Die Entscheidungskomplexität logischer Theorien: Eine Studie anhand der Presburger Arithmetik

Diplomarbeit

zur Erlangung des akademischen Grades
„Diplomingenieur“
in der Studienrichtung
Technische Mathematik
(Studienzweig: Informations- und Datenverarbeitung)

von

Clemens Grabmayer

eingereicht am

Institut für Mathematik
der technisch-naturwissenschaftlichen Fakultät
an der
Johannes Kepler Universität Linz

bei

Ao. Univ. Prof. Dr. phil. Alexander Leitsch

(Institut für Computersprachen,
Abteilung für Anwendungen der Formalen Logik,
Technische Universität Wien)

Linz, August 1997

Danksagung

Für das letztendliche Doch-Zustandekommen und das Gelingen (: ich meine damit hier nur das äußere Es-zustande-bringen-haben-Können) dieser Diplomarbeit muß ich mich und möchte ich mich sehr herzlich bedanken

(1) bei *Herrn Professor Alexander Leitsch*, der es mir gestattete und ermöglichte, diese vor langer Zeit begonnene[1] Diplomarbeit dennoch fertigzustellen; ich bin ihm deshalb zu großem Dank verpflichtet, den ich hiermit aussprechen möchte (*Danke recht schön, Herr Professor Leitsch!*);

(2) bei den *Mitarbeitern des ZID* (Zentraler-Informatik-Dienst) der Universität Linz, die mich während des Tippens und Erstellens des LaTeX-Typoskriptes in ihrem Visualisierungslabor freundlich geduldet haben (*Danke dafür!*);

(3) (und dabei zuallervorderst) bei *(Egregio Dottore) Johann Messner* vom ZID, Abteilung für Supercomputing, der mir das *eigentlich* und vieles mehr *überhaupt* erst möglich gemacht hat und dem ich dankbar bin, dafür: Daß ich auf seiner früheren HP-Desktop-Workstation "riscy" die Diplomarbeit im LaTeX schreiben durfte, daß ich das Visualisierungslabor des ZID benutzen durfte, daß ich zusätzliche LaTeX-Software (für die float-Objekte und das Diagramm-package XYPIC von Kristoffer H. Rose) verwenden konnte (Hans hat die für mich beschafft und installiert), daß er mir oft mit Rat und Tat, d.h. mit einem „schnellen hack", zur Seite gestanden, genauer, auch gesessen ist, und vielleicht am wichtigsten: Daß er mir ein Vorbild an Wißbegierde, Einfallsreichtum (in der Suche nach jeder machbaren, menschenfreundlichen Möglichkeit (–keine Widerrede, Hans!)) und beim Aufzeigen einer Möglichkeit, wie man einen *so-called* Dienstleistungs-Job ausüben und (mehr als) ausfüllen kann, dabei helfen und gleichzeitig dennoch vielleicht auch selber daran lernen kann. – Ich bin ihm dafür wirklich zu *sehr* großem Dank verpflichtet. (Für den (Süd-)Tiroler im Manne J.M. in einfacheren Worten, aber ganz explizit: ICH DANK' DIR WIRKLICH RECHT SCHÖN FÜR ALLES, HANS !!);

(4) bei meiner Mutter *Herta Grabmayer* für vieles, neben begleitender (formal-gestalterischer) Kritik an den LaTeX-Ausdrucken auch für so „Geringfügigkeiten" wie "much useful discussion" (schwyzerdütsch auch: „Schwätzen" genannt), „Vergessen" von Hundertern[2], „ausdauernde Lieferung von Essensrationen" und noch so

[1] Eine hier über weite Strecken versuchte Offenheit und Explizitheit darf ich an einer für mich unangenehmeren Stelle nicht so einfach aufgeben: Das Thema und die Aufgabenstellung der Diplomarbeit erhielt ich Ende Februar 1986.

[2] (ja, ich weiß: genauer, eigentlich: späteres, diesbezügliches mehrmaliges Vergessen des Haushaltsbuch-Führens über so ein „Ereignis")

ganz schön viel einiges mehr (Fahrt nach Hagenberg, Beratung und Organisation in Repro-Angelegenheiten, ... , eine erschöpfende Aufzählung kann hier nicht erfolgen); sie hat mir damit sehr geholfen und ist mir wirklich beigestanden (*Ich bedanke mich für das alles und mehr wirklich recht herzlich, Mutter!*);

(5) bei meinem Vater *Erwin Grabmayer* neben vielem anderem vor allem für eine große weiße Tischplatte, auf der sich die nötigen Berechnungen, Beweise und Einzelheiten gut ausbreiten konnten (wenn auch vielleicht: gar zu sehr, wie Prof. Leitsch hier möglicherweise einwenden würde) (*Danke recht schön, Vater!*).

Ich bin leider nicht in der Lage, jenem größeren Kreis von Lehrern an der Universität, von denen ich lernen durfte, und von Menschen, die ich oft auch nur über und durch ihre Bücher kennengelernt habe, einzeln, namentlich und ausführlich dafür zu danken; außer ein ganz kleinwenig vielleicht dadurch, indem ich allgemein sagen könnte und möchte, daß ich mich vom Wissen, genommen zu haben, in die Pflicht genommen fühle und weiß.

Ein solcher größerer Kreis von Menschen würde aber jedenfalls (ich schäme mich der Nennung dieser berühmten Namen) Franz Kafka, Simone Weil und Mascha Kaléko ganz bestimmt umfassen[3]. (Während des Korrekturlesens fiel mir auf, daß in der vorstehenden Liste der Name Ludvík Vaculíks doch sehr zu Unrecht abgeht, wenngleich er dieser in etwas anderer Hinsicht doch unzweifelhaft auch angehört).

Linz, den 25. August 1997

Clemens Grabmayer
Mannheimstrasse 6/3/21
A-4040 Linz
Österreich
e-mail: clemens.grabmayer@jk.uni-linz.ac.at

[3] Aus einer begründeten Scheu, damit etwa einen Anschein zu erwecken, mich dadurch—*needless to say:* völlig unverdient—in die Gesellschaft großer Namen begeben zu wollen, nenne ich hier keine Namen von Mathematikerinnen und Mathematikern. Natürlich gibt es auch auf diesem Gebiet, das ich studieren durfte und konnte, viele Menschen aus der Vergangenheit und der Gegenwart, deren Leistungen, Worte, Arbeiten und Bücher ich bewundere und die für mich sehr wichtig waren und sind.

Korrekturen der 1. Fassung

In der vorliegenden Version meiner Diplomarbeit sind gegenüber der abgegebenen Version vom 25. August 1997 nachträglich eine Reihe von weitgehend sehr kleineren Fehlern, auf die ich in der Zwischenzeit selbst aufmerksam geworden bin oder auf die mich jemand aufmerksam gemacht hat (recht schönen Dank für einen solchen Hinweis an Herrn Doz. Dr. Konrad Kiener), korrigiert worden und darin sind weiters eine geringe Anzahl von formalen Änderungen der LaTeX-Oberfläche erfolgt.

Die bislang letzte solche Korrektur erfolgte am 24. April 1998.

Clemens Grabmayer Linz, 24. April 1998

„Durissima est hodie conditio scribendi libros Mathematicos. Nisi enim servaveris genuinam subtilitatem, propositionum, instructionum, conclusionum; liber non erit Mathematicus; sin autem servaveris; lectio efficitur morosissima.“ [„Es ist heute sehr schwer, mathematische Bücher zu schreiben. Wenn man sich nicht um die Feinheiten bei Sätzen, Erläuterungen, Beweisen und Folgerungen kümmert, so wird es kein mathematisches Buch; wenn man es aber tut, so wird die Lektüre äußerst langweilig“][4]

Und an anderer Stelle:

„Et habet ipsa etiam prolixitas phrasium suam obscuritatem, non minorem quam concisa brevitas“ [„Und es hat selbst die ausführliche Darlegung ihre Dunkelheit, keine geringere als die lakonische Kürze“][4]

Johannes Kepler, Astronomia Nova, 1609[5]

[4] Beide Zitate und ihre jeweiligen Übersetzungen sind der Einleitung zu [Rem84] entnommen.

[5] [Ich fühle die Nötigkeit, die Leserin, den Leser um Entschuldigung dafür zu ersuchen, daß ich den Namen und einige Worte des großen Astronomen, Naturforschers, Mathematikers und Astrologen Johannes Kepler, Namensgeber und Namenspatron der Universität Linz, an der ich studiert habe, hier verwende und dadurch also in einen Zusammenhang mit mir und meiner Diplomarbeit bringe; in einen Zusammenhang, der aber weder inhaltlich besteht, noch sonst auf eine von mir irgendwie intendierte *objektive* Weise hergestellt werden sollte oder auch nur hergestellt werden wollte. *Subjektiv* besteht eine persönliche Beziehung von mir zu Kepler einfach in einem großen Respekt, den ich gerade auch den praktischen mathematischen Arbeiten Keplers (deren eine sehr wichtige, die *Nova Stereometria Doliorum Vinariorum* (Neue Stereometrie der Weinfässer), er 1615 in Linz geschrieben hat) entgegenbringe. Ich habe die (für mich greifbare) Prägnanz der beiden obigen Zitate sehr gern, vor allem aber die des zweiten, weil es eine von mir selber beim Niederschreiben von Beweisen sehr oft gefühlte Schwierigkeit viel besser und treffender ausdrückt, als ich das selbst könnte. C.G.]

Inhaltsverzeichnis

1 Entscheidbarkeit, Unentscheidbarkeit, Schwerentscheidbarkeit **7**

1.1 Einleitung 7
1.2 Entscheidbarkeit formal-logischer Systeme 13
1.3 Grundbegriffe der Komplexitätstheorie, Beziehung zu logischen Entscheidungsproblemen 18
1.4 IOTM-Turingmaschinen 32
1.5 Obere und untere Schranken für die Entscheidungskomplexität 42
1.6 Praktische Bedeutung von oberen und unteren Schranken für Entscheidungskomplexität einer entscheidbaren Theorie 49

2 Presburger Arithmetik **57**

2.1 Die Theorie TAZ 58
2.2 Die Presburger Arithmetik ganzer Zahlen $PreAZ$ 90
2.3 Die Presburger Arithmetik natürlicher Zahlen $PreAN$ 97
2.4 Der Zusammenhang zwischen $PreAZ$ und $PreAN$ 105
2.5 Die Presburger Arithmetik natürlicher Zahlen im Kontext der Peano-Arithmetik und anderer zahlentheoretischer Theorien 1. Ordnung . . 113
2.6 Entscheidungskomplexität der Theorien der Presburger Arithmetik 117

3 Aufarbeitung der Arbeit [FiR74] **139**

3.1 Zusammenstellung der Hauptresultate aus [FiR74] 142
3.2 Diskussion der genauen Gestalt der in [FiR74] erzielten Komplexitätsresultate 149
3.3 Für die Beweise verwendete Klasse von Turingmaschinen, benötigte Bezeichnungen 154
3.4 Allgemeiner Teil der Komplexitätsbeweise 171

3.5 Beweis von Satz 3.1.3 (Spezieller Beweisteil in [FiR74] bei der Erzielung von $RA \notin NTime(2^{cn})$ für ein $c \in \mathbb{R}$, $c > 0$) 222
3.6 Beweis von Satz 3.1.1 (Spezieller Beweisteil in [FiR74] bei der Erzielung von $Th(\langle \mathbb{N}_0; 0, 1, + \rangle) \notin NTime(2^{2^{cn}})$ für ein $c \in \mathbb{R}$, $c > 0$) 234
3.7 Anwendung der Methoden und einer Idee aus [FiR74] zur Erzielung von $TAZ \notin NTime(2^{2^{cn}})$ für ein $c \in \mathbb{R}$, $c > 0$ 243

A Anhang: Die Arbeit [FiR74] 262

Literaturverzeichnis 290

Verzeichnis von Formelgrammatiken

1.3.1 Die LR(1)-Grammatik $G_{T^{((M))}}$ 25
2.6.1 Die LR(1)-Formelgrammatik G_{PreA} für Theorien der Presburger Arithmetik 118

Kapitel 1

Entscheidbarkeit, Unentscheidbarkeit, Schwerentscheidbarkeit

1.1 Einleitung

Im Zuge der Entwicklung zu immer größerer formaler Strenge traten in der Mathematik und in der Logik (wobei vorher bereits v.a. auf dem Gebiet der Analysis bedeutende Erfolge dabei erzielt worden waren) zuende des 19. Jahrhunderts formal-axiomatische Untersuchungen hervor (G. Frege: „Begriffsschrift, eine der arithmetischen nachgebildete Formelsprache des reinen Denkens“, 1879; D. Hilbert: „Grundlagen der Geometrie“, 1899).

Dabei rückte das Bemühen in den Vordergrund, einer betrachteten mathematischen oder logischen Theorie klare und einfach einzusehende Grundaussagen (Axiome) an die Spitze zu stellen, aus denen dann mit Hilfe von vorher ebenfalls genau festzulegenden logischen Schlußregeln der gesamte Inhalt der Theorie (also jede beliebige einzelne, gültige Aussage der Theorie) nun auf strikt formalem Weg abgeleitet werden kann. Hierbei war nicht die verwendete axiomatische Methode das völlig Neue (diese wurde schon viel früher mit großem Erfolg z.B. von R. Descartes benutzt und hatte schon im Altertum durch Euklids „Elemente“ zu großer formaler Eleganz von Arbeiten beigetragen) als vielmehr der dabei erreichte Grad an formaler Präzision.

Eine darüber hinausgehende, größere Bedeutung erhielten diese formal-axiomatischen Bestrebungen um die Zeit der Wende zum 20. Jhdt. im Verlauf der durch die Entdeckung von Antinomien und Paradoxien in der Cantorschen Mengenlehre[1] ausgelösten „Grundla-

[1] u.a.: (A) Paradoxie von Burali-Forti, 1897 (Cantor, 1895); (B) Paradoxie von Cantor, 1899 (Menge aller Mengen); (C) Russel's paradox, 1902-3 (Menge aller Mengen, die sich nicht selbst als Menge enthalten); (D) Paradoxie von Richard, 1905 (semantische Paradoxie, z.B.: „kleinste Zahl, die in nicht weniger als

genkrise“ der Mathematik. Denn es hatte sich bei diesen Antinomien um widersprüchliche Aussagen gehandelt, die im Formalismus der Cantorschen Mengenlehre ausgedrückt werden konnten und gleichzeitig aus den gemeinhin akzeptierten Grundtatsachen der Theorie mittels ebenfalls gebräuchlicher logischer Schlußweisen hergeleitet worden waren. Dadurch war einerseits deutlich geworden, daß eine formale Grundlegung der gesamten Mathematik nicht so ohne weiteres im Rahmen der Cantorschen Mengenlehre erfolgen konnte, wie bis dahin vielfach gehofft worden war. (Im günstigsten Fall mußten also genauere Einschränkungen und nähere Spezifikationen an die beteiligten Grundannahmen, ausdrückbaren Aussagen und Schlußweisen gefunden werden, um auf eingeschränkte Weise erneut widerspruchsfrei Mengenlehre betreiben zu können). Andererseits waren aber auch die gebräuchlichen Formen der Theoriebildung in der Mathematik und Logik ins Zwielicht geraten und bedurften einer weitergehenden Untersuchung, Behandlung und Klärung.

Bei den Anstrengungen, diese Situation zu überwinden, traten in der Grundlagenwissenschaft nach und nach im wesentlichen drei Strömungen in Erscheinung: Eine *logizistische*, eine *formalistische* und eine *intuitionistische* Richtung.

Im *Logizismus* vereinte sich dabei die Auffassung, Mathematik und Logik wären im wesentlichen dasselbe, alle mathematischen Objekte und Strukturen könnten durch geeignete logische Konstrukte verstanden, erfaßt und ersetzt werden und mathematische Beweise wären im Grunde nichts anderes als logische Herleitungen (Deduktionen). Als Begründer dieser erst in späterer Zeit so bezeichneten Richtung wird oft G. Frege angesehen, da Frege in seiner „Begriffsschrift“ als erster ein wirklich formal-präzises System deduktiver Logik vorstellte. Dieses System basierte wesentlich auf einer den Schreibweisen der Mathematik entlehnten, aber von Frege ausgebauten und verfeinerten exakten Formelsprache, bei deren Verwendung es erstmals möglich war, logische Schlußweisen zwischen einzelnen Formeln (also logische Deduktionen) als genau beschreibbare symbolische Operationen auf und zwischen den beteiligten Formeln (also exakt spezifizierten Zeichenketten-Objekten der Formelsprache) anzusehen und dann zu definieren. – Die später erfolgte Formalisierung von Logik-Kalkülen 1. Ordnung (etwa der Prädikatenlogik 1. Ordnung durch D. Hilbert und einigen seiner Mitarbeiter) verdankt sich auch wesentlich den formal-logischen Grundlagen aus Freges „Begriffsschrift“[2] (und außerdem den Arbeiten des italienischen Logikers G. Peano).

Weitergeführt wurden die Gedanken von G. Frege und von G. Peano über die Forma-

dreizehn Worten bezeichnet werden kann“).

