_{s_1^1(\text{PSI}, i)}(j) = j$ für alle $j \in \mathbb{N}$ und folglich $s_1^1(\text{PSI}, i) \in ID$.

“ \Leftarrow ” Für $i \notin TOT$ gilt $\varphi_i(j) = \perp$ für ein $j \in \mathbb{N}$, also $\varphi_{\text{PSI}}(i, j) \neq j$ mit Definition von ψ . Mit (10.7) erhält man $\varphi_{s_1^1(\text{PSI}, i)}(j) \neq j$ und folglich $s_1^1(\text{PSI}, i) \notin ID$.

Mit den Sätzen 10.1 und 9.3 ist das Totalitätsproblem TOT nicht semi-entscheidbar. Mit Korollar 10.5 ist ID dann ebenfalls nicht semi-entscheidbar. ■

Da das Identitätsproblem ID ein Spezialfall des Äquivalenzproblems EQV ist, können wir ID auf EQV reduzieren und damit zeigen:

Korollar 10.9. EQV ist nicht semi-entscheidbar.

Beweis. Die Identitätsfunktion ist berechenbar, etwa durch ein Programm IDENT . Mit $\varrho : \mathbb{N} \rightarrow \mathbb{N}$ definiert durch $\varrho(i) := \pi^2(\text{IDENT}, i)$ gilt $i \in ID \Leftrightarrow \varrho(i) \in EQV$, d.h. $ID \preceq_{\varrho} EQV$, denn ϱ ist offensichtlich total und berechenbar. Mit Satz 10.8 und Korollar 10.5 ist dann auch EQV nicht semi-entscheidbar. ■

Bemerkung 10.10. Der Beweis von Korollar 10.9 illustriert die Nützlichkeit von Satz 10.4 in Form von Korollar 10.5: Es ist oft schwieriger, die (semi-)Unentscheidbarkeit eines allgemeinen Problems – wie etwa EQV – direkt zu beweisen, anstatt die (semi-)Unentscheidbarkeit eines Spezialfalls des Problems – wie etwa ID – direkt nachzuweisen und dann eine berechenbare Reduktion des Spezialfalls auf das allgemeine Problem anzugeben.

Als Konsequenz von Korollar 10.9 ist es also unmöglich das gewünschte Verifikationswerkzeug zu implementieren. Nun könnte man als Alternative ja versuchen statt dessen nicht-Äquivalenz algorithmisch festzustellen. Beispielsweise könnte man dann maschinell feststellen, daß ein Programm P nicht das Gleiche leistet wie dessen optimierte Version, bei Modifikation von P also (mindestens) ein Fehler gemacht wurde. Dieser Ansatz gelingt allerdings nur, falls das Komplement des Äquivalenzproblems

$$\overline{EQV} := \{\pi^2(i, j) \in \mathbb{N} \mid \varphi_i \neq \varphi_j\}$$

semi-entscheidbar ist. Dies ist jedoch nicht der Fall:

Satz 10.11. \overline{EQV} ist nicht semi-entscheidbar.

Beweis. Sei $\psi : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ definiert durch

$$\psi(i, n) := \begin{cases} n & , \text{ falls } \varphi_i(i) \neq \perp, \\ \perp & , \text{ falls } \varphi_i(i) = \perp. \end{cases}$$

Für das Programm $\text{PSI} \in \mathcal{P}$ mit

```

procedure PSI(i, n) <=
begin var y, z;
  y := n;
  z := APPLY(PAIR2(i, i));
  return(y)
end

```

gilt $\psi = \llbracket \text{PSI} \rrbracket$, d.h. ψ ist mit PSI berechenbar und folglich gilt $\psi = \varphi_{\text{PSI}}$. Mit dem s-m-n-Theorem 10.6 gilt dann

$$\varphi_{\text{PSI}}(i, n) = \varphi_{s_1^1(\text{PSI}, i)}(n) \quad (10.9)$$

sowie für das Komplement \overline{S} des Selbstanwendungsproblems

$$i \in \overline{S} \Leftrightarrow \varphi_{\text{PSI}}(i, n) = \perp \text{ für ein } n \in \mathbb{N} \quad (10.10)$$

denn für $i \in \overline{S}$ gilt $\varphi_i(i) = \perp$ und mit Definition von ψ dann $\varphi_{\text{PSI}}(i, n) = \perp$ für ein $n \in \mathbb{N}$. Gilt $\varphi_{\text{PSI}}(i, n) = \perp$ für ein $n \in \mathbb{N}$, so erhält man $\varphi_i(i) = \perp$ mit Definition von ψ , also $i \in \overline{S}$.

Wir zeigen jetzt, daß das \overline{S} mittels der (totalen und berechenbaren) Funktion $\pi^2(s_1^1(\text{PSI}, i), \text{IDENT})$ auf \overline{EQV} reduzierbar ist, d.h. es gilt

$$i \in \overline{S} \Leftrightarrow \pi^2(s_1^1(\text{PSI}, i), \text{IDENT}) \in \overline{EQV} \quad (10.11)$$

denn

$$\begin{aligned}
& i \in \overline{S} \\
\Leftrightarrow & \varphi_{\dagger\text{PSI}}(i, n) = \perp \text{ für ein } n \in \mathbb{N} && , \text{ mit 10.10} \\
\Leftrightarrow & \varphi_{\dagger\text{PSI}}(i, n) \neq n \text{ für ein } n \in \mathbb{N} && , \text{ mit Definition von } \psi \\
\Leftrightarrow & \varphi_{s_1^1(\dagger\text{PSI}, i)}(n) \neq n \text{ für ein } n \in \mathbb{N} && , \text{ mit 10.9} \\
\Leftrightarrow & \varphi_{s_1^1(\dagger\text{PSI}, i)}(n) \neq \varphi_{\dagger\text{IDENT}}(n) \text{ für ein } n \in \mathbb{N} \\
\Leftrightarrow & \varphi_{s_1^1(\dagger\text{PSI}, i)} \neq \varphi_{\dagger\text{IDENT}} \\
\Leftrightarrow & \pi^2(s_1^1(\dagger\text{PSI}, i), \dagger\text{IDENT}) \in \overline{EQV} .
\end{aligned}$$

Mit Korollar 8.9 ist das Komplement \overline{S} des Selbstanwendungsproblems nicht semi-entscheidbar, und mit Korollar 10.5 ist \overline{EQV} dann ebenfalls nicht semi-entscheidbar. ■

Mit Korollar 10.9 bzw. Satz 10.11 ist natürlich nicht ausgeschlossen, daß man die Äquivalenz von bestimmten Programmen maschinell beweisen bzw. widerlegen kann. Mit diesen Aussagen ist lediglich gezeigt, daß es kein Verfahren gibt mit dem die Äquivalenz für alle äquivalenten Programme bewiesen bzw. für alle nicht-äquivalenten Programme widerlegt werden kann.

10.5. Der Satz von Rice

Wir betrachten noch einmal das Verifikationsproblem, das schon in Abschnitt 10.4 angesprochen wurde. Im allgemeinen ist man an *Eigenschaften* der Funktionen, die von einem Programm berechnet werden, interessiert. Für die Prozedur **GGT** aus Abbildung 2.4 möchte man beispielsweise wissen, ob $\llbracket \text{GGT} \rrbracket$ eine *idempotente* Funktion ist, d.h. $\llbracket \text{GGT} \rrbracket(x, x) = x$, ob $\llbracket \text{GGT} \rrbracket$ *assoziativ* ist, d.h. $\llbracket \text{GGT} \rrbracket(x, \llbracket \text{GGT} \rrbracket(y, z)) = \llbracket \text{GGT} \rrbracket(\llbracket \text{GGT} \rrbracket(x, y), z)$, oder ob $\llbracket \text{GGT} \rrbracket$ *kommutativ* ist, d.h. $\llbracket \text{GGT} \rrbracket(x, y) = \llbracket \text{GGT} \rrbracket(y, x)$.

Um beispielsweise die Assoziativität von $\llbracket \text{GGT} \rrbracket$ zu verifizieren, betrachten wir die Menge $\Phi_{\text{ass}} = \{\phi \in \llbracket \mathcal{P} \rrbracket \mid \phi \text{ ist assoziativ}\}$ und versuchen dann zu entscheiden, ob $\llbracket \text{GGT} \rrbracket \in \Phi_{\text{ass}}$ gilt. In Φ_{ass} sind alle berechenbaren arithmetischen assoziativen Funktionen enthalten, also etwa auch die Addition und die Multiplikation, aber z.B. nicht die (abgerundete) Division. Im Unterschied zum Äquivalenzproblem *EQV* aus Abschnitt 10.4, bei dem entschieden werden soll, ob zwei Programme die gleiche Funktion berechnen, fragen wir hier allgemein, ob die Funktion, die durch ein bestimmtes Programm berechnet wird, eine bestimmte Eigenschaft hat.

Natürlich stellt sich die Frage, wie man Mengen von Funktionen, wie z.B. Φ_{ass} , *repräsentiert*. Da wir nur berechenbare Funktionen betrachten, können wir anstatt

Φ_{ass} die Menge \mathcal{P}_{ass} aller Programme P mit $\llbracket P \rrbracket(x, \llbracket P \rrbracket(y, z)) = \llbracket P \rrbracket(\llbracket P \rrbracket(x, y), z)$ betrachten. Diese Menge kodieren wir dann, wodurch wir die Menge $\natural\Phi_{ass} := \natural\mathcal{P}_{ass} = \{i \in \mathbb{N} \mid \varphi_i \in \Phi_{ass}\}$ erhalten. Anstatt “ $\llbracket \text{GGT} \rrbracket \in \Phi_{ass}$?” fragen wir jetzt also, ob $\natural\text{GGT} \in \natural\Phi_{ass}$ gilt, denn $\llbracket \text{GGT} \rrbracket \in \Phi_{ass}$ gdw. $\natural\text{GGT} \in \natural\Phi_{ass}$.

Damit dieser Ansatz zur Programmverifikation gelingt, muß $\natural\Phi_{ass}$ *entscheidbar* sein. Dies ist jedoch nicht der Fall, wie folgender Satz zeigt:

Satz 10.12. (Satz von Rice) Sei $\emptyset \subsetneq \Phi \subsetneq \llbracket \mathcal{P} \rrbracket$ und sei $\natural\Phi = \{i \in \mathbb{N} \mid \varphi_i \in \Phi\}$. Dann ist $\natural\Phi$ nicht entscheidbar.

Beweis. Sei $\theta : \mathbb{N} \mapsto \mathbb{N}$ mit $\theta \in \llbracket \mathcal{P} \rrbracket$ und $\theta \neq \omega$ beliebig gewählt, sei THETA eine \mathcal{P} -Prozedur mit $\llbracket \text{THETA} \rrbracket = \theta$ und sei die \mathcal{P} -Prozedur PROC gegeben durch

```

procedure PROC(i, j) <=
begin var res;
  if SEMI_DECIDE_S(i)
    then res := THETA(j)
    else res := CYCLE1(j)
  end_if;
return(res)
end

```

(10.12)

wobei SEMI_DECIDE_S mit $\llbracket \text{SEMI_DECIDE_S} \rrbracket = \tilde{\chi}_S$ ein semi-Entscheidungsverfahren für das Selbstanwendungsproblem S ist, vgl. Korollar 7.12. Mit dem s-m-n-Theorem 10.6 gilt dann

$$\varphi_{s_1^1(\natural\text{PROC}, i)}(j) = \varphi_{\natural\text{PROC}}(i, j) = \llbracket \text{PROC} \rrbracket(i, j) \quad (10.13)$$

und damit ist $\varrho : \mathbb{N} \rightarrow \mathbb{N}$, definiert durch

$$\varrho(i) := s_1^1(\natural\text{PROC}, i), \quad (10.14)$$

total und berechenbar. Weiter gilt mit (10.12)

$$\llbracket \text{PROC} \rrbracket(i, j) = \begin{cases} \theta(j) & , \text{ falls } i \in S \\ \omega(j) & , \text{ falls } i \notin S \end{cases} \quad (10.15)$$

und für $i \in S$ damit dann $\llbracket \text{PROC} \rrbracket(i, j) = \theta(j)$ für alle $j \in \mathbb{N}$, also

$$i \in S \Rightarrow \varphi_{s_1^1(\natural\text{PROC}, i)} = \theta. \quad (10.16)$$

mit (10.13). Für $i \notin S$ gilt $\llbracket \text{PROC} \rrbracket(i, j) = \omega(j)$ für alle $j \in \mathbb{N}$, und damit

$$i \notin S \Rightarrow \varphi_{s_1^1(\natural\text{PROC}, i)} = \omega. \quad (10.17)$$

Angenommen, es gilt $\omega \notin \Phi$. Mit $\Phi \neq \emptyset$ gilt dann o.B.d.A. $\theta \in \Phi$,⁴ und damit

$$\begin{aligned} i \in S &\Leftrightarrow \varphi_{s_1^1(\mathfrak{h}\text{PROC}, i)} \in \Phi && , \text{ mit (10.16) und (10.17),} \\ &\Leftrightarrow s_1^1(\mathfrak{h}\text{PROC}, i) \in \mathfrak{h}\Phi && , \text{ mit Definition von } \mathfrak{h}\Phi, \\ &\Leftrightarrow \varrho(i) \in \mathfrak{h}\Phi && , \text{ mit (10.14),} \end{aligned}$$

d.h. $S \preceq_{\varrho} \mathfrak{h}\Phi$. Mit der Unentscheidbarkeit von S , vgl. Korollar 7.3, folgt dann mit Korollar 10.5, daß $\mathfrak{h}\Phi$ nicht entscheidbar ist.

Andernfalls gilt $\omega \in \Phi$ und mit $\Phi \subsetneq \llbracket \mathcal{P} \rrbracket$ dann o.B.d.A. $\theta \notin \Phi$.⁵ Man erhält

$$\begin{aligned} i \notin S &\Leftrightarrow \varphi_{s_1^1(\mathfrak{h}\text{PROC}, i)} \in \Phi && , \text{ mit (10.17) und (10.16),} \\ &\Leftrightarrow s_1^1(\mathfrak{h}\text{PROC}, i) \in \mathfrak{h}\Phi && , \text{ mit Definition von } \mathfrak{h}\Phi, \\ &\Leftrightarrow \varrho(i) \in \mathfrak{h}\Phi && , \text{ mit (10.14),} \end{aligned}$$

d.h. $\overline{S} \preceq_{\varrho} \mathfrak{h}\Phi$. Mit der Unentscheidbarkeit von \overline{S} , vgl. Korollar 8.9, folgt dann ebenfalls, mit Korollar 10.5, daß $\mathfrak{h}\Phi$ nicht entscheidbar ist. ■

Der Satz von Rice zeigt also, daß es unmöglich ist zu entscheiden, ob die von einem Programm berechnete Funktion bestimmte Eigenschaften besitzt. Ausgenommen sind dabei die “trivialen” Eigenschaften, die für kein Programm – Fall $\Phi = \emptyset$ – und für alle Programme – Fall $\Phi = \llbracket \mathcal{P} \rrbracket$ – gelten, denn dann gilt $\mathfrak{h}\Phi = \emptyset$ bzw. $\mathfrak{h}\Phi = \mathfrak{h}\mathcal{P}$, und damit ist $\mathfrak{h}\Phi$ trivialerweise bzw. mittels \mathfrak{h} ? (vgl. Satz 4.13) entscheidbar.

Mit Satz 10.12 ist natürlich nicht ausgeschlossen, daß man für gewisse Funktionen irgendwelche Eigenschaften nachweisen kann, und so etwa der Nachweis von $\llbracket \text{GGT} \rrbracket \in \Phi_{ass}$ trotzdem gelingt. Mit dem Satz von Rice ist es dagegen unmöglich, ein terminierendes (und korrektes) Verfahren anzugeben, mit dem beispielsweise $\llbracket \text{PROG} \rrbracket \in \Phi_{ass}$ für *jedes* Programm $\text{PROG} \in \mathcal{P}$ bewiesen oder widerlegt werden kann.

10.6. Weitere Probleme

Wir geben hier ohne Beweis (einige) weitere Ergebnisse aus der Berechenbarkeitstheorie bzw. der mathematischen Logik an – weiteres dazu findet man in den Lehrbüchern des Literaturverzeichnisses:

⁴ Mit $\omega \notin \Phi$ und $\Phi \neq \emptyset$ enthält Φ mindestens eine Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$ mit $\phi \neq \omega$. Da $\theta : \mathbb{N} \mapsto \mathbb{N}$ mit $\theta \in \llbracket \mathcal{P} \rrbracket$ und $\theta \neq \omega$ *beliebig* gewählt war, gilt alles, was bislang über θ gezeigt wurde, auch für ϕ . Wir dürfen daher tatsächlich “o.B.d.A.” $\theta \in \Phi$ annehmen.

⁵ Mit $\omega \in \Phi$ und $\Phi \subsetneq \llbracket \mathcal{P} \rrbracket$ enthält $\llbracket \mathcal{P} \rrbracket$ mindestens eine Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$ mit $\phi \neq \omega$ und $\phi \notin \Phi$. Da $\theta : \mathbb{N} \mapsto \mathbb{N}$ mit $\theta \in \llbracket \mathcal{P} \rrbracket$ und $\theta \neq \omega$ *beliebig* gewählt war, gilt alles, was bislang über θ gezeigt wurde, auch für ϕ . Wir dürfen daher tatsächlich “o.B.d.A.” $\theta \notin \Phi$ annehmen.

1. Die Menge TAU der Tautologien, also der wahren aussagenlogischen Formeln, ist entscheidbar. Zum Beweis implementiere man die Wahrheitstafelmethode (und verifiziere die Implementierung).
2. Die Menge AG der allgemeingültigen Formeln der Prädikatenlogik erster Stufe ist semi-entscheidbar, vgl. Anmerkung 9.5. Konsequenz ist, daß man einen Automatischen Beweiser implementieren kann, der für jede allgemeingültige Formel einen Beweis berechnet.
3. Die Menge \overline{AG} der nicht-allgemeingültigen Formeln der Prädikatenlogik erster Stufe ist nicht semi-entscheidbar. Konsequenz ist, daß der Automatische Beweiser aus 2. für unendlich viele (nicht-allgemeingültige) Formeln beim Beweisversuch in eine Endlosschleife gerät.
4. Aus 3. folgt (mit Satz 8.7): Die Menge AG der allgemeingültigen Formeln der Prädikatenlogik erster Stufe ist unentscheidbar.
5. Die Menge Pr aller wahren Formeln, die über die Nachfolgerfunktion und die Addition in \mathbb{N} Aussagen treffen, ist entscheidbar (Presburger Arithmetik).
6. Die Menge Ar der wahren Formeln der Arithmetik, d.h. alle wahren Formeln, die über die Nachfolgerfunktion, die Addition und die Multiplikation (und eventuell weitere arithmetische Funktion) in \mathbb{N} Aussagen treffen, ist nicht semi-entscheidbar (Erster Gödelscher Unvollständigkeitssatz). Konsequenz ist, daß jedes korrekte Beweisverfahren für Aussagen der Arithmetik unvollständig ist, d.h. für gewisse wahre Formeln keinen Beweis berechnen kann.
7. Aus 6. folgt (mit Satz 8.7): Die Menge Ar der wahren Formeln der Arithmetik ist unentscheidbar.
8. Die Menge \overline{Ar} der falschen Formeln der Arithmetik ist nicht semi-entscheidbar (Erster Gödelscher Unvollständigkeitssatz). Konsequenz ist, daß jedes korrekte Widerlegungsverfahren für Aussagen der Arithmetik unvollständig ist, d.h. für gewisse falsche Formeln kein Gegenbeispiel berechnen kann.
9. Die Menge Ar^\forall der wahren universellen Formeln der Arithmetik, d.h. der wahren Formeln der Form $\forall \dots \forall \phi$ mit “ ϕ ist quantorfrei”, ist nicht semi-entscheidbar.
10. Die Menge Ar^\exists der wahren existentiellen Formeln der Arithmetik, d.h. der wahren Formeln der Form $\exists \dots \exists \phi$ mit “ ϕ ist quantorfrei”, ist semi-entscheidbar (denn $\mathbb{N} \times \dots \times \mathbb{N}$ ist rekursiv aufzählbar, so daß man alle Be-

gungen für die existentiell quantifizierten Variablen systematisch erzeugen und ϕ damit in berechenbarer Weise überprüfen kann).

11. Die Menge \mathcal{E}_P aller wahren Formeln, die Aussagen über Eigenschaften eines Programms P einer berechnungsvollständigen Programmiersprache treffen, ist nicht semi-entscheidbar (folgt aus 6.). Konsequenz ist, daß jedes korrekte Verifikationsverfahren für Programme einer berechnungsvollständigen Programmiersprache unvollständig ist, d.h. für gewisse wahre Aussagen keinen Beweis berechnen kann.
12. Aus 11. folgt (mit Satz 8.7): Die Menge \mathcal{E}_P aller wahren Formeln, die Aussagen über Eigenschaften eines Programms P einer berechnungsvollständigen Programmiersprache treffen, ist unentscheidbar.
13. Die Menge $\overline{\mathcal{E}_P}$ aller falschen Formeln, die Aussagen über Eigenschaften eines Programms P einer berechnungsvollständigen Programmiersprache treffen, ist nicht semi-entscheidbar (folgt aus 8.). Konsequenz ist, daß jedes korrekte Widerlegungsverfahren für Programmaussagen unvollständig ist, d.h. für gewisse falsche Aussagen kein Gegenbeispiel berechnen kann.
14. Die Menge \mathcal{E}_P^\forall der wahren universellen Formeln über Eigenschaften eines Programms P einer berechnungsvollständigen Programmiersprache ist nicht semi-entscheidbar (folgt aus 9.).
15. Die Menge \mathcal{E}_P^\exists der wahren existentiellen Formeln über Eigenschaften eines Programms P einer berechnungsvollständigen Programmiersprache ist semi-entscheidbar (folgt aus 10.). Konsequenz ist, daß man ein vollständiges Testwerkzeug für \mathcal{E}_P^\forall implementieren kann, d.h. ein Testwerkzeug, das jede falsche – als universelle Formel formulierte – Behauptung über ein Programm widerlegen kann. Mit 14. gerät solch ein Testwerkzeug allerdings für unendlich viele (wahre, universell formulierte) Programmaussagen in eine Endlosschleife.

11. PRIMITIV-REKURSIVE UND μ -REKURSIVE FUNKTIONEN

In diesem Abschnitt stellen wir ein weiteres Rechenmodell vor, die auf *S. C. Kleene* zurückgehenden μ -rekursiven Funktionen. Für den Informatiker ist dieses Rechenmodell auch deshalb interessant, da die Definition μ -rekursiver Funktionen in gewisser Weise als eine Vorform der *applikativen Programmierung*, also der *funktionalen Programmierung*, aufgefaßt werden kann.