[2]Später wurde jedoch zugleich mit einer Paradoxie in der Mengenlehre, der Russelschen Paradoxie, 1903, auch ein Widerspruch im System Freges von B. Russell entdeckt. Frege selbst wandte sich gegen Ende seines Lebens vom Logizismus völlig ab, “on the grounds that logic alone could not provide objects for which properties such as equality or set-membership can be appraised” [„weil die Logik alleine keine Objekte bereitstellen kann, in Beziehung auf die über die Gültigkeit von Eigenschaften wie Gleichheit und Mengenzugehörigkeit beurteilbare Aussagen gemacht werden können“, C.G.] [GG81]; [GG81] fügt an: “The rejection of a life-long position is a rare achievement in mankind. It reveals a special kind of greatness.”

lisierung mathematischer Theorien in einem rein logischen Symbolismus später v.a. durch die Arbeit von A.N. Whitehead und B. Russell. Diese stellten mit ihrem berühmten Werk „Principia Mathematica“, 1910–13, den Anspruch, nunmehr eine zuverlässige Basis für die gesamte Mathematik mit rein logischen Mitteln geschaffen zu haben. Der Formalismus der Principia Mathematica erwies sich aber als sehr umständlich zu handhaben, sodaß sich die meisten Mathematiker trotz der Umfassendheit und Exaktheit dieses Konzeptes nicht dazu bewegen ließen, ihn als die Grundlage ihres Arbeitens zu übernehmen. Diese zögernde Haltung den Principia Mathematica gegenüber stand aber im Gegensatz zur weitgehend allgemeinen Reaktion auf einen anderen formal-axiomatischen Ausweg nach dem (vorläufigen) Zusammenbruch der Cantorschen Mengenlehre, nämlich der Axiomatisierung der Mengenlehre durch E. Zermelo und A. Fraenkel.

Als ein weiterer wichtiger Vertreter logizistischer Standpunkte nach Russell und Whitehead ist F.P. Ramsey zu nennen. Über die Entwicklung des Logizismus als einer die Grundlagen der Mathematik begründenden Position urteilt [GG81] folgendermaßen:

> „During the inter-war period logicism fell quite substantially in reputation; although it influenced logicians both as an early example of a comprehensive mathematico-logical system and as a source of techniques, the philosophical position itself won few followers.“

Die *formalistische* Richtung bei der Untersuchung der Grundlagen der Mathematik geht ganz wesentlich auf das Wirken und die Arbeit von D. Hilbert zurück. Hilbert versuchte eine Grundlegung für die gesamte Mathematik durch eine präzisierte und verschärfte Weise in der Benutzung der formal-axiomatischen Methode zu erreichen: Nach der Formalisierung einer mathematischen Theorie in einem exakt aufzubauenden formalen System sollte vom Anschauungs- und Vorstellungsmaterial der Theorie nur noch das zurückbehalten werden, was davon in die Axiome eingegangen ist, die sich aber wie das formale System selbst für den Rahmen weiterer Untersuchungen ausschließlich noch auf abstrakte Bereiche von unspezifizierten Individuen beziehen sollten. Eine Fundierung einer mathematischen Theorie sollte dann durch den Nachweis der Widerspruchsfreiheit des zugehörigen formalen Systems geschehen können (die formalistische Position geht hierbei davon aus, daß die Widerspruchsfreiheit einer formalisierten mathematischen Theorie auch die (mathematische) Existenz der dieser Theorie bzw. der Formalisierung der Theorie zugrundeliegenden mathematischen Begriffe impliziert[3]).

[3] „Wenn man einem Begriffe Merkmale erteilt, die einander widersprechen, so sage ich: der Begriff existiert mathematisch nicht. So existiert z.B. mathematisch nicht eine reelle Zahl, deren Quadrat gleich -1 ist. Gelingt es jedoch zu beweisen, daß die dem Begriffe erteilten Merkmale bei Anwendung einer endlichen Anzahl von logischen Schlüssen niemals zu einem Widerspruche führen können, so sage ich, daß damit die mathematische Existenz des Begriffes, z.B. einer Zahl oder einer Funktion, die gewisse Forderungen erfüllt, bewiesen worden ist.“ (Hilbert in [Hi1900]). – Es folgen die Sätze: „In dem vorliegenden Falle, wo es sich um die Axiome der reellen Zahlen in der Arithmetik handelt, ist der Nachweis der Widerspruchslosigkeit

Durch eine solche Vorgehensweise sollten die Mathematiker (wenn die Widerspruchsfreiheit von umfassenden mathematischen Theorien bewiesen werden könnte) der Verpflichtung enthoben werden, ihre Begriffe in jedem Einzelfall tiefgehend begründen und ihre Methoden immer ausführlich rechtfertigen zu müssen. Hilbert hatte dabei als Ziel die Fundierung und Begründung der gesamten Mathematik vor Augen; das Problem, diese Absicht wirklich umfassend durchzuführen, erschien ihm als ein zwar schwieriges, aber in endgültiger Weise zu einem positiven Abschluß zu bringendes Unternehmen. Auf dem Weg zur Erreichung dieses Zieles stand die Suche nach sog. „finiten" Widerspruchsfreiheitsbeweisen im Mittelpunkt, d.h. Beweisen, die „mit konkreten Objekten in konstruktiver Weise umgehen"[4] bzw. „die sich an die Grenzen der grundsätzlichen Vorstellbarkeit von Objekten sowie der grundsätzlichen Ausführbarkeit von Prozessen [halten] und sich somit im Rahmen konkreter Betrachtung [vollziehen]" ([HiBe68], S.32). Hilbert und Bernays geben (z.B. in [HiBe68], S.16 f.) Gründe dafür an, warum nur solche „finite" Widerspruchsfreiheitsbeweise eine unbezweifelbare Gewähr dafür bieten, formale mathematische Theorien sicher zu begründen. Die Forderung und Suche nach solchen Beweisen beruhte auch wesentlich auf einem von Hilbert und Ackermann 1922 für ein arithmetisches Teilsystem (im wesentlichen einer Axiomatisierung der Arithmetik natürlicher Zahlen mittels der Peanoschen Axiome ohne Einschluß des Induktionsaxioms) angegebenen finiten Widerspruchsfreiheitsbeweis[5]. Die Verallgemeinerung eines solchen Beweises für stärkere Systeme erwies sich jedoch als sehr schwierig und letztlich (in der von Hilbert und seinen Mitarbeitern beabsichtigten Weise) sogar als undurchführbar zufolge der berühmten Unableitbarkeitssätze von K. Gödel, 1931. Dadurch (und durch Überlegungen von u.a. A. Tarski) wurde deutlich, daß das formalistische Programm in der geplanten Umfassendheit (die u.a. den Nachweis der Übereinstimmung der Begriffe „Wahrheit"[6] und „Beweisbarkeit"[7] in allen wichtigen

---

der Axiome zugleich der Beweis für die mathematische Existenz des Inbegriffs der reellen Zahlen oder des Kontinuums. In der Tat, wenn der Nachweis für die Widerspruchslosigkeit der Axiome völlig gelungen sein wird, so verlieren die Bedenken, welche bisweilen gegen die Existenz des Inbegriffs der reellen Zahlen gemacht worden sind, jede Berechtigung." (Ein solcher allgemeiner und endgültig über alle Zweifel erhabener Widerspruchsfreiheitsbeweis konnte aber in diesem Fall (v.a. auch wegen Limitationen über die Art eines solchen Beweises zufolge der Gödelschen Sätze, 1931) bis heute wohl nicht erbracht werden, obwohl an der Eigenschaft der Widerspruchsfreiheit der klassischen Kontinuumsanalysis—aus praktischen Gründen (daß Widersprüche nicht aufgetreten sind)—kaum gezweifelt wird).

[4] "Proofs which deal with concrete objects in a constructive manner are said to be *finitary*." ([Shoe67],p.3)

[5] An diesem Widerspruchsfreiheitsbeweis kann umgekehrt auch anschaulich nachverfolgt werden, welcher gedankliche Weg zur Formulierung der Forderung nach der „Finitheit" von Beweisen und Objekten geführt hat bzw. wie dieser Begriff von Hilbert und seinen Schülern anfangs verstanden wurde.

[6] (als Eigenschaft einer formalen Aussage einer formalisierten Theorie, wenn diese Aussage in Beziehung zu einem—der Theoriebildung eig. zugrundeliegenden—Anschauungsbereich inhaltlich aufgefaßt, d.h. darin „interpretiert" wird.)

[7] (als formal-präzis definierte Eigenschaft einer formalen Aussage innerhalb des Deduktionssystems einer formalisierten Theorie)

formalisierten mathematischen Theorien gefordert hatte) nicht durchgeführt werden konnte.

Die dritte Richtung, der *Intuitionismus*, ist wesentlich mit dem Namen L. Brouwer verbunden, in geringerem Ausmaß auch mit den Arbeiten von H. Weyl, A. Heyting und den von Brouwer als Prae-Intuitionisten bezeichneten Mathematikern L. Kronecker, H. Poincaré, E. Borel und H. Lebesque. – Für Brouwer bestand gesicherte mathematische Erkenntnis einzig in solchen Sätzen, die Aussagen über konstruktiv-angebbare Operationen mit der Anschauung klar zugänglichen Objekten machen. Dadurch sind Aussagen, in denen auf als Ganzheit vorliegende unendliche Mengen wie etwa das „abgeschlossene Kontinuum“ $\mathbb{R}$ oder auch nur die Menge $\mathbb{N}$ Bezug genommen wird, ausgeschlossen und müssen—um *intuitionistisch* dennoch Sinn zu erhalten—vollständig zu solchen Aussagen umgebildet werden, in denen nur mehr anschauliche Konstruktionen bzw. formale Ausdrücke, die solche Konstruktionen formalisieren, eine Rolle spielen (falls für eine jeweils einzeln zu betrachtende Aussage eine solche Umbildung überhaupt möglich ist und diese nicht aus prinzipiellen „intuitionistischen“ Gründen als unzulässige Aussage bzw. Fragestellung betrachtet und ausgeschlossen werden muß). Dabei sind vom Standpunkt Brouwers aus v.a. alle solchen Sätze unakzeptabel, die nur unter Verwendung des Prinzips des *tertium non datur* bewiesen werden konnten, also der Annahme, für eine vorliegende mathematische Aussage könne nur eine von zwei Alternativen zutreffen, entweder die Gültigkeit oder die Ungültigkeit der Aussage. Brouwer widersetzte sich auch energisch der Formalisierung mathematischer Theorien durch formale Systeme, in denen die Gültigkeit von Sätzen losgelöst von intuitiv klar faßbaren, beschreibbaren und konkreten Objekten als die rein formal definierte Eigenschaft der Ableitbarkeit aus beliebig wählbaren Grundaussagen betrachtet wird. Aus diesem Grund war für ihn auch der Nachweis der Widerspruchsfreiheit für eine formalisierte mathematische Theorie kein Grund, dieses formale System als einen Formalismus gesicherten mathematischen Wissens anzuerkennen oder zu übernehmen. Er äußerte sich darüber einmal (Jahrestagung 1923, Marburg) drastisch so[8]:

> „Eine durch keinen Widerspruch zu hemmende unrichtige Theorie ist darum nicht weniger unrichtig, so wie eine durch kein reprimierendes Gericht zu hemmende verbrecherische Politik darum nicht weniger verbrecherisch ist.“

Dagegen beschreibt [vD94] die grundlegende Einstellung Brouwers zur Mathematik in folgenden Worten:

> „Ganz kurz gefaßt kann man sagen, daß für Brouwer die Mathematik eine inhaltliche geistige Tätigkeit war, ein geistiges Schöpfen und Konstruieren, unabhängig von Logik, Sprache und Erfahrung, und sich frei entwickelnd.“

Über diese Fragen der Betrachtung und Begründung der Grundlagen der Mathematik kam es in den 1920er Jahren zu einem teilweise sehr erbittert und persönlich geführten

[8] (zitiert nach [vD94])

Streit zwischen Hilbert und Brouwer, dessen die Fundamente der Mathematik betreffender Teil erst durch das weitere Fortschreiten der Grundlagenwissenschaft „entschieden“ (oder in neuem Licht gesehen) worden ist. Dabei erwiesen sich die übertriebenen Ansprüche und Hoffnungen des formalistischen Ansatzes als unhaltbar, viele der davon inspirierten Formalismen jedoch als wichtig und beinahe als unverzichtbar. Und auch die Formalismen weitgehend ablehnende Position Brouwers konnte sich nicht durchsetzen, aber seine Herangehensweise an viele Fragen beeinflußte die Forschung an formalen Systemen dennoch nachhaltig und maßgeblich.

An dieser Stelle sollte einschränkend zur früher hergestellten ursächlichen Beziehung zwischen der durch das Auftreten der Paradoxien in der Cantorschen Mengenlehre verursachten „Grundlagenkrise“ und verschiedenen Arbeiten, die einen Ausweg daraus ermöglichten oder nahelegten, gesagt werden, daß ein solcher Zusammenhang ursprünglich oft nicht bestand. [vD94] weist darauf hin, daß die „plötzliche Blüte der Grundlagenwissenschaft“ nur teilweise auf das Auftauchen der Paradoxien zurückzuführen ist und daß die Antinomien als Ausgangspunkt nicht überschätzt werden dürfen. Wohl sei die Arbeit von A.N. Whitehead und B. Russell mehr oder weniger direkt darauf zurückzuführen, aber schon im Falle von Hilberts „Die Grundlagen der Geometrie“ sei ein Zusammenhang mit Bemühungen zur Grundlegung der Mathematik nicht direkt gegeben, denn die Arbeit sei eher als Sammlung formaler Forschungen in der Geometrie entstanden. Und auch Zermelos Axiomatisierung der Mengenlehre sei eher durch die allgemeine Kritik an seinem Beweis des Wohlordnungsatzes als durch die Paradoxien veranlaßt gewesen. Sodaß insgesamt das Vermeiden der Paradoxien für Brouwer, Hilbert und Zermelo ein zwar „angenehmes Nebenprodukt“, aber nicht das Hauptziel ihrer Arbeit gewesen sei.

1.2 Entscheidbarkeit formal-logischer Systeme

Es war jedoch wesentlich den Bestrebungen der formalistischen Richtung zu verdanken (in geringerem Ausmaß auch Ergebnissen der logizistischen Richtung), daß durch die axiomatische Erfassung von mathematischen Theorien in mit Deduktionskalkülen überbauten formalen Systemen verschiedene wichtige, die Grundlagen betreffende Fragen erstmals präzise gestellt und formal exakt behandelt werden konnten. Das waren v.a. Fragen nach der *Widerspruchsfreiheit*, der „Konsistenz" einer formal-axiomatischen Theorie, nach der *deduktiven Abgeschlossenheit* (Vollständigkeit in weiter zu präzisierendem Sinn) und nach der *Entscheidbarkeit* (oder der Lösung des Entscheidungsproblems) formal-logischer Systeme.

Die Frage nach der Widerspruchsfreiheit einer formal-axiomatischen Theorie—die, wie schon erwähnt, von zentraler Bedeutung für das formalistische Programm war—konnte auf das entsprechende formal-logische System bezogen exakt als die Frage gestellt werden, ob in ihm keine einander logisch entgegengesetzten Formeln (formalen Aussagen) gleichzeitig herleitbar sind. Die Frage, ob alle in einer Theorie behandelbaren mathematischen Probleme lösbar sind (ob also in dieser Theorie das *principium tertii exclusi* mit Recht angewendet werden darf) konnte auf die exakt formalisierte Theorie bezogen präzis als die Frage nach deren deduktiver Abgeschlossenheit behandelt werden. Und zwar in dem Sinn, daß gefragt wird, ob darin jeder formalisierbare Satz entweder selbst oder in Gestalt seiner Negation als Theorem der Theorie abgeleitet werden kann. Das Problem der Entscheidbarkeit trat in Beziehung zu einer formalisierten Theorie als die Frage in Erscheinung, ob es eine Methode bzw. ein Verfahren gibt, mit der bzw. mit dem zu jeder vorgelegten Formel der Theorie effektiv[9] und d.h. durch die mechanische Ausführung von im Verfahren genau festgelegten Schritten nach endlich vielen solcher Schritte festgestellt und also entschieden werden kann, ob die Formel ein Theorem der Theorie ist oder ob das nicht der Fall ist.

Entscheidungsprobleme stellten sich in der Folge im Zusammenhang mit den gerade entwickelten logischen Kalkülen und ebenso auch für Axiomatisierungen bekannter mathematischer Theorien wie etwa der durch die Peanoschen Axiome axiomatisierten Theorie natürlicher Zahlen.

Etwas konkreter, aber dennoch mit unspezifizierten Begriffen und also weitgehend un-

[9] Der hier und im folgenden öfter verwendete (und verbreitete) Wortgebrauch, von einem „effektiven Verfahren" in leichtem Gegensatz zu einem (allg.) „Verfahren" zu handeln, ist so zu verstehen, daß ein „effektives Verfahren" immer als ein solches verstanden wird, das für beliebige zulässige Ausgangsobjekte nach der Ausführung endlich vieler Schritte zu einem Resultat gelangt. („Zulässigkeit" von Ausgangsobjekten ist hier als eine äußere Spezifikation jener Dinge, mit denen das Verfahren überhaupt umgehen kann, aufzufassen). – Diese bezüglich allen zulässigen Ausgangsobjekten bestehende Terminationseigenschaft wird für ein „Verfahren" (:ohne den Zusatz „effektiv") nicht von vorne herein vorausgesetzt und konstituiert einen Unterschied in der Verwendung dieser beiden Begriffe, der im wesentlichen dem Unterschied zwischen (total-)rekursiven und partiell-rekursiven Funktionen analog bzw. nachgebildet ist bzw. diesem zugrundeliegt.

formal wird die Entscheidbarkeit formaler Systeme in Logikbüchern zuerst oft so definiert: Ein *Entscheidungsverfahren* für ein formales System F ist eine Methode, mit der zu einer gegebenen Formel von F in einer endlichen Anzahl von Schritten entschieden werden kann, ob die Formel ein Theorem ist oder nicht. Das *Entscheidungsproblem* für F besteht in der Aufgabe, entweder ein Entscheidungsverfahren für F zu finden, oder zu beweisen, daß ein solches nicht existieren kann ([Shoe67]). Auf die etwas allgemeinere Situation einer Menge E und einer Teilmenge $A \subseteq E$ übertragen kann analog definiert werden: Ein *Entscheidungsverfahren* für A in E ist eine Methode, mit der zu einem gegebenen Element $a \in E$ in einer endlichen Anzahl von Schritten entschieden werden kann, ob $a \in A$ oder $a \notin A$ gilt. Analog zu oben besteht das *Entscheidungsproblem* für A in E in der Aufgabe, entweder ein Entscheidungsverfahren für A in E zu finden oder die Nicht-Existenz eines solchen zu beweisen.

In einer solchen Definition ist aber immer noch weitgehend unpräzisiert geblieben, was unter einem „Verfahren“ und einer „Methode“ genau verstanden werden soll. Eine solche Ausdrucksweise entsprach der Situation der Logik vor der Entwicklung exakter Verfahrensbegriffe in den 1930er Jahren, als besonders von den Hauptvertretern der formalistischen Richtung noch gehofft worden war, solche Entscheidungsprobleme in den neu entstandenen formalen Systemen und Logik-Kalkülen nach und nach auf positive Weise durch die Konstruktion von Entscheidungsverfahren lösen zu können. In dieser Richtung hatte es ja auch erste Teilerfolge gegeben, wie zum Beispiel den Nachweis der Entscheidbarkeit des Klassenkalküls durch L. Löwenheim (1915), also der Feststellbarkeit der Allgemeingültigkeit prädikatenlogischer Ausdrücke, die nur einstellige Prädikatenvariable enthalten. Ein weiteres berühmtes Resultat war der Vollständigkeits- und Entscheidbarkeitsbeweis von M. Presburger (1929) für eine Axiomatisierung der Theorie der Addition ganzer (und im weiteren auch natürlicher) Zahlen (vgl. Kap. 2).

Allerdings verstärkten sich gegen Ende der 1920er Jahre bei einigen Mathematikern der Eindruck und die Vermutung, daß speziell das (als Fragestellung) zentrale Entscheidungsproblem für den logischen Kalkül der Prädikatenlogik 1. Ordnung (in [HA28]: der „engere Prädikatenkalkül“), das von Hilbert und Ackermann in [HA28] noch—optimistisch klingend—so formuliert wurde:

> „Das Entscheidungsproblem ist gelöst, wenn man ein Verfahren kennt, das bei einem vorgelegten logischen Ausdruck durch endlich viele Operationen die Entscheidung über die Allgemeingültigkeit bzw. Erfüllbarkeit erlaubt.“,

nicht auf positive Weise gelöst werden kann (Indizien für einen begründeten Skeptizismus in dieser Richtung hatte J. v. Neumann in [vN27][10] geliefert).

Der Nachweis der *Unentscheidbarkeit* eines formalen Systems erforderte aber, da er die Nicht-Existenz eines (effektiven) Entscheidungsverfahrens für dieses System zeigen sollte,

[10] (zitiert nach [Ga94])

eine genaue Definition des Begriffs „effektives Verfahren“. Denn nur auf der Basis einer solchen Definition kann überhaupt argumentiert werden, daß die Methoden der dadurch präzisierten Verfahrensklasse (möglicherweise, wenn so ein Beweis gelingt) nicht ausreichen, um ein bestimmtes Problem in völliger Allgemeinheit zu lösen. Andererseits sollte diese Klasse aber auch umfassend genug sein, um wirklich alle durch ein „effektives Verfahren“ möglichen Berechnungen (bzw. Konstruktions- oder Entscheidungsprozesse) auch mit Verfahren dieser präzisierten Verfahrensklasse durchführen zu können. Dies natürlich deshalb, weil andernfalls vielleicht eine größere Verfahrensklasse definiert werden könnte, auf die sich bezüglich der zuerst betrachteten Klasse erzielten Unlösbarkeitsaussagen möglicherweise nicht übertragen lassen, sodaß solchen Aussagen dann nur noch eine sehr eingeschränkte Bedeutung zukäme.

Überlegungen zur Klärung dieser Situation führten auf den vorerst etwas vagen Begriff der „berechenbaren Funktion“, der aber von verschiedenen Ausgangspunkten aus von A. Church, S.C. Kleene, A. Turing, E. Post und K. Gödel auf verschiedene Weise präzisiert worden ist, mit dem Erfolg, daß sich alle diese Definitionen der berechenbaren Funktion als äquivalent erwiesen. Überlegungen solcher Art führten A. Church auf die heute als „Churche These“ (1936) berühmte und wohlbegründete Annahme, daß alle überhaupt durch ein Verfahren, einen Algorithmus berechenbaren bzw. angebbaren Funktionen auch schon berechenbar im Sinne einer der oben erwähnten (und als untereinander äquivalent erkannten) Präzisierungen dieses Begriffes sind. Besonders überzeugend in dieser Richtung wirkte auf viele Mathematiker dabei die von A. Turing vorgestellte Definition von „Berechenbarkeit“, die auf einer genauen Analyse des mechanischen Vorgangs einer Rechnung (durch einen Menschen) beruhte und Turing zu einem einfachen abstrakten Maschinenmodell, der (bald so genannten:) Turingmaschine, die solche Rechnungen ebenfalls bewerkstelligen kann, hinführten.

Nur durch das Akzeptieren der Churchen These wurde das erste Unentscheidbarkeitsresultat möglich und wurde von A. Church 1936 und—unabhängig—von A. Turing 1937 ausgesprochen: Die Unentscheidbarkeit der Prädikatenlogik 1. Ordnung, also die Aussage, daß das „Entscheidungsproblem“ im Hilbertschen Sinne (d.h. das für den „engeren Prädikatenkalkül“) unlösbar ist bzw. das Entscheidungsproblem für die Prädikatenlogik 1. Ordnung nicht in positiver Weise (durch das Finden eines Entscheidungsverfahrens) lösbar ist.

Zuvor hatte allerdings K. Gödel 1931 schon die formale Unvollständigkeit und also die deduktive Unabgeschlossenheit von Theorien 1. Ordnung, die konkret angebbare Axiomatisierungen von Gebieten sind, die die elementare Zahlentheorie (Peano-Arithmetik) enthalten, bewiesen (Gödel bezog sich dabei auf den Formalismus der Principia Mathematica) und damit auch den Grundstein zu den Unentscheidbarkeitsresultaten von Church und Turing gelegt. Einen noch größeren Rückschlag für das formalistische Programm als dieser Unvollständigkeitssatz stellte jedoch ein zweiter Unableitbarkeitssatz von K. Gödel dar: Dieser besagt, daß die Widerspruchsfreiheit eines hinreichend umfassenden (und das

heißt erneut: eines die elementare Zahlenarithmetik beinhaltenden) und auf konkret angebbare Weise axiomatisierbaren formal-logischen Systems nicht mit den Mitteln dieses Systems und d.h. in diesem System selber bewiesen werden kann. Damit konnte die Hoffnung der Hauptexponenten der formalistischen Richtung auf eine durch einen „finiten" Widerspruchsfreiheitsbeweises sich gründende Sicherstellung aller mathematischer Methoden nicht mehr ganz ohne weiters aufrecht erhalten werden (ein „finiter" Widerspruchsfreiheitsbeweis muß wegen des Ergebnisses von Gödel also auch auf Evidenzen basieren, die von den in der elementaren Arithmetik formalisierbaren Begriffen verschieden sind; trotzdem wurden solche Widerspruchsfreiheitsbeweise für vergleichbare Systeme z.B. von G. Gentzen, 1936, und auch von K. Gödel, 1958, gefunden bzw. angegeben). Das formalistische Programm Hilberts kann dadurch nicht als gescheitert angesehen werden, obwohl ihm der angestrebte endgültige Abschluß bei der Errichtung unantastbarer Fundamente der Mathematik (hauptsächlich infolge des zweiten Gödelschen Unableitbarkeitssatzes) sicherlich versagt blieb.

Unter Verwendung eines der für die „Berechenbarkeit" gefundenen exakten Begriffe kann man nun auch die früher gegebene inhaltliche Definition der Entscheidbarkeit, die auf „effektive Verfahren" Bezug nahm, durch eine formal exakte ersetzen. In Logikbüchern wird dafür weitgehend der Begriff der „rekursiven" Funktion verwendet, dessen Präzisierung v.a. auf K. Gödel zurückgeht; ausschlaggebend für die verbreitete Verwendung dieses Verfahrensbegriffes ist sicherlich, daß darin ausschließlich zahlentheoretische Funktionen und Operationen zwischen solchen (und also gebräuchliche mathematische Objekte) auftreten und daß dieser Begriff weiters noch eng mit den Gödelschen Unableitbarkeitssätzen in Verbindung steht, die in der Logik seit ihrer Entdeckung eine zentrale Stellung einnehmen. Für eine Definition des Begriffs der (total-)„rekursiven" Funktion sei hier (z.B.) auf [Shoe67], Chapt. 6, verwiesen.

Zum Zweck der neuen Definition der Entscheidbarkeit einer formal-logischen Theorie ist es nötig, diese Theorie in naiv-mengentheoretischen Begriffen auch als Tripel $T = (\Sigma_T, Fo_T, Thm_T)$ mit Zeichenalphabet Σ_T, Formelmenge $Fo_T \subseteq \Sigma_T^*$ und Theoremmenge $Thm_T \subseteq Fo_T$ auffassen zu können (es handelt sich dabei um die Verwendung von Schreibweisen aus der Mengenlehre zum Zweck der einfachen formalen und symbolischen Durchführung dieser Definition und nicht um eine Einbettung der Theorie T in ein Axiomensystem der Mengenlehre).

Eine **Gödelnummerierung** für T sei eine injektive Funktion $\langle\cdot\rangle\colon \Sigma_T^* \to \mathbb{N}_0$, die auch eine (ein-)eindeutige Verbindung zwischen den Formeln von T und einer Menge von natürlichen Zahlen, den sog. *Gödelzahlen* herstellt und die auf augenscheinliche Weise effektiv sein soll: D.h. zu jeder Zeichenkette $w \in \Sigma_T^*$ soll $\langle w\rangle$ auf effektive Weise berechnet werden können und von einem vorgelegten $n \in \mathbb{N}_0$ soll ebenso effektiv festgestellt werden können, ob ein $w \in \Sigma_T^*$ mit $\langle w\rangle = n$ existiert, und—wenn das der Fall ist—soll zu n dieses w auch

tatsächlich konstruiert werden können[11]. $n \in \mathbb{N}$ heißt dann **Gödelzahl** für eine Formel $\mathbf{A} \in Fo_T$ bzgl. einer Gödelnummerierung $\langle\cdot\rangle$, wenn $n = \langle\mathbf{A}\rangle$.

Definition 1.2.1. Entscheidbarkeit einer formalisierten Theorie.
Sei $T = (\Sigma_T, Fo_T, Thm_T)$ eine (in dieser Gestalt aufgefaßte, formal-logische) Theorie T. Sei Thm_T^* das folgende einstellige Prädikat über den natürlichen Zahlen $\mathbb{N}_0$:

$$\begin{aligned} Thm_T^*(x) \longleftrightarrow\ & x \text{ ist Gödelzahl eines Theorems von } T \\ \big(\longleftrightarrow\ & \text{es git eine Formel } \mathbf{A} \in Fo_T \text{ mit } \vdash_T \mathbf{A} \text{ und } x = \langle\mathbf{A}\rangle\ \big) \end{aligned}$$

Dann ist T **entscheidbar** *genau dann, wenn (das Prädikat) Thm_T^* rekursiv[12] [13] ist.*

Man sieht leicht ein, daß Definition 1.2.1 nicht von der speziellen Wahl einer Gödelnummerierung abhängig ist und daß die Definition weiters auch mit der früheren inhaltlichen vereinbar ist, weil eine Gödelnummerierung $\langle\cdot\rangle$ für eine Theorie T eine Hilfskonstruktion ist, um einerseits aus einem effektiven Entscheidungsverfahren für T eine effektiv berechenbare Funktion $c_{Thm_T^*}$, die Thm_T^* berechnet (i.e. charakteristische Funktion von Thm_T ist), zu gewinnen und andererseits aus einem effektiv berechenbaren Prädikat[13] Thm_T^* ein Entscheidungsverfahren für T aufzubauen.

Längere Zeit hindurch hielt man die Arbeit an solchen Theorien, die als entscheidbar erkannt worden waren, für abgeschlossen, da für diese Theorien durch den Nachweis der Entscheidbarkeit nunmehr ja effektive Verfahren zur Verfügung standen, mit denen—zumindestens theoretisch—alle darin auftretenden Fragen auf jetzt genau festgelegte, mechanischen Regeln folgende Rechnung zuverlässig richtig und eindeutig entschieden werden konnten. Andererseits bestand an diesen Theorien (wie etwa der Presburger Arithmetik (als Additionsarithmetik [z.B.] der natürlichen Zahlen)) auch kein unmittelbares mathematisches Interesse, da diese nur sehr kleine Teilgebiete der Mathematik umfaßten, in denen kaum offende Fragen von (damaligem) Interesse bestanden (diese Situation unterschied sich aber völlig von jener in den als unentscheidbar erkannten Theorien).

[11] Solche Gödelnummerierungen existieren immer, vgl. z.B. [Shoe67], Chapt. 6, oder [BoJe74], Chapt. 15, p. 171. Sie wurden zuerst von K. Gödel in [Gö31] eingeführt.

[12] „Rekursiv“ ist hier im Sinne von (total-)rekursiv (d.h. partiell-rekursiv und total) wie z.B. in [Shoe67], Chapt. 6, p. 109, zu verstehen, wo total-rekursive Funktionen direkt und ohne ausgesprochene Bezugnahme auf die Klasse der partiell-rekursiven Funktionen definiert werden.

[13] Weiters ist ein ganzzahliges Prädikat $P(n)$ als rekursiv definiert, wenn die charakteristische Funktion $c_P(n)$ (die für n mit $P(n)$ gleich 1, sonst gleich 0 gesetzt wird) rekursiv ist.

1.3 Grundbegriffe der Komplexitätstheorie, Beziehung zu logischen Entscheidungsproblemen

Obwohl Überlegungen, unter unentscheidbaren Systemen verschiedene Schwierigkeitsgrade ihrer Unentscheidbarkeit zu finden, schon länger bestanden, fand die Beschäftigung mit Schwierigkeitsstufen der Entscheidbarkeit von entscheidbaren Systemen—die sog. *Komplexitätstheorie*—ihren Ausgangspunkt erst in den 1960er Jahren angeregt durch die stürmische Entwicklung des Computers. Damit wurde es nämlich möglich und interessant, Probleme aus entscheidbaren logischen Systemen auch auf Rechenmaschinen zu übertragen und mit deren Hilfe in ganz neuem und größerem Maßstab zu lösen. Im Zusammenhang damit stellte sich aber (wie auch für viele andere Verfahren und Algorithmen, die schon länger bekannt waren) die Frage nach dem Rechenaufwand, den ein Verfahren bei seiner Ausführung auf einem Computer an vorhandenen oder benötigten Betriebsressourcen erfordert. Unter solchen Gesichtspunkten mußten ältere Verfahren oft völlig neu überdacht und konstruiert werden, um überhaupt auf einem Rechner eingesetzt werden zu können. Hierdurch taten sich viele neue theoretische Fragen von oftmals direkter praktischer Relevanz auf, Fragen nach der Komplexität eines Problems, also Fragen, ob und wie verschiedene real auftretende Probleme entsprechend dem ihrer Lösung inhärenten Schwierigkeitsgrad klassifiziert werden können.

Für allgemeine komplexitätstheoretische Untersuchungen ist es nötig, von einem umfassenden, jedoch zugleich auch präzisen Begriff einer „Problemstellung“ bzw. eines „Problems auszugehen, um die große Fülle und Vielfalt von in der Informatik auftretenden Problemen in einem gemeinsamen Formalismus studieren zu können. [Jo90] tut das, indem er Probleme als eine „totale“ Relation von Zeichenketten ansieht:

Definition 1.3.1. Probleme.
Ein **Problem** *ist eine Menge X von geordneten Paaren (I, A) von Zeichenketten $I, A \in \{0,1\}^*$, wobei I jeweils eine* **Instanz** *und A eine* **Antwort** *des Problems genannt wird und weiters jedes $I \in \{0,1\}^*$ als die erste Komponente von mindestens einem Paar in X auftritt (diese letzte Bedingung bezeichnet [Jo90] als die Eigenschaft der „Totalität“ der Relation X auf Zeichenketten über dem Alphabet $\{0,1\}$).*

Für die Begriffe „Wort“, „Verkettung von Symbolen“ und „Sprachen“ (über einem gegebenen Symbolalphabet) werden in der theoretischen Informatik zumeist Festsetzungen wie etwa die folgenden verwendet:

Definition 1.3.2. Wörter, Symbolverkettung, Sprachen.
Σ sei ein endliches Symbolalphabet.