μ -rekursive Funktionen werden mittels zweier Definitionsprinzipien gebildet: Zunächst wird die Klasse der *primitiv-rekursiven Funktionen* eingeführt. Man kann zeigen, daß diese Klasse genau die arithmetischen Funktionen enthält, die man mittels sogenannter *loop*-Programme erhält. Dies sind \mathcal{P} -Programme, die anstatt *while*-Anweisungen nur Schleifenanweisungen in der Art von *for*-Schleifen enthalten, so wie sie aus einigen Programmiersprachen (beispielsweise FORTRAN, PASCAL oder ADA) bekannt sind. Mit dieser Einschränkung ist offensichtlich, daß nicht jede berechenbare Funktion primitiv-rekursiv sein kann, denn jedes *loop*-Programm muß ja terminieren, und somit können nicht-totale berechenbare Funktionen nicht primitiv-rekursiv sein.

Um dieser Einschränkung zu begegnen, wird der sogenannte (unbeschränkte) μ -Operator eingeführt, durch den beliebige – also auch *nicht-terminierende* – Schleifen modelliert werden können. Man erhält mittels des μ -Operators und der primitiv-rekursiven Funktionen die Klasse der μ -rekursiven Funktionen, von der wir zeigen, daß sie identisch der Klasse der \mathcal{P} -berechenbaren Funktionen ist.

11.1. Primitiv-rekursive Funktionen

Das Definitionsprinzip für primitiv-rekursive Funktionen ist vergleichbar dem Definitionsprinzip von Prozeduren in funktionalen Programmiersprachen. Ausgangspunkt sind die sogenannten *Grundfunktionen*, die man sich als bereits implementiert vorstellen kann. Wie schon bei Definition der Programmiersprache \mathcal{P} werden nur solche Grundfunktionen vorausgesetzt, die für die Definition des Rechenmodells unabdingbar sind.

Definition 11.1. (Grundfunktionen)

Als Grundfunktionen werden bezeichnet

1. die 0-stellige Funktion $Z : \rightarrow \mathbb{N}$ mit $Z := 0$,
2. die 1-stellige Funktion $S : \mathbb{N} \rightarrow \mathbb{N}$ mit $S(x) := x + 1$, und die
3. die k -stelligen Projektionsfunktionen $P_i^k : \mathbb{N}^k \rightarrow \mathbb{N}$ mit $P_i^k(x_1, \dots, x_k) := x_i$ für jedes $k > 0$ und alle i mit $1 \leq i \leq k$. ■

Mit bereits definierten Funktionen können weitere Funktionen definiert werden. Beispielsweise können wir mittels bereits definierter Funktionen *half* und *times* für abgerundete Division durch 2 und Multiplikation eine Funktion *sum-up* durch $sum-up(x) := half(times(x, S(x)))$ definieren. Man nennt dieses Definitionsprinzip "Definition durch Einsetzung".

Definition 11.2. (Definition durch Einsetzung)

Seien $f : \mathbb{N}^k \mapsto \mathbb{N}$, $g : \mathbb{N}^m \mapsto \mathbb{N}$ und $h_1, \dots, h_m : \mathbb{N}^k \mapsto \mathbb{N}$ Funktionen mit $k, m \geq 0$ sowie

$$f(\vec{x}) := g(h_1(\vec{x}), \dots, h_m(\vec{x})) .$$

Dann ist die Funktion f definiert durch Einsetzung (mittels der Funktionen g und h_1, \dots, h_m).¹ ■

Allein mit Grundfunktionen und durch Einsetzung können noch keine interessanten Funktionen, wie etwa Addition, Multiplikation u.s.w., definiert werden. Wir erlauben daher zusätzlich die Definition von Funktionen durch ein *Rekursionsprinzip*:

Definition 11.3. (Definition durch primitive Rekursion)

Seien $f : \mathbb{N}^{k+1} \mapsto \mathbb{N}$, $g : \mathbb{N}^k \mapsto \mathbb{N}$ und $h : \mathbb{N}^{k+2} \mapsto \mathbb{N}$ Funktionen mit $k \geq 0$ sowie

1. $f(0, \vec{x}) := g(\vec{x})$ und
2. $f(x + 1, \vec{x}) := h(f(x, \vec{x}), x, \vec{x})$.

Dann ist die Funktion f definiert durch primitive Rekursion (mittels der Funktionen g und h). ■

¹ \vec{x} steht als Abkürzung für ein k -Tupel x_1, \dots, x_k von Variablensymbolen.

$$\begin{aligned}
& plus(1, 2) \\
\Rightarrow & S_1^3(plus(0, 2), 0, 2) && , \text{ mit (iii)} \\
\Rightarrow & S(P_1^3(plus(0, 2), 0, 2)) && , \text{ mit (i)} \\
\Rightarrow & S(plus(0, 2)) && , \text{ mit Definition 11.1(3.)} \\
\Rightarrow & S(P_1^1(2)) && , \text{ mit (ii)} \\
\Rightarrow & S(2) && , \text{ mit Definition 11.1(3.)} \\
\Rightarrow & 3 && , \text{ mit Definition 11.1(2.)}
\end{aligned}$$

Abbildung 11.1: Berechnung von $plus(1, 2)$ mit primitiv-rekursiven Funktionen

Mit Grundfunktionen, Definition durch Einsetzung und durch primitive Rekursion erhalten wir eine einfache funktionale Programmiersprache. Funktionen, die durch Programme dieser Programmiersprache berechnet werden können, werden *primitiv-rekursiv* genannt:

Definition 11.4. (Primitiv-rekursive Funktionen)

Eine Funktion $f : \mathbb{N}^k \rightarrow \mathbb{N}$ mit $k \geq 0$ heißt primitiv-rekursiv, gdw. gilt:

1. f ist eine Grundfunktion, oder
2. f ist definiert durch Einsetzung mittels primitiv-rekursiver Funktionen, oder
3. f ist definiert durch primitive Rekursion mittels primitiv-rekursiver Funktionen. ■

Beispielsweise können wir die Addition natürlicher Zahlen als primitiv-rekursive Funktion “programmieren”. Wir definieren dazu

- (i) $S_1^3(x_1, x_2, x_3) := S(P_1^3(x_1, x_2, x_3))$,
- (ii) $plus(0, y) := P_1^1(y)$, und
- (iii) $plus(x + 1, y) := S_1^3(plus(x, y), x, y)$.

Nach den Definitionen 11.4(1.) und 11.1 sind S , P_1^1 und P_1^3 primitiv-rekursive Funktionen. Die Funktion S_1^3 entsteht durch Einsetzung nach den Forderungen von Definition 11.2, und ist damit nach Definition 11.4(2.) ebenfalls primitiv-rekursiv. Damit genügen die Definitionen (ii) und (iii) den Forderungen (1.) und (2.) von Definition 11.4, also ist $plus$ eine primitiv-rekursive Funktion.

Durch Anwenden der definierenden Gleichungen *links := rechts* von links nach rechts können wir Ausdrücke über primitiv-rekursiven Funktionen ausrechnen. Abbildung 11.1 zeigt als Beispiel die Berechnung von $plus(1, 2)$.

Eine Funktion ist primitiv-rekursiv, wenn sie nach Definition 11.4 gebildet werden kann. Anders gesagt, man muß unterscheiden zwischen der *Definition* einer Funktion und der *Funktion* selbst. Beispielsweise ist die durch $plus'(0, y) := P_1^1(y)$ und $plus'(x + 1, y) := plus'(x, S(y))$ definierte *Funktion* primitiv-rekursiv (denn man zeigt leicht $plus'(n, m) = plus(n, m)$ für alle $n, m \in \mathbb{N}$), $plus'$ ist jedoch *nicht* primitiv-rekursiv *definiert*, da die Forderung (2.) von Definition 11.3 nicht erfüllt ist.²

11.2. Definitionsprinzipien für primitiv-rekursive Funktionen

Mit Definition 11.4 wird ein starres Schema zur Definition primitiv-rekursiver Funktionen angegeben. Konsequenz ist, daß die Programmierung umständlich und unübersichtlich ist, wie schon anhand der Definition von $plus$ ersichtlich. Als Abhilfe gehen wir so vor, wie schon zuvor bei der Programmiersprache \mathcal{P} : Wir führen abkürzende Schreibweisen ein, die jedoch immer auf die Originalforderungen zurückgeführt werden können. Nachfolgend verwenden wir dann sowohl die Originalsprache als auch die komfortablere, erweiterte Sprache, je nachdem, wie es für den jeweiligen Zweck am bequemsten ist.

Lemma 11.5. (Primitiv-rekursive Hilfsfunktionen)

1. Die Funktionen $C_n^k : \mathbb{N}^k \rightarrow \mathbb{N}$ mit $C_n^k(x_1, \dots, x_k) = n$ sind für jedes $k \in \mathbb{N}$ und jedes $n \in \mathbb{N}$ primitiv-rekursiv.
2. Die Funktion $pred : \mathbb{N} \rightarrow \mathbb{N}$, definiert durch $pred(0) = 0$ und $pred(x+1) := x$ ist primitiv-rekursiv.
3. Die Funktion $if : \mathbb{N}^3 \rightarrow \mathbb{N}$ mit $if(0, y_1, y_2) = y_2$ und $if(x + 1, y_1, y_2) := y_1$ ist primitiv-rekursiv.
4. Die Paar-Funktion π^2 und ihre Projektionsfunktionen π_1^2 und π_2^2 sind primitiv-rekursiv.

Beweis. Übung. ■

² Solche Unterscheidungen zwischen Syntax und Semantik sind auch von anderswo bekannt. Beispielsweise ist eine *Grammatik* mit den beiden Regeln $S \rightarrow AA$ und $A \rightarrow a$ nicht regulär, die dadurch definierte *Sprache* $\{aa\}$ dagegen schon.

Lemma 11.6. (Definition durch allgemeine Einsetzung)

Seien $g_1 : \mathbb{N}^{m_1} \mapsto \mathbb{N}, \dots, g_j : \mathbb{N}^{m_j} \mapsto \mathbb{N}$, sei t ein Ausdruck, in dem neben den Grundfunktionen nur Funktionssymbole aus $\{g_1, \dots, g_j\}$, nur Variablensymbole aus $\{x_1, \dots, x_k\}$ und natürliche Zahlen n vorkommen, und sei die Funktion $f : \mathbb{N}^k \mapsto \mathbb{N}$ mit $k > 0$ definiert durch

$$f(x_1, \dots, x_k) := t .$$

Dann kann f durch Grundfunktionen und Einsetzung definiert werden.

Beweis. Wir zeigen die Behauptung durch strukturelle Induktion über t .

Induktionsanfang “ $t = n \in \mathbb{N}$ ”: Durch Induktion über n zeigt man leicht $S_n = n$ für jede Funktion $S_n : \rightarrow \mathbb{N}$ definiert durch $S_0 := Z$ und $S_{n+1} := S(S_n)$. Jede Funktion S_n genügt damit der Forderung von Definition 11.2, und mit $f(x_1, \dots, x_k) = S_n$ genügt f ebenfalls dieser Forderung.

Induktionsanfang “ $t = x_i$ ”: Dann gilt $f(x_1, \dots, x_k) := P_i^k(x_1, \dots, x_k)$, und folglich genügt f der Forderung von Definition 11.2.

Induktionsschritt “ $t = g(t_1, \dots, t_m)$ mit $g \in \{g_1, \dots, g_j\}$ ”: Wir definieren für jedes $i \in \{1, \dots, m\}$ die Funktionen $f_i : \mathbb{N}^k \mapsto \mathbb{N}$ durch $f_i(x_1, \dots, x_k) := t_i$, von denen wir nach Induktionshypothese annehmen dürfen, daß sie alternativ den Forderungen von Definition 11.2 genügend definiert werden können. Mit $f(x_1, \dots, x_k) := g(f_1(x_1, \dots, x_k), \dots, f_m(x_1, \dots, x_k))$ genügt dann auch f der Forderung von Definition 11.2. ■

Satz 11.7. (Definition durch strukturelle Rekursion)

Seien $g_1 : \mathbb{N}^{m_1} \mapsto \mathbb{N}, \dots, g_j : \mathbb{N}^{m_j} \mapsto \mathbb{N}$ Funktionen, sei $f : \mathbb{N}^{k+1} \mapsto \mathbb{N}$ eine Funktion, und seien t_1 und t_2 Ausdrücke, in denen neben den Grundfunktionen nur Funktionssymbole aus $\{f, g_1, \dots, g_j\}$, das Variablensymbol x , die Variablensymbole aus \vec{x} und natürliche Zahlen n vorkommen. Sei weiter die Funktion f definiert durch:

1. $f(0, \vec{x}) := t_1$, so daß f und x nicht in t_1 vorkommen, und
2. $f(x + 1, \vec{x}) := t_2$, so daß $t' = f(x, \vec{x})$ für jeden Teilausdruck $t' = f(\dots)$ von t_2 gilt.

Dann kann f durch Grundfunktionen, Einsetzung und primitive Rekursion definiert werden.

Beweis. Mit Lemma 11.6 gibt es eine durch Grundfunktionen und Einsetzung definierte Funktion $g : \mathbb{N}^k \mapsto \mathbb{N}$ mit (i) $g(\vec{x}) = t_1$.

Sei jetzt z eine Variable und sei $C[z]$ ein Ausdruck mit $t_2 = C[z/f(x, \vec{x})]$.³ Dann ist $C[z]$ ein Ausdruck, in dem außer der Variablen z höchstens die Variablen

³ $C[z/t]$ entsteht aus $C[z]$, indem jedes Vorkommen von z in $C[z]$ durch t ersetzt wird.

x, \vec{x} , Funktionssymbole aus $\{g_1, \dots, g_j\}$ sowie natürliche Zahlen n vorkommen. Nach Lemma 11.6 kann somit eine Funktion $h : \mathbb{N}^{k+2} \mapsto \mathbb{N}$ mit $h(z, x, \vec{x}) = C[z]$ durch Einsetzung definiert werden. Es gilt (ii) $f(x+1, \vec{x}) = t_2 = C[z/f(x, \vec{x})] = h(f(x, \vec{x}), x, \vec{x})$, und mit (i) und (ii) kann f dann den Forderungen von Definition 11.4 genügend definiert werden. ■

Satz 11.7 erlaubt eine wesentlich einfachere Definition von primitiv-rekursiven Funktionen und legt die Vermutung nahe, daß die Funktionen, mit denen wir in der Praxis umgehen, überwiegend primitiv-rekursiv sind. So genügen etwa die Definitionen der Multiplikation und der Fakultätsfunktion in nachfolgendem Beispiel nicht dem starren Schema von Definition 11.4, die so definierten Funktionen sind jedoch nach Satz 11.7 primitiv-rekursiv.

Beispiel 11.8. (Definition durch strukturelle Rekursion)

1. $times(0, y) := 0$ und $times(x+1, y) := plus(y, times(x, y))$.
2. $fact(0) := 1$ und $fact(x+1) := plus(times(fact(x), x), fact(x))$. ■

Mit Satz 11.7 kann man ein weiteres, mächtiges Definitionsprinzip angeben, nämlich die Definition von Funktionen durch gegenseitige Rekursion. Dieses Definitionsprinzip wird im folgenden noch nützlich sein.

Satz 11.9. (Gegenseitige Rekursion)

Sei $k \geq 0$ und seien $g_1, \dots, g_j : \mathbb{N}^k \mapsto \mathbb{N}$ sowie $h_1, \dots, h_j : \mathbb{N}^{j+1+k} \mapsto \mathbb{N}$ Funktionen. Dann gilt

$$f_i(x, \vec{x}) = \pi_i^j(F(x, \vec{x})) \quad (11.1)$$

für alle Funktionen $f_1, \dots, f_j : \mathbb{N}^{k+1} \mapsto \mathbb{N}$ mit

1. $f_i(0, \vec{x}) := g_i(\vec{x})$ und
2. $f_i(x+1, \vec{x}) := h_i(f_1(x, \vec{x}), \dots, f_j(x, \vec{x}), x, \vec{x})$

und eine durch primitive Rekursion mittels $g_1, \dots, g_j, h_1, \dots, h_j, \pi_1^j, \dots, \pi_j^j$ definierte Funktion $F : \mathbb{N}^{k+1} \mapsto \mathbb{N}$.

Beweis. Sei $F : \mathbb{N}^{k+1} \mapsto \mathbb{N}$ definiert durch

$$F(0, \vec{x}) := \pi^j(g_1(\vec{x}), \dots, g_j(\vec{x})) \quad (11.2)$$

$$\begin{aligned} F(x+1, \vec{x}) &:= \pi^j(h_1(\pi_1^j(F(x, \vec{x})), \dots, \pi_j^j(F(x, \vec{x})), x, \vec{x}), \\ &\quad \dots \\ &\quad h_j(\pi_1^j(F(x, \vec{x})), \dots, \pi_j^j(F(x, \vec{x})), x, \vec{x})). \end{aligned} \quad (11.3)$$

Wir zeigen (11.1) für alle $i \in \{1, \dots, j\}$ durch Induktion über x :

Im Induktionsanfang gilt $f_i(0, \vec{x}) = g_i(\vec{x}) = \pi_i^j(\pi^j(g_1(\vec{x}), \dots, g_j(\vec{x}))) = \pi_i^j(F(0, \vec{x}))$ mit Definition von f_i und (11.2). Im Induktionsschritt erhält man

$$\begin{aligned} f_i(x+1, \vec{x}) &= h_i(f_1(x, \vec{x}), \dots, f_j(x, \vec{x}), x, \vec{x}) && \text{, mit Definition von } f_i \\ &= h_i(\pi_1^j(F(x, \vec{x})), \dots, \pi_j^j(F(x, \vec{x})), x, \vec{x}) && \text{, mit Induktionshypothese} \\ &= \pi_i^j(F(x+1, \vec{x})). && \text{, mit (11.3).} \end{aligned}$$

■

Korollar 11.10. (Primitiv-rekursive Funktionen durch gegenseitige Rekursion) Sei $k \geq 0$ und seien $g_1, \dots, g_j : \mathbb{N}^k \rightarrow \mathbb{N}$ sowie $h_1, \dots, h_j : \mathbb{N}^{j+1+k} \rightarrow \mathbb{N}$ primitiv-rekursive Funktionen. Dann sind die Funktionen $f_1, \dots, f_j : \mathbb{N}^{k+1} \mapsto \mathbb{N}$, gegeben durch

1. $f_i(0, \vec{x}) := g_i(\vec{x})$ und
2. $f_i(x+1, \vec{x}) := h_i(f_1(x, \vec{x}), \dots, f_j(x, \vec{x}), x, \vec{x})$,

für alle $i \in \{1, \dots, j\}$ primitiv-rekursiv.

Beweis. Mit Satz 11.9 gilt (*) $f_i(x, \vec{x}) = \pi_i^j(F(x, \vec{x}))$ für eine durch primitive Rekursion mittels $g_1, \dots, g_j, h_1, \dots, h_j, \pi_1^j, \dots, \pi_j^j$ definierte Funktion $F : \mathbb{N}^{k+1} \mapsto \mathbb{N}$. Mit Definition 11.4 ist F primitiv-rekursiv, denn die Funktionen g_i, h_i und π_i^j sind primitiv-rekursiv, und mit (*) sind dann auch alle Funktionen f_i primitiv-rekursiv. ■

Beispiel 11.11. (Gegenseitige Rekursion) Die Funktionen $even : \mathbb{N} \mapsto \mathbb{N}$ und $odd : \mathbb{N} \mapsto \mathbb{N}$, definiert durch

1. $even(0) := C_1^0 = 1$,
2. $even(x+1) := P_2^2(even(x), odd(x)) = odd(x)$,
3. $odd(0) := C_0^0 = 0$, und
4. $odd(x+1) := P_1^2(even(x), odd(x)) = even(x)$

sind mit Korollar 11.10 primitiv-rekursiv. Für die Begriffe aus Satz 11.9 ergibt sich

1. $F(0) := \pi^2(C_1^0, C_0^0) = \pi^2(1, 0)$ sowie
2. $F(x + 1) := \pi^2(P_2^2(\pi_1^2(F(x)), \pi_2^2(F(x))), P_1^2(\pi_1^2(F(x)), \pi_2^2(F(x))))$
 $= \pi^2(\pi_2^2(F(x)), \pi_1^2(F(x))),$

und mit (11.1) dann $even(x) = \pi_1^2(F(x))$ sowie $odd(x) = \pi_2^2(F(x))$. Für F erhält man z.B.

- $F(1) = \pi^2(\pi_2^2(F(0)), \pi_1^2(F(0))) = \pi^2(0, 1),$
- $F(2) = \pi^2(\pi_2^2(F(1)), \pi_1^2(F(1))) = \pi^2(1, 0),$
- $F(3) = \pi^2(\pi_2^2(F(2)), \pi_1^2(F(2))) = \pi^2(0, 1),$
- ■

11.3. Werteverlaufsrekursion

Bislang steht uns nur die strukturelle Rekursion zur Definition von Funktionen zur Verfügung, denn bei rekursiver Definition einer Funktion f ist im Rekursionsfall nur der *direkte* Vorgänger x des Rekursionsparameters $x + 1$ im rekursiven Aufruf erlaubt. Beispielsweise ist so nicht ersichtlich, ob die *Fibonacci*-Funktion $fib : \mathbb{N} \rightarrow \mathbb{N}$, definiert durch

$$\begin{aligned} (1.) \quad & fib(0) := 1 \text{ und} \\ (2.) \quad & fib(x + 1) := if(x, plus(fib(x), fib(pred(x))), 1) \end{aligned} \tag{11.4}$$

primitiv-rekursiv ist, denn Definitionsgleichung (11.4-2.) genügt (wegen des rekursiven Aufrufs $fib(pred(x))$) weder Forderung (2.) von Definition 11.3 noch Forderung (2.) von Satz 11.7.

In gängigen funktionalen Programmiersprachen dürfen Funktionen sogar *Funktionsparameter* besitzen. Beispielsweise kann man dort eine Funktion $SUM : \mathbb{N} \times (\mathbb{N} \mapsto \mathbb{N}) \mapsto \mathbb{N}$ (Eingabe von SUM ist also eine natürliche Zahl sowie eine *Funktion*, die natürliche Zahlen in natürliche Zahlen abbildet) als

$$\begin{aligned} (1.) \quad & SUM(0, F) := F(0) \text{ und} \\ (2.) \quad & SUM(x + 1, F) := F(x + 1) + SUM(x, F) \end{aligned} \tag{11.5}$$

angeben, und damit dann durch

$$\begin{aligned} (1.) \quad & exp2(0) := 1 \text{ und} \\ (2.) \quad & exp2(x + 1) := S(SUM(x, exp2)) \end{aligned} \tag{11.6}$$

die Exponentiation zur Basis 2 definieren (es gilt $\text{exp}2(n) = 2^n$).⁴ Hier ist noch weniger ersichtlich, ob mit (11.6-1.) und (11.6-2.) eine primitiv-rekursive Funktion definiert wird.

Um dies zu untersuchen, betrachten wir die Funktion SUM eingehender: Es gilt offensichtlich $SUM(x, F) = F(x) + F(x-1) + \dots + F(0)$. Die Summanden können wir auch in einer Liste $\langle F(x), F(x-1), \dots, F(0) \rangle$ abspeichern, um dann die Summe der Listenelemente zu bilden. Für $\text{exp}2(x+1)$ erhält man so die Liste $\langle \text{exp}2(x), \text{exp}2(x-1), \dots, \text{exp}2(0) \rangle$. Diese Liste beschreibt den *Werteverlauf* bei Berechnung von $\text{exp}2(x+1)$.

Für eine Funktion $\text{exp}2^* : \mathbb{N} \mapsto \mathbb{N}$, mit der man die π^2 -Kodierung der Werteverlaufsliste von $\text{exp}2$ erhält, d.h.

$$\text{exp}2^*(x+1) := \pi^2(\text{exp}2(x), \pi^2(\text{exp}2(x-1), \dots, \pi^2(\text{exp}2(0), 0) \dots)) \quad (11.7)$$

gilt

$$\text{exp}2(x) = S(\text{sum}(x, \text{exp}2^*(x))) \quad (11.8)$$

denn man erhält $\text{exp}2(x)$ ja durch Aufsummieren der Elemente der (dekodierten) Liste $\text{exp}2^*(x)$. Hierbei verwenden wir die Hilfsfunktionen ntl , nth und sum , definiert durch⁵

$$\begin{aligned} (1.) \quad \text{ntl}(0, y) &:= y & (4.) \quad \text{sum}(0, y) &:= 0 \\ (2.) \quad \text{ntl}(x+1, y) &:= \pi_2^2(\text{ntl}(x, y)) & (5.) \quad \text{sum}(x+1, y) &:= \\ (3.) \quad \text{nth}(x, y) &:= \pi_1^2(\text{ntl}(x, y)) & & \text{plus}(\text{nth}(x, y), \text{sum}(x, y)) . \end{aligned} \quad (11.9)$$

Mit Satz 11.7 sind ntl , nth und sum primitiv-rekursive Funktionen. Mit (11.8) kann $\text{exp}2$ allein durch (i) Einsetzung mittels (ii) primitiv-rekursiver Funktionen, nämlich S und sum , und (iii) der *Werteverlaufsfunktion* $\text{exp}2^*$ definiert werden. Wir zeigen, daß allein aus (i) – (iii) folgt, daß $\text{exp}2$ primitiv-rekursiv ist.

Definition 11.12. (Werteverlaufsfunktion)

Für eine Funktion $f : \mathbb{N}^{k+1} \mapsto \mathbb{N}$ ist die Werteverlaufsfunktion $f^* : \mathbb{N}^{k+1} \mapsto \mathbb{N}$ definiert durch

$$1. f^*(0, \vec{x}) := 0 \quad \text{und} \quad 2. f^*(x+1, \vec{x}) := \pi^2(f(x, \vec{x}), f^*(x, \vec{x})). \quad \blacksquare$$

⁴ Auch die Paar-Funktion kann durch $\text{pair}^2(x, y) := \text{minus}(SUM(\text{plus}(x, y), S), \text{pred}(y))$ mittels SUM definiert werden, denn man zeigt leicht $\text{pair}^2(x, y) = \pi^2(x, y)$.

⁵ Bei diesen Funktionen wird y als die π^2 -Kodierung einer linearen Liste aufgefaßt. Mit $\text{ntl}(x, y)$ erhält man dann die (Kodierung der) Liste, die aus der Dekodierung von y durch Elimination der ersten x Elemente entsteht. Mit $\text{nth}(x, y)$ erhält man das $x+1$. Listenelement (der Dekodierung) von y . Mit $\text{sum}(x, y)$ werden schließlich die ersten x Elemente der (dekodierten) Liste y aufsummiert.

Da mit der Paar-Funktion π^2 endliche Listen durch natürliche Zahlen kodiert werden (π^2 entspricht dabei dem Listenkonstruktor, mit π_1^2 erhält man das erste Element einer nicht-leeren Liste und mit π_2^2 die Liste ohne das erste Listenelement), repräsentiert $f^*(x+1, \vec{x})$ die π^2 -Kodierung der Liste $\langle f(x, \vec{x}), f(x-1, \vec{x}), \dots, f(0, \vec{x}) \rangle$.⁶ Wir zeigen, daß jede Funktion f (und ihre Werteverlaufsfunktion f^*) *primitiv-rekursiv* sein muß, falls f allein durch Einsetzung mittels einer primitiv-rekursiven Funktion h und ihrer Werteverlaufsfunktion f^* definiert werden kann:

Satz 11.13. (Werteverlaufsrekursion, engl. *course-of-values recursion*)

Sei $h : \mathbb{N}^{k+2} \mapsto \mathbb{N}$ primitiv-rekursiv und sei $f : \mathbb{N}^{k+1} \mapsto \mathbb{N}$ eine Funktion mit

$$f(x, \vec{x}) = h(f^*(x, \vec{x}), x, \vec{x}) . \quad (11.10)$$

Dann ist f primitiv-rekursiv.

Beweis. Für alle $x \in \mathbb{N}$, $\vec{x} \in \mathbb{N}^k$ gilt

$$f^*(0, \vec{x}) = 0 \quad (11.11)$$

mit Definition 11.12(1.) sowie

$$f^*(x+1, \vec{x}) = \pi^2(h(f^*(x, \vec{x}), x, \vec{x}), f^*(x, \vec{x})) \quad (11.12)$$

denn

$$\begin{aligned} & f^*(x+1, \vec{x}) \\ = & \pi^2(f(x, \vec{x}), f^*(x, \vec{x})) \quad , \text{ mit Definition 11.12(2.)} \\ = & \pi^2(h(f^*(x, \vec{x}), x, \vec{x}), f^*(x, \vec{x})) \quad , \text{ mit (11.10) .} \end{aligned}$$

Mit Satz 11.7 ist f^* wegen (11.11) und (11.12) primitiv-rekursiv, und folglich ist f mit (11.10) primitiv-rekursiv.⁷ ■

⁶ Da die durch $f^*(x, \vec{x})$ kodierte Liste genau x Elemente enthält, die Länge dieser Liste also bekannt ist, muß die natürliche Zahl 0 nicht von der Kodierung 0 der leeren Liste unterschieden werden, vgl. Bemerkung 4.5. Beispielsweise stellt die Definition von *sum* in (11.9-4 und 11.9-5.) sicher, daß nicht versucht wird, das erste Element der leeren Liste zu bestimmen, falls $x \leq$ der Länge der aus Dekodierung von y gewonnenen Liste ist.

⁷ Das "Gegenstück" zur Werteverlaufsrekursion ist die *Noethersche Induktion* mit der üblichen (transitiven) $<$ -Relation auf \mathbb{N} . Hier zeigt man eine Behauptung $\forall x: \mathbb{N}. P(x)$ durch Nachweis von $P(0)$ und $\forall x: \mathbb{N}. (\forall x': \mathbb{N}. x' < x+1 \rightarrow P(x')) \rightarrow P(x+1)$, während man bei der *Peano Induktion* (dem "Gegenstück" zur primitiven Rekursion) nur $\forall x: \mathbb{N}. P(x) \rightarrow P(x+1)$ als Schrittfall zur Verfügung hat.

Mit Nachweis von (11.8) rechtfertigt Satz 11.13 also die Behauptung, daß $exp2$ tatsächlich primitiv-rekursiv ist.⁸ Genauso folgt mit Satz 11.13 aus dem Nachweis von

$$fib(x) = if(x, plus(\pi_1^2(fib^*(x)), \pi_1^2(\pi_2^2(fib^*(x)))), 1) \quad (11.13)$$

daß die *Fibonacci*-Funktion primitiv-rekursiv ist.

11.4. Ein Rechenmodell für primitiv-rekursive Funktionen

Bei Definition der Programmiersprache \mathcal{P} wurde eine explizite Trennung zwischen *Syntax* und *Semantik* vorgenommen, d.h., zum einen wurde in Definition 2.1 festgelegt, welche formalsprachlichen Ausdrücke überhaupt als Programme aufgefaßt werden, und zum anderen, was die Bedeutung solcher Programme ist. Mit Angabe einer *operationalen* Semantik wurde in Definition 2.7 zugleich ein Rechenmodell für \mathcal{P} -Programme definiert.

Es fällt auf, daß bei Definition des Begriffs der primitiv-rekursiven Funktionen solch eine explizite Trennung zwischen Syntax und Semantik zu fehlen scheint, und insbesondere, daß überhaupt kein Rechenmodell angegeben wird. Dies hat sicher historische Gründe, denn zu Beginn des letzten Jahrhunderts gab es noch keine programmierbaren Rechner, geschweige denn Programmiersprachen.

Gleichwohl gibt es auch hier eine Unterscheidung zwischen Syntax und Semantik, nur wird diese eben nicht weiter betont:⁹ Die Definitionen 11.1, 11.2 und 11.3 geben die Syntax einer (fiktiven) Programmiersprache PRF für primitiv-rekursive Funktionen an, denn dort wird festgelegt, welche objektsprachlichen Ausdrücke überhaupt erlaubt sind, um primitiv-rekursive Funktionen zu definieren. Die Semantik dieser Ausdrücke wird dann mit Definition 11.4 gegeben, denn hier ist von semantischen Objekten – nämlich *Funktionen* – die Rede, die ausschließlich durch Gleichungen definiert werden, die den Definitionen 11.1, 11.2 und 11.3 genügen.

Ein Rechenmodell wird – im Unterschied zu \mathcal{P} -Programmen und den in Kapitel 12 vorgestellten *Turingmaschinen* – dabei jedoch nicht formal definiert. Dies ist vielmehr *implizit* durch die Anwendung der definierenden Gleichungen gegeben. Solch ein Rechenmodell kann man durch einen Kalkül explizit machen: Als Sprache dieses Kalküls verwenden wir die Menge \mathcal{T} aller Terme über den Grundfunktionen sowie den Funktionen, die durch Einsetzung oder primitive Rekursion definiert

⁸ Es gilt $exp2(x+1) = 1 + exp2(x) + \dots + exp2(0)$ mit (11.5) und (11.6). Mit (11.9-5.) gilt $sum(x+1, y) = n_0 + \dots + n_x$ für die π^2 -Kodierung y einer Liste $\langle n_x, \dots, n_0 \rangle$, und folglich $S(sum(x+1, exp2^*(x+1))) = 1 + exp2(0) + \dots + exp2(x)$.

⁹ Ohne solch eine Unterscheidung könnten die primitiv-rekursiven – und darauf aufbauend die μ -rekursiven – Funktionen auch schwerlich ein Beitrag zur Berechenbarkeitstheorie sein.

(P) $\frac{P_i^k(t_1, \dots, t_k)}{t_i}$	(E) $\frac{f(\vec{t})}{g(h_1(\vec{t}), \dots, h_m(\vec{t}))}$
(Pr1) $\frac{f(Z, \vec{t})}{g(\vec{t})}$	(Pr2) $\frac{f(S(n), \vec{t})}{h(f(n, \vec{t}), n, \vec{t})}$, falls $n \in \mathcal{N}$
(Pr3) $\frac{g(t, \vec{t})}{g(t', \vec{t})}$,	falls $t \Rightarrow t'$ und $g = S$ oder g ist durch primitive Rekursion definiert

Abbildung 11.2: Ein Kalkül für primitiv-rekursive Funktionen

sind, und $\mathcal{N} \subset \mathcal{T}$ bezeichnet die Menge aller Terme über Z und S . Die Kalkülregeln (P), (E) (Pr1) und (Pr2) in Abbildung 11.2 gewinnt man unmittelbar aus den Definitionen 11.1, 11.2 und 11.3, wobei angenommen wird, daß bei primitiver Rekursion Funktionen in der Form $f(Z, \vec{x}) := g(\vec{x})$ sowie $f(S(x), \vec{x}) := h(f(x, \vec{x}), x, \vec{x})$ gegeben sind. Die zusätzliche Regel (Pr3) ist erforderlich, um etwa Ausdrücke der Form $plus(plus(n_1, n_2), n_3)$ auszurechnen, indem zunächst $plus(n_1, n_2)$ mittels (Pr3) zu n_4 ausgerechnet wird, um anschließend $plus(n_4, n_3)$ auszurechnen (denn ohne (Pr3) wäre keine Regel auf $plus(plus(n_1, n_2), n_3)$ anwendbar).

Die Regeln des Kalküls definieren eine Relation $\Rightarrow \subset \mathcal{T} \times \mathcal{T}$ durch: $t_1 \Rightarrow t_2$ gdw. $\frac{t_1}{t_2}$ eine Regel des Kalküls ist. Gerechnet wird durch schrittweise Anwendung der Kalkülregeln, wobei gilt:¹⁰

$n \in \mathcal{N}$ ist das *Ergebnis der Berechnung* von $t \in \mathcal{T}$ gdw. $t \Rightarrow^* n$.

Die Semantik der Terme aus \mathcal{N} ist durch Definition 11.1(1, 2) gegeben, wodurch jedes $n \in \mathbb{N}$ durch den Term $S^{(n)}(Z)$ repräsentiert wird. Mit \Rightarrow wird damit das Rechenmodell für primitiv-rekursive Funktionen explizit gemacht. Beispielsweise entsteht die Berechnung von $plus(1, 2)$ aus Abbildung 11.1 durch Anwendung dieser Kalkülregeln.¹¹ Man kann so einem nach Definition 11.4 gegebenen Funktionssymbol f die primitiv-rekursive Funktion $\llbracket f \rrbracket : \mathbb{N}^k \rightarrow \mathbb{N}$ durch

$$\llbracket f \rrbracket(n_1, \dots, n_k) = n \text{ gdw. } f(S^{(n_1)}(Z), \dots, S^{(n_k)}(Z)) \Rightarrow^* S^{(n)}(Z)$$

¹⁰ \Rightarrow^* bezeichnet die reflexive und transitive Hülle von \Rightarrow .

¹¹ Formal präzise erhält man die Herleitung $plus(S(Z), S(S(Z))) \Rightarrow \dots \Rightarrow S(S(S(Z)))$.

als operationale Semantik zuordnen, und $\llbracket \text{PRF} \rrbracket$ bezeichnet dann die Klasse aller primitiv-rekursiven Funktionen.¹²

11.5. loop-berechenbare Funktionen

Man kann zeigen, daß jede primitiv-rekursive Funktion \mathcal{P} -berechenbar ist. Es kann sogar eine noch stärkere Aussage bewiesen werden:

Mit den **while**-Anweisungen der Programmiersprache \mathcal{P} kann man beliebige Schleifenprogramme schreiben. Insbesondere auch solche Programme, die nur Schleifen in der Art von *for*-Schleifen enthalten, die aus Programmiersprachen wie FORTRAN, PASCAL oder ADA bekannt sind. Solche Schleifen terminieren immer, denn die Anzahl der Abarbeitungen des Schleifenrumpfs ist immer durch einen festen Wert begrenzt. Wir nennen \mathcal{P} -Programme, die nur Schleifen in der Art von *for*-Schleifen enthalten *loop-Programme*, und Funktionen, die durch *loop*-Programme berechnet werden können, *loop-berechenbar*. Man kann zeigen, daß die Klasse der primitiv-rekursiven Funktionen identisch der Klasse der *loop*-berechenbaren Funktionen ist.

Definition 11.14. (*loop*-Programme, Programmiersprache $\mathcal{P}_{\text{loop}}$)

Wir erlauben in \mathcal{P} -Programmen *loop*-Anweisungen, d.h. zusätzliche Programm-anweisungen der Form

`loop y do STA end_loop`

wobei *y* eine lokale Variable, die sogenannte Laufvariable der *loop*-Anweisung, und *STA* eine Programmanweisung ist, in der *y* nicht vorkommt.

Ein *loop*-Programm ist ein \mathcal{P} -Programm, in dem (anstatt **while**-Anweisungen) nur *loop*-Anweisungen vorkommen.¹³ $\mathcal{P}_{\text{loop}}$ bezeichnet die Menge aller *loop*-Programme, und $\mathcal{P}_{\text{loop}}[k] \subseteq \mathcal{P}[k]$ ist die Menge aller $\mathcal{P}_{\text{loop}}$ -Programme mit *k* formalen Parametern. ■

Die Semantik eines *loop*-Programms definieren wir durch Übersetzung in die Programmiersprache \mathcal{P} :

¹² Wie man sich leicht überzeugt ist der Kalkül *deterministisch*, d.h. auf jeden Term $t \in \mathcal{T}$ ist *höchstens eine* Kalkülregel anwendbar. Des weiteren zeigt man leicht, daß es für jeden Term $t \in \mathcal{T}$ *genau ein* $n \in \mathcal{N}$ mit $t \Rightarrow^* n$ gibt.

¹³ Insbesondere ist P ein *loop*-Programm, wenn P weder **while**- noch *loop*-Anweisungen enthält.

```

procedure PLUS(x,y) <=
begin var res,z;
  res := y;
  z := x;
  loop z do res := SUCC(res) end_loop;
  return(res)
end

procedure TIMES(x,y) <=
begin var res,z;
  res := 0;
  z := x;
  loop z do res := PLUS(res,y) end_loop;
  return(res)
end

procedure PLUS(x,y) <=
begin var res,z;
  res := y; z := x;
  while z ≠ 0 do res := SUCC(res); z := PRED(z) end_while;
  return(res)
end

procedure TIMES(x,y) <=
begin var res',z',res,z;
  res' := 0; z' := x;
  while z' ≠ 0 do
    res := y; z := res';
    while z ≠ 0 do res := SUCC(res); z := PRED(z) end_while;
    res' := res;
    z' := PRED(z')
  end_while;
  return(res')
end

procedure FAC(x) <=
begin var res,y,z;
  res := 1;
  y := x;
  z := x;
  loop y do
    res := TIMES(z,res);
    z := PRED(z)
  end_loop;
  return(res)
end

```

Abbildung 11.3: $\mathcal{P}_{\text{loop}}$ -Programme (und ihre \mathcal{P} -Übersetzungen) zur Berechnung der Addition, der Multiplikation sowie der Fakultätsfunktion

Definition 11.15. (Semantik von loop-Programmen)

Eine loop-Anweisung der Form “loop y do STA end_loop” wird aufgefaßt als abkürzende Schreibweise für eine while-Anweisung der Form

```
while y ≠ 0 do
  STA;
  y := PRED(y)
end_while . ■
```

In Definition 11.14 garantiert die Forderung für Laufvariable, daß diese im Rumpf einer loop-Anweisung nicht verändert werden können. Damit wird sichergestellt, daß loop-Anweisungen auch tatsächlich genauso wie for-Schleifen abgearbeitet werden. Andernfalls wären loop-Anweisungen der Form loop y do y := SUCC(y) end_loop möglich, mit denen man durch

```
while y ≠ 0 do
  y := SUCC(y);
  y := PRED(y)
end_while
```

nicht-terminierende Programmfragmente erhielte.¹⁴

Beispiel 11.16. (loop-Programme) Abbildung 11.3 definiert loop-Programme zur Berechnung von Addition, Multiplikation und der Fakultätsfunktion, sowie die \mathcal{P} -Programme für Addition und Multiplikation, die bei Elimination der Hilfsprozeduren und der Übersetzung der loop-Anweisungen in while-Anweisungen entstehen. ■

Wir zeigen nun mit den folgenden Sätzen, daß die Klasse der loop-berechenbaren Funktionen identisch der Klasse der primitiv-rekursiven Funktionen ist.

Satz 11.17. Jede primitiv-rekursive Funktion ist $\mathcal{P}_{\text{loop}}$ -berechenbar.

Beweis. Ausgehend von der induktiven Definition der primitiv-rekursiven Funktionen definieren wir für jede primitiv-rekursive Funktion $f : \mathbb{N}^k \mapsto \mathbb{N}$ ein $\mathcal{P}_{\text{loop}}$ -Programm $P_f \in \mathcal{P}_{\text{loop}}[k]$ mit $\llbracket P_f \rrbracket = f$.

¹⁴ Um nicht-Terminierung auszuschließen reicht es, lediglich *Zuweisungen* an Laufvariable zu verbieten. Die Verwendung von Laufvariablen y in Programmausdrücken wird nur aus beweistechnischen Gründen verboten, da dies andernfalls den Beweis von Satz 11.21 durch die *implizite* Zuweisung $y := \text{PRED}(y)$ unnötig erschweren würde. Dort, wo ein “lesender” Zugriff auf die Laufvariable erforderlich ist, muß dann ein “Doppelgänger” verwendet werden, wie etwa die Programmvariable z in der Prozedur FAC aus Abbildung 11.3.

<pre> procedure P'_f(x, x1, ..., xk) <= begin var y, z, R; R := P_g(x1, ..., xk); y := x; z := x; loop z do R := P_h(R, MINUS(x, y), x1, ..., xk); y := PRED(y) end_loop; return(R) end </pre>	<pre> procedure P_f(x, x1, ..., xk) <= begin var y, z, R; R := P_g(x1, ..., xk); y := x; z := x; while z ≠ 0 do R := P_h(R, MINUS(x, y), x1, ..., xk); y := PRED(y); z := PRED(z) end_while; return(R) end </pre>
---	--

Abbildung 11.4: Die Prozeduren P'_f und P_f zum Beweis von Satz 11.17

Induktionsanfang “ f ist eine Grundfunktion”: Für die $\mathcal{P}_{1\text{oop}}$ -Programme

```

      procedure Z() <= begin var y; y := 0; return(y) end
      procedure S(x) <= begin var y; y := SUCC(x); return(y) end
procedure P_i^k(x_1, ..., x_k) <= begin var y; y := x_i; return(y) end

```

gilt $\llbracket Z \rrbracket = Z$, $\llbracket S \rrbracket = S$ und $\llbracket P_i^k \rrbracket = P_i^k$.

Induktionsschritt “ f ist definiert durch Einsetzung”: Sei f gegeben durch $f(\vec{x}) := g(h_1(\vec{x}), \dots, h_m(\vec{x}))$. Dann sind die Funktionen h_1, \dots, h_m und g primitiv-rekursiv und somit nach Induktionsvoraussetzung $\mathcal{P}_{1\text{oop}}$ -berechenbar. Mit dem Beweis von Satz 3.3 ist dann auch f $\mathcal{P}_{1\text{oop}}$ -berechenbar, denn in diesem Beweis werden keine **while**-Anweisungen verwendet.