Ein **Wort** *w über Σ ist eine endliche Kette von Symbolen aus Σ. Die* **Symbolverkettung** *$S_1 \circ S_2$ zweier Symbole $S_1, S_2 \in \Sigma$ sei das Wort bestehend aus erstem Zeichen S_1 und zweitem Zeichen S_2. Die* **Verkettung** *$w_1 \circ w_2$ zweier Worte w_1 und w_2 über Σ*

sei das Wort, das aus den Zeichen von w_1 gefolgt nach rechts von den Zeichen von w_2 besteht. $\boldsymbol{\epsilon}$ *sei das* **Leerwort**, *i.e. jenes Wort, das aus* 0 *Zeichen aus* Σ *besteht. Die* **Länge** $|w|$ *eines Wortes* w *ist die Anzahl der darin vorkommenden Symbole, d.h. genauer, es gilt die folgende rekursive Festsetzung: Für* $w = \epsilon$ *gilt* $|w| = 0$*; für* $w = S$ *mit* $S \in \Sigma$ *ist* $|w| = 1$*; für* $w = w_1 \circ w_2$*, wobei* w_1 *und* w_2 *Wörter über* Σ *sind, gilt* $|w| = |w_1| + |w_2|$*. Für jedes Wort* $w = S_{i_0} \circ S_{i_1} \circ \ldots \circ S_{i_{n-1}}$ *über* Σ *mit* $|w| = n$ *und* $S_{i_j} \in \Sigma$ $(0 \leq j < n)$ *sei* $w(j) := S_{i_j}$ $(0 \leq j < n)$*;* $w^{\boldsymbol{R}} := S_{i_{n-1}} \circ S_{i_{n-2}} \circ \ldots \circ S_{i_1} \circ S_{i_0}$ *sei das* **von rückwärts nach vorne gelesene Wort** w*.* Σ^+ *sei die Menge aller Wörter* w *der Länge* ≥ 1 *über* Σ*;* $\Sigma^* := \Sigma^+ \cup \{\epsilon\}$*. Eine* **Sprache** L *über Alphabet* Σ *ist eine Menge* $L \subseteq \Sigma^*$*, das* **Komplement** $\mathrm{co}-L$ **einer Sprache** L *über* Σ *sei* $\boldsymbol{co-L} := \Sigma^* \setminus L$*.*

Zur Beschreibung von Grundmengen von Wörtern werden weiters manchmal Schreibweisen verwendet, die aus der Beschreibung von regulären Ausdrücken bzw. von Mengen von regulären Ausdrücken entlehnt sind: so bezeichnet für ein Alphabet Σ und zwei Symbole $a, \$ \in \Sigma$ z.B. die Menge $\Sigma^*(\Sigma \setminus \{a\}) \cup \{a, \$a, \$\$a\}$ $(\subseteq \Sigma^*)$, die Menge aller Wörter aus Σ^*, die entweder gleich a oder $\$a$ oder $\$\$a$ sind, oder ein letztes Symbol aus Σ ungleich a besitzen.

(Es sei an dieser Stelle erneut darauf hingewiesen, daß die Verwendung von mengentheoretischen Symbolismen in dieser und in den folgenden Definitionen nur der Verwendung von mengentheoretischen Schreibweisen entspricht, um—wie in weiten Teilen der Mathematik üblich—komplizierte Sachverhalte in einer einheitlichen Sprache auszudrücken, und daß diese Schreibweisen bei der Bezeichnung informatischer Objekte hier theoretisch immer umgangen werden könnten (aber um den Preis großen Aufwands und des Verlustes der gebräuchlichen mathematischen Ausdrucksweise)).

Als Beispiele für Definition 1.3.1 seien hier zwei Probleme angegeben, das Problem der „Isomorphie von Graphen“ und das logische Problem der “aussagenlogischen Erfüllbarkeit“:

ISOMORPHIE VON GRAPHEN

Instanz: Zwei ungerichtete Graphen $G = (V, E)$ und $G = (V', E')$, wobei V und V' endliche Mengen von Ecken und E und E' endliche Mengen von Kanten (d.s. ungeordnete Paare von Ecken) von V und V' sind.

Antwort: "`Ja`", wenn es eine bijektive Funktion $f : V \to V'$ gibt, so, daß für alle $u, v \in V$ gilt: $\{u, v\} \in E \Leftrightarrow \{f(u), f(v)\} \in E'$;
"`Nein`", andernfalls.

AUSSAGENLOGISCHE ERFÜLLBARKEIT

Instanz: Eine Liste von Literalen $U = (u_1, \overline{u_1}, u_2, \overline{u_2}, \ldots, u_n, \overline{u_n})$, eine Folge von Klausen $C = (c_1, \ldots, c_n)$, wobei jede Klause eine Teilmenge von U ist.

Antwort: "`Ja`", wenn es eine Wahrheitsbelegung für die Variablen $u_1, \ldots, u_n$ gibt, die alle Klausen in C erfüllt, d.h. eine Teilmenge $U \subseteq U'$ so, daß $|U' \cap \{u_i, \overline{u_i}\}| = 1$ $(1 \leq i \leq n)$ und $|U' \cap c_i| \geq 1$ $(1 \leq i \leq m)$;
"`Nein`", andernfalls.

Um diese Problemstellungen als Probleme im Sinne von Definition 1.3.1 aufzufassen, ist es nötig, jeweils von einer einfachen Weise, Graphen bzw. Literale und Klausen durch binäre Zeichenketten darzustellen, auszugehen und weiters zwei verschiedene Binärwörter $a_{\mathtt{J}}, a_{\mathtt{N}} \in \{0,1\}^*$ für die Antworten "`Ja`" und "`Nein`" festzulegen und die Problemstellungen davon ausgehend folgendermaßen zu definieren:

$$\{(x, a_{\mathtt{J}} / \ x \text{ besteht aus 2 Darstellungen des gleichen Graphen G}\} \cup$$
$$\cup \{(x, a_{\mathtt{N}} / \ x \text{ besteht nicht aus 2 Darstellungen des gleichen Graphen G}\}$$

für ISOMORPHIE VON GRAPHEN (ähnlich kann für AUSSAGENLOGISCHE ERFÜLLBARKEIT vorgegangen werden).

Eine solche Problemspezifikation ist natürlich noch unvollständig, da eine genau Festlegung der Darstellung von Graphen bzw. Listen und Literalen und Listen von Klausen als Binärwörter hier nicht erfolgt ist. Die Art dieser (weitergehenden und genauen) Festlegung könnte bei komplexitätstheoretischen Untersuchungen sehr wohl eine Rolle spielen (und müßte präzis geschehen), tut das aber für „vernünftige" Darstellungen des Problems meistens kaum, da verschiedene solche Darstellungen oft mit geringem Aufwand ineinander übergeführt werden können (d.h. mit oftmals weit geringerem Aufwand als zur Lösung des Problems bezüglich einer dieser Darstellungen nötig ist.)

Ein weiterer Grund dafür, warum die angegebenen Problemspezifikationen unvollständig sind (selbst wenn genaue Darstellungen der Instanzen und Antworten gegeben

sind), besteht darin, daß nicht alle Binärwörter Darstellungen von sinnvollen Probleminstanzen sein müssen (in den obigen Beispielen muß nicht jedes Binärwort Darstellung eines Graphen oder einer Liste von Literalen und einer Folge von Klausen sein). Nach der Definition eines Problems muß aber auch für solche inhaltsleere Instanzen des Problems eine Antwort definiert sein. Diese könnte als "`Nein`" gesetzt werden, es könnte aber auch gewünscht sein, in diesen Fällen "`Instanz_stellt_keine_sinnvolle_Fragestellung_dar`" als Antwort zu erhalten.

In der Definition eines Problems ist nicht gefordert worden, daß Antworten immer eindeutig sind. So könnte eine geänderte Problemstellung im Fall der ISOMORPHIE VON GRAPHEN durchaus so aussehen, daß zu einer Instanz, die eine Darstellung isomorpher Graphen ist, als Anworten sowohl "`Ja`" als auch jede beliebige Funktion zwischen den Eckenmengen V und V', die eine solche Isomorphie herstellt, zugelassen sind.

Definition 1.3.3. *Ein Problem ist ein* **funktionales Problem**, *wenn zu jeder Instanz genau eine Antwort existiert. – Ein Problem ist ein* **Entscheidungs-Problem**, *wenn es ein funktionales Problem ist, das nur die möglichen Antworten "`Ja`" und "`Nein`" (bzw. nur zwei beliebige verschiedene Antworten) besitzt.*

Entscheidungs-Probleme sind unmittelbar mit Sprachen $L \subseteq \{0,1\}^*$ verknüpft: Zu jedem Entscheidungs-Problem X gibt es eine Sprache $L(X) \subseteq \{0,1\}^*$ mit

$$L(X) = \{I \in \{0,1\}^* / (I, \text{“}\texttt{Ja}\text{”}) \in X\}$$

und zu jeder Sprache $L \subseteq \{0,1\}^*$ existiert ein Entscheidungs-Problem

$$X(L) := \{(I, \text{“}\texttt{Ja}\text{”}) / I \in L\} \cup \{(I, \text{“}\texttt{Nein}\text{”}) / I \notin L\};$$

so, daß für die dadurch definierten Zuweisungen jeweils die eine die Umkehrung der anderen ist. – Eine solche Entsprechung von Entscheidungs-Problemen und Sprachen besteht auch über beliebigen Alphabeten.

Das Entscheidungsproblem (: im logischen Sinn) für eine Theorie T, wobei T als $T = (\Sigma_T, Fo_T, Thm_T)$ aufgefaßt wird, läßt sich in dem hier betrachteten formalen Rahmen z.B. auf zwei Arten, als funktionales Problem und als Entscheidungs-Problem darstellen.

ENTSCHEIDUNGSPROBLEM (1) für die Theorie $T = (\Sigma_T, Fo_T, Thm_T)$

Instanz: Ein Wort $x \in \Sigma_T^*$.

Antwort: „`ist_Theorem_von_`T“, falls $x \in Thm_T$;
„`ist_Formel_von_`T`,_kein_Theorem_von_`T“, falls $x \in Fo_T \setminus Thm_T$;
„`ist_keine_Formel_von_`T“, falls $x \notin Fo_T$.

ENTSCHEIDUNGSPROBLEM (2) für die Theorie $T = (\Sigma_T, Fo_T, Thm_T)$

Instanz: Ein Wort $x \in \Sigma_T^*$.

Antwort: „`ist_Theorem_von_`T“, falls $x \in Thm_T$;
„`ist_kein_Theorem_von_`T“, falls $x \notin Thm_T$.

Der Unterschied in der Problemspezifikation zwischen diesen beiden Problemstellungen könnte bei Untersuchungen die Entscheidungskomplexität (und also die Komplexität dieser beiden Probleme) betreffend durchaus Unterschiede ergeben und spielt jedenfalls im Hinblick auf die Auswahl von Methodenklassen, die zur Lösung in Frage kommen, eine Rolle. Trotzdem ist so eine Unterscheidung praktisch eher von nur untergeordneter Bedeutung, da der zusätzliche Lösungsaufwand für ENTSCHEIDUNGSPROBLEM (1) gegenüber ENTSCHEIDUNGSPROBLEM (2) im wesentlichen im Aufwand zur Entscheidung, ob eine gegebene Zeichenkette $x \in \Sigma_T^*$ eine Formel von T darstellt oder nicht, besteht. Die Eigenschaft, „Formel von T“ zu sein, ist aber allermeistens von erheblich niedrigerer Komplexität als die des „eigentlichen“ Entscheidungsproblems, des ENTSCHEIDUNGSPROBLEMs (2).

In vielen Fällen von logischen Theorien sind die obigen Problemstellungen aber noch aus einem anderen Grund ungenügend genau. Denn oftmals kann die genaue Gestalt von Formeln nicht völlig beibehalten werden, will man zu „realistischen“ Aussagen über die Entscheidungskomplexität gelangen. So ist zum Beispiel die ausschließlich unäre Indizierung von Symbolen und Variablen (die in logischen Systemen und Kalkülen oft so definiert wurde) problematisch, weil diese leicht zu exponentiell längeren Formeln führen kann im Vergleich zu sinnvoll und am wirklichen Einsatz auf einem Computer orientiert geschriebenen und gehandhabten Formeln (in denen vernünftigerweise nur n-är indizierte Symbole ($n \in \mathbb{N}$, $n \geq 2$) vorkommen). Weiters wird in der Logik häufig mit einem unbegrenzten Symbolvorrat operiert, Rechenmaschinen können aber nur über endlichen Alphabeten sinnvoll arbeiten. – Insgesamt entsteht also die Forderung, daß die aufgrund einer bestimmten Formelsyntax erreichten Komplexitätsresultate auf eine realistische Situation des Einsatzes eines Entscheidungsverfahrens auf einem Computer (wenigstens theoretisch) übertragbar sein sollten; d.h. also, daß die auf der Basis einer bestimmten Syntax erzielten

Komplexitätsresultate nicht schon durch formale Eigenarten dieser Syntax in realitätsferner Weise verzerrt sein sollten und solcherart vielleicht mehr die Komplexität dieser Syntax-Besonderheiten als die Komplexität des Entscheidungsproblems selbst beschreiben.

Aus allen diesen Gründen soll eine Theorie $T = (\Sigma_T, Fo_T, Thm_T)$ auch als Tripel $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ aufgefaßt werden können, wobei $T^{((M))}$ für die Theorie T in „*Maschinen-behandelbarer Form*“ steht, $\Sigma_{T^{((M))}}$ ein endliches Zeichenalphabet ist, $Fo_{T^{((M))}}$ die darin ausdrückbare Formelsprache von T ist und $Thm_{T^{((M))}}$ die den Theoremen von T entsprechende Formelsprache von $Fo_{T^{((M))}}$ ist.

Die Formelsprache $Fo_{T^{((M))}}$ muß dabei unter Beachtung der Einschränkungen wie oben sinnvoll gewählt werden, jedenfalls aber so, daß jeder Formel $\mathbf{A}$ von T eine Formel $\mathbf{A}^{((M))}$ von $T^{((M))}$ und umgekehrt jeder Formel $\boldsymbol{\mathcal{A}}$ von $T^{((M))}$ eine Formel $\mathbf{A}^{(\boldsymbol{\mathcal{A}})}$ von T zugeordnet werden kann (für Elemente aus $Fo_{T^{((M))}}$ werden im folgenden fettgedruckte kalligraphische Buchstaben gewählt), sodaß jedenfalls immer

$$\mathbf{A}^{(\mathbf{A}^{((M))})} \qquad \text{gleich} \qquad \mathbf{A}$$

gilt (dem entspricht die Forderung, daß $T^{((M))}$ auch eine allgemeinere Syntax als T besitzt, in die die Syntax von T „eingebettet“ werden kann.)

Als Beispiel einer wie hier geforderten Formelsprache für eine logische Theorie 1. Ordnung (in der Präzisierung dieses Konzeptes durch [Shoe67], das als Logik-Kalkül in dieser Arbeit weitgehend verwendet wird) mit endlich vielen nichtlogischen (Funktions- und Prädikats-) Symbolen sei hier eine LR(1)-Grammatik $G_{T^{((M))}}$ angegeben, die als Sprache pränex geschriebene Formeln (wie sie dem System in [Shoe67] zugrundeliegen) einer Theorie T mit nichtlogischen Symbolen $\mathbf{e}_1, \ldots, \mathbf{e}_{n^{(1)}}$ (Konstantensymbole), $\mathbf{f}_{1,1}, \ldots \mathbf{f}_{1,n_1^{(2)}}$ (1-stellige Funktionssymbole), $\ldots$, $\mathbf{f}_{m^{(2)},1}, \ldots, \mathbf{f}_{m^{(2)},n^{(2)}_{m^{(2)}}}$ ($m^{(2)}$-stellige Funktionssymbole), $\mathbf{p}_{1,1}, \ldots, \mathbf{p}_{1,n_1^{(3)}}$ (1-stellige Prädikatssymbole), $\ldots$, $\mathbf{p}_{m^{(3)},1}, \ldots, \mathbf{p}_{m^{(3)},n^{(3)}_{m^{(3)}}}$ ($m^{(3)}$-stellige Prädikatssymbole), besitzt (wobei $n^{(1)}$, $m^{(2)}$, $n_1^{(2)}, \ldots, n^{(2)}_{m^{(2)}}, \ldots$, $m^{(3)}$, $n_1^{(3)}, \ldots, n^{(3)}_{m^{(3)}} \in \mathbb{N}_0$)[14].