Induktionsschritt “ f ist definiert durch primitive Rekursion”: Sei f gegeben durch $f(0, \vec{x}) := g(\vec{x})$ und $f(x + 1, \vec{x}) := h(f(x, \vec{x}), x, \vec{x})$. Dann sind die Funktionen g und h primitiv-rekursiv und somit nach Induktionsvoraussetzung $\mathcal{P}_{1\text{oop}}$ -berechenbar, etwa durch $\mathcal{P}_{1\text{oop}}$ -Prozeduren P_g und P_h . Damit definieren wir eine $\mathcal{P}_{1\text{oop}}$ -Prozedur P'_f , aus der wir durch Elimination der **loop**-Anweisung die \mathcal{P} -Prozedur P_f erhalten, s. Abbildung 11.4. Für die **while**-Anweisung dieser Proze-

dur gilt bei Aufruf von $\mathbf{P}_f(n, \vec{n})$ die Schleifeninvariante

$$\begin{aligned} & \{n \geq y \wedge R = f(n - y, \vec{n})\} \\ & \mathbf{while\ } z \neq 0 \mathbf{\ do\ } \dots \mathbf{\ end_while} \\ & \{n \geq y \wedge R = f(n - y, \vec{n})\} \end{aligned} \tag{11.14}$$

denn für $n \geq y \wedge R = f(n - y, \vec{n})$ sowie $y \neq 0$ erhält man nach einmaliger Ausführung des Schleifenrumpfs $R = \llbracket \mathbf{P}_h \rrbracket(f(n - (y + 1), \vec{n}), n - (y + 1), \vec{n}) = h(f(n - (y + 1), \vec{n}), n - (y + 1), \vec{n})$, da mit der Induktionshypothese $\llbracket \mathbf{P}_h \rrbracket = h$ gilt. Für $n' := n - (y + 1)$ gilt damit $R = h(f(n', \vec{n}), n', \vec{n}) = f(n' + 1, \vec{n})$. Mit $n \geq y$ vor Ausführung des Schleifenrumpfs gilt nach Ausführung $n \geq y + 1$, also $n > y$, damit dann $n' + 1 = n - y$ und somit $R = f(n - y, \vec{n})$.

Mit $n = y$ und $R = \llbracket \mathbf{P}_g \rrbracket(\vec{n}) = g(\vec{n}) = f(0, \vec{n}) = f(n - y, \vec{n})$ ist die Schleifen-
vorbereitung auch vor der erstmaligen Ausführung der **while**-Anweisung erfüllt, und folglich gilt $R = f(n - y, \vec{n})$ mit (11.14) nach der letztmaligen Ausführung des Schleifenrumpfs. Da $y = 0$ nach Terminierung der **while**-Anweisung gilt, erhält man schließlich $R = f(n, \vec{n})$ als Ergebnis der Ausführung von $\mathbf{P}_f(n, \vec{n})$. ■

Bemerkung 11.18. Mit den Begriffen aus Abschnitt 11.4 lautet die Behauptung von Satz 11.17:

$$\forall \phi \in \mathbb{N}^k \rightarrow \mathbb{N}. \phi \in \llbracket \mathbf{PRF} \rrbracket \curvearrowright \phi \in \llbracket \mathcal{P}_{1\text{oop}} \rrbracket. \tag{11.15}$$

Eine äquivalente Formulierung von (11.15) ist die Aussage

$$\forall f \in \mathbf{PRF}. \exists P \in \mathcal{P}_{1\text{oop}}. \llbracket f \rrbracket = \llbracket P \rrbracket. \tag{11.16}$$

Angenommen, wir geben eine totale Funktion $\mathbf{c} : \mathbf{PRF} \rightarrow \mathcal{P}_{1\text{oop}}$ an, so daß wir

$$\forall f \in \mathbf{PRF}. \llbracket f \rrbracket = \llbracket \mathbf{c}(f) \rrbracket \tag{11.17}$$

beweisen können. Dann ist auch (11.16) – und folglich (11.15) – gezeigt, denn (11.17) impliziert offensichtlich (11.16). Wenn wir sogar eine algorithmische Funktion \mathbf{c} angeben, so beschreibt \mathbf{c} einen Compiler, der Programme der (fiktiven) Programmiersprache **PRF** für primitiv-rekursive Funktionen in äquivalente $\mathcal{P}_{1\text{oop}}$ -Programme übersetzt.

Tatsächlich haben wir Satz 11.17 durch Nachweis der stärkeren Behauptung (11.17) bewiesen, denn wir haben für jede Definition f einer primitiv-rekursiven Funktion ein $\mathcal{P}_{1\text{oop}}$ -Programm $\mathbf{c}(f)$ – im Beweis durch \mathbf{P}'_f bezeichnet – angegeben, das die gleiche Funktion wie f berechnet. Da der Beweis von Satz 11.17 konstruktiv ist (vgl. Abschnitt 3.3), ist die Funktion \mathbf{c} sogar algorithmisch: Wir können

aus dem Beweis direkt ablesen, wie zu einer gegebenen Definition f einer primitiv-rekursiven Funktion ein äquivalentes $\mathcal{P}_{\text{loop}}$ -Programm $c(f)$ zu konstruieren ist.

Anders gesagt, Satz 11.17 wurde bewiesen, indem ein Compiler für PRF-Programme zunächst spezifiziert und dann gezeigt wurde, daß dieser Compiler auch korrekt ist.

Zum Nachweis, daß jedes `loop`-Programm eine primitiv-rekursive Funktion berechnet, simulieren wir die Interpretation von `loop`-Programmen durch primitiv-rekursive Funktionen. Dazu müssen wir zeigen, daß die Interpretationsfunktionen *value* und *eval*, vgl. Definitionen 2.6 und 2.7, primitiv-rekursiv sind (vorausgesetzt, daß *eval* nur auf $\mathcal{P}_{\text{loop}}$ -Programme angewendet wird). Wir definieren dazu:

Definition 11.19. ($\llbracket \text{EXPR} \rrbracket$ und $\llbracket \text{STA}(\mathbf{y}) \rrbracket$)

Sei EXPR ein Programmausdruck sowie STA eine Programmanweisung von \mathcal{P} , in denen genau k Programmvariable $\mathbf{y}_1, \dots, \mathbf{y}_k$ vorkommen, und sei $M_P^{\vec{n}} \subseteq \mathbb{N} \times \mathbb{N}$ mit $\vec{n} = (n_1, \dots, n_k)$, so daß $\text{value}(M_P^{\vec{n}}, \mathbf{y}_i) = n_i$ für jedes $i \in \{1, \dots, k\}$. Dann ist die Funktion $\llbracket \text{EXPR} \rrbracket : \mathbb{N}^k \rightarrow \mathbb{N}$ definiert durch

$$\llbracket \text{EXPR} \rrbracket(\vec{n}) := \text{value}(M_P^{\vec{n}}, \text{EXPR}) .$$

Weiter definieren wir für jedes $i \in \{1, \dots, k\}$ eine Funktion $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket : \mathbb{N}^k \mapsto \mathbb{N}$ durch

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) := \text{value}(\text{eval}(M_P^{\vec{n}}, \text{STA}), \mathbf{y}_i) . \quad \blacksquare$$

Wir zeigen zuerst, daß *value* primitiv-rekursiv ist:

Satz 11.20. Für jeden Programmausdruck EXPR ist $\llbracket \text{EXPR} \rrbracket$ primitiv-rekursiv.

Beweis. Seien $\mathbf{y}_1, \dots, \mathbf{y}_k$ die Programmvariablen von EXPR , und sei $M_P^{\vec{n}} \subseteq \mathbb{N} \times \mathbb{N}$ mit $\vec{n} = (n_1, \dots, n_k)$, so daß $\text{value}(M_P^{\vec{n}}, \mathbf{y}_i) = n_i$ für jedes $i \in \{1, \dots, k\}$. Wir zeigen die Behauptung durch strukturelle Induktion über EXPR .

Induktionsanfang “ $\text{EXPR} = \mathbf{m} \in \mathbb{N}$ ”: Es gilt $\llbracket \text{EXPR} \rrbracket(\vec{n}) = \text{value}(M_P^{\vec{n}}, \mathbf{m}) = \mathbf{m} = C_{\mathbf{m}}^k(\vec{n})$, und mit Lemma 11.5(1) ist $\llbracket \text{EXPR} \rrbracket$ primitiv-rekursiv.

Induktionsanfang “ $\text{EXPR} = \mathbf{y}_i$ ”: Es gilt $\llbracket \text{EXPR} \rrbracket(\vec{n}) = \text{value}(M_P^{\vec{n}}, \mathbf{y}_i) = n_i = P_i^k(\vec{n})$, und mit Definition 11.4(1) ist $\llbracket \text{EXPR} \rrbracket$ primitiv-rekursiv.

Induktionsschritt “ $\text{EXPR} = \text{SUCC}(\text{EXPR}')$ ”: Es gilt

$$\begin{aligned}
& \llbracket \text{EXPR} \rrbracket(\vec{n}) \\
&= \text{value}(M_P^{\vec{n}}, \text{SUCC}(\text{EXPR}')) \\
&= 1 + \text{value}(M_P^{\vec{n}}, \text{EXPR}') \\
&= 1 + \llbracket \text{EXPR}' \rrbracket(\vec{n}) \\
&= S(\llbracket \text{EXPR}' \rrbracket(\vec{n}))
\end{aligned}$$

und mit Definition 11.4(2) ist $\llbracket \text{EXPR} \rrbracket$ primitiv-rekursiv, denn die Funktion $\llbracket \text{EXPR}' \rrbracket$ ist nach Induktionshypothese primitiv-rekursiv.

Induktionsschritt “ $\text{EXPR} = \text{PRED}(\text{EXPR}')$ ”: Man erhält

$$\llbracket \text{EXPR} \rrbracket(\vec{n}) = \begin{cases} 0 & , \text{ falls } \text{value}(M_P^{\vec{n}}, \text{EXPR}') = 0 \\ m & , \text{ falls } \text{value}(M_P^{\vec{n}}, \text{EXPR}') = m + 1 \end{cases}$$

und folglich

$$\llbracket \text{EXPR} \rrbracket(\vec{n}) = \begin{cases} \llbracket \text{EXPR}' \rrbracket(\vec{n}), & \text{ falls } \llbracket \text{EXPR}' \rrbracket(\vec{n}) = 0 \\ \llbracket \text{EXPR}' \rrbracket(\vec{n}) - 1, & \text{ falls } \llbracket \text{EXPR}' \rrbracket(\vec{n}) > 0 . \end{cases}$$

Damit gilt $\llbracket \text{EXPR} \rrbracket(\vec{n}) = \text{pred}(\llbracket \text{EXPR}' \rrbracket(\vec{n}))$, und mit Lemma 11.5(2) sowie Definition 11.4(2) ist $\llbracket \text{EXPR} \rrbracket$ primitiv-rekursiv, denn die Funktion $\llbracket \text{EXPR}' \rrbracket$ ist nach Induktionshypothese primitiv-rekursiv. ■

Als nächstes zeigen wir, daß die Interpretationsfunktion *eval* ebenfalls primitiv-rekursiv ist, solange diese nur auf Anweisungen von **loop**-Programmen angewendet wird: Für eine Programmanweisung **STA** berechnen wir die Speicherbelegung, die bei Ausführung von **STA** entsteht, und bestimmen damit dann den Wert jeder Programmvariablen nach Ausführung von **STA**. Mit $\llbracket \text{STA}(\mathbf{y}) \rrbracket$ erhält man so für jede Programmvariable **y** von **STA** eine *primitiv-rekursive* Funktion, die eine Speicherbelegung (vor Ausführung von **STA**) in den Wert der lokalen Variablen **y** (nach Ausführung von **STA**) abbildet.

Satz 11.21. Für jede Anweisung **STA** eines $\mathcal{P}_{\text{loop}}$ -Programms und jede Programmvariable **y** in **STA** ist $\llbracket \text{STA}(\mathbf{y}) \rrbracket$ primitiv-rekursiv.

Beweis. Seien $\mathbf{y}_1, \dots, \mathbf{y}_k$ die Programmvariablen von **STA** und sei $M_P^{\vec{n}} \subseteq \mathbb{N} \times \mathbb{N}$ mit $\vec{n} = (n_1, \dots, n_k)$, so daß $\text{value}(M_P^{\vec{n}}, \mathbf{y}_i) = n_i$ für jedes $i \in \{1, \dots, k\}$. Wir zeigen die Behauptung für jedes \mathbf{y}_i mit $i \in \{1, \dots, k\}$ durch strukturelle Induktion über **STA**.

Induktionsanfang “STA = SKIP”: Es gilt

$$\begin{aligned}
& \llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) \\
&= \text{value}(\text{eval}(M_P^{\vec{n}}, \text{SKIP}), \mathbf{y}_i) \quad , \text{ mit Def. 11.19} \\
&= \text{value}(M_P^{\vec{n}}, \mathbf{y}_i) \quad , \text{ mit Def. 2.7} \\
&= n_i \quad , \text{ mit Def. 2.6} \\
&= P_i^k(\vec{n}),
\end{aligned}$$

und mit Definition 11.4(1) ist $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ primitiv-rekursiv.

Induktionsanfang “STA = $\mathbf{y}_h := \text{EXPR}$ ”: Es gilt

$$\begin{aligned}
& \llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) \\
&= \text{value}(\text{eval}(M_P^{\vec{n}}, \mathbf{y}_h := \text{EXPR}), \mathbf{y}_i) \quad , \text{ mit Def. 11.19} \\
&= \text{value}(M_P^{\vec{n}}[\mathbf{y}_h \leftarrow \llbracket \text{EXPR} \rrbracket(\vec{n})], \mathbf{y}_i) \quad , \text{ mit Def. 2.7} \\
&= \text{value}(M_P^{(n_1, \dots, n_{h-1}, \llbracket \text{EXPR} \rrbracket(\vec{n}), n_{h+1}, \dots, n_k)}, \mathbf{y}_i). \quad , \text{ mit Def. 2.4}
\end{aligned}$$

Für $i = h$ erhält man damit $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = \llbracket \text{EXPR} \rrbracket(\vec{n})$, und mit Satz 11.20 ist $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ primitiv-rekursiv. Für $i \neq h$ gilt $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = n_i = P_i^k(\vec{n})$, und mit Definition 11.4(1) ist $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ auch in diesem Fall primitiv-rekursiv.

Induktionsschritt “STA = if EXPR then STA1 else STA2 end_if”: Man erhält

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = \begin{cases} \text{value}(\text{eval}(M_P^{\vec{n}}, \text{STA1}), \mathbf{y}_i), & \text{falls } \text{value}(M_P^{\vec{n}}, \text{EXPR}) > 0 \\ \text{value}(\text{eval}(M_P^{\vec{n}}, \text{STA2}), \mathbf{y}_i), & \text{falls } \text{value}(M_P^{\vec{n}}, \text{EXPR}) = 0, \end{cases}$$

und folglich

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = \begin{cases} \llbracket \text{STA1}(\mathbf{y}_i) \rrbracket(\vec{n}), & \text{falls } \llbracket \text{EXPR} \rrbracket(\vec{n}) > 0 \\ \llbracket \text{STA2}(\mathbf{y}_i) \rrbracket(\vec{n}), & \text{falls } \llbracket \text{EXPR} \rrbracket(\vec{n}) = 0. \end{cases}$$

Damit gilt $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = \text{if}(\llbracket \text{EXPR} \rrbracket(\vec{n}), \llbracket \text{STA1}(\mathbf{y}_i) \rrbracket(\vec{n}), \llbracket \text{STA2}(\mathbf{y}_i) \rrbracket(\vec{n}))$, und mit Lemma 11.5(3), Satz 11.20 und Definition 11.4(2) ist $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ primitiv-rekursiv, denn $\llbracket \text{STA1}(\mathbf{y}_i) \rrbracket$ und $\llbracket \text{STA2}(\mathbf{y}_i) \rrbracket$ sind nach Induktionsvoraussetzung primitiv-rekursiv.

Induktionsschritt “ $\text{STA} = \text{STA1}; \text{STA2}$ ”: Für (i) $n'_i := \text{value}(\text{eval}(M_P^{\vec{n}}, \text{STA1}), \mathbf{y}_i)$ und (ii) $\vec{n}' := (n'_1, \dots, n'_k)$ erhält man

$$\begin{aligned}
& \llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) \\
&= \text{value}(\text{eval}(M_P^{\vec{n}}, \text{STA1}; \text{STA2}), \mathbf{y}_i) && \text{, mit Def. 11.19} \\
&= \text{value}(\text{eval}(\text{eval}(M_P^{\vec{n}}, \text{STA1}), \text{STA2}), \mathbf{y}_i) && \text{, mit Def. 2.7} \\
&= \text{value}(\text{eval}(M_P^{\vec{n}}[\mathbf{y}_1 \leftarrow n'_1, \dots, \mathbf{y}_k \leftarrow n'_k], \text{STA2}), \mathbf{y}_i) && \text{, mit Def. 2.8 und (i)} \\
&= \text{value}(\text{eval}(M_P^{\vec{n}'}, \text{STA2}), \mathbf{y}_i) && \text{, mit Def. 2.4 und (ii).}
\end{aligned}$$

Damit gilt $\text{value}(\text{eval}(M_P^{\vec{n}'}, \text{STA2}), \mathbf{y}_i) = \llbracket \text{STA2}(\mathbf{y}_i) \rrbracket(\vec{n}')$ sowie $n'_i = \llbracket \text{STA1}(\mathbf{y}_i) \rrbracket(\vec{n})$, also

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = \llbracket \text{STA2}(\mathbf{y}_i) \rrbracket(\llbracket \text{STA1}(\mathbf{y}_1) \rrbracket(\vec{n}), \dots, \llbracket \text{STA1}(\mathbf{y}_k) \rrbracket(\vec{n})) .$$

Nach Induktionsvoraussetzung sind $\llbracket \text{STA1}(\mathbf{y}_i) \rrbracket$ und $\llbracket \text{STA2}(\mathbf{y}_i) \rrbracket$ primitiv-rekursiv, und folglich ist $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ nach Definition 11.4(2) ebenfalls primitiv-rekursiv.

Induktionsschritt “ $\text{STA} = \text{loop } \mathbf{y}_h \text{ do } \text{STA}' \text{ end_loop}$ ”: Wir nehmen o.B.d.A. $h = 1$ an und definieren für jedes $i \in \{2, \dots, k\}$ eine Funktion $f_i : \mathbb{N}^k \mapsto \mathbb{N}$ durch¹⁵

$$f_i(n, \vec{n}) := \text{value}(\text{eval}^{(n)}(M_P^{\vec{n}}, \text{STA}'), \mathbf{y}_i) \quad (11.18)$$

Damit gilt

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = f_i(n_h, \vec{n}) . \quad (11.19)$$

Man erhält

$$\boxed{f_i(0, \vec{x}) = P_i^k(\vec{x})} \quad (11.20)$$

denn

$$\begin{aligned}
& f_i(0, \vec{n}) \\
&= \text{value}(\text{eval}^{(0)}(M_P^{\vec{n}}, \text{STA}'), \mathbf{y}_i) && \text{, mit (11.18)} \\
&= \text{value}(M_P^{\vec{n}}, \mathbf{y}_i) && \text{, mit Def. } \text{eval}^{(n)} \\
&= n_i && \text{, mit Def. 2.6} \\
&= P_i^k(\vec{n})
\end{aligned}$$

sowie

$$\boxed{f_i(x+1, \vec{x}) = \llbracket \text{STA}'(\mathbf{y}_i) \rrbracket(f_2(x, \vec{x}), \dots, f_k(x, \vec{x}))} \quad (11.21)$$

¹⁵ Es gelte $\text{eval}^{(0)}(M_P, \text{STA}) := M_P$ und $\text{eval}^{(n+1)}(M_P, \text{STA}) := \text{eval}(\text{eval}^{(n)}(M_P, \text{STA}), \text{STA})$.

denn für (i) $n'_i := \text{value}(\text{eval}^{(n)}(M_P^{\vec{n}}, \text{STA}'), \mathbf{y}_i)$ und (ii) $\vec{n}' := (n'_2, \dots, n'_k)$ erhält man

$$\begin{aligned}
& f_i(n+1, \vec{n}) \\
= & \text{value}(\text{eval}^{(n+1)}(M_P^{\vec{n}}, \text{STA}'), \mathbf{y}_i) && , \text{ mit (11.18)} \\
= & \text{value}(\text{eval}(\text{eval}^{(n)}(M_P^{\vec{n}}, \text{STA}'), \text{STA}'), \mathbf{y}_i) && , \text{ mit Def. } \text{eval}^{(n)} \\
= & \text{value}(\text{eval}(M_P^{\vec{n}}[\mathbf{y}_2 \leftarrow n'_2, \dots, \mathbf{y}_k \leftarrow n'_k], \text{STA}'), \mathbf{y}_i) && , \text{ mit Def. 2.8 und (i)} \\
= & \text{value}(\text{eval}(M_P^{\vec{n}'}, \text{STA}'), \mathbf{y}_i) && , \text{ mit Def. 2.4 und (ii)} \\
= & \llbracket \text{STA}'(\mathbf{y}_i) \rrbracket(\vec{n}') && , \text{ mit Definition 11.19} \\
= & \llbracket \text{STA}'(\mathbf{y}_i) \rrbracket(f_2(n, \vec{n}), \dots, f_k(n, \vec{n})) && , \text{ mit (i), (ii) und (11.18)}.
\end{aligned}$$

Wegen (11.20) und (11.21) sind alle Funktionen f_i mit Korollar 11.10 primitiv-rekursiv, denn alle Funktionen $\llbracket \text{STA}'(\mathbf{y}_i) \rrbracket$ sind nach Induktionsvoraussetzung primitiv-rekursiv. Mit (11.19) ist dann auch jede Funktion $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ mit $i \in \{2, \dots, k\}$ primitiv-rekursiv. Schließlich gilt $\llbracket \text{STA}(\mathbf{y}_h) \rrbracket = 0$, vgl. Definition 11.15, und damit sind alle Funktionen $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ primitiv-rekursiv. ■

Der Nachweis, daß jede loop-berechenbare Funktion auch primitiv-rekursiv ist, folgt jetzt unmittelbar:

Korollar 11.22. *Jede $\mathcal{P}_{\text{loop}}$ -berechenbare Funktion ist primitiv-rekursiv.*

Beweis. Sei

```

procedure P( $\mathbf{x}_1, \dots, \mathbf{x}_k$ ) <=
begin var  $\mathbf{y}_1, \dots, \mathbf{y}_l$ ; STA; return( $\mathbf{y}_i$ ) end

```

ein $\mathcal{P}_{\text{loop}}$ -Programm. Dann gilt $\llbracket P \rrbracket(\vec{n}) = \text{value}(\text{eval}(M_P^{\vec{n}}, \text{STA}), \mathbf{y}_i) = \llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n})$, und mit Satz 11.21 ist $\llbracket P \rrbracket$ primitiv-rekursiv. ■

Bemerkung 11.23. *Auch der Beweis von Satz 11.21 ist konstruktiv, denn für jede lokale Variable \mathbf{y}_i in einer Programmanweisung STA wird eine konkrete Definition g_i für eine primitiv-rekursive Funktion $\llbracket g_i \rrbracket$ angegeben, für die dann $\llbracket g_i \rrbracket = \llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ gilt. Somit wird auch Korollar 11.22 (wie schon dessen Rückrichtung in Satz 11.17) durch Spezifikation und Verifikation eines Compilers $c : \mathcal{P}_{\text{loop}} \rightarrow \text{PRF}$ bewiesen, vgl. Anmerkung 11.18.*

11.6. Die Ackermann-Funktion

Man zeigt leicht, daß jede primitiv-rekursive Funktion *total* ist:

Satz 11.24. *Jede primitiv-rekursive Funktion ist total.*

Beweis. Sei f eine beliebige primitiv-rekursive Funktion. Wir zeigen die Totalität von f durch Induktion über den Aufbau der primitiv-rekursiven Funktionen.

Induktionsanfang “ f ist eine Grundfunktion”: In diesem Fall ist die Behauptung offensichtlich.

Induktionsschritt “ f ist definiert durch Einsetzung”: Für $f(\vec{x}) := g(h_1(\vec{x}), \dots, h_m(\vec{x}))$, vgl. Definition 11.2, sind die Funktionen h_1, \dots, h_m und g nach Induktionsvoraussetzung total. Damit muß auch f total sein.

Induktionsschritt “ f ist definiert durch primitive Rekursion”: Für f , gegeben wie in Definition 11.4, definieren wir für jedes $x \in \mathbb{N}$ eine Funktion $f_x : \mathbb{N}^k \rightarrow \mathbb{N}$ mit $f_x(\vec{x}) := f(x, \vec{x})$ und zeigen durch Induktion über x , daß jede dieser Funktionen total ist.

Induktionsanfang $x = 0$: Es gilt $f_0(\vec{x}) = f(0, \vec{x}) = g(\vec{x})$, also ist f_0 total, da g nach Induktionsvoraussetzung (der äußeren Induktion) total ist.

Induktionsschritt $x = x' + 1$: Es gilt $f_{x'+1}(\vec{x}) = f(x'+1, \vec{x}) = h(f(x', \vec{x}), x', \vec{x}) = h(f_{x'}(\vec{x}), x', \vec{x})$. Nach Induktionsvoraussetzung (der inneren Induktion) ist f_x total, und h ist nach Induktionsvoraussetzung (der äußeren Induktion) ebenfalls total. Folglich muß auch $f_{x'+1}$ total sein.

Damit ist auch f total, denn für beliebige natürliche Zahlen x, \vec{x} gilt $f(x, \vec{x}) = f_x(\vec{x})$, und mit der Totalität von f_x ist dann auch $f(x, \vec{x})$ definiert. ■

Aus Abschnitt 10.1 wissen wir, daß es für jede Programmiersprache, in der nur totale Funktionen programmiert werden können, eine totale berechenbare Funktion gibt, die durch kein Programm dieser Programmiersprache berechnet werden kann. Fassen wir das Definitionsprinzip für primitiv-rekursive Funktionen als Programmiersprache auf, so folgt mit Satz 11.24 sofort, daß es eine totale berechenbare Funktion gibt, die nicht primitiv-rekursiv ist.

Ein konkretes Beispiel dafür wurde zuerst von *W. Ackermann* angegeben und später von *R. Peter* vereinfacht. Man definiert die (vereinfachte) Ackermann-Funktion $ack: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ durch

1. $ack(0, y) := y + 1$,
2. $ack(x + 1, 0) := ack(x, 1)$, und
3. $ack(x + 1, y + 1) := ack(x, ack(x + 1, y))$.

Satz 11.25. Die Ackermann-Funktion ist total.

Beweis. Sei $(x, y) \gg (x', y')$ gdw. $x > x'$ oder $x = x'$ und $y > y'$. Wir zeigen $ack(x, y) \in \mathbb{N}$ für alle $x, y \in \mathbb{N}$ durch Induktion über \gg .

Induktionsanfang $(0, y)$: Dann gilt $ack(0, y) := y + 1 \in \mathbb{N}$.

Induktionsschritt $(x + 1, 0)$: Nach Induktionsvoraussetzung gilt $ack(x, 1) \in \mathbb{N}$ und mit $ack(x + 1, 0) = ack(x, 1)$ dann auch $ack(x + 1, 0) \in \mathbb{N}$.

Induktionsschritt $(x + 1, y + 1)$: Nach Induktionsvoraussetzung gilt $ack(x + 1, y) \in \mathbb{N}$ sowie dann auch $ack(x, ack(x + 1, y)) \in \mathbb{N}$. Mit $ack(x + 1, y + 1) = ack(x, ack(x + 1, y))$ erhält man $ack(x + 1, y + 1) \in \mathbb{N}$. ■

Es gilt:

Satz 11.26. Die Ackermann-Funktion ist nicht primitiv-rekursiv.

Zum Beweis von Satz 11.26 zeigt man, daß ack stärker als jede primitiv-rekursive Funktion wächst. Einen formalen Beweis dafür findet man beispielsweise in [Hermes(1971)] und [Wagner(1994)].

Bemerkung 11.27. In Abschnitt 11.1 wurden verallgemeinerte Definitionsschemata für primitiv-rekursive Funktionen angegeben, wobei jedoch geschachtelte Rekursionen, d.h. Ausdrücke der Form $f(\dots f(\dots))$ auf der rechten Seite einer definierenden Gleichung nicht erlaubt wurden. Mit Satz 11.26 wird auch der Grund für dieses Verbot offensichtlich. Dies bedeutet natürlich nicht, daß mit geschachtelten Rekursionen nur Funktionen definiert werden können, die nicht primitiv-rekursiv sind. Beispielsweise wird mit $f(0) := 0$ und $f(x + 1) := 1 + f(f(x))$ eine primitiv-rekursive Funktion definiert, denn man zeigt leicht $f(n) = n$ für alle $n \in \mathbb{N}$ durch Induktion über n . Allerdings wandelt man bei geschachtelten Rekursionen auf einem schmalen Grat: Die (fast genauso wie f definierten) Funktionen f' und f'' , gegeben durch $f'(0) := 1$ und $f'(x + 1) := 1 + f'(f'(x))$ sowie $f''(0) := 0$ und $f''(x + 1) := 2 + f''(f''(x))$ sind nicht total (und mit Satz 11.24 dann auch nicht primitiv-rekursiv).

11.7. μ -rekursive Funktionen

Da mit primitiver Rekursion nicht alle berechenbaren Funktionen definiert werden können, wird ein zusätzliches Definitionsprinzip eingeführt:

Definition 11.28. (Definition durch Minimierung, μ -Operator)

Sei $f : \mathbb{N}^{k+1} \mapsto \mathbb{N}$ eine Funktion mit $k \geq 0$ und sei die Funktion $\mu f : \mathbb{N}^k \mapsto \mathbb{N}$ gegeben durch

$$\mu f(\vec{x}) := \begin{cases} x & , \text{ falls } f(x, \vec{x}) = 0 \text{ und } f(x', \vec{x}) \in \mathbb{N} \setminus \{0\} \text{ für alle } x' < x \\ \perp & , \text{ andernfalls.} \end{cases}$$

Dann ist die Funktion μf definiert durch (unbeschränkte) Minimierung (der Funktion f). ■

Beispiel 11.29. (Definition durch Minimierung)

1. Es gilt $\mu plus(0) = 0$ und $\mu plus(y + 1) = \perp$ sowie $\mu times(y) = 0$.
2. Sei $g : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ definiert durch $g(x, y) = y - x^2$. Es gilt $\mu g(y) = z$ gdw. $y - z^2 = 0$ und $y - \bar{z}^2 \in \mathbb{N} \setminus \{0\}$ für alle $\bar{z} < z$, d.h. $\bar{z}^2 < y \leq z^2$, also $\bar{z} < \sqrt{y} \leq z$. Damit gilt $\mu g(y) = \lceil \sqrt{y} \rceil$, d.h. $\mu g(y)$ approximiert \sqrt{y} als die kleinste natürliche Zahl, deren Quadrat größer oder gleich y ist.
3. Sei $f_h : \mathbb{N} \times \mathbb{N} \mapsto \mathbb{N}$ definiert durch $f_h(x, y) = (h(x) - y) + (y - h(x))$ für eine berechenbare Funktion $h : \mathbb{N} \mapsto \mathbb{N}$. Mit $\mu f_h(y) = z$ gilt für alle $z' < z$:

$$\begin{aligned} & (h(z) - y) + (y - h(z)) = 0 \wedge (h(z') - y) + (y - h(z')) \in \mathbb{N} \setminus \{0\} \\ \text{gdw. } & h(z) - y = 0 \wedge y - h(z) = 0 \wedge ((h(z') - y) \neq 0 \vee (y - h(z')) \neq 0) \\ \text{gdw. } & h(z) \leq y \leq h(z) \wedge (h(z') > y \vee y > h(z')) \\ \text{gdw. } & h(z) = y \neq h(z') . \end{aligned}$$

Damit berechnet $\mu f_h(y)$ das kleinste h -Urbild z von y , falls $y \in \text{Bild}(h)$ und $\{0, \dots, z - 1\} \subseteq \text{Def}(h)$. Für $y \notin \text{Bild}(h)$ gilt $\mu f_h(y) = \perp$, und folglich $\text{Def}(\mu f_h) \subseteq \text{Bild}(h)$.

- (i) Ist h nicht total, so gilt $|\text{Def}(\mu f_h)| < \infty$, d.h. die Minimierung nicht-totaler Funktionen ist wenig nützlich, vgl. Bemerkung 11.32. Man erhält z.B. $\text{Def}(\mu f_{\log_2}(y)) = \emptyset$, denn $\log_2(0) = \perp$.¹⁶

¹⁶ Mit $\log_2(2^x) := x$ und $\log_2(y) = \perp$, falls y keine 2er-Potenz ist.

- (ii) Ist h total, so gilt $\text{Def}(\mu f_h) = \text{Bild}(h)$, also z.B. $\mu f_S(0) = \perp$ und $\mu f_S(y+1) = y$ sowie $\mu f_{2^x}(y) = \log_2(y)$, falls y eine 2er-Potenz ist, und $\mu f_{2^x}(y) = \perp$ andernfalls.
- (iii) Ist h total und surjektiv, so ist μf_h ebenfalls total, wie beispielsweise bei $\mu f_{\lfloor x/2 \rfloor}(y) = 2y$. ■

Ist $f : \mathbb{N}^{k+1} \mapsto \mathbb{N}$ eine berechenbare Funktion, so können wir $\mu f(\vec{n})$ für alle $\vec{n} \in \mathbb{N}^k$ allein mittels f berechnen: Für $n := 0$ starten wir die Berechnung von $f(n, \vec{n})$. Gilt $f(n, \vec{n}) = \perp$, so endet diese Berechnung nicht, folglich endet auch die Berechnung von $\mu f(\vec{n})$ nicht, und wir erhalten $\mu f(\vec{n}) = \perp$. Andernfalls testen wir, ob $f(n, \vec{n}) = 0$ gilt. Im positiven Fall ist dann n das Ergebnis von $\mu f(\vec{n})$. Im negativen Fall setzen wir $n := n + 1$ und beginnen von vorne. Damit erhalten wir das kleinste n mit $f(n, \vec{n}) = 0$ sowie $f(n', \vec{n}) \in \mathbb{N} \setminus \{0\}$ für alle $n' < n$ als Ergebnis von $\mu f(\vec{n})$, falls ein n mit $f(n, \vec{n}) = 0$ überhaupt existiert. Andernfalls gilt entweder (i) $f(n, \vec{n}) \in \mathbb{N} \setminus \{0\}$ für alle $n \in \mathbb{N}$ oder aber (ii) $f(n, \vec{n}) \notin \mathbb{N}$ und $f(n', \vec{n}) \in \mathbb{N} \setminus \{0\}$ für alle $n' < n$. In Fall (i) hält die Schleife nie, und damit ist \perp das Ergebnis von $\mu f(\vec{n})$. In Fall (ii) gilt $f(n, \vec{n}) = \perp$, und folglich erhält man auch hier \perp als Ergebnis von $\mu f(\vec{n})$.

Anhand dieser Überlegung ist offensichtlich, daß man mittels des μ -Operators ein Konzept in Art einer Schleife erhält, denn die Funktion f wird solange mit (festem \vec{n} und) jeweils um 1 erhöhtem Argument n aufgerufen, bis das Schleifenabbruchkriterium “ $f(n, \vec{n}) = 0$ ” erfüllt ist. Damit erhält man ein explizites Rechenmodell für (die nachfolgend definierten) μ -rekursive Funktionen durch Erweiterung des Kalküls aus Abschnitt 11.4 um drei zusätzliche Regeln wie in Abbildung 11.5.¹⁷ Hierbei ist $\mu \hat{f}$ eine Hilfsfunktion, die die “Hochzählschleife” des μ -Operators modelliert: Mit (M1) wird die Laufvariable dieser Schleife mit Z initialisiert, mit (M2) erhält man das Ergebnis von $\mu f(\vec{t})$, falls ein solches existiert, und mit (M3) wird die Laufvariable bei Fehlschlag von (M2) um 1 erhöht.

Damit wird auch die Motivation für die Forderung (*) “ $f(x', \vec{x}) \in \mathbb{N} \setminus \{0\}$ für alle $x' < x$ ” aus Definition 11.28 ersichtlich: Ersetzt man (*) durch (**) “ $f(x', \vec{x}) \neq 0$ für alle $x' < x$ ”, also “ $f(x', \vec{x}) = \perp$ oder $f(x', \vec{x}) \in \mathbb{N} \setminus \{0\}$ für alle $x' < x$ ”, so kann μf (selbst für eine berechenbare Funktion f) nicht notwendigerweise iterativ berechnet werden.

¹⁷ Bei diesen Regelschemata steht \vec{x} für eine Folge beliebiger Ausdrücke, bestehend aus Funktionssymbolen und natürlichen Zahlen. Der Wert $n \in \mathbb{N}$ für die Laufvariable darf nur durch (M1) – (M3) gesetzt werden.

(M1)	$\frac{\mu f(\vec{t})}{\mu \hat{f}(Z, \vec{t})}$	
(M2)	$\frac{\mu \hat{f}(n, \vec{t})}{n}$	falls $n \in \mathcal{N}$ und $f(n, \vec{t}) \Rightarrow^* Z$
(M3)	$\frac{\mu \hat{f}(n, \vec{t})}{\mu \hat{f}(S(n), \vec{t})}$	falls $f(n, \vec{t}) \Rightarrow^* S(n')$ mit $n, n' \in \mathcal{N}$

Abbildung 11.5: Erweiterung des Rechenmodells für den μ -Operator

Beispiel 11.30. (μ -Operator) Sei die Funktion $f : \mathbb{N} \mapsto \mathbb{N}$ definiert durch $f(0) := \perp$ und $f(x+1) := 0$. Nach Definition 11.28 gilt $\mu f = \perp$, denn $f(0) := \perp$, und man erhält genau dieses Ergebnis bei iterativer Berechnung von f . Ersetzt man jedoch Forderung (*) in Definition 11.28 durch die Forderung (**), so gilt $\mu f = 1$, die iterative Berechnung von f liefert jedoch \perp . ■

Ausgehend von den Grundfunktionen erlauben wir jetzt bei Angabe einer Funktion neben “Definition durch Einsetzung” und “Definition durch primitive Rekursion” auch “Definition durch Minimierung”. Man erhält so die Klasse der μ -rekursiven Funktionen als eine echte Obermenge der primitiv-rekursiven Funktionen:

Definition 11.31. (μ -rekursive Funktionen)

Eine Funktion $f : \mathbb{N}^k \mapsto \mathbb{N}$ mit $k \geq 0$ heißt μ -rekursiv, gdw. gilt:

1. f ist eine Grundfunktion, oder
2. f ist definiert durch Einsetzung mittels μ -rekursiver Funktionen, oder
3. f ist definiert durch primitive Rekursion mittels μ -rekursiver Funktionen, oder
4. f ist definiert durch Minimierung einer μ -rekursiven Funktion. ■

Bemerkung 11.32. Der μ -Operator ist natürlich nicht prinzipiell auf das erste Argument einer zu minimierenden Funktion beschränkt, denn man kann leicht mittels μf und Grundfunktionen einen μ -Operator $\mu f.x_i$ definieren, der das i .te Argument x_i einer Funktion f minimiert.

In manchen Lehrbüchern wird bei Definition des μ -Operators “ $f(x, \vec{x}) = 1$ ” anstatt “ $f(x, \vec{x}) = 0$ ” gefordert. Es sollte offensichtlich sein, daß solche Unterschiede für die definierte Theorie unerheblich sind. Des weiteren findet man in einigen Texten lediglich die schwächere Forderung (**) “ $f(x', \vec{x}) \neq 0$ für alle $x' < x$ ” anstatt Forderung (*) “ $f(x', \vec{x}) \in \mathbb{N} \setminus \{0\}$ für alle $x' < x$ ”. Dafür wird dann jedoch bei Definition der μ -rekursiven Funktionen “4. f ist definiert durch Minimierung einer totalen μ -rekursiven Funktion” anstatt 11.31(4) verlangt, s.a. Beispiel 11.29(3.(i)). Diese Einschränkung stellt sicher, daß die Berechnung von μf durch die iterative Berechnung von f trotzdem gelingt. (In Beispiel 11.30 darf der μ -Operator dann nicht auf die Funktion f angewendet werden).

Trotzdem gibt es einen gravierenden Unterschied zwischen diesen beiden Alternativen, und zwar in der Frage, ob wir die Notation zur Definition μ -rekursiver Funktionen als eine (fiktive) Programmiersprache μRF auffassen können: Von einer Programmiersprache wird sinnvollerweise gefordert, daß entschieden werden kann, ob ein vorliegender Text den syntaktischen Konventionen der Sprache genügt, vgl. die Entscheidungsfunktion *parse* im Beweis von Satz 4.13(3.1). Es muß also entscheidbar sein, ob ein Text tatsächlich ein Programm der Programmiersprache darstellt. Für unsere Definition der μ -rekursiven Funktionen trifft das sicherlich zu, denn es ist entscheidbar, ob eine Funktion als Grundfunktion, durch Einsetzung, durch primitive Rekursion oder durch Minimierung definiert wurde. Fordert man jedoch “4. f ist definiert durch Minimierung einer totalen μ -rekursiven Funktion” in Definition 11.31, so verliert man die Entscheidbarkeit. Jetzt muß ein Syntaxanalysator (als eine berechenbare Funktion *parse*) entscheiden, ob eine μ -rekursive Funktion total ist, um die korrekte Anwendung des μ -Operators zu überprüfen. Nach Satz 10.1 ist jedoch die Totalität einer berechenbaren Funktion noch nicht einmal semi-entscheidbar, und damit ist die Alternativdefinition μ -rekursiver Funktionen als Programmiersprache ungeeignet.

Schränkt man die Anwendbarkeit des μ -Operators noch weiter ein, und zwar auf primitiv-rekursiv definierte Funktionen, so ist die resultierende Programmiersprache offensichtlich entscheidbar. Allerdings stellt sich dann die Frage, ob diese Einschränkung nicht auch eine Einschränkung der so definierten Klasse der μ -rekursiven Funktionen (im Vergleich zu Definition 11.31) nach sich zieht. Mit dem Kleeneschen Normalformsatzes (Satz 11.41) kann gezeigt werden, daß dies nicht der Fall ist.

Bemerkung 11.33. Die Programmiersprache μRF ist nicht strikt, da Funktionsaufrufe nicht call-by-value sondern call-by-name ausgewertet werden (man spricht in solch einem Fall von lazy evaluation anstatt eager evaluation).¹⁸ Beispielsweise gilt $P_1^2(42, \mu\text{S}) \Rightarrow^+ 42$ sowie $\text{times}(0, \mu\text{S}) \Rightarrow^+ 0$ für die primitiv-rekursive Funktion times aus Beispiel 11.8, obwohl die Berechnung von μS nicht terminiert (denn $\mu\text{S} \not\Rightarrow^+ n$ für jedes $n \in \mathbb{N}$).

Die Nachfolgerfunktion S sowie alle Funktionen, die durch primitive Rekursion definiert wurden, sind (wegen Regelschema (Pr3) aus Abbildung 11.2) dagegen strikt bzgl. des ersten Arguments.¹⁹ Beispielsweise gilt $\text{times}(\mu\text{S}, 0) \not\Rightarrow^+ n$ für alle $n \in \mathbb{N}$. Insbesondere ist damit auch die Funktion if aus Lemma 11.5 strikt in ihrem Bedingungsargument, d.h. $\text{if}(b, \dots, \dots) \not\Rightarrow^+ n$ für alle $n \in \mathbb{N}$, wenn $b \not\Rightarrow^+ n$ für alle $n \in \mathbb{N}$.

Beispiel 11.34. (μ -rekursive Funktionen) Alle Funktionen aus Beispiel 11.29 sind μ -rekursiv. Weiter gilt für die Funktionen aus diesem Beispiel:

1. μplus ist nicht primitiv-rekursiv, μtimes ist primitiv-rekursiv.
2. μg ist primitiv-rekursiv.
3. μf_{\log_2} , μf_{S} und μf_{2^x} sind nicht primitiv-rekursiv, $\mu f_{\lfloor x/2 \rfloor}$ ist primitiv-rekursiv. ■

Wir zeigen jetzt, daß die Klasse der μ -rekursiven Funktionen identisch der Klasse der \mathcal{P} -berechenbaren Funktionen ist. Den Beweis für die Behauptung, daß μ -rekursive Funktionen \mathcal{P} -berechenbar sind, gewinnen wir aus dem Beweis der Behauptung, daß primitiv-rekursive Funktionen $\mathcal{P}_{1\text{oop}}$ -berechenbar sind (Satz 11.17). Wir müssen diesen Beweis lediglich noch für den Fall ergänzen, in dem eine Funktion mittels Minimierung definiert wird. Dies gelingt, da jetzt beliebige `while`-Anweisungen zur Verfügung stehen:

Satz 11.35. Jede μ -rekursive Funktion ist \mathcal{P} -berechenbar.

Beweis. Ausgehend von der induktiven Definition der μ -rekursiven Funktionen definieren wir für jede μ -rekursive Funktion $f : \mathbb{N}^k \mapsto \mathbb{N}$ ein \mathcal{P} -Programm $P_f \in \mathcal{P}[k]$ mit $\llbracket P_f \rrbracket = f$.

¹⁸ Eine Funktion ϕ ist strikt gdw. $\phi(\dots, \perp, \dots) = \perp$, d.h. der Funktionswert ist undefiniert sobald eines der Argumente undefiniert ist.

¹⁹ Erweitert man das Definitionsprinzip der primitiven Rekursion, so daß auch Rekursion auf einem anderen als dem ersten Argument erlaubt ist, so sind solche Funktionen strikt bzgl. ihres Rekursionsarguments.

Induktionsanfang “ f ist eine Grundfunktion”: Wir definieren P_f wie im Beweis von Satz 11.17.

Induktionsschritt “ f ist definiert durch Einsetzung”: Man zeigt die Behauptung wie im Beweis von Satz 11.17.