[14] Es handelt sich bei $\mathbf{e}_1, \ldots, \mathbf{e}_{n^{(1)}}$, $\mathbf{f}_{1,1}, \ldots \mathbf{f}_{1,n_1^{(2)}}$, $\ldots$, $\mathbf{f}_{m^{(2)},1}, \ldots, \mathbf{f}_{m^{(2)},n^{(2)}_{m^{(2)}}}$, $\mathbf{p}_{1,1}, \ldots \mathbf{p}_{1,n_1^{(3)}}$, $\ldots$, $\mathbf{p}_{m^{(3)},1}, \ldots, \mathbf{p}_{m^{(3)},n^{(3)}_{m^{(3)}}}$ um syntaktische Variable für Konstanten-, Funktions- und Prädikatssymbole einer Theorie T , also um Platzhalter für konkrete, hierdurch vorerst noch nicht weiter (als durch ihre jeweilige Stelligkeit) festgelegte, nichtlogische Symbole von T (vgl. dazu den Gebrauch und die Schreibweise syntaktischer Variable für nichtlogische Symbole von Theorien 1.Ordung in [Shoe67]).

$G_{T^{((M))}}$ besitzt dabei als Terminalalphabet die Menge

$$\Sigma_{T^{((M))}} := \{\ \neg, \vee, \exists, \&, \rightarrow, \leftrightarrow, \forall, =, x, y, z, w, 0, 1, 2, \ldots, 9,$$
$$\mathbf{f}_{1,1}, \ldots \mathbf{f}_{1,n_1^{(2)}}, \ldots\ldots \mathbf{f}_{m^{(2)},1}, \ldots \mathbf{f}_{m^{(2)},n^{(2)}_{m^{(2)}}},$$
$$\mathbf{e}_1, \ldots, \mathbf{e}_{n^{(1)}}, \mathbf{p}_{1,1}, \ldots \mathbf{p}_{1,n_1^{(3)}}, \ldots \mathbf{p}_{m^{(3)},1}, \ldots, \mathbf{p}_{m^{(3)},n^{(3)}_{m^{(3)}}}\ \}^{15}$$

und die in Grammatik 1.3.1 angebenen Produktionen in BNF[16].

Hiervon ausgehend kann diese Theorie T zum Zweck der realistischeren Untersuchung ihrer Entscheidungskomplexität mit leicht abgeänderter Syntax (abgeändert gegenüber der in [Shoe67] gebrauchten Syntax) als Tripel $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ mit $\Sigma_{T^{((M))}}$ wie angegeben und mit

$$Fo_{T^{((M))}} := L(G_{T^{((M))}}), \qquad Thm_{T^{((M))}} := \{\boldsymbol{\mathcal{A}} \in Fo_{T^{((M))}} / \vdash_T \mathbf{A}^{(\boldsymbol{\mathcal{A}})}\},$$

aufgefaßt werden. Hierbei ist $L(G_{T^{((M))}})$ die von $G_{T^{((M))}}$ erzeugte Formelsprache und $\mathbf{A}^{(\boldsymbol{\mathcal{A}})}$ eine auf sinnvolle und augenscheinliche Weise zu jeder Formel $\boldsymbol{\mathcal{A}} \in Fo_{T^{((M))}}$ definierte, ihr in T entsprechende Formel (dafür müssen dezimale Indizes durch Strichindizes ersetzt werden und Formeln, die die logischen Symbole &, $\rightarrow$, $\leftrightarrow$ und $\forall$ enthalten, durch logisch äquivalente Formeln, die diese Symbole nicht mehr enthalten, ersetzt werden).

Der Unterschied in der Syntax zwischen $T^{((M))}$ und T besteht genau (1) in der dezimalen Indizierung von Variablen in $T^{((M))}$ gegenüber unärer Indizierung $x', x'', x''', \ldots$ in T und (2) darin, daß in der Syntax von Formeln in $T^{((M))}$ auch die logischen Symbole &, $\rightarrow$, $\leftrightarrow$ und $\forall$ als zulässige Symbole vorkommen, während diese Symbole im Formalismus von [Shoe67] nur „definierte Symbole“ sind und also dort nur als abkürzende Schreibweisen für Formeln, in denen diese Symbole nicht vorkommen, auftreten bzw. gebraucht werden.

Für ein anderes Beispiel einer Formelgrammatik (für Theorien der Presburger Arithmetik) vgl. Grammatik 2.6.1, Abschnitt 2.6, Kapitel 2.

Die für die Komplexitätstheorie bedeutsame Fragestellung besteht nun nicht so sehr darin, für gegebene konkrete einzelne Instanzen eines Problems den Aufwand, der zum Finden einer zugehörigen Antwort nötig ist, zu ermitteln (das ist natürlich aber für praktische

[15] Hierbei sei angenommen, daß die syntaktischen Variablen für die Konstanten-, Funktions- und Prädikatssymbole für einerseits untereinander paarweise verschiedene und andererseits auch von den übrigen Zeichen in $\Sigma_{T^{((M))}}$ verschiedene Symbole stehen.

[16] Backus-Naur-Form

[17] In dieser Definition von $G_{T^{((M))}}$ in BNF sind die Konstantensymbole $\mathbf{e}_1, \ldots, \mathbf{e}_{n^{(1)}}$, die Funktionssymbole $\mathbf{f}_{1,1}, \ldots, \mathbf{f}_{m^{(2)},n^{(2)}_{m^{(2)}}}$, und die Prädikatssymbole $\mathbf{p}_{1,1}, \ldots, \mathbf{p}_{m^{(3)},n^{(3)}_{m^{(3)}}}$, die als syntaktische Variable für konkrete, hier nicht festgelegte Symbole von T stehen, nicht fettgedruckt worden, obwohl sie Terminalsymbole bezeichnen. Allerdings sind sie selbst keine Terminalsymbole und in der Darstellung einer Grammatik in BNF kommt die Eigenschaft, fettgedruckt zu werden, nur den Terminalsymbolen zu. In der Darstellung von $G_{T^{((M))}}$ hier sind diese Symbole daher erneut syntaktische Variable (und also Platzhalter), nun allerdings für konkrete, hier nicht weiter spezifizierte Terminalsymbole, die, falls sie an die Stelle der synt. Var. gesetzt würden, fettgedruckt erscheinen müßten.

Grammatik 1.3.1 LR(1)-Grammatik $G_{T^{((M))}}$: [17]

<formula>::= <at_formula>|¬<formula>|∨<formula><formula>
∃<variable><formula>|&<formula><formula>|
→<formula><formula>|↔<formula><formula>|
∀<variable><formula>

<at_formula>::= =<term><term>|<1_ary_pred_symb><term>|
<2_ary_pred_symb><term><term>| ...
... |<$m^{(3)}$_ary_pred_symb>$\underbrace{\texttt{<term> ... <term>}}_{m^{(3)}}$

<1_ary_pred_symb>::= $\mathrm{p}_{1,1}|\mathrm{p}_{1,2}|\ \ldots\ |\mathrm{p}_{1,n_1^{(3)}}$

<2_ary_pred_symb>::= $\mathrm{p}_{2,1}|\mathrm{p}_{2,2}|\ \ldots\ |\mathrm{p}_{2,n_2^{(3)}}$

$\vdots$

<$m^{(3)}$_ary_pred_symb>::= $\mathrm{p}_{m^{(3)},1}|\mathrm{p}_{m^{(3)},2}|\ \ldots\ |\mathrm{p}_{m^{(3)},n^{(3)}_{m^{(3)}}}$

<term>::= <variable>|<const_symb>|<1_ary_funct_symb><term>
<2_ary_funct_symb><term><term>| ...
... |<$m^{(2)}$_ary_funct_symb>$\underbrace{\texttt{<term> ... <term>}}_{m^{(2)}}$

<variable>::= $\boldsymbol{x}|\boldsymbol{y}|\boldsymbol{z}|\boldsymbol{w}|\boldsymbol{x}$<dec_ind>$|\boldsymbol{y}$<dec_ind>$|\boldsymbol{z}$<dec_ind>$|\boldsymbol{w}$<dec_ind>

<dec_ind>::= $_0|_1|\ \ldots\ |_9|_1$<dec_ind_str>$|\ \ldots\ |_9$<dec_ind_str>

<dec_ind_str>::= $_0|_1|\ \ldots\ |_9|_0$<dec_ind_str>$|\ \ldots\ |_9$<dec_ind_str>

<const_symb>::= $\mathrm{e}_1|\mathrm{e}_2|\ \ldots\ |\mathrm{e}_{n^{(1)}}$

<1_ary_funct_Symb>::= $\mathrm{f}_{1,1}|\mathrm{f}_{1,2}|\ \ldots\ |\mathrm{f}_{1,n_1^{(2)}}$

<2_ary_funct_Symb>::= $\mathrm{f}_{2,1}|\mathrm{f}_{2,2}|\ \ldots\ |\mathrm{f}_{2,n_2^{(2)}}$

$\vdots$

<$m^{(2)}$_ary_funct_Symb>::= $\mathrm{f}_{m^{(2)},1}|\mathrm{f}_{m^{(2)},2}|\ \ldots\ |\mathrm{f}_{m^{(2)},n^{(2)}_{m^{(2)}}}$

Aufgabenstellungen oft von großer Bedeutung), sondern in der Frage, wieviel Aufwand (in einem näher zu definierenden Sinn verstanden) eine allgemeine Methode zur Lösung eines Problems benötigt. Also etwa in der Frage, wie sich dieser Aufwand als Funktion einer von der Instanz abhängigen Größe (zumeist deren Länge als Zeichenkette) abschätzen oder beschränken läßt.

Definition 1.3.4. *Eine* **effektive Methode** *M zur Lösung eines Problems X ist hierbei also eine effektive Methode oder ein effektives Verfahren, mit dem zu jeder gegebenen Instanz I von X in einer endlichen Anzahl von Schritten eine zugehörige Antwort A gefunden werden kann.*

(Die hierin ausgesprochene Lösbarkeit durch ein effektives Verfahren (oder eine effektive Methode) verweist natürlich im Lichte der Churchen These darauf, daß Probleme, die durch ein solches Verfahren lösbar sind, auch von einem Verfahren aus einer der präzisierten Verfahrensklassen gelöst werden können; für allgemeine komplexitätstheoretische Untersuchungen ist es aber nicht sinnvoll, die Klasse der betrachteten Verfahren von vorne herein auf nur ein Berechnungsmodell zu beschränken, da—obwohl gegenüber diesen Modellen keine zusätzlichen Probleme gelöst werden können—doch interessante Unterschiede in der Berechnungskomplexität zwischen Methoden aus verschiedenen „universellen“[18] Klassen bestehen könnten. – Dennoch finden in der Komplexitätstheorie —aus später anzudeutenden Gründen—hauptsächlich nur Klassen von Turingmaschinen als Verfahrenskonzepte Anwendung.)

Definition 1.3.5. *Sei X ein Problem, M eine effektive Methode zur Lösung von X, R eine von M beanspruchte Ressource.*

Dann seien

$$\begin{aligned} Rc_{M,R}\colon \{0,1\}^* &\to \mathbb{N}_0 \\ x \mapsto Rc_{M,R} :=\ & \textit{Von der Methode } M \textit{ zum Finden einer} \\ & \textit{Antwort } A \textit{ zur Instanz } x \textit{ des Problems } X \\ & \textit{beanspruchte Quantität an Ressource } R \end{aligned}$$

und

$$\begin{aligned} R_M\colon \mathbb{N}_0 &\to \mathbb{N}_0 \\ n \mapsto R_M(n) :=\ & \max\{Rc_{M,R}(x)/x \in \{0,1\}^*, |x| = n\} \end{aligned}$$

die Funktionen, die Instanzen $x \in \{0,1\}^*$ den Aufwand zur Lösung des Problems X mittels

[18] Hierbei steht eine „universelle Verfahrensklasse“ für eine solche Klasse, bezüglich der sich jedes algorithmische Verfahren auch von einem dieser Gesamtheit angehörigen Verfahren ausführen oder simulieren läßt. Im Lichte der Churchen These bedeutet das, daß eine solche Klasse einer der präzisierten Klassen (λ-Definierbarkeit, Turingmaschinen, partiell-rekursive Funktionen, Markov-Algorithmen, ...) äquivalent ist (es also effektive gegenseitige Simulationen gibt).

M bzw. jeder Zahl $n \in \mathbb{N}_0$ den über alle $x \in \{0,1\}^*$ mit $|x| = n$ maximierten Aufwand zur Lösung von Instanz x von X mittels M zuweisen.

Die Funktion $R_M(n)$ ist ein *worst-case-Maß* und schätzt den zur Lösung einer Instanz x mit $|x| = n$ nötigen Aufwand an Ressource R nur nach oben ab (den Aufwand *im schlimmsten Fall*). Bei vielen praktischen Problemstellungen könnte sich natürlich auch ein *average-case-Maß* (ein Aufwandsmaß für den *durchschnittlichen Fall*) als interessant erweisen. Average-case-Analysen erweisen sich oft als erheblich schwieriger als worst-case-Analysen und bilden (bisher) nur einen kleineren Teil der Komplexitätstheorie.

Definition 1.3.6. Wachstumsordnungen von Funktionen
Seien $f, g: \mathbb{N}_0 \to \mathbb{R}_0^+$ Funktionen.

(i) *„f ist* **assymptotisch durch g beschränkt**“ *($f \leq_{\text{ae}} g$)*[19]*:* $\iff$
$\iff (\exists n_0 \in \mathbb{N}_0)(\forall n \geq n_0,\ n \in \mathbb{N})\ (f(n) \leq g(n))$.
„f ist **unendlich oft kleiner gleich** *als g“ ($f \leq_{\text{io}} g$)*[19] *:* $\iff$
$\iff (\forall n_0 \in \mathbb{N}_0)(\exists n \geq n_0,\ n \in \mathbb{N})\ (f(n) \leq g(n))$.
Analoge Festsetzungen hierzu seien auch für $=_{\text{ae}}$, $\neq_{\text{ae}}$, $\geq_{\text{ae}}$, $<_{\text{ae}}$, $>_{\text{ae}}$, $=_{\text{io}}$, $\neq_{\text{io}}$, $\geq_{\text{io}}$, $<_{\text{io}}$ und $>_{\text{io}}$ getroffen.

(ii) *f, g seien so, daß $f, g \neq_{\text{ae}} 0$.*
„f und g **nähern sich assymptotisch an**“ *($f \sim g$) :* $\iff$
$\iff \lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$.

(iii) *Es gelten folgende Bezeichungen für Wachstumsklassen von Funktionen:*

$$\begin{aligned}
\boldsymbol{O(g)} &:= \{h: \mathbb{N}_0 \to \mathbb{R}_0^+ \ /\ (\exists k \in \mathbb{N})(h \leq_{\text{ae}} k \cdot g)\}\ ; \\
\boldsymbol{\Omega(g)} &:= \{h: \mathbb{N}_0 \to \mathbb{R}_0^+ \ /\ (\exists k \in \mathbb{N})(h \geq_{\text{ae}} k^{-1} \cdot g)\}\} \\
\boldsymbol{o(g)} &:= \{h: \mathbb{N}_0 \to \mathbb{R}_0^+ \ /\ (\forall k \in \mathbb{N})(h \leq_{\text{ae}} k^{-1} \cdot g)\}\} \\
\boldsymbol{\omega(g)} &:= \{h: \mathbb{N}_0 \to \mathbb{R}_0^+ \ /\ (\forall k \in \mathbb{N})(h \geq_{\text{ae}} k \cdot g)\} \\
\boldsymbol{\Theta(g)} &:= O(g) \cap \Omega(g)\ .
\end{aligned}$$

Die dadurch definierten Aussagen $f \in O(g)$ [$f \in \Omega(g)$, $f \in o(g)$, $f \in \omega(g)$, $f \in \Theta(g)$] werden in Worten durch „f **wächst nicht schneller als** *g“ [„f* **wächst nicht langsamer als** *g“, „f* **wächst langsamer als** *g“, „f* **wächst schneller als** *g“, „f und g* **wachsen gleich schnell**“*] ausgedrückt.*

[19] ae steht hier für “almost everywhere” , also für „fast überall“, io für “infinitely often”, also „unendlich oft“. Hier sind die deutsche Bezeichnungen wie in [Rei90] u.a. deshalb vermieden worden, da „f.ü.“ im Deutschen wohl eher für eine Aussage in der Analysis und in der Maßtheorie gebräuchlich ist.

Für Mengen $\mathcal{G}$ von Funktionen von $\mathbb{N}_0$ nach $\mathbb{R}_0^+$ gelten die Setzungen:

$$\boldsymbol{O(\mathcal{G})} := \bigcup_{g\in\mathcal{G}} O(g)\ ; \qquad \boldsymbol{\Omega(\mathcal{G})} := \bigcup_{g\in\mathcal{G}} \Omega(g)\ ;$$
$$\boldsymbol{o(\mathcal{G})} := \bigcap_{g\in\mathcal{G}} o(g)\ ; \qquad \boldsymbol{\omega(\mathcal{G})} := \bigcap_{g\in\mathcal{G}} \omega(g)$$

Um die einem Problem X inhärente Lösungs-Komplexität zu untersuchen (und sich diesem unpräzisen Begriff auf exakt-definitorische Weise zu nähern), ist es notwendig, dieses Problem gegenüber einer Klasse C von Methoden, die als Lösungsmethoden in Frage kommen sollen, anzuschauen und nach „optimalen" Lösungsmethoden für X aus C zu fragen.