Induktionsschritt “ f ist definiert durch primitive Rekursion”: Man zeigt die Behauptung wie im Beweis von Satz 11.17, da die schwächere Induktionsvoraussetzung “die Funktionen g und h sind μ -rekursiv” ausreicht, um die μ -Rekursivität von f zu zeigen.

Induktionsschritt “ f ist definiert durch Minimierung”: Sei f gegeben durch Minimierung einer μ -rekursiven Funktion $g : \mathbb{N}^{k+1} \mapsto \mathbb{N}$, also $f = \mu g$. Dann ist g nach Induktionsvoraussetzung \mathcal{P} -berechenbar, etwa durch eine \mathcal{P} -Prozedur P_g . Damit definieren wir die \mathcal{P} -Prozedur

```

procedure  $P_f(x_1, \dots, x_k) \Leftarrow$ 
begin var res;
  res := 0;
  while  $P_g(res, x_1, \dots, x_k) \neq 0$  do
    res := SUCC(res)
  end_while;
  return(res)
end

```

und zeigen $\llbracket P_f \rrbracket(\vec{n}) = \mu g(\vec{n})$ für alle $\vec{n} \in \mathbb{N}^k$:

Fall “ $g(n, \vec{n}) = 0$ für ein $n \in \mathbb{N}$ sowie $g(n', \vec{n}) \in \mathbb{N} \setminus \{0\}$ für alle $n' < n$ ”: Dann gilt $\mu g(\vec{n}) = n$ und die Berechnung von $P_g(res, x_1, \dots, x_k)$ terminiert solange $res = n' \leq n$ gilt. Da der Schleifentest für alle $n' < n$ erfolgreich ist, wird res solange hochgezählt bis $res = n$ gilt. Mit $\llbracket P_g \rrbracket(res, \vec{n}) = 0$ wird die Abarbeitung der Schleife beendet, und die Ausführung von $P_f(x_1, \dots, x_k)$ terminiert mit Ergebnis $n = \mu g(\vec{n})$.

Fall “ $g(n, \vec{n}) = \perp$ für ein $n \in \mathbb{N}$ sowie $g(n', \vec{n}) \in \mathbb{N} \setminus \{0\}$ für alle $n' < n$ ”: Dann gilt $\mu g(\vec{n}) \notin \mathbb{N}$ und die Berechnung von $P_g(res, x_1, \dots, x_k)$ terminiert solange $res = n' < n$ gilt. Da der Schleifentest für alle $n' < n$ erfolgreich ist, wird res solange hochgezählt bis $res = n$ gilt. Hier terminiert die Berechnung von $P_g(res, x_1, \dots, x_k)$ jedoch nicht mehr. Also terminiert auch die Ausführung von $P_f(x_1, \dots, x_k)$ nicht, und somit gilt $\llbracket P_f \rrbracket(\vec{n}) = \perp = \mu g(\vec{n})$.

Fall “ $g(n, \vec{n}) \in \mathbb{N} \setminus \{0\}$ für alle $n \in \mathbb{N}$ ”: Dann gilt $\mu g(\vec{n}) \notin \mathbb{N}$ und die Berechnung von $P_g(res, x_1, \dots, x_k)$ terminiert immer. Da mit $\llbracket P_g \rrbracket(n, n_1, \dots, n_k) \neq 0$ der

Schleifentest jedoch für alle n erfolgreich ist, terminiert die **while**-Schleife in \mathcal{P}_f nicht. Also terminiert die Ausführung von $\mathcal{P}_f(x_1, \dots, x_k)$ nicht, und somit gilt $\llbracket \mathcal{P}_f \rrbracket(\vec{n}) = \perp = \mu g(\vec{n})$. ■

Bemerkung 11.36. Wie bei Beweis von Satz 11.17 wird auch Satz 11.35 durch Spezifikation eines Compilers $c : \mu\text{RF} \rightarrow \mathcal{P}$ und dessen Korrektheitsnachweis bewiesen, vgl. Anmerkung 11.18.

Zum Beweis, daß jede \mathcal{P} -berechenbare Funktion μ -rekursiv ist, zeigen wir, daß jede Funktion $\llbracket \text{STA}(\mathbf{y}) \rrbracket$, die eine Speicherbelegung (vor Ausführung von STA) in den Wert einer Programmvariablen \mathbf{y} (nach Ausführung von STA) abbildet, μ -rekursiv ist. Der Beweis folgt dabei dem Beweis von Satz 11.21 und ist lediglich für **while**-Anweisungen (anstatt **loop**-Anweisungen) anzupassen. Wie in diesem Beweis ist auch hier die Definition von Funktionen durch gegenseitige Rekursion erforderlich:

Korollar 11.37. (μ -rekursive Funktionen durch gegenseitige Rekursion)

Sei $k \geq 0$ und seien $g_1, \dots, g_j : \mathbb{N}^k \mapsto \mathbb{N}$ sowie $h_1, \dots, h_j : \mathbb{N}^{j+1+k} \mapsto \mathbb{N}$ μ -rekursive Funktionen. Dann sind die Funktionen $f_1, \dots, f_j : \mathbb{N}^{k+1} \mapsto \mathbb{N}$, gegeben durch

1. $f_i(0, \vec{x}) := g_i(\vec{x})$ und
2. $f_i(x+1, \vec{x}) := h_i(f_1(x, \vec{x}), \dots, f_j(x, \vec{x}), x, \vec{x})$,

für alle $i \in \{1, \dots, j\}$ μ -rekursiv.

Beweis. Mit Satz 11.9 gilt (*) $f_i(x, \vec{x}) = \pi_i^j(F(x, \vec{x}))$ für eine durch primitive Rekursion mittels $g_1, \dots, g_j, h_1, \dots, h_j, \pi_1^j, \dots, \pi_j^j$ definierte Funktion $F : \mathbb{N}^{k+1} \mapsto \mathbb{N}$. Mit Definition 11.31 ist F μ -rekursiv, denn die Funktionen g_i, h_i und π_i^j sind μ -rekursiv, und mit (*) sind dann auch alle Funktionen f_i μ -rekursiv. ■

Satz 11.38. Für jede Anweisung STA eines \mathcal{P} -Programms und jede Programmvariable \mathbf{y} in STA ist $\llbracket \text{STA}(\mathbf{y}) \rrbracket$ μ -rekursiv.

Beweis. Seien $\mathbf{y}_1, \dots, \mathbf{y}_k$ die Programmvariablen von STA und sei $M_{\mathcal{P}}^{\vec{n}} \subseteq \mathbb{N} \times \mathbb{N}$ mit $\vec{n} = (n_1, \dots, n_k)$, so daß $\text{value}(M_{\mathcal{P}}^{\vec{n}}, \mathbf{y}_i) = n_i$ für jedes $i \in \{1, \dots, k\}$. Wir zeigen die Behauptung für jedes \mathbf{y}_i mit $i \in \{1, \dots, k\}$ durch strukturelle Induktion über STA.

Induktionsanfang “STA = SKIP”: Man zeigt wie im Beweis von Satz 11.21, daß $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ primitiv-rekursiv ist.

Induktionsanfang “ $\text{STA} = \mathbf{y}_h := \text{EXPR}$ ”: Man zeigt wie im Beweis von Satz 11.21, daß $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ primitiv-rekursiv ist.

Induktionsschritt “ $\text{STA} = \text{if EXPR then STA1 else STA2 end_if}$ ”: Man zeigt

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = \text{if}(\llbracket \text{EXPR} \rrbracket(\vec{n}), \llbracket \text{STA1}(\mathbf{y}_i) \rrbracket(\vec{n}), \llbracket \text{STA2}(\mathbf{y}_i) \rrbracket(\vec{n}))$$

wie im Beweis von Satz 11.21. Mit Lemma 11.5(3), Satz 11.20 und Definition 11.31(2) ist $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ μ -rekursiv, denn $\llbracket \text{STA1}(\mathbf{y}_i) \rrbracket$ und $\llbracket \text{STA2}(\mathbf{y}_i) \rrbracket$ sind nach Induktionsvoraussetzung μ -rekursiv.

Induktionsschritt “ $\text{STA} = \text{STA1}; \text{STA2}$ ”: Man zeigt

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = \llbracket \text{STA2}(\mathbf{y}_i) \rrbracket(\llbracket \text{STA1}(\mathbf{y}_1) \rrbracket(\vec{n}), \dots, \llbracket \text{STA1}(\mathbf{y}_k) \rrbracket(\vec{n}))$$

wie im Beweis von Satz 11.21. Nach Induktionsvoraussetzung sind $\llbracket \text{STA1}(\mathbf{y}_i) \rrbracket$ und $\llbracket \text{STA2}(\mathbf{y}_i) \rrbracket$ μ -rekursiv, und folglich ist $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ nach Definition 11.31(2) ebenfalls μ -rekursiv.

Induktionsschritt “ $\text{STA} = \text{while EXPR do STA}' \text{ end_while}$ ”: Wie im Beweis von Satz 11.21 definieren für jedes $i \in \{1, \dots, k\}$ die Funktionen $f_i : \mathbb{N}^k \mapsto \mathbb{N}$ durch

$$f_i(n, \vec{n}) := \text{value}(\text{eval}^{(n)}(M_P^{\vec{n}}, \text{STA}'), \mathbf{y}_i) \quad (11.22)$$

und damit gilt

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = f_i(m, \vec{n}) \quad (11.23)$$

falls die Auswertung von STA nach m Schleifendurchläufen terminiert. Man erhält wie im Beweis von Satz 11.21

$$\boxed{f_i(0, \vec{x}) = P_i^k(\vec{x})} \quad (11.24)$$

sowie

$$\boxed{f_i(x+1, \vec{x}) = \llbracket \text{STA}'(\mathbf{y}_i) \rrbracket(f_1(x, \vec{x}), \dots, f_k(x, \vec{x}))} \quad (11.25)$$

Wegen (11.24) und (11.25) sind alle Funktionen f_i nach Korollar 11.37 μ -rekursiv, denn alle Funktionen $\llbracket \text{STA}'(\mathbf{y}_i) \rrbracket$ sind nach Induktionsvoraussetzung μ -rekursiv. Folglich ist die Funktion

$$\langle \text{EXPR} \rangle(n, \vec{n}) := \llbracket \text{EXPR} \rrbracket(f_1(n, \vec{n}), \dots, f_k(n, \vec{n}))$$

ebenfalls μ -rekursiv, denn $\langle \text{EXPR} \rangle (n, \vec{n})$ ist definiert durch Einsetzung mittels der primitiv-rekursiven Funktion $\llbracket \text{EXPR} \rrbracket$ und den μ -rekursiven Funktionen f_i .

Wir zeigen jetzt

$$\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = f_i(\mu \langle \text{EXPR} \rangle(\vec{n}), \vec{n}) . \quad (11.26)$$

Fall “Die Auswertung von STA terminiert nach m Schleifendurchläufen”: Dann gilt $\langle \text{EXPR} \rangle (m', \vec{n}) \in \mathbb{N} \setminus \{0\}$ für alle $m' < m$ sowie $\langle \text{EXPR} \rangle (m, \vec{n}) = 0$, folglich $\mu \langle \text{EXPR} \rangle(\vec{n}) = m$, und mit (11.23) dann (11.26).

Fall “Die Auswertung von STA terminiert nicht”: Dann gilt $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n}) = \perp$ sowie $\langle \text{EXPR} \rangle (m, \vec{n}) \neq 0$ für alle $m \in \mathbb{N}$, folglich $\mu \langle \text{EXPR} \rangle(\vec{n}) = \perp$, und damit auch $f_i(\mu \langle \text{EXPR} \rangle(\vec{n}), \vec{n}) = \perp$.

Da f_i und $\mu \langle \text{EXPR} \rangle$ μ -rekursiv sind, ist mit (11.26) auch jede Funktion $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ μ -rekursiv. ■

Der Nachweis, daß jede \mathcal{P} -berechenbare Funktion auch μ -rekursiv ist, folgt jetzt unmittelbar:

Korollar 11.39. *Jede \mathcal{P} -berechenbare Funktion ist μ -rekursiv.*

Beweis. Sei

```
procedure P( $\mathbf{x}_1, \dots, \mathbf{x}_k$ ) <=
begin var  $\mathbf{y}_1, \dots, \mathbf{y}_l$ ; STA; return( $\mathbf{y}_i$ ) end
```

ein \mathcal{P} -Programm. Dann gilt $\llbracket P \rrbracket(\vec{n}) = \text{value}(\text{eval}(M_{\mathcal{P}}^{\vec{n}}, \text{STA}), \mathbf{y}_i) = \llbracket \text{STA}(\mathbf{y}_i) \rrbracket(\vec{n})$, und mit Satz 11.38 ist $\llbracket P \rrbracket$ μ -rekursiv. ■

Bemerkung 11.40. Auch der Beweis von Satz 11.38 ist konstruktiv, denn für jede lokale Variable \mathbf{y}_i in einer Programmanweisung STA wird eine konkrete Definition für $\llbracket \text{STA}(\mathbf{y}_i) \rrbracket$ angegeben. Somit wird auch dieser Satz (wie schon dessen Rückrichtung in Satz 11.35) durch Spezifikation und Verifikation eines Compilers $c : \mathcal{P} \rightarrow \mu\text{RF}$ bewiesen, vgl. Anmerkung 11.36.

Des weiteren kann gezeigt werden:

Satz 11.41. (Kleenescher Normalformsatz)

Für jede μ -rekursive Funktion $f : \mathbb{N}^k \mapsto \mathbb{N}$ existieren primitiv-rekursive Funktionen $g, h : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$, so daß $f(\vec{x}) = h(\mu g(\vec{x}), \vec{x})$ für alle $\vec{x} \in \mathbb{N}^k$.

Bemerkung 11.42. Konsequenz von Satz 11.41 ist insbesondere, daß bei Definition μ -rekursiver Funktionen die Anwendung des μ -Operators auf primitiv-rekursiv definierte Funktionen beschränkt werden kann. Mit dieser Forderung (anstatt der in Anmerkung 11.32 diskutierten Alternativen) bleibt die resultierende Programmiersprache μRF entscheidbar.

12. TURINGMASCHINEN

Turingmaschinen sind in der Berechenbarkeitstheorie ein allgemein akzeptiertes mathematisches Modell für programmierbare Rechner, siehe Kapitel 1 und Abschnitt 3.2. In diesem Kapitel werden Turingmaschinen definiert und anschließend bewiesen, daß Turingmaschinen nicht mehr leisten können als \mathcal{P} -Programme. Mit diesem Nachweis ist dann gezeigt, daß die Programmiersprache \mathcal{P} berechnungsvollständig ist und somit – unter Voraussetzung der Gültigkeit der Churchschen These – jede arithmetische Funktion, die nicht \mathcal{P} -berechenbar ist, auch nicht intuitiv berechenbar ist.

12.1. Definition und Rechenmodell

Definition 12.1. (Turingmaschine)

Eine Turingmaschine TM ist ein 7-Tupel $(Z, z_{start}, z_{stop}, \Gamma, \square, \Sigma, \delta)$ für das gilt:

- Z ist die endliche Menge der Zustände von TM ,
- $z_{start} \in Z$ ist der Anfangszustand von TM ,
- $z_{stop} \in Z$ ist der Endzustand von TM ,
- Γ ist das endliche Arbeitsalphabet von TM ,
- $\square \in \Gamma$ ist ein ausgezeichnetes Symbol des Arbeitsalphabets von TM ,
- $\Sigma \subseteq \Gamma \setminus \{\square\}$ ist das nicht-leere Eingabealphabet von TM ,
- δ ist eine totale Funktion $\delta : (Z \setminus \{z_{stop}\}) \times \Gamma \rightarrow Z \times \Gamma \times \{\leftarrow, \circlearrowleft, \rightarrow\}$, die Übergangsfunktion von TM .

Die Funktionen $f, l : \Gamma^* \rightarrow \Gamma$ und $r, b : \Gamma^* \rightarrow \Gamma^*$ (für first, last, rest und butlast) sind definiert durch

- $f(\varepsilon) := l(\varepsilon) := \square$,
- $r(\varepsilon) := b(\varepsilon) := \varepsilon$, sowie

- $f(a\alpha) := l(\alpha) := a$
- $r(a\alpha) := b(\alpha) := \alpha$.

mit $a \in \Gamma$ und $\alpha \in \Gamma^*$. Ein Wort $\alpha z \beta \in \Gamma^* Z \Gamma^*$ mit $\alpha \beta \in \Gamma^*$ wird eine Konfiguration der Turingmaschine genannt. Wir definieren die Konfigurationsrelation \vdash_{TM} als die kleinste Relation auf $\Gamma^* Z \Gamma^*$ mit:

1. $\alpha z \beta \vdash_{TM} b(\alpha) z' l(\alpha) b' r(\beta)$, falls $\delta(z, f(\beta)) = (z', b', \leftrightarrow)$, siehe (12.1),
2. $\alpha z \beta \vdash_{TM} \alpha z' b' r(\beta)$, falls $\delta(z, f(\beta)) = (z', b', \odot)$, siehe (12.2), oder
3. $\alpha z \beta \vdash_{TM} \alpha b' z' r(\beta)$, falls $\delta(z, f(\beta)) = (z', b', \leftrightarrow)$, siehe (12.3).

Eine Konfiguration $\alpha' z' \beta'$ mit $\alpha z \beta \vdash_{TM} \alpha' z' \beta'$ heißt Folgekonfiguration der Konfiguration $\alpha z \beta$. Eine Konfiguration $\alpha z_{stop} \beta$ heißt Endkonfiguration.

Die von einer Turingmaschine TM berechnete Funktion $\phi_{TM} : \Sigma^* \mapsto \Sigma^*$ ist definiert durch $\phi_{TM}(\beta) := \beta'$ genau dann, wenn es $\alpha', \gamma' \in \Gamma^*$ sowie ein $c \in \Gamma \setminus \Sigma$ gibt, so daß für alle $\alpha, \gamma \in \{\square\}^*$ gilt: $\alpha z_{start} \beta \gamma \vdash_{TM}^* \alpha' z_{stop} \beta' c \gamma'$. ■

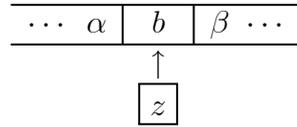
Die Arbeitsweise einer Turingmaschine kann man sich wie folgt vorstellen: Die Turingmaschine besitzt einen unendlich großen Speicher, das nach beiden Seiten unbegrenzte *Arbeitsband*, auf dem Worte aus Γ^* gespeichert sind. Das Arbeitsband ist in Speicherzellen unterteilt, wobei in jeder Speicherzelle ein Symbol aus Γ gespeichert ist. Da jedes Wort aus Γ^* endliche Länge besitzt, wird unterstellt, daß in den restlichen Speicherzellen das Sonderzeichen \square abgespeichert ist. Ein Arbeitsband, auf dem das Wort $a_1 a_2 \dots a_{j-1} a_j \in \Gamma^+$ gespeichert ist, illustrieren wir durch:

...	□	□	a_1	a_2	...	a_{j-1}	a_j	□	□	...
-----	---	---	-------	-------	-----	-----------	-------	---	---	-----

Weiter besitzt die Turingmaschine einen *endlichen Speicher*, der durch die endliche Menge der Zustände modelliert wird, sowie einen *Lesekopf*, der auf eine Speicherzelle des Arbeitsbands zeigt.

Die Turingmaschine arbeitet synchron, d.h. in jedem Arbeitsschritt werden der Zustand, das Arbeitsband und die Position des Lesekopfs verändert. Der "Arbeitszustand" der Turingmaschine kann dabei zu jedem Zeitakt durch eine Konfiguration $\alpha z b \beta \in \Gamma^* Z \Gamma^+$ mit $\alpha \beta \in \Gamma^*$ beschrieben werden, in der die Maschine im Zustand z ist, links vom Lesekopf das Wort α und rechts daran anschließend das Wort $b \beta$ auf dem Arbeitsband abgespeichert ist. Der Lesekopf zeigt also auf

das erste Zeichen b von $b\beta$. Eine Konfiguration ist damit ein ‘‘Schnappschuß’’ des ‘‘Arbeitszustands’’ der Maschine zu einem gegebenen Zeitpunkt.



Eine Konfiguration $\alpha z b \beta \in \Gamma^ Z \Gamma^+$*

Die Folgekonfiguration, die in einem Arbeitsschritt entsteht, wird durch die Übergangsfunktion δ bestimmt. Da δ einen endlichen Graphen besitzt – denn sowohl Z als auch Γ sind endlich – kann die Übergangsfunktion für $\Gamma = \{b_1, \dots, b_l\}$ und $Z = \{z_1, \dots, z_{k+1}\}$ mit Endzustand z_{k+1} durch eine endliche Tabelle mit Einträgen der Form

$Z \setminus \Gamma$	b_1	b_2	\dots	b_{l-1}	b_l
z_1	$\delta(z_1, b_1)$	$\delta(z_1, b_2)$	\dots	$\delta(z_1, b_{l-1})$	$\delta(z_1, b_l)$
z_2	$\delta(z_2, b_1)$	$\delta(z_2, b_2)$	\dots	$\delta(z_2, b_{l-1})$	$\delta(z_2, b_l)$
\dots	\dots	\dots	\dots	\dots	\dots
z_{k-1}	$\delta(z_{k-1}, b_1)$	$\delta(z_{k-1}, b_2)$	\dots	$\delta(z_{k-1}, b_{l-1})$	$\delta(z_{k-1}, b_l)$
z_k	$\delta(z_k, b_1)$	$\delta(z_k, b_2)$	\dots	$\delta(z_k, b_{l-1})$	$\delta(z_k, b_l)$

Der Graph der Übergangsfunktion δ als Tabelle

dargestellt werden. Linearisiert man diese Tabelle zu einer endlichen Liste

z_1, b_1	$\delta(z_1, b_1)$		\dots	\dots
z_1, b_2	$\delta(z_1, b_2)$		z_k, b_1	$\delta(z_k, b_1)$
\dots	\dots	\dots	z_k, b_2	$\delta(z_k, b_2)$
z_1, b_{l-1}	$\delta(z_1, b_{l-1})$		\dots	\dots
z_1, b_l	$\delta(z_1, b_l)$		z_k, b_{l-1}	$\delta(z_k, b_{l-1})$
\dots	\dots		z_k, b_l	$\delta(z_k, b_l)$

Das Programm einer Turingmaschine als Turingtafel

so erhält man die *Turingtafel*, d.h. das Programm der Turingmaschine. Damit ist ein *Turingprogramm* eine endliche Folge von Tripeln $(z, b, (z', b', D))$ mit $z, z' \in Z$, $b, b' \in \Gamma$, $D \in \{\leftarrow, \circlearrowleft, \rightarrow\}$ und $\delta(z, b) = (z', b', D)$.

In jedem Arbeitstakt liest die Turingmaschine in der Konfiguration $\alpha z b \beta$ – also im Zustand z mit Lesekopf positioniert auf die Speicherzelle mit Inhalt b – das Zeichen aus der Speicherzelle des Arbeitsbands, auf die der Lesekopf zeigt, und reagiert gemäß den Anweisungen des Programms. Mit $\delta(z, b) = (z', b', D)$ geht die Maschine in den neuen Zustand z' über, überschreibt das Zeichen, auf das der Lesekopf zeigt, mit b' und bewegt den Lesekopf um eine Position nach links, falls $D = \leftarrow$, oder nach rechts, falls $D = \rightarrow$. Für $D = \circlearrowleft$ bleibt die Position des Lesekopfs unverändert.¹ Damit gibt es drei Möglichkeiten, eine Folgekonfiguration zu erhalten, vgl. Definition 12.1:

$$\begin{array}{c} \cdots \alpha \mid a \mid b \mid \beta \cdots \\ \uparrow \\ \boxed{z} \end{array} \quad \vdash_{TM} \quad \begin{array}{c} \cdots \alpha \mid a \mid b' \mid \beta \cdots \\ \uparrow \\ \boxed{z'} \end{array} \quad (12.1)$$

Folgekonfiguration für $\delta(z, b) := (z', b', \leftarrow)$ mit Definition 12.1(1)

$$\begin{array}{c} \cdots \alpha \mid b \mid \beta \cdots \\ \uparrow \\ \boxed{z} \end{array} \quad \vdash_{TM} \quad \begin{array}{c} \cdots \alpha \mid b' \mid \beta \cdots \\ \uparrow \\ \boxed{z'} \end{array} \quad (12.2)$$

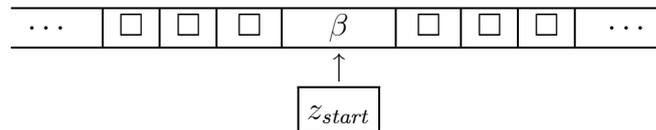
Folgekonfiguration für $\delta(z, b) = (z', b', \circlearrowleft)$ mit Definition 12.1(2)

$$\begin{array}{c} \cdots \alpha \mid b \mid c \mid \beta \cdots \\ \uparrow \\ \boxed{z} \end{array} \quad \vdash_{TM} \quad \begin{array}{c} \cdots \alpha \mid b' \mid c \mid \beta \cdots \\ \uparrow \\ \boxed{z'} \end{array} \quad (12.3)$$

Folgekonfiguration für $\delta(z, b) = (z', b', \rightarrow)$ mit Definition 12.1(3)

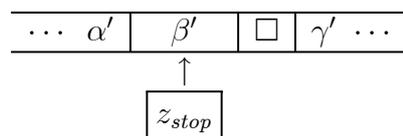
¹ Natürlich *muß* die Maschine weder den Zustand noch das Arbeitsband ändern: Mit $z' := z$ bzw. $b' := b$ bleibt die Maschine im gleichen Zustand bzw. läßt das Arbeitsband unverändert.

Um $\phi_{TM}(\beta)$ für ein $\beta \in \Sigma^*$ zu berechnen, wird die Turingmaschine in der Konfiguration



Startkonfiguration zur Berechnung von $\phi_{TM}(\beta)$

gestartet. Daran anschließend werden Schritt für Schritt Folgekonfigurationen berechnet. Falls dabei eine Endkonfiguration



Endkonfiguration bei Berechnung von $\phi_{TM}(\beta)$

mit $\beta' \in \Sigma^*$ erreicht wird, so hält die Turingmaschine mit β' als Ergebnis der Berechnung. Falls nie eine Endkonfiguration erreicht wird, so gilt $\phi_{TM}(\beta) = \perp$.

Bemerkung 12.2. Die Definition der Turingmaschine ist in der Literatur nicht einheitlich. Manche Autoren verwenden Maschinen mit mehreren Arbeitsbändern, mit einem oder mehreren einseitig begrenzten Arbeitsbändern, mit mehreren Endzuständen, mit partiellen Übergangsfunktionen, u.s.w. Allen diesen Varianten ist gemeinsam, daß sie äquivalent sind, d.h. daß sie die gleichen Funktionen berechnen können. Die verschiedenen Versionen sind allein durch den Zweck motiviert, der in einem bestimmten Anwendungskontext verfolgt wird. Des weiteren können Turingmaschinen auch indeterministisch definiert werden, ohne jedoch dadurch mehr Funktionen berechnen zu können. In der Berechenbarkeitstheorie spielt es daher keine Rolle, ob die deterministische oder die indeterministische Definition einer Turingmaschine verwendet wird. Bei Untersuchungen zur Komplexität von Problemen ist der Unterschied dagegen relevant.

12.2. Turing-berechenbare Funktionen

Um arithmetische Funktionen durch eine Turingmaschine zu berechnen, müssen natürliche Zahlen durch die Worte des Eingabealphabets dargestellt werden. Wir verwenden hier Bitworte, vgl. Abschnitt 4.4, d.h. wir stellen natürliche Zahlen n mittels der Funktion $dual : \mathbb{N} \rightarrow \{0, 1\}^+$ als Worte $dual(n) \in \{0, 1\}^+$ dar.²

Definition 12.3. (Turing-berechenbare Funktionen)

Eine Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$ ist Turing-berechenbar genau dann, wenn

$$\phi(n) = \begin{cases} \perp & , \text{ falls } \phi_{TM}(dual(n)) \notin \text{Bild}(dual) \\ dual^{-1}(\phi_{TM}(dual(n))) & , \text{ falls } \phi_{TM}(dual(n)) \in \text{Bild}(dual) \end{cases}$$

für eine Turingmaschine $TM = (Z, z_{start}, z_{stop}, \{0, 1, \square\}, \square, \{0, 1\}, \delta)$ und für alle $n \in \mathbb{N}$ gilt. ■

Beispiel 12.4. Wir zeigen, daß die Vorgängerfunktion $pred : \mathbb{N} \rightarrow \mathbb{N}$ mit $pred(0) := 0$ und $pred(n+1) := n$ Turing-berechenbar ist: Sei die Turingmaschine TM_{PRED} gegeben durch

$$TM_{PRED} := (Z, z_{start}, z_{stop}, \{0, 1, \square\}, \square, \{0, 1\}, \delta)$$

mit $Z := \{z_{start}, z_{one}, z_{done}, z_{back}, z_{dec}, z_{strip}, z_{stop}\}$ und δ definiert durch das Turingprogramm

(1)	$z_{start}, 0$	$z_{stop}, 0, \circlearrowleft$	(10)	$z_{back}, 0$	$z_{back}, 0, \leftarrow$
(2)	$z_{start}, 1$	$z_{one}, 1, \leftrightarrow$	(11)	$z_{back}, 1$	$z_{back}, 1, \leftarrow$
(3)	$z_{one}, 0$	$z_{one}, 0, \leftrightarrow$	(12)	z_{back}, \square	$z_{strip}, \square, \leftrightarrow$
(4)	$z_{one}, 1$	$z_{one}, 1, \leftrightarrow$	(13)	z_{start}, \square	$z_{start}, \square, \circlearrowleft$
(5)	z_{one}, \square	$z_{done}, \square, \leftarrow$	(14)	z_{dec}, \square	$z_{dec}, \square, \circlearrowleft$
(6)	$z_{done}, 1$	$z_{back}, 0, \leftarrow$	(15)	z_{done}, \square	$z_{done}, \square, \circlearrowleft$
(7)	$z_{done}, 0$	$z_{dec}, 1, \leftarrow$	(16)	$z_{strip}, 0$	$z_{stop}, \square, \leftrightarrow$
(8)	$z_{dec}, 0$	$z_{dec}, 1, \leftarrow$	(17)	$z_{strip}, 1$	$z_{stop}, 1, \circlearrowleft$
(9)	$z_{dec}, 1$	$z_{back}, 0, \leftarrow$	(18)	z_{strip}, \square	$z_{strip}, \square, \circlearrowleft$

Dann geht die Maschine bei Eingabe 0 mit (1) in den Endzustand über, Ergebnis der Berechnung ist 0. Bei Eingabe eines Wortes 1... geht die Maschine vom

² Da \mathbb{N} unendlich ist, können wir \mathbb{N} nicht als Eingabealphabet verwenden (vgl. Bemerkung 2.5). Die Verwendung von Bitworten ist nicht zwingend – jedes (endliche, nicht-leere) Alphabet ist geeignet.

Startzustand mit (2) in den Zustand z_{one} über und liest mit (3) und (4) das Eingabewort ein. Ist das letzte Zeichen des Eingabeworts eingelesen, so geht die Maschine mit (5) in den Zustand z_{done} über, der Lesekopf wird nach links bewegt und steht dann auf dem letzten Zeichen s des Eingabeworts.

Fall $s = 1$: Mit (6) geht die Maschine in den Zustand z_{back} über und ersetzt dabei das letzte Zeichen 1 durch 0 (um 1 vom Eingabewort zu subtrahieren).

Fall $s = 0$: Mit (7) geht die Maschine in den Zustand z_{dec} über und ersetzt dabei das letzte Zeichen 0 durch 1 (um 1 vom Eingabewort zu subtrahieren). Solange die Maschine im Zustand z_{dec} 0 liest, wird mit (8) 0 durch 1 ersetzt und der Lesekopf nach links bewegt (um den Übertrag, der bei Subtraktion von 1 entstand, im Eingabewort weiterzureichen). Wenn im Zustand z_{dec} 1 gelesen wird, so wird dieses Zeichen mit (9) durch 0 ersetzt (der Übertrag ist jetzt verarbeitet), und die Maschine geht in den Zustand z_{back} über. (Da die Maschine nur in den Zustand z_{done} gelangt, wenn 1 mindestens einmal im Eingabewort vorkommt, jedoch $s \neq 1$ für das letzte Zeichen s des Eingabeworts gilt, ist gewährleistet, daß die Maschine tatsächlich irgendwann 1 im Zustand z_{dec} liest.)

Im Zustand z_{back} wird mit (10) und (11) der Lesekopf solange nach links bewegt, bis \square gelesen wird. Jetzt ist der Anfang des beschriebenen Arbeitsbands wieder erreicht, die Maschine geht mit (12) in den Zustand z_{strip} über, ersetzt mit (16) ein führendes 0-Bit, bewegt den Lesekopf nach rechts und geht in den Endzustand z_{stop} über.³ Falls im Zustand z_{strip} jedoch 1 gelesen wird, so geht die Maschine statt dessen mit (17) in den Endzustand z_{stop} über. Damit steht der Lesekopf in jedem Fall auf dem ersten Zeichen des um 1 subtrahierten Eingabeworts.⁴

Somit gilt:

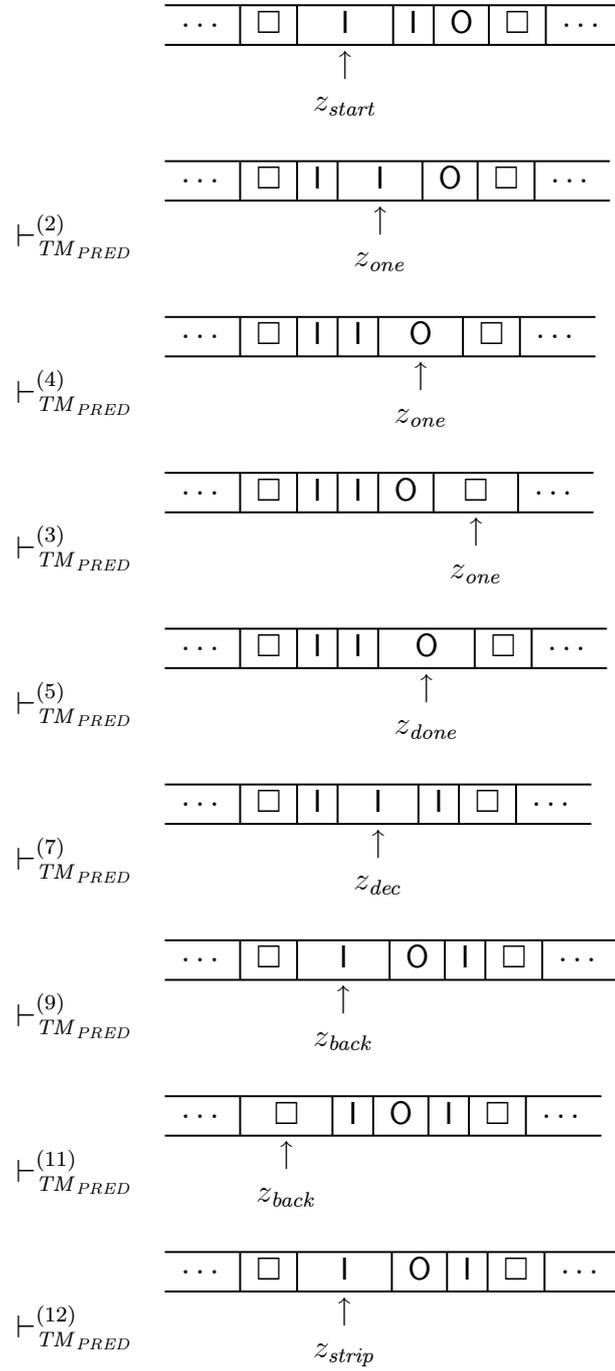
1. $\phi_{TM_{PRED}}(dual(n)) \in Bild(dual)$ sowie
2. $0 = dual^{-1}(\phi_{TM_{PRED}}(dual(0)))$ und
3. $n = dual^{-1}(\phi_{TM_{PRED}}(dual(n+1)))$,

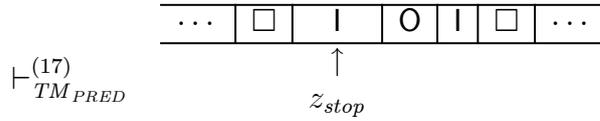
also $pred(n) = dual^{-1}(\phi_{TM}(dual(n)))$, d.h. $pred$ ist Turing-berechenbar

Beispielsweise erhält man $\phi_{TM_{PRED}}(110) = 101$ (also $\phi_{TM_{PRED}}(dual(6)) = dual(5)$), denn

³ Dies ist erforderlich, da bei Dekrementierung einer 2er Potenz, z.B. 100, zunächst ein Bitwort mit führendem 0-Bit – im Beispiel 011 – entsteht.

⁴ Regel (18) dient nur dazu, die Forderung nach einer *totalen* Übergangsfunktion zu erfüllen – diese Regel kann nie angewendet werden.





■

12.3. Berechnungsvollständigkeit von \mathcal{P}

Wir zeigen jetzt, daß jede Turing-berechenbare arithmetische Funktion auch \mathcal{P} -berechenbar ist. Zum Beweis übersetzen wir das Programm einer Turingmaschine TM in ein \mathcal{P} -Programm \mathbf{TM} und zeigen, daß \mathbf{TM} die gleiche Funktion berechnet wie TM .

Sei $TM = (Z, z_0, z_k, \{\square, \text{O}, | \}, \square, \{\text{O}, | \}, \delta)$ eine Turingmaschine mit $Z = \{z_0, \dots, z_k\}$. Aus TM konstruieren wir *uniform* das \mathcal{P} -Programm \mathbf{TM} wie in Abbildung 12.1. Dabei repräsentieren wir die Zeichen des Arbeitsalphabets mittels $\# : \{\square, \text{O}, | \} \rightarrow \{0, 1, 2\}$ durch natürliche Zahlen, und zwar mit $\#\square := 0$, $\#\text{O} := 1$ und $\#| := 2$. Die Zustände aus Z werden durch die natürlichen Zahlen aus $\{0, \dots, k\}$ dargestellt.

Eine Konfiguration $a_1 \dots a_m z_i b_1 \dots b_n$ von TM wird durch $\#a_1 \dots \#a_m i \#b_1 \dots \#b_n$ kodiert. Im Programm \mathbf{TM} wird eine solche Konfiguration durch die lokalen Variablen **alpha**, **head**, **beta** und **state** repräsentiert, wobei gilt:

- **alpha** = $\pi^2(\#a_m, \pi^2(\#a_{m-1}, \pi^2(\dots \pi^2(\#a_2, \pi^2(\#a_1, 0)) \dots))$,
- **head** = $\#b_1$,
- **beta** = $\pi^2(\#b_2, \pi^2(\#b_3, \pi^2(\dots \pi^2(\#b_{n-1}, \pi^2(\#b_n, 0)) \dots))$, und
- **state** = i .

Für ein Eingabewort $b_1 \dots b_n \in \{\text{O}, | \}^*$ wird \mathbf{TM} mit $\pi^2(\#b_1, \pi^2(\#b_2, \pi^2(\dots \pi^2(\#b_{n-1}, \pi^2(\#b_n, 0)) \dots))$ aufgerufen. Mit den ersten vier Zuweisungen im \mathcal{P} -Programm \mathbf{TM} werden die lokalen Variablen durch die Repräsentation $0 \dots 00\#b_1 \dots \#b_n 0 \dots 0$ der Startkonfiguration $\square \dots \square z_0 b_1 \dots b_n \square \dots \square$ initialisiert.

In der *while*-Schleife wird anschließend das durch δ gegebene Turingprogramm abgearbeitet. Dieses Turingprogramm wird durch geschachtelte *case*-Anweisungen repräsentiert. In jedem Fall einer inneren *case*-Anweisung befindet sich die Maschine im Zustand **state** $\neq k$ und liest das Zeichen **head**. Für **state** = i und **head** = $\#b_j$ ändert das Programm die lokalen Variablen **alpha**, **head**, **beta** und **state** gemäß dem Wert von $\delta(z_i, b_j)$. Dies geschieht durch die Programmfragmente in Abbildung 12.2.

Gilt vor einem Schleifendurchlauf **state** = k , so ist der Endzustand erreicht, und die *while*-Schleife bricht ab.

```

procedure TM(x) <=
begin var alpha, head, beta, state, y;
  alpha := 0;      head := PAIR12(x);
  beta := PAIR22(x); state := 0;
  while state ≠ k do
    case state of
      0 : ...
        :
      i : case head of
            :
            #bj: DELTA-zi-bj
            :
          end_case
        :
      k-1 : ...
      other : SKIP
    end_case
  end_while;
  y := STRIP(PAIR2(head, beta));
  return(y)
end

```

Abbildung 12.1: Ein \mathcal{P} -Programm zur Simulation einer Turingmaschine

<pre> state := m; head := PAIR₁²(alpha); alpha := PAIR₂²(alpha); beta := PAIR²(#b_n, beta); </pre>	<pre> state := m; head := PAIR₁²(beta); alpha := PAIR²(#b_n, alpha); beta := PAIR₂²(beta); </pre>	<pre> state := m; head := #b_n; </pre>
$\delta(z_i, b_j) := (z_m, b_h, \leftarrow)$	$\delta(z_i, b_j) := (z_m, b_h, \circlearrowleft)$	$\delta(z_i, b_j) := (z_m, b_h, \leftrightarrow)$

Abbildung 12.2: Programmfragmente des \mathcal{P} -Programms TM für $DELTA$ - z_i - b_j

Für

- **alpha** = $\pi^2(\#a'_{m'}, \pi^2(\#a'_{m'-1}, \pi^2(\dots \pi^2(\#a'_2, \pi^2(\#a'_1, 0)) \dots))$,
- **head** = $\#b'_1$, und
- **beta** = $\pi^2(\#b'_2, \pi^2(\#b'_3, \pi^2(\dots \pi^2(\#b'_{n'-1}, \pi^2(\#b'_{n'}, 0)) \dots))$

befindet sich die Turingmaschine TM dann in der Endkonfiguration $a'_1 \dots a'_{m'} z_k b'_1 \dots b'_{n'}$, repräsentiert durch $\#a'_1 \dots \#a'_{m'} k \#b'_1 \dots \#b'_{n'}$. Damit gilt $\phi_{TM}(b_1 \dots b_n) = b'_1 \dots b'_{n''} \in \{\mathbf{O}, \mathbf{I}\}^*$ für ein n'' mit $0 \leq n'' \leq n'$ und $b'_{n''+1} = \square$. Das \mathcal{P} -Programm **TM** berechnet mittels einer Prozedur **STRIP** die Repräsentation $\pi^2(\#b'_1, \pi^2(\#b'_2, \pi^2(\dots \pi^2(\#b'_{n''-1}, \pi^2(\#b'_{n''}, 0)) \dots))$ von $\phi_{TM}(b_1 \dots b_n)$ und hält mit diesem Ergebnis.

Für einen formalen Beweis der \mathcal{P} -Berechenbarkeit von Turing-berechenbaren Funktionen muß das \mathcal{P} -Programm **TM** verifiziert werden. Da dies manuell, d.h. ohne Rechnerunterstützung durch ein geeignetes Verifikationswerkzeug, zu aufwendig ist, skizzieren wir hier nur den Beweis.

Zunächst definieren wir eine Funktion $encode : \{\square, \mathbf{O}, \mathbf{I}\}^* \rightarrow \mathbb{N}$ durch $encode(\varepsilon) := 0$ und $encode(a_1 \dots a_m) := \pi^2(\#a_1, \pi^2(\#a_2, \pi^2(\dots \pi^2(\#a_{m-1}, \pi^2(\#a_m, 0)) \dots))$, mit der wir dann das Lemma

Lemma 12.5. *Wenn $\alpha z_i \beta \vdash_{TM} \alpha' z_h \beta'$, dann*

$$\begin{aligned} & \{\mathbf{alpha} = encode(\overleftarrow{\alpha}), \mathbf{state} = i, \mathbf{head} = \#f(\beta), \mathbf{beta} = encode(r(\beta))\} \\ & \quad \mathbf{case\ state\ of\ \dots\ end_case} \\ & \{\mathbf{alpha} = encode(\overleftarrow{\alpha'}), \mathbf{state} = h, \mathbf{head} = \#f(\beta'), \mathbf{beta} = encode(r(\beta'))\} \end{aligned}$$

formulieren können.⁵ Mit einem Beweis von Lemma 12.5 wird verifiziert, daß der Rumpf der *while*-Schleife der \mathcal{P} -Prozedur **TM** die Übergangsfunktion δ korrekt implementiert. Der Beweis wird (unter Verwendung von Definition 2.8) durch Fallunterscheidung nach den drei möglichen Fällen, eine Folgekonfiguration zu bilden, geführt, vgl. Definition 12.1(1,2,3) und Abbildung 12.2. Mit einem weiteren Lemma

⁵ $\overleftarrow{\alpha}$ entsteht durch Umkehrung der Reihenfolge der Symbole in α . $\{P\} \mathbf{STA} \{Q\}$ ist die übliche *Hoare*-Notation und bedeutet: Wenn die Aussage P (über Programmvariable) vor Ausführung der Programmanweisung **STA** gilt und die Ausführung von **STA** terminiert, so gilt die Aussage Q nach Ausführung von **STA**.