Eine *optimale* Lösungsmethode M für das Problem X bezüglich der Methodenklasse C wäre dabei eine solche effektive Methode M aus C zur Lösung von X, sodaß für alle anderen Lösungsmethoden M' aus C für das Problem X gilt: $R_M(n) \leq_{\text{ae}} R_{M'}(n)$.

Es sind nun aber verschiedene Fälle vorstellbar und auch tatsächlich möglich, in denen optimale Lösungsmethoden nicht existieren: (1) Es ist denkbar, daß es Lösungsmethoden M und M' für X aus C gibt, für die R_M und $R_{M'}$ zwar $\leq_{\text{ae}}$-minimale[20] Elemente (unter allen $R_{\tilde{M}}$ für Lösungsmethoden $\tilde{M}$ für X aus C) sind, die jedoch bezüglich $\leq_{\text{ae}}$ unvergleichbar sind, d.h. also, für die $R_M >_{\text{io}} R_{M'}$ und $R_M <_{\text{io}} R_{M'}$ gelten. (2) Es kann geschehen, daß auch minimale Elemente bezüglich $\leq_{\text{ae}}$ nicht existieren. (So ein Fall könnte z.B. dann eintreten, wenn für ein Problem X zu jedem $\alpha > 0$ Lösungsmethoden M_α mit $R_{M_\alpha} \in O(n^{1+\alpha})$ existieren, nicht jedoch eine Methode M mit $R_M \in O(n)$[21]. – Es gibt Umstände, unter denen so ein Fall wirklich eintritt[22].)

Aus diesen Gründen und einer Reihe weiterer (etwa, daß für viele Methodenklassen C zu einer Lösungsmethode M aus C auch für alle $c > 0$, $c \in \mathbb{R}$ Lösungsmethoden M_c aus C mit $R_{M_c}(n) \sim c \cdot R_M(n)$ existieren, daß also der Lösungsaufwand durch beliebige Faktoren beschleunigt werden kann) ist in vielen Fällen von Problemen der entsprechende Lösungsaufwand nur nach oben und nach unten eingrenzbar. Die Frage, wie genau das geschehen kann, ist aber von großem komplexitätstheoretischen Interesse.

In einer sehr allgemeinen Weise können nun Komplexitätsschranken für den Lösungsaufwand eines Problems wie in [Jo90] so definiert werden:

---

[20] $\leq_{\text{ae}}$ ist nun reflexiv und transitiv, nicht aber antisymmetrisch; um eine Ordnung $\leq'_{\text{ae}}$ daraus zu erhalten, müßte $\leq_{\text{ae}}$ auf $=_{\text{ae}}$-Äquivalenzklassen fortgesetzt werden. Geht man von so einer Fortsetzung aus, dann kann für $\leq_{\text{ae}}$ in Beziehung zu einer Klasse $\mathcal{K} \subseteq \mathbb{R}_0^{+\mathbb{N}_0}$ von Funktionen gesetzt werden:

$$f : \mathbb{N}_0 \to \mathbb{R}_0^+ \text{ ist in } \mathcal{K} \leq_{\text{ae}}\text{-}\textit{minimal}: \iff \neg(\exists g \in \mathcal{K})\ (g \leq_{\text{ae}} f\ \&\ g \neq_{\text{io}} f).$$

[21] In diesem Fall könnte es aber z.B. eine optimale Lösungsmethode M mit $R_M(n) \in O(n \log n)$ geben.

[22] Vgl. den Beschleunigungssatz ("*Speed-up Theorem*") von Blum, zB. in [HoUl79], p. 308.

Definition 1.3.7. Obere und untere Schranken.
Sei X ein Problem, C eine Klasse von Methoden, R eine von Methoden aus C beanspruchte Ressource, $t : \mathbb{N}_0 \to \mathbb{R}_0^+$.

(i) $t(n)$ ist eine **obere Schranke** *für den Aufwand zur Lösung von X mit Methoden aus C bezüglich Ressource R genau dann, wenn eine effektive Methode M aus C existiert, die X löst und für die gilt: $R_M(n) \in O(t(n))$.*

(ii) $t(n)$ ist eine **untere Schranke** *für den Aufwand zur Lösung von X mit Methoden aus C bezüglich Ressource R genau dann, wenn für alle effektiven Methoden M aus C, die X lösen, gilt: $R_M(n) \in \Omega(t(n))$.*

Eine obere Schranke $t_o(n)$ für den Lösungsaufwand von Problem X bezüglich Methoden aus C ist also mit der Gültigkeit der Aussage verknüpft, daß (jedenfalls:) *eine* Lösungsmethode M aus C existiert, für die sich das Wachstumsverhalten von $R_M(n)$ nach oben durch $t_o(n)$ beschränken läßt (sodaß also $R_M(n)$ nicht schneller als $t_o(n)$ wächst). Eine untere Schranke $t_u(n)$ für den Lösungsaufwand von Problem X mit Methoden aus C impliziert dagegen die Aussage, daß sich das Wachstumsverhalten von $R_M(n)$ für *jede* Lösungsmethode M aus C für X nach unten durch $t_u(n)$ abschätzen läßt (sodaß also für jede solche Lösungsmethode M $R_M(n)$ nicht langsamer als $t_u(n)$ wächst).

Es ist damit leicht zu sehen, daß diese beiden Begriffe einander zwar ausschließen, nicht jedoch einfach das Gegenteil zueinander sind, denn die Verneinungen von „$t(n)$ ist obere Schranke ... “ bzw. „$t(n)$ ist untere Schranke für X bzgl. Methoden M aus C“ führen auf die Aussagen:

$$(\forall M \in C,\ M \text{ ist Lös.meth. für X})(\forall c \in \mathbb{N})\ (R_M(n) >_{\text{io}} c \cdot t(n)) \qquad \text{bzw.}$$
$$(\exists M \in C,\ M \text{ ist Lös.meth. für X})(\forall c \in \mathbb{N})\ (R_M(n) <_{\text{io}} c^{-1} \cdot t(n))$$

In der hier angebenen Form schließen sich diese Bezeichnungen gegenseitig nicht aus. Es handelt sich bei Definition 1.3.7 aber nur um ungefähre Festsetzungen für allgemeine Methodenklassen, die bei der Betrachtung einzelner, genau spezifizierter Klassen oft deren speziellen Eigenschaften angepaßt werden müssen, um in solchen konkreten Zusammenhängen sinnvolle und brauchbare Begriffe zu bilden. So ist es begrifflich wünschenswert, daß sich die Eigenschaften, untere Schranke zu sein, bzw. obere Schranke zu sein, gegenseitig ausschließen (wenngleich aber nicht unbedingt die Nötigkeit besteht, zu fordern, daß sie das Gegenteil voneinander ausdrücken). Weiters scheint für die meisten bedeutsamen komplexitätstheoretischen Zwecke und Überlegungen die Erklärung unterer Schranken in Definition 1.3.7 deutlich zu einschränkend ausgefallen zu sein (wenngleich wohl im Bemühen entstanden, unanschaulichere Situationen begrifflich auf alle Fälle zu vermeiden).

So wäre es allgemein vielleicht besser, statt

$$(\forall M \in C,\ M \text{ ist Lös.meth. für } X)(\exists c \in \mathbb{N})\ (R_M(n) \geq_{\text{ae}} c^{-1} \cdot t(n))\ , \tag{1.1}$$

also der Bedingung an $t(n)$, untere Schranke für den Lösungsaufwand von X mit Methoden aus C zu sein, nur

$$(\forall M \in C,\ M \text{ ist Lös.meth. für X})(\exists c \in \mathbb{N})\ (R_M(n) \geq_{\text{io}} c^{-1} \cdot t(n))\ , \tag{1.2}$$

als an eine untere Schranke $t(n)$ zu richtende Bedingung zu verwenden. (1.2) ist schwächer als (1.1), schließt aber für alle Lösungsmethoden M aus C für X nicht aus, daß es unendlich viele n gibt, für die M sehr effizient, beispielsweise konstant oder qualitativ kleiner als $t(n)$ ist; und es scheint nicht sinnvoll, eine solche Situation bei der Definition von unteren Schranken auszuschließen. – Noch weitergehend könnte argumentiert werden, daß die wesentliche interessante Eigenschaft unterer Schranken eigentlich nur darin besteht, keine obere Schranke zu sein, also

$$(\forall M \in C,\ M \text{ ist Lös.meth. für X})(\forall c \in \mathbb{N})\ (R_M(n) >_{\text{io}} c \cdot t(n))\ , \tag{1.3}$$

zu erfüllen. (1.3) formuliert die Eigenschaft von $t(n)$, daß sich das Wachstumsverhalten von $R_M(n)$ für keine Lösungsmethode $M \in C$ für X nach oben durch $t(n)$ begrenzen läßt (d.h. daß $R_M(n)$ für keine solche Lösungsmethode nicht schneller als $t(n)$ wächst). Und diese Aussage ist für sinnvolle Funktionen $t(n)$ (d.h. etwa monoton wachsenden Funktionen oder monoton wachsenden Funktionen, die einer bekannten Wachstumsklassen angehören) oft von größerem Interesse als eine Aussage, daß sich $R_M(n)$ für keine Lösungsmethode $M \in C$ für X im Wachstumsverhalten nach oben durch $t(n)$ begrenzen läßt[23]. – Bezüglich (1.3) könnte allenfalls noch weiters die Frage gestellt werden, wie „dicht“ jene $n \in \mathbb{N}_0$, für die $R_M(n) >_{\text{io}} c \cdot t(n)$ gilt, in $\mathbb{N}$ liegen.

Im früher skizzierten Fall eines Problems X, zu dem für jedes $\alpha > 0$ Lösungsmethoden M_α mit $R_{M_\alpha}(n) \in O(n^{1+\alpha})$ existieren, nicht jedoch eine Lösungsmethode M_0 mit $R_{M_0}(n) \in O(n)$, wären für alle $\alpha > 0$ die Funktionen $n^{1+\alpha}$ obere Schranken für den Lösungsaufwand. Entlang von Definition 1.3.7 könnte von n^1 nur gesagt werden, daß das keine obere Schranke ist; (1.1) muß nicht erfüllt sein, (1.3) und (1.2) sind es hingegen schon

[23] Hierfür ist natürlich entscheidend, daß ein praktisches Interesse weitgehend immer möglichst effizienten Algorithmen zur Lösung eines Problems P gilt, sowie Aussagen, welchen Begrenzungen die Suche nach solchen Algorithmen aus prinzipiellen Gründen unterworfen ist, und nicht Sätzen über die ausschließliche Existenz von *guarantiert* ineffektiven Algorithmen für die Lösung von P (d.h. solchen Algorithmen, die für weitgehend alle Eingaben nur sehr ineffektiv sind). – Als eine in diesem Zusammenhang zu nennende Ausnahme könnten aber in der Komplexitätstheorie betrachtete Fragestellungen gelten, die ihre Motivation aus der Kryptographie beziehen. Hierbei kann nämlich für den Nachweis der „Sicherheit“ von Kodes auch der Beweis von stärkeren Eigenschaften unterer Schranken für bestimmte Probleme erforderlich oder zumindestens wünschenswert sein.

((1.3) formuliert die Eigenschaft, nicht obere Schranke zu sein, (1.2) folgt aus (1.3)). In diesem Fall wäre es aber schon auch angebracht, von einer linearen unteren Schranke für den Lösungsaufwand von X sprechen zu können.

Viele der in der Komplexitätstheorie auftretenden Schrankenfunktionen können nach ihrer Zugehörigkeit zu einer der folgenden Mengen von Komplexitätsfunktionen klassifiziert werden:

Definition 1.3.8. Mengen von Komplexitätsfunktionen.

Seien **1**, id, exp *und* log *die wie folgt definierten Grundfuktionen:*

$$\mathbf{1}\colon \mathbb{N}_0 \to \mathbb{N}_0\,, \quad n \mapsto 1 \qquad \mathrm{id}\colon \mathbb{N}_0 \to \mathbb{N}_0\,, \quad n \mapsto n \qquad \exp\colon \mathbb{N}_0 \to \mathbb{R}_0^+\,, \quad n \mapsto e^n \qquad \log\colon \mathbb{N}_0 \to \mathbb{R}_0^+\,, \quad n \mapsto \begin{cases} 0 & \dots n = 0 \\ \ln n & \dots n \geq 1 \end{cases}$$

Unter einer **Komplexitätsfunktion** *sei eine beliebige zahlentheoretische Funktion* $t\colon \mathbb{N}_0 \to \mathbb{R}_0^+$ *verstanden.*
Sei im weiteren nun $t\colon \mathbb{N}_0 \to \mathbb{R}_0^+$ *eine beliebige Komplexitätsfunktion.*
Von besonderem Interesse sind oft die folgenden, sich von t *herleitenden Mengen von Komplexitätsfunktionen*[24]*:*

$\boldsymbol{CON} := O(\mathbf{1})$	konstant
$\boldsymbol{Lin(t)} := \Theta(\mathrm{id})$	linear
$\boldsymbol{Pol(t)} := \bigcup_{k\in\mathbb{N}} O(t^k)$	polynomial
$\boldsymbol{Log(t)} := \Theta(\log t)$	logarithmisch
$\boldsymbol{LLog(t)} := \Theta(\log(\log t))$	zweifach logarithmisch
$\boldsymbol{PLog(t)} := Pol(Log(t))$	polynomial logarithmisch
$\boldsymbol{ExL(t)} := exp(\Theta(t))$	exponentiell linear
$\boldsymbol{ExP(t)} := exp(Pol(t))$	exponentiell
$\boldsymbol{EPLog(t)} := exp(PLog(t))$	exponentiell polylogarithmisch
$\boldsymbol{EExL(t)} := exp(exp(\Theta(t)))$	doppelt exponentiell linear
$\boldsymbol{EExP(t)} := exp(exp(Pol(t)))$	doppelt exponentiell polynomial

Bezüglich der häufig vorkommenden Identitätsfunktion id schreibt man als Abkürzung für $Lin(id)$ *auch* $\boldsymbol{LIN}$*, für* $Pol(id)$ *auch* $\boldsymbol{POL}$ *und gelangt auf analoge Weise ebenso zu Festsetzungen für* $\boldsymbol{LOG}$, $\boldsymbol{PLOG}$, $\boldsymbol{LLOG}$, $\boldsymbol{EPLOG}$, $\boldsymbol{EXL}$, $\boldsymbol{EXP}$, $\boldsymbol{EEXL}$ *und* $\boldsymbol{EEXP}$.

[24] Bei der Festlegung dieser Mengen unter Verwendung früherer Definitionen werden—wie auch in [Rei90]—für Funktionen $f\colon \mathbb{N}_0 \to \mathbb{R}_0^+$ und Funktionenmengen $\mathcal{G} \subseteq \mathbb{R}_0^{+\mathbb{N}_0}$ an einigen Stellen unausgesprochen natürliche Setzungen der Gestalt $f(\mathcal{G}) := \{f(g)/g \in \mathcal{G}\}$ benutzt.

1.4 IOTM-Turingmaschinen als Berechnungsmodelle in der Komplexitätstheorie

Das in der Komplexitätstheorie am weitesten verbreitete Berechnungsmodell ist das der Turingmaschine, wobei aber viele verschiedene Varianten dieser Maschine betrachtet werden. Der Grund dafür, daß hauptsächlich nur dieses Modell verwendet wird, liegt einerseits in seiner Einfachheit und Anschaulichkeit und andererseits darin, daß sich die schwierigsten (und vielfach noch ungelösten) Fragestellungen der Komplexitätstheorie besonders gut in der Bezugnahme auf Klassen von Turingmaschinen formulieren lassen. Als ein weiterer dafür entscheidender Grund kommt noch hinzu, daß viele interessante komplexitätstheoretische Fragen Problemkomplexitäten betreffen, die viel höher sind als der Aufwand, der zur Übertragung eines Verfahrens von einer Turingmaschine auf eine Maschine eines anderen „vernünftigen" Maschinenmodells (entsprechend vergleichbaren Typs) oder umgekehrt nötig ist. Diese Aussage ist im Lichte der sog. INVARIANZ-THESE zu verstehen, die besagt: *„Sinnvolle" Maschinen können einander gegenseitig mit einer polynomial-Zeit-beschränkten Erhöhung der Rechenzeit und einer linear-beschränkten Erhöhung des Speicherplatzbedarfes simulieren*[25]. Viele interessante Komplexitätsklassen sind nun aber gegenüber polynomial-Zeit- *und* linear-Speicherplatz-beschränkten Transformationen abgeschlossen.

Als Präzisierung eines Turingmaschinen-Modells seien hier im folgenden IOTM's (*input-output-Turingmaschinen*) beschrieben, das sind Turingmaschinen mit einem Eingabeband, von dem nur gelesen wird, einem Ausgabeband, auf das nur geschrieben wird und einem oder mehreren Arbeitsbändern (alle Bänder sind einseitig, rechtsseitig unendlich). Für diese Turingmaschinen kann der zur Lösung eines Problems nötige Aufwand besonders gut analysiert werden.

Die *Länge* einer Berechnung einer IOTM M bei Eingabe w ist die Anzahl der Schritte in der Berechnung; der von einer Berechnung erforderte *Speicherplatz* bei Eingabe x ist die Gesamtanzahl der während der Berechnung auf einem der Arbeitsbänder aufgesuchten Bandkästchen. Die von einer Berechnung produzierte *Ausgabe* ist das am Ende der Berechnung auf dem Ausgabeband stehende, nicht mit dem Leersymbol # (Blank) endende, nach rechts hin aber von unendlich vielen Blanks begrenzte Wort.

Da also in den Speicherplatzbedarf einer von einer IOTM ausgeführten Berechnung die für die Eingabe und die Ausgabe (auf dem Eingabe- bzw. dem Ausgabeband) verwendeten Bandkästchen nicht eingerechnet werden, ist es möglich, daß eine IOTM eine Sprache L

[25] "INVARIANCE THESIS: *"Reasonable" machines can simulate each other within a polynomially bounded overhead in time and a constant-factor overhead in space."* (zitiert aus: [vEB90]; dort finden sich außerdem einige Bemerkungen über den möglichen Bereich der Gültigkeit dieser Aussage sowie über den Zusammenhang mit der sog. PARALLEL COMPUTATION THESIS: "Whatever can be solved in polynomially bounded space on a reasonable sequential machine can be solved in polynomially bounded time on a reasonable parallel machine, and vice versa.").

oder eine Funktion f mit sub-linear (z.B. logarithmisch) begrenztem Speicherplatz akzeptiert bzw. berechnet. Dadurch können sehr feine Unterschiede der Berechnungskomplexität von Problemen untersucht werden.

Die hier besprochenen Begriffe sollen im folgenden formal dargestellt werden:

Definition 1.4.1. IOTM–Maschinen.
Eine IOTM M ist ein 10-Tupel $M = (k, Q, \Sigma, \Gamma, \Delta, \delta, q_0, \$, \#, F)$ wobei die auftretenden Bezeichungen folgende Bedeutung haben:

- k ... *Anzahl der Arbeitsbänder*
- Q ... *endliche Menge von Zuständen*
- Σ ... *endliches Eingabealphabet ($\$ \notin \Sigma$)*
- Γ ... *endliches Alphabet für die Arbeitsbänder ($\# \in \Gamma$)*
- Δ ... *endliches Ausgabealphabet ($\#$, "`don't_print_output`"$\notin \Delta$)*
- δ ... *Übergangsrelation, es gilt:*

$$\delta \subseteq \big((Q \backslash F) \times (\Sigma \cup \{\$\}) \times \Gamma^k\big) \times \big(Q \times \{\texttt{left}, \texttt{right}, \texttt{stay}\} \times (\Gamma \times \{\texttt{left}, \texttt{right}\})^k \times ((\Delta \cup \{\#, \text{“}\texttt{don't\_print\_output}\text{”}\}) \times \{\texttt{right}, \texttt{stay}\})\big)$$

- q_0 ... *Anfangszustand*
- $\$$ ... *Anfangs- und Endmarkierung für die Eingabe*
- $\#$ ... *Leersymbol*
- F ... *Menge von Endzuständen ($F \subseteq Q$)*

(Das Symbol $\$$ dient zur Markierung des Eingabewortes w auf beiden Seiten, auf dem Eingabeband steht bei Eingabe w damit zu jedem Zeitpunkt $\$w\$$ und der Bereich dieses Wortes wird während einer Berechnung nie verlassen.)

Eine IOTM heißt **deterministisch**, *wenn sich die Übergangsrelation δ als (möglicherweise partielle)* **Übergangsfunktion**

$$\delta\colon\ \big((Q \backslash F) \times (\Sigma \cup \{\$\}) \times \Gamma^k\big) \to \big(Q \times \dots\big)$$

auffassen läßt, andernfalls **nichtdeterministisch**.

Ein **Zug** *von M besteht im Lesen eines Symbols vom Eingabeband, im Lesen je eines Symbols von einem der Arbeitsbänder, dem Schreiben eines Symbols auf je eines der Arbeitsbänder, dem Bewegen des Schreib-Lese-Kopfes (SLK) auf jedem der Arbeitsbänder auf ein benachbartes Bandkästchen und möglicherweise dem Bewegen des SLKes um ein Bandkästchen auf dem Eingabeband nach rechts oder links sowie (ebenfalls: möglicherweise) dem Schreiben eines Symbols und dem Nach-rechts-Bewegen des SLKes auf dem Ausgabeband und schließlich noch im Übergang in einen neuen (inneren Maschinen-)Zustand— alles in einer durch die Übergangsfunktion δ bestimmten Weise.*

Definition 1.4.2. Konfigurationen.

Eine **Konfiguration** *einer IOTM M ist ein Element aus der Menge*

$$C_M = Q \times \$\Sigma^*\$ \times \left(\Gamma^*(\Gamma \setminus \{\#\}) \cup \{\epsilon\}\right)^k \times \left((\Delta \cup \{\#\})^*\Delta \cup \{\epsilon\}\right) \times \mathbb{N}_0^{k+2}$$

(ϵ das Leerwort) und kann die Beschreibung des augenblicklichen Arbeitszustandes von M während einer Berechnung sein, eine Beschreibung, die den augenblicklichen Zustand, indem sich die Maschine befindet, den Inhalt des Eingabebandes, den Inhalt der Arbeitsbänder und des Ausgabebandes (als jene Wörter, die nicht mit dem Leersymbol enden, nach rechts hin aber durch unendlich viele folgende Leersymbole begrenzt sind) sowie die Positionen der SLKe auf den Bändern zum betrachteten Zeitpunkt beinhält bzw. beschreibt.

Wenn in einer Konfiguration α ein Endzustand $q \in F$ auftritt, so ist α eine **Endkonfiguration**. *Die* **Anfangskonfiguration $\sigma_M(x)$ für ein Eingabewort** $x \in \Sigma^*$ *ist*

$$\sigma_M(x) = (q_0, \$x\$, \underbrace{\epsilon, \ldots, \epsilon}_{k+1}, \underbrace{0, \ldots, 0}_{k+2}) \,.$$

Definition 1.4.3. Berechnungspfade, von IOTM's erhaltene Ausgabe.

Für eine gegebene IOTM M und zwei Konfigurationen α, β von M schreibt man $\alpha \vdash_M \beta$ („β ist der **Nachfolger** *von α“ bzw. „β ist (eine)* **Nachfolge-Konfiguration** *von α“) genau dann, wenn die Konfiguration β aus der Konfiguration α in einem Zug von M entsteht.*

Der reflexive und transitive Abschluß der Relation $\vdash_M$ sei $\vdash_M^*$; der transitive Abschluß von $\vdash_M$ sei $\vdash_M^+$.

Für $l \in \mathbb{N}_0$ bedeute $\alpha \vdash_M^{(l)} \beta$, daß es Konfigurationen $\alpha_0, \alpha_1, \ldots, \alpha_l$ mit $\alpha_0 = \alpha$ und $\alpha_0 \vdash_M \alpha_1 \vdash_M \alpha_2 \vdash_M \ldots \vdash_M \alpha_l$ und $\alpha_l = \beta$ gibt.

Ein **Berechungspfad** *C von M für Eingabewort $x \in \Sigma^*$ ist eine endliche Folge $C = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ ($n \in \mathbb{N}_0$) von Konfigurationen mit $\alpha_0 = \sigma_M(x)$ sowie mit $\alpha_0 \vdash_M \alpha_1 \vdash_M \alpha_2 \vdash_M \ldots \vdash_M \alpha_n$; n ist seine* **Länge**.

Ein **akzeptierender Berechnungspfad** *C von M* **für Eingabewort** $x \in \Sigma^*$ *ist ein Berechnungspfad von M für Eingabewort x, dessen letzte Konfiguration eine Endkonfiguration ist.*

Ein akzeptierender Berechnungspfad $C = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ ($n \in \mathbb{N}_0$) von M für Eingabewort $x \in \Sigma^*$ **erhält Ausgabe** *$w \in (\Delta \cup \{\#\})^*$ genau dann, wenn w der in α_n dargestellte Inhalt des Ausgabebandes ist.*

Ein Berechnungspfad $C_1 = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ heißt ein **Teilpfad** *eines anderen Berechnungspfades $C_2 = (\beta_0, \beta_1, \ldots, \beta_m)$, falls $n \leq m$ und $\alpha_0 = \beta_0, \ldots, \alpha_n = \beta_n$.*

Definition 1.4.4. Von einer IOTM akzeptierte Sprachen bzw. berechnete Funktionen.

M sei eine IOTM mit Eingabealphabet Σ und Ausgabealphabet Δ;
$f\colon \Sigma^* \to \Delta^*$ sei eine Funktion, weiters sei $x \in \Sigma^*$. Dann sei definiert:

(i) M **akzeptiert** x : $\iff$ *es gibt einen akz. Berechnungspfad von M für Eing.wort x.*

(ii) Die von M **akzeptierte Sprache** *$L(M)$ sei durch die Festsetzung*
$L(M) := \{x \in \Sigma^* / M \text{ akzeptiert } x\}$
gegeben.

(iii) M sei im besonderen eine deterministische IOTM.

M **berechnet die Funktion** f : $\iff$

$\iff$ $(\forall x \in \Sigma^*)$ $\big(M$ *akzeptiert x und der (dann eindeutig existierende) Berechnungspfad C von M für Eingabewort x erhält Ausgabe $f(x)\big)$*

Für nichtdeterministische IOTM's kann eine Definition einer von M „berechneten" Funktion $f\colon \Sigma^* \to \Delta^*$ wegen der möglichen Vielzahl von für ein Eingabewort $x \in \Sigma^*$ existierenden akzeptierenden Berechnungspfaden C und der dementsprechend weiters vorstellbaren Vielzahl von durch solche Berechnungspfade C erhaltenen Ausgaben nicht auf eine direkte und einheitliche Weise erfolgen, sondern erfordert die weitere Voraussetzung zusätzlicher einschränkender Bedingungen. In der Wahl solcher Bedingungen bestehen jedoch mannigfache Freiheiten und solcherart verschieden durchgeführte Festsetzungen führen auf Begriffe und Komplexitätsklassen von durch nichtdeterministische IOTM's berechnete Funktionen mit sehr unterschiedlichen Eigenschaften bzw. unterschiedlicher Größe. Eine in den hier betrachteten Zusammenhängen der Untersuchung der Entscheidungskomplexität von entscheidbaren Theorien sinnvolle Möglichkeit könnte etwa in der Festsetzung für eine IOTM M (mit Eingabealphabet Σ und Ausgabealphabet Δ) und eine Funktion $f\colon \Sigma^* \to \Delta^*$ der Form

$$\begin{aligned} &M \text{ berechnet die Funktion } f\colon \iff \\ &\iff (\forall x \in \Sigma^*)\,(\exists C \text{ akz. Ber.pfad von } M \text{ für Eing.wort } x) \\ &\qquad (\ C \text{ erhält Ausgabe } f(x)\ ) \ \& \\ &\qquad \& \ (\forall C \text{ akz. Ber.pfad von } M \text{ für Eing.wort } x) \\ &\qquad\quad (\ C \text{ erhält Ausgabe } f(x)\ ) \end{aligned} \tag{1.4}$$

bestehen. (Eine andere und einschränkendere Möglichkeit hätte in der Forderung nach der eindeutigen Existenz von akzeptierenden Berechnungspfaden liegen können; diese führt

aber—sehr wahrscheinlich—oftmals auf kleinere Komplexitätsklassen von durch nichtdeterministische IOTM's berechnete Funktionen.)

Die Länge einer Berechnung und der von einer Berechnung beanspruchte Speicherplatz seien wie folgt festgesetzt:

Definition 1.4.5. Berechnungslängen, Speicherplatzbedarf einer IOTM.
Sei M ine IOTM, $w \in \Sigma^*$, C eine Berechnung von M auf Eingabe w. Die **Länge** *von C wird mit $|C|$ geschrieben und sei gleich n, falls $C = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ $(n \in \mathbb{N}_0)$. Der* **Speicherplatzbedarf** *$SP(C)$ von C sei als die Gesamtanzahl der während C mindestens einmal aufgesuchten Bandkästchen auf einem der Arbeitsbänder definiert.*

Davon ausgehend können Rechenzeit- und Speicherplatzbedarfsfunktionen abhängig von der Länge des Eingabewortes definiert werden.

Definition 1.4.6. Rechenzeit- und Speicherplatzbedarfs-Funktionen.
Sei M eine IOTM, Σ ihr Eingabealphabet.
Dann seien die Rechenzeitfunktion $Min-RZ_M$ sowie die Speicherplatzbedarfsfunktion $Min-SP_M$ wie folgt definiert:

$$Min-RZ_M \colon \Sigma^* \to \mathbb{N}_0 \cup \{\perp\}$$

$$x \mapsto Min-RZ_M(x) := \begin{cases} \perp & \ldots M \text{ akzeptiert } x \text{ nicht} \\ \min\{|C| \ / \ C \text{ ist akz. Ber.pfad von } M \text{ auf } x\} & \\ & \ldots M \text{ akzeptiert } x \end{cases}$$

$$Min-SP_M \colon \Sigma^* \to \mathbb{N}_0 \cup \{\perp\}$$

$$x \mapsto Min-SP_M(x) := \begin{cases} \perp & \ldots M \text{ akzeptiert } x \text{ nicht} \\ \min\{SP(C) \ / \ C \text{ ist akz. Ber.pfad von } M \text{ auf } x\} & \\ & \ldots M \text{ akzeptiert } x \end{cases}$$

Im Fall, daß M eine deterministische IOTM ist, werden statt $Min-RZ_M$ und $Min-SP_M$ vorwiegend die Rechenzeitfunktion RZ_M und die Speicherplatzbedarfsfunktion SP_M definiert durch:

$$RZ_M : \Sigma^* \to \mathbb{N}_0 \cup \{\perp\} \qquad SP_M : \Sigma^* \to \mathbb{N}_0 \cup \{\perp\}$$
$$x \mapsto RZ_M(x) := Min-RZ_M(x) \qquad x \mapsto SP_M(x) := Min-SP_M(x)$$

verwendet (um der Tatsache Rechnung zu tragen, daß ein akzeptierender Berechnungspfad für ein gegebenes Eingabewort—falls ein solcher existiert—dann immer eindeutig vorliegt.)

An dieser Stelle soll darauf hingewiesen werden, daß in einigen Büchern über Komplexitätstheorie Rechenzeit- und Speicherplatzfunktionen anders und nur für eine eingeschränkte Maschinenklasse definiert werden. Und zwar werden dort die Funktionen RZ_M

und SP_M auch für nichtdeterministische Maschinen M erklärt und zwar als:

$$RZ_M(x) := \max\{|C| \,/ C \text{ ist Berechnungspfad von } M \text{ für Eingabewort } x\}$$
$$SP_M(x) := \max\{SP(C)/C \text{ ist Berechnungspfad von } M \text{ für Eingabewort } x\}$$
$$(x \text{ ein zulässiges Eingabewort})$$

Eine solche Definition ist aber nur unter der zusätzlichen, an M zu richtenden Bedingung sinnvoll-möglich, daß für alle Eingabewörter x der „Berechnungsbaum“ aller Berechnungspfade von M auf Eingabe x endlich ist (damit die Maximumsbildung durchgeführt werden kann) bzw. (was im Lichte des Lemmas von König dasselbe bedeutet), daß es keinen unendlichen Berechnungspfad C von M auf Eingabewort x gibt (d.i. keine unendliche Konfigurationenfolge $C = (\alpha_0, \alpha_1, \alpha_2, \dots)$ mit $\sigma_M(x) = \alpha_0 \vdash_M \alpha_1 \vdash_M \alpha_2 \vdash_M \dots$). – Diese Forderung an die zu betrachtenden Turingmaschinen schränkt die zur Problemlösung in Frage kommende Maschinenklasse zwar ein, in Beziehung zu den in der Komplexitätstheorie vornehmlich untersuchten Problemen (welchen entscheidbare Sprachen zugrundeliegen) allerdings nur in unwesentlichen Maß. Die bezüglich solchen Maschinen definierten Komplexitätsklassen entsprechen außerdem in den allermeisten Fällen ziemlich direkt den hier im folgenden unter Zugrundelegung von Definition 1.4.6 definierten.

Diese geänderten Definitionen und Setzungen werden hierher allerdings nicht übernommen, da die Konstruktion von IOTM's der eingeschränkten Klasse zumeist schon die Kenntnis über Aufwandsschranken (im hier definierten Sinn) für hier definierte IOTM's erfordern und also zusätzliche Überlegungen sind, die das Wesen nichtdeterministischer Berechnungen auch verschleiern könnten (wenn die Zusammenhänge nicht immer vollständig mitbedacht würden).

Ausgehend von den in Definition 1.4.6 definierten Rechenzeit- und Speicherplatzbedarfsfunktionen kann nun gefragt werden, in welcher Weise der zum Akzeptieren einer Sprache oder der Berechnung einer Funktion nötige Rechenzeit- oder Speicherplatz-Aufwand einer IOTM abhängig von der Eingabelänge durch eine Schrankenfunktion begrenzt werden kann. Das führt auf die folgende Definition:

Definition 1.4.7. Rechenzeit- und Speicherplatzschranken für IOTM's.
Σ, Δ endliche Alphabete, $L \subseteq \Sigma^*$ eine Sprache, $f\colon \Sigma^* \to \Delta^*$, M eine IOTM mit Eingabealphabet Σ und Ausgabealphabet Δ, $s, t\colon \mathbb{N}_0 \to \mathbb{R}_0^+$ Funktionen.

(i) M akzeptiert L **mit Rechenzeitschranke** *$t(n)$:* $\iff$

$$\iff L(M) = L \;\&\; (\forall \textit{ bis auf endlich viele } x \in L)$$
$$(\, Min\text{-}RZ_M(x) \leq t(|x|)\,);$$

M akzeptiert L **mit Speicherplatzschranke** *$t(n)$:* $\iff$

$$\iff L(M) = L \;\&\; (\forall \textit{ bis auf endlich viele } x \in L) \\ (\, Min\text{-}SP_M(x) \leq t(|x|)\,)\,;$$

M akzeptiert L **mit Rechenzeitschranke** $t(n)$ **und mit Speicherplatzschranke** $s(n)$*:* $\iff$

$$\iff L(M) = L \;\& \\ \&\; (\forall \textit{ bis auf endlich viele } x \in L)(\exists \textit{akz. Ber. } C \textit{ von } M \textit{ auf } x) \\ \big(\,|C| \leq t(|x|) \;\&\; SP(C) \leq s(|x|)\,\big)$$

(ii) M sei eine deterministische IOTM.
M berechnet f **mit Rechenzeitschranke** $t(n)$*:* $\iff$

$$\iff M \textit{ berechnet } f \;\&\; (\forall \textit{ bis auf endlich viele } x \in \Sigma^*) \\ (\, Min\text{-}RZ_M(x) \leq t(|x|)\,)\,;$$

daraus ergeben sich analog zu (i) Definitionen für
„ ... **mit Speicherplatzschranke** $s(n)$“, „ ... **mit Rechenzeitschranke** $t(n)$ **und mit Speicherplatzschranke** $s(n)$“.

(iii) Die in (i) und (ii) definierten Rechenzeit- und Speicherplatzfunktionen werden (jeweils) **strikte Rechenzeit-** *und* **strikte Speicherplatzschranken** *genannt, falls die in (i) und (ii) für die Abschätzung des Rechenzeit- bzw. Speicherplatzbedarfsaufwandes einer IOTM verwendeten,* für fast alle *Werte* $x \in L$ *bzw.* $x \in \Sigma^*$ *gültigen* $\leq$*-Ungleichungen durch* für alle $x \in L$ *bzw.* $x \in \Sigma^*$ *gültige* $\leq$*-Ungleichungen ersetzt werden.*

Analog zur Definition in (ii) könnten nun auch bzgl. der Festsetzung (1.4) einer von einer nichtdeterministischen IOTM M berechneten Funktion $f\colon \Sigma^* \to \Delta^*$ Rechenzeitschranken $t(n)$ und Speicherplatzschranken $s(n)$ bzw. gleichzeitig gültige Rechenzeitschranken $t(n)$ und Speicherplatzschranken $s(n)$ für die Berechnung von f durch M erklärt werden.

Mit Hilfe der Bezeichnungen aus Definition 1.4.7 lassen sich nun *Komplexitätsklassen* von Sprachen und Funktionen definieren, und zwar jeweils als eine Gesamtheit aller Sprachen bzw. Funktionen, die zu einer vorgegebenen Schrankenfunktion von einer IOTM mit durch diese Funktion beschränktem (bzw. strikt beschränktem) (Rechenzeit- oder Speicherplatz- oder Rechenzeit- *und* Speicherplatz-) Aufwand akzeptiert bzw. berechnet werden können.

Definition 1.4.8. IOTM-Komplexitätsklassen.
Seien $s, t\colon \mathbb{N}_0 \to \mathbb{R}_0^+$ *Funktionen.*

(i) Es gelten folgende Bezeichnungen für Komplexitätsklassen von Sprachen bezüglich IOTM's:

$$\begin{aligned}\boldsymbol{DTime(t(n))} := \{L/(\exists\Sigma\ &\textit{endl.Alph.})\\ &(\exists\ \textit{det. IOTM } M\ \textit{mit Eing.alph. } \Sigma)\\ &\quad(L \subseteq \Sigma^*\ \&\ M\ \textit{akzeptiert } L\\ &\qquad\textit{mit Rechenzeitschranke } t(n))\};\end{aligned}$$

$$\begin{aligned}\boldsymbol{NTime(t(n))} := \{L/(\exists\Sigma\ &\textit{endl.Alph.})\\ &(\exists\ \textit{IOTM } M\ \textit{mit Eing.alph. } \Sigma)\\ &\quad(L \subseteq \Sigma^*\ \&\ M\ \textit{akzeptiert } L\\ &\qquad\textit{mit Rechenzeitschranke } t(n))\};\end{aligned}$$

$$\begin{aligned}\boldsymbol{DTimeSpace(t(n), s(n))} := &\\ \{L/(\exists\Sigma\ &\textit{endl.Alph.})(\exists\ \textit{det. IOTM } M\ \textit{mit Eing.alph. } \Sigma)\\ &\big(L \subseteq \Sigma^*\ \&\ M\ \textit{akzeptiert } L\\ &\quad\textit{mit Rechenzeitschranke } t(n)\\ &\quad\textit{und mit Speicherplatzschranke } s(n)\big)\}.\end{aligned}$$

Analog dazu seien auch die Komplexitätsklassen $\boldsymbol{DSpace(s(n))}$, $\boldsymbol{NSpace(s(n))}$ *und* $\boldsymbol{NTimeSpace(t(n), s(n))}$ *definitorisch festgesetzt. Will man das der Sprache zugrundeliegende Alphabet* Σ *hervorheben, so sei dazu weiters noch z.B.*

$$\boldsymbol{DTime_\Sigma(t(n))} := \{L \subseteq \Sigma^*/(\exists\ \textit{det. IOTM } M)\ (M\ \textit{akz. } L\ \textit{mit Rz.schr. } t(n))\}\ ^{26}$$

festgesetzt (ähnliches in allen anderen Fällen).

[26] Da in diesem Fall ein Alphabet Σ fixiert ist, handelt es sich um eine (Komplexitäts-) Menge von Sprachen über dem Alphabet Σ.

(ii) Es gelten folgende Bezeichnungen für Komplexitätsklassen von berechenbaren Funktionen:

$$\boldsymbol{DFTime(t(n))} := \{f/(\exists\ \Sigma, \Delta\ \textit{endl. Alphabete})\ (\exists\ \textit{det. IOTM } M \textit{ mit Eing.alph. } \Sigma \textit{ und Ausg.alph. } \Delta)\ (M \textit{ berechnet } f\colon \Delta^* \to \Sigma^* \textit{ mit Rechenzeitschranke } t(n))\}$$

Auf zu den Definitionen in (i) und (ii) analoge Weise seien nun auch die Komplexitätsklassen $\boldsymbol{DFSpace(s(n))}$, $\boldsymbol{DFTimeSpace(t(n), s(n))}$, *sowie die Komplexitätsmengen* $\boldsymbol{DFTime_{\Sigma,\Delta}(t(n))}$, $\boldsymbol{DFSpace_{\Sigma,\Delta}(s(n))}$ *und* $\boldsymbol{DFTimeSpace_{\Sigma,\Delta}(t(n), s(n))}$ *(für endliche Alphabete* Σ,Δ*) festgesetzt.*

(iii) Analog zu (i) und (ii) seien die Komplexitätsklassen $\boldsymbol{DTime^*(t(n))}$, $\boldsymbol{DSpace^*(s(n))}$, ... , $\boldsymbol{DFTime^*(t(n))}$, ... *etc. bezüglich strikter Rechenzeit- bzw. Speicherplatzschranken* $t(n)$ *bzw.* $s(n)$ *definiert.*

(iv) Im folgenden werden auch bezüglich Funktionenmengen (von Schrankenfunktionen) definierte Komplexitätsklassen verwendet. Für eine Menge $\mathcal{G} \subseteq \mathbb{N}_0^{\mathbb{R}_0^+}$ *von Funktionen sei bezüglich der Rechenzeit deterministischer IOTM's beispielsweise die Komplexitätsklasse*

$$\boldsymbol{DTime(\mathcal{G})} := \bigcup_{g\in\mathcal{G}} DTime(g)$$

definiert; ähnliche Setzungen seien aber auch bezüglich aller anderen bisher festgelegten Arten von Komplexitätsklassen vereinbart.

Analog zur Festsetzung in Definition 1.4.8 könnten an dieser Stelle abhängig von den hier früher erfolgten Setzungen für von einer nichtdeterministischen IOTM berechneten Funktionen sowie von Schrankenfunktionen dafür nun etwa auch Komplexitätsklassen $NFTime(t(n))$, $NFSpace(s(n))$ sowie auch $NFTimeSpace(t(n), s(n))$ für Schrankenfunktionen $t, s\colon \mathbb{N}_0 \to \mathbb{R}_0^+$ definiert werden, $NFTime(t(n))$ z.B. analog zu $DFTime(t(n))$ durch

$$\boldsymbol{NFTime(t(n))} := \{f/(\exists\ \Sigma, \Delta \text{ endl. Alphabete})\ (\exists \text{ IOTM } M \text{ mit Eing.alph. } \Sigma \text{ und Ausg.alph. } \Delta)\ (M \text{ berechnet } f\colon \Delta^* \to \Sigma^* \text{ mit R.z.schranke } t(n))\}.$$

Die Verwendung solcher Komplexitätsklassen wird hier jedoch—außer an einer Stelle im folgenden zur Begründung einer die Entscheidungskomplexität von entscheidbaren Theorien betreffenden Definition—vermieden und umgangen werden (hauptsächlich deshalb, weil

diese in der Komplexitätstheorie eher nicht gebräuchlich und v.a. auch nicht standardisiert sind).

In einigen später behandelten Komplexitätsaussagen kommen die Komplexitätsklassen $\boldsymbol{ATime(t(n))}$, $\boldsymbol{ASpace(s(n))}$ und $\boldsymbol{ATimeAlter(t(n), a(n))}$ bezüglich alternierender Turingmaschinen vor. Für eine Definition alternierender Turingmaschinen und dieser Klassen von durch solche Maschinen (Rechen-)Zeit-beschränkt, Speicherplatz-beschränkt bzw. Rechenzeit- und Alternationen-beschränkt erkennbaren Sprachen sei auf [Rei90] oder auf die grundlegende Arbeit von A. Chandra, D. Kozen und D. Stockmeyer [CKS81] mit dem Titel "Alternation" verwiesen.

Komplexitätsklassen bezüglich fast überall gültigen und strikten Schrankenfunktionen sind in vielen Fällen gleich; so gilt z.B. jedenfalls

$$DSpace(s(n)) = DSpace^*(s(n))$$

für alle Schranken $s\colon \mathbb{N}_0 \to \mathbb{N}_0$ mit $s(n) \geq 1$ $(n \in \mathbb{N}_0)$, und

$$DTime(t(n)) = DTime^*(t(n))$$

für alle Zeitschranken $t\colon \mathbb{N}_0 \to \mathbb{N}_0$ mit $t(n) \geq n+1$ $(n \in \mathbb{N}_0)$ und $\liminf_{n\to\infty} \frac{t(n)}{n} = \infty$ [27].

Die Bezeichnungen für fast überall gültige bzw. strikte Schrankenfunktionen und gesonderte Komplexitätsklassen bzgl. beider Begriffe wurden hier deshalb definiert, weil in der Literatur beide Wege der Definition auftreten und sich bestimmte kleinere Unterschiede zwischen diesen Begriffen u.U. dort ergeben, wo entsprechende Simulationsresultate nicht angewendet werden können. So ist für manche in Kapitel 3 angestellte Überlegungen die Verwendung von Komplexitätsklassen bzgl. strikter Schrankenfunktionen nötig.

[27] Diese Aussagen folgen (z.B.) sofort aus einem Band-Kompressions-Satz und einem Satz über die lineare Beschleunigung von Turingmaschinen in [HoUl79] ("tape compression" in Theorem 12.2, p. 288; "linear speed up" in Theorem 12.3, p. 290).

1.5 Obere und untere Schranken für die Entscheidungskomplexität entscheidbarer logischer Theorien

IOTM's können auf verschiedene Weise zur Lösung von wie früher abstrakt definierten Problemen herangezogen werden. Da für jedes Problem X nach Definition 1.3.2 zu jeder Instanz $I \in \{0,1\}^*$ jedenfalls eine Antwort A existiert, besitzt X jedenfalls ein funktionales Teilproblem X'. Ein funktionales Problem X' kann nun von einer IOTM M dadurch gelöst werden, daß M jene Funktion $f\colon \{0,1\}^* \to \{0,1\}^*$ berechnet, die jeder Instanz I die zugehörige Antwort A zuweist. Ein Entscheidungs-Problem kann demgemäß von einer IOTM M dadurch gelöst werden, daß M die Funktion $f\colon \{0,1\}^* \to \{a_{\mathtt{J}}, a_{\mathtt{N}}\}$ mit $a_{\mathtt{J}}, a_{\mathtt{N}} \in \{0,1\}^*$ berechnet, wobei $a_{\mathtt{J}}, a_{\mathtt{N}}$ jene Antwort-Zeichenketten sind, die den Antworten „`Ja`“ und „`Nein`“ entsprechen und f jeder Instanz I genau die Antwort $a_{\mathtt{J}}$ oder $a_{\mathtt{N}}$ in Übereinstimmung mit der Definition von X' zuweist.

Auf eingeschränkte Weise können Entscheidungs-Probleme X von IOTM's (bzw. von Mehrbandturingmaschinen, die IOTM's ohne Ausgabeband entsprechen) dadurch gelöst werden, daß M die—wie früher definierte—Sprache $L(X)$ akzeptiert. In diesem Fall kann für ein $I_1 \in \{0,1\}^*$ nur die Antwort „`Ja`“ erzielt werden, und zwar dann und damit, daß festgestellt wird, daß M die Instanz I_1 akzeptiert (also im Fall von $I_1 \in L(X) = \{I \in \{0,1\}^* / (I, \text{“}\mathtt{Ja}\text{”}) \in X\}$). Falls $I_1 \notin L(X)$, erfolgt keine Antwort.

Vollständig könnte ein Entscheidungsproblem X auf diese Weise nur dadurch gelöst werden, daß zwei Maschinen M_1 und M_2 existieren, wobei M_1 die Sprache $L(X)$ akzeptiert und M_2 die Sprache $\text{co}-L(X)$; denn unter solchen Umständen könnten für eine beliebige Instanz I die Maschinen M_1 und M_2 parallel betrieben oder ausgeführt werden und es könnte jedenfalls nach endlich vielen Schritten festgestellt werden, ob $I \in L(X)$ (falls M_1 die Instanz I akzeptiert) oder $I \notin L(X)$ (falls M_2 die Instanz I akzeptiert) gilt, und davon abhängig könnte dann die Antwort „`Ja`“ oder „`Nein`“ erzielt bzw. gegeben werden.

Eine derartige Aufspaltung der Lösung eines Entscheidungs-Problems zur Betrachtung der Lösung zweier Teilprobleme spielt v.a. bei der Untersuchung der Komplexität eines Entscheidungs-Problems bezüglich der Verwendung von nichtdeterministischen Turingmaschinen bzw. IOTM's eine wichtige Rolle (so man nicht von bestimmten, der jeweiligen Problemstellung angemessenen Festsetzungen einer Definition von durch nichtdeterministische IOTM's berechnete Funktionen und dazu entsprechend errichteten Komplexitätsklassen ausgeht.)

Es ist im Fall der Verwendung von Turingmaschinen als Berechnungsmodell allerdings nicht mehr nötig, als Alphabet für Problemstellungen einzig $\{0,1\}$ zuzulassen. Es kann immer von beliebigen endlichen Alphabeten ausgegangen werden. Der Grund dafür liegt darin, daß es lineare-Rechenzeit- und linear-Speicherplatz-beschränkte gegenseitige Simulationen von Turingmaschinen über verschiedenen Bandalphabeten Γ bei gleichem Eingabealphabet Σ gibt (Alphabet-Reduktions-Satz), sodaß sich wesentliche Komplexitätsaus-

sagen für auf die gleiche Weise, aber über verschiedenen Alphabeten formulierte Probleme immer mit höchstens linearer Aufwandserhöhung übertragen lassen.

Das Entscheidungsproblem für eine entscheidbare logische Theorie wurde früher auf zwei Arten, als funktionales Problem und als Entscheidungs-Problem spezifiziert und kann von IOTM's daher wie hier beschrieben—verschieden—gelöst werden. Bezüglich ENTSCHEIDUNGSPROBLEM (1) kommt dabei die Funktion

$$THM_{T^{((M))}} : \Sigma^*_{T^{((M))}} \to \{ \text{“ist\_Theorem\_von\_T”}, \text{“ist\_Formel,\_kein\_Theorem\_T”}, \text{“ist\_keine\_Formel\_von\_T”} \} \tag{1.5}$$

$$x \mapsto \begin{cases} \text{“ist\_Theorem\_von\_T”} & \