Lemma 12.6. Wenn $\alpha z_i \beta \vdash_{TM}^{(\ell)} \alpha' z_h \beta'$, dann

$$\begin{aligned} & \{\text{alpha} = \text{encode}(\overleftarrow{\alpha}), \text{state} = i, \text{head} = \#f(\beta), \text{beta} = \text{encode}(r(\beta))\} \\ & \quad (\text{case state of } \dots \text{end_case})^\ell \\ & \{\text{alpha} = \text{encode}(\overleftarrow{\alpha'}), \text{state} = h, \text{head} = \#f(\beta'), \text{beta} = \text{encode}(r(\beta'))\} \end{aligned}$$

wird verifiziert, daß alle Folgekonfiguration einer Konfiguration durch die Ausführung der *while*-Schleife in TM korrekt modelliert werden. Der Beweis wird – unter Verwendung von Lemma 12.5 – durch Induktion über die Länge ℓ der Konfigurationsfolge geführt. Mit Lemma 12.6 erhält man dann

Lemma 12.7. Wenn $\alpha z_i \beta \vdash_{TM}^* \alpha' z_k \beta'$, dann

$$\begin{aligned} & \{\text{alpha} = \text{encode}(\overleftarrow{\alpha}), \text{state} = i, \text{head} = \#f(\beta), \text{beta} = \text{encode}(r(\beta))\} \\ & \quad \text{while state} \neq k \text{ do case state of } \dots \text{end_case end_while} \\ & \{\text{alpha} = \text{encode}(\overleftarrow{\alpha'}), \text{state} = k, \text{head} = \#f(\beta'), \text{beta} = \text{encode}(r(\beta'))\} \end{aligned}$$

und damit

Lemma 12.8. $\llbracket \text{TM} \rrbracket(\text{encode}(\beta)) = \text{encode}(\phi_{TM}(\beta))$ für alle $\beta \in \{\mathbf{O}, \mathbf{1}\}^*$.

Jetzt kann gezeigt werden, daß die Programmiersprache \mathcal{P} berechnungsvollständig ist:

Satz 12.9. Wenn $\phi : \mathbb{N} \mapsto \mathbb{N}$ Turing-berechenbar ist, so ϕ auch \mathcal{P} -berechenbar.

Beweis. Sei eine Turingmaschine TM mit

$$\phi(n) = \begin{cases} \perp & , \text{ falls } \phi_{TM}(\text{dual}(n)) \notin \text{Bild}(\text{dual}) \\ \text{dual}^{-1}(\phi_{TM}(\text{dual}(n))) & , \text{ falls } \phi_{TM}(\text{dual}(n)) \in \text{Bild}(\text{dual}) \end{cases} \quad (12.4)$$

gegeben wie in Definition 12.3. Sei weiter $\text{decode} : \mathbb{N} \mapsto \{\square, \mathbf{O}, \mathbf{1}\}^*$ definiert durch $\text{decode}(i) = \perp$, falls $i \notin \text{Bild}(\text{encode})$, und andernfalls $\text{decode}(0) := \varepsilon$ und $\text{decode}(i+1) := \#^{-1}(\pi_1^2(i+1))\text{decode}(\pi_2^2(i+1))$. Man zeigt leicht $\text{decode}(\text{encode}(\alpha)) = \alpha$ für alle $\alpha \in \{\square, \mathbf{O}, \mathbf{1}\}^*$ durch strukturelle Induktion über α . Mit Lemma 12.8 gilt dann

$$\text{decode}(\llbracket \text{TM} \rrbracket(\text{encode}(\text{dual}(n)))) = \phi_{TM}(\text{dual}(n)) \quad (12.5)$$

für alle $n \in \mathbb{N}$ und folglich

$$\text{dual}^{-1}(\text{decode}(\llbracket \text{TM} \rrbracket(\text{encode}(\text{dual}(n)))))) = \text{dual}^{-1}(\phi_{TM}(\text{dual}(n))) \quad (12.6)$$

mit $dual^{-1}(\alpha) = \perp$, falls $\alpha \notin \text{Bild}(dual)$. Die Funktionen $dual$ und $encode$ sind algorithmisch, und offensichtlich ist (*) $encode \circ dual : \mathbb{N} \rightarrow \mathbb{N}$ \mathcal{P} -berechenbar, etwa durch eine \mathcal{P} -Prozedur **PACK**. Ebenso sind die Funktionen $dual^{-1}$ und $decode$ algorithmisch, und ebenso offensichtlich ist (**) $dual^{-1} \circ decode : \mathbb{N} \mapsto \mathbb{N}$ mit $dual^{-1}(decode(i)) = \perp$, falls $i \notin \text{Bild}(encode)$ oder $decode(i) \notin \text{Bild}(dual)$, \mathcal{P} -berechenbar, etwa durch eine \mathcal{P} -Prozedur **UNPACK**. Damit erhält man für die \mathcal{P} -Prozedur

```

procedure PHI-TM(y) <=
begin var z;
  z := UNPACK(TM(PACK(y)));
  return(z)
end

```

(12.7)

schließlich

$$\begin{aligned}
& \llbracket \text{PHI-TM} \rrbracket(n) \\
&= \llbracket \text{UNPACK} \rrbracket(\llbracket \text{TM} \rrbracket(\llbracket \text{PACK} \rrbracket(n))) && , \text{ mit (12.7)} \\
&= dual^{-1}(decode(\llbracket \text{TM} \rrbracket(encode(dual(n))))) && , \text{ mit (*) und (**)} \\
&= dual^{-1}(\phi_{TM}(dual(n))) && , \text{ mit (12.6)}
\end{aligned}$$

also $\llbracket \text{PHI-TM} \rrbracket(n) = \phi(n)$ mit (12.4). ■

Bemerkung 12.10. Die Behauptung von Satz 12.9 entspricht den Behauptungen der Sätze 11.17 und 11.35 für primitiv-rekursive bzw. μ -rekursive (anstatt Turing-berechenbare) Funktionen und wird wie diese durch Definition und Verifikation eines Compilers bewiesen (vgl. Abbildungen 12.1 und 12.2 sowie Anmerkungen 11.18 und 11.36).

Mit (der Kontraposition von) Satz 12.9 ist gezeigt, daß jede Funktion $\phi : \mathbb{N} \mapsto \mathbb{N}$, die nicht \mathcal{P} -berechenbar ist, auch nicht Turing-berechenbar ist. Somit ist ϕ dann – unter der Voraussetzung der Gültigkeit der Churchschen These – auch nicht intuitiv berechenbar.

Mit Satz 12.9 ist jedoch noch nicht bewiesen, daß “ \mathcal{P} -berechenbar” und “Turing-berechenbar” äquivalente Begriffe sind, dazu fehlt noch:

Satz 12.11. Wenn $\phi : \mathbb{N} \mapsto \mathbb{N}$ \mathcal{P} -berechenbar ist, so ϕ auch Turing-berechenbar.

Um diesen Satz direkt zu beweisen, muß ein Interpretierer für \mathcal{P} -Programme mittels einer Turingmaschine implementiert werden, ein beweistechnisch sehr aufwendiges Unterfangen. Mit Satz 11.39 kann man alternativ zeigen, daß jede μ -rekursive Funktion auch Turing-berechenbar ist. Einen Beweis dazu findet man etwa in [Hermes(1971)] oder in [Lewis and Papadimitriou(1981)].

Akzeptiert man die Gültigkeit der Churchschen These, so ist die Behauptung von Satz 12.11 jedoch kaum überraschend. Denn angenommen, diese Behauptung ist falsch, so existiert ein \mathcal{P} -Programm **PROG** mit $\llbracket \text{PROG} \rrbracket \neq \phi_{TM}$ für jede Turingmaschine TM , und folglich wäre die Churchsche These widerlegt.

13. BEGRIFFE UND SCHREIBWEISEN

- Für eine Menge N bezeichnet
 - 2^N die *Potenzmenge* von N ,
 - \overline{N} das *Komplement* von N ,
 - N^k die Menge aller endlichen Folgen von Elementen aus N der Länge k , und auch das kartesische Produkt $N_1 \times \dots \times N_k$ mit $N_i = N$ für alle $i \in \{1, \dots, k\}$,
 - N^* die Menge aller endlichen Folgen (beliebiger Länge) von Elementen aus N , und
 - N^+ die Menge $N^* \setminus \{\varepsilon\}$, d.h. N^* ohne die leere Folge ε .
- Mit $\phi : M \mapsto N$ bezeichnen wir eine Funktion von M nach N und nennen
 - ϕ *arithmetisch*, gdw. $N = \mathbb{N}$ und $M = \mathbb{N}^k$ für ein $k \in \mathbb{N}$,
 - ϕ *total* (in Kurzschreibweise $\phi : M \rightarrow N$), gdw. $\phi(m)$ für alle $m \in M$ definiert ist, d.h. $\phi(m) \in N$ für alle $m \in M$ gilt,
 - ϕ *partiell*, gdw. ϕ nicht total ist, d.h. $\phi(m)$ für mindestens ein $m \in M$ undefiniert ist, also $\phi(m) \notin N$ gilt (wir schreiben in einem solchen Fall auch $\phi(m) = \perp$),¹
 - $Def(\phi) \subseteq M$ mit $Def(\phi) := \{m \in M \mid \phi(m) \neq \perp\}$ den *Definitionsbereich* von ϕ ,²
 - $Bild(\phi) \subseteq N$ mit $Bild(\phi) := \{n \in N \mid \phi(m) = n \text{ für ein } m \in M\}$ den *Bildbereich* von ϕ , und

¹ Das Symbol \perp ist ein *Metazeichen* (d.h. eine Kurzschreibweise) für Undefiniertheit und nicht etwa das *Ergebnis* der Anwendung von ϕ auf m . Anders gesagt, im Unterschied zu einer natürlichen Zahl als Ergebnis von $\phi(m)$ kann man mit \perp nicht “rechnen”.

² “ $\phi(m) \neq \perp$ ” steht für “ $\exists n \in N. \phi(m) = n$ ” und “ $\phi(m) \neq n$ ” steht für “ $\phi(m) = \perp$ oder $\exists n' \in N \setminus \{n\}. \phi(m) = n'$ ”.

- (falls ϕ injektiv ist) $\phi^{-1} : N \mapsto M$ die Umkehrfunktion von ϕ , d.h. es gilt $\phi^{-1}(\phi(m)) = m$, falls $\phi(m) \neq \perp$, und $\phi(\phi^{-1}(n)) = n$, falls $\phi^{-1}(n) \neq \perp$.
- Für zwei Funktionen $\phi : N_1 \times \dots \times N_k \mapsto N$ und $\psi : N \mapsto N$ ist die *Funktionalkomposition* $\psi \circ \phi : N_1 \times \dots \times N_k \mapsto N$ von ψ und ϕ gegeben durch $\psi \circ \phi(n_1, \dots, n_k) = \psi(\phi(n_1, \dots, n_k))$, und wir definieren $\psi^{(k)} : N \mapsto N$ durch $\psi^{(0)}(n) = n$ und $\psi^{(i+1)}(n) = \psi^{(i)} \circ \psi(n) = \psi \circ \psi^{(i)}(n)$.
- Mit $\omega_{M \mapsto N}$ bezeichnen wir die *überall undefinierte* Funktion von M nach N , d.h. die Funktion, für die $\phi(m) = \perp$ für alle $m \in M$ gilt. Für $M = N = \mathbb{N}$ schreiben wir kurz ω anstatt $\omega_{\mathbb{N} \mapsto \mathbb{N}}$.
- Für $r \in \mathbb{R}$ ist $\lfloor r \rfloor$ (genannt *floor* r) die größte natürliche Zahl n mit $n \leq r$ und $\lceil r \rceil$ (genannt *ceiling* r) die kleinste natürliche Zahl n mit $r \leq n$. ■

LITERATURVERZEICHNIS

- [Hermes(1971)] Hermes, H., *Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit - Einführung in die Theorie der rekursiven Funktionen*, 2nd ed., Springer-Verlag, Berlin, Heidelberg, New York, 1971.
- [Jones(1997)] Jones, N. D., *Computability and Complexity: From a Programming Perspective*, The MIT Press, Cambridge, Massachusetts, London, England, 1997.
- [Kfoury et al.(1982)Kfoury, Moll, and Arbib] Kfoury, A. J., R. N. Moll, and M. A. Arbib, *A Programming Approach to Computability*, 2nd ed., Springer-Verlag, Berlin, Heidelberg, New York, 1982.
- [Lewis and Papadimitriou(1981)] Lewis, H., and C. Papadimitriou, *Elements of the Theory of Computation*, Prentice-Hall, 1981.
- [Mendelson(1964)] Mendelson, E., *Mathematical Logic*, D. Van Nostrand, 1964.
- [Rogers Jr.(1988)] Rogers Jr., H., *Theory of Recursive Functions and Effective Computability*, The MIT Press, Cambridge, Massachusetts, 1988.
- [Wagner(1994)] Wagner, K. W., *Theoretische Informatik — Grundlagen und Modelle*, Springer, Berlin, Heidelberg, New York, 1994.

INDEX

- Äquivalenzproblem, 88
- Abarbeitung von \mathcal{P} -Programmen, 24
 - beschränkt, 64
- abzählbar, 46, 77
- ack*, 118
- Ackermann*, *W.*, 118
- Ackermann*-Funktion, 118
- add*, 36
- algorithmisch, 32
- Algorithmus, 10
- APPLY, 53
- Arbeitsband, 130
- Arithmetik, 94
- aufsteigend rekursiv aufzählbar, 74
- Aufzählungs
 - funktion, 71
 - monoton, 74
 - verfahren, 71
 - monoton, 75
- Ausführung
 - funktion, 23
 - von Programmanweisungen, 23
- Auswertung
 - funktion, 23
 - von Programmausdrücken, 23
- b, 129
- berechenbar
 - intuitiv, 27
 - loop-, 108
 - \mathcal{P} -, 26
 - $\mathcal{P}_{\text{loop}}$ -, 108
 - Turing-, 134
- berechnungs
 - äquivalent, 28
 - vollständig, 11, 29
- Bildbereich, 143
- Bild*(ϕ), 143
- Block, 13
- C_n^k , 99
- call-by-name, 124
- call-by-value, 124
- case, 19
- charakteristische Funktion, 55
- Church*, *A.*, 28
- Churchsche These, 28
- COMPOSE, 27
- computable*, 26
- cont*, 22
- course-of-values recursion, 105
- CYCLE_k, 24
- decidable*, 55
- decode*, 140
- Definition
 - durch allgemeine Einsetzung, 100
 - durch Einsetzung, 97
 - durch gegenseitige Rekursion, 101, 102, 126
 - durch Minimierung, 120
 - durch primitive Rekursion, 97
 - durch strukturelle Rekursion, 100
- Definitionsbereich, 143
- Def*(ϕ), 143
- Diagonalisierung, 47, 82
- dovetailing*, 68

$dual^{-1}$, 43
eager evaluation, 124
Einsetzung, 97
 allgemeine, 100
encode, 139
Endkonfiguration, 130
entscheidbar, 55
 semi-, 59
Entscheidungsverfahren, 55
 semi-, 59
EQUAL, 15
EQV, 88
eval, 23
eval⁽ⁿ⁾, 116
EXP, 84
expressions_P, 23

f, 129
FAC, 109
Fibonacci-Funktion, 103
Folgekonfiguration, 130, 132
Funktion
 Ackermann-, 118
 algorithmisch, 32
 arithmetisch, 143
 berechnete, 25, 130
 charakteristische, 55
 Fibonacci-, 103
 intuitiv berechenbar, 27
 loop-berechenbar, 108
 μ -rekursiv, 28, 96, 122
 \mathcal{P} -berechenbar, 26
 \mathcal{P}_{loop} -berechenbar, 108
 partiell, 143
 primitiv-rekursiv, 96, 98
 semi-charakteristische, 59
 strikt, 124
 total, 143
 Turing-berechenbar, 134

 überall undefiniert, 144
 universelle, 52
 Werteverlauf, 104
Funktionalkomposition, 144

Gödel, K., 32, 94
Gödelisierung, 33
GE, 18
gegenseitige Rekursion, 101, 102, 126
GGT, 18, 20
Grundfunktion, 97

H, 54
half, 97
HALT, 50
halt, 51
Haltefunktion, 51
Halteproblem, 50, 54
 spezielles, 54
hd, 36

ID, 88
IDENT, 89
Identitätsproblem, 88
if, 99
if, 13
Induktion
 Noethersche, 105
 Peano, 105
initialer Speicher, 22
Interpretationskosten, 62
Interpreter, 52, 53
intuitiv berechenbar, 27

Kleene, S. C., 28, 96
Kleenescher Normalformsatz, 128
Kode, 43
 -tabelle, 42
Kodierung
 von Datentypen, 32

- von Listen, 32, 36, 38
 - von Programmen, 41
- Konfiguration, 130
- Konfigurationsrelation, 130
- KURIOS, 49
- l, 129
- λ -Kalkuel, 28
- Laufvariable, 108
- Laufzeitbeschränkung, 62
- lazy evaluation, 124
- Lesekopf, 130
- Listen, 36
- lokale Variable, 13
- loop, 108
 - Anweisung, 108
 - Programm, 96, 108
 - berechenbar, 108
- MINUS, 18
- monoton
 - Aufzählungsfunktion, 74
 - Aufzählungsverfahren, 75
- μ -Operator, 96, 120, 123, 128
- μ -rekursive Funktion, 28, 96, 122
- μ RF, 123, 128
- nth*, 104
- ntl*, 104
- \mathcal{P} , 12
 - Programm, 12
 - erweitert, 14, 19
 - Interpretierer, 52, 53
 - parametrisiert, 85
 - Prozedur, 12
 - parametrisiert, 85
 - berechenbar, 26
- $\mathcal{P}_{\text{loop}}$, 108
 - berechenbar, 108
- $\mathcal{P}_{\text{loop}}[k]$, 108
- P_i^k , 97
- Paar-Funktion, 34, 99
 - verallgemeinert, 38
- PACK, 141
- pairing function*, 34, 38
- PAIR², 35
- PAIR₁², 35
- PAIR₂², 36
- PAIR^k, 38
- PAIR_n^k, 38
- Parameter
 - aktuell, 17, 25
 - formal, 12
- Parametrisierung, 84
- Peter, R.*, 118
- PHI-TM, 141
- PLUS, 109
- PRED, 13
- pred, 99
- Presburger Arithmetik, 94
- PRF, 106
- primitiv-rekursive Funktion, 96, 98
- primitive Rekursion, 97
- Problem, 54
 - endlich, 56
 - entscheidbar, 55
 - kofinit, 58
 - komplementär, 58
 - reduzierbar, 83
 - semi-entscheidbar, 59
- Programm
 - anweisung, 13
 - Ausführung von, 23
 - ausdruck, 13
 - Auswertung von, 23
 - kodierungsfunktion, 43
 - variable, 13
 - loop-, 96, 108

Projektionsfunktion, 97
 Prozedur, 12
 -aufruf, 17
 -rumpf, 12
 parametrisiert, 85

 r, 129
 RAM, 7
 random access machine, 7
 recursive, 26, 55
 reduzierbar, 83
 Registermaschine, 7
 Rekursion
 gegenseitige, 101, 102, 126
 primitive, 97
 strukturelle, 100
 Werteverlauf, 105
 rekursiv aufzählbar, 71, 77
 aufsteigend, 74
 return, 13
 Rice, H.G., 92

 S, 54
 S, 97
 s-m-n-Theorem, 86
 s_P , 65
 Schrittfunktion
 universelle, 65
 von \mathcal{P} -Programmen, 64
 Schrittzählfunktion, 63
 Selbstanwendbarkeitsproblem, 54
 Selbstanwendungsfunktion, 48
 self, 48
 Semantik, 11
 axiomatisch, 21
 denotational, 21
 operational, 21, 25
 von loop-Programmen, 110
 von $\mathcal{P}_{\text{loop}}$ -Programmen, 110
 von \mathcal{P} -Programmen, 14, 25
 von Programmaufrufen, 25
 von Prozeduraufrufen, 25
 semi
 -Entscheidungsverfahren, 59
 -charakteristische Funktion, 59
 -entscheidbar, 59
 SKIP, 13
 Speicher, 21, 130
 -adresse, 22
 -bedarf, 22
 -modell, 22
 -zelle, 22, 130
 initial, 22
 statements_P, 23
 STEP, 66
 step, 63
 strikt, 124
 strukturelle Rekursion, 100
 SUCC, 13
 sum, 104
 sum-up, 97

 TIMES, 109
 tl, 36
 TM, 137
 TOT, 81
 Totalitätsproblem, 81
 Turing, A., 28
 Turing
 -berechenbar, 134
 -maschine, 6, 11, 28, 129, 133
 indeterministisch, 133
 -programm, 132
 -tafel, 132
 -vollständig, 11

 up, 52
 Übergangsfunktion, 129
 Umkehrfunktion, 144
 universelle

Funktion, 52	$\psi^{(k)}$, 144
Schrittfunktion, 65	$\psi \circ \phi$, 144
UNPACK, 141	Γ , 129
<i>value</i> , 23	$\gamma^?$, 33
Werteverlaufs	\wedge , 19
-funktion, 104	\vee , 19
-rekursion, 105	\neg , 19
while, 14	ε , 36, 143
\mathbb{Z} , 97	\sqsubseteq , 79
$\omega_{M \mapsto N}$, 144	$M(i)$, 22
ω , 144	M^{init} , 22
N^* , 143	$M_P^{(n_1, \dots, n_k)}$, 25
N^k , 143	$M[j \leftarrow n]$, 22
\overline{N} , 143	$M(\mathbf{z})$, 22
N^+ , 143	$M[\mathbf{z} \leftarrow n]$, 22
2^N , 143	\mathcal{N} , 107
α_M , 71	\mathbb{N} , 12
$\underline{\alpha}$, 139	$\natural P$, 43
$A_{\mathcal{P}}$, 42	$\natural \mathcal{P}$, 43
$[[P]]$, 25	$\mathcal{P}[k]$, 14
$[[\mathcal{P}]]$, 26	φ_i , 46
$[[P^{STEP}]]$, 64	ϕ_{TM} , 130
$[[PRF]]$, 108	π^2 , 34, 99
$[[EXPR]]$, 113	π_1^2 , 35, 99
$[[STA(\mathbf{y})]]$, 113	π_2^2 , 35, 99
\mathbb{O} , 42	π^{-2} , 35
\mathbb{I} , 42	π^k , 38, 41
\square , 129	π_h^k , 38, 41
\perp , 143	\Rightarrow , 107
χ_M , 54	\preceq_ρ , 83
$\tilde{\chi}_M$, 59	Σ , 129
\cong_M , 59	$\langle i, n \rangle$, 21
δ , 129	\mathcal{T} , 106
\mathcal{F}_{tot} , 47	\leftrightarrow , 129
$M \mapsto N$, 143	\hookrightarrow , 129
ϕ^{-1} , 144	\circlearrowleft , 129
$M \rightarrow N$, 143	\vdash_{TM} , 130
	$[\dots]$, 144
	$[\dots]$, 144

\vec{x} , 97

Z , 129

z_{start} , 129

z_{stop} , 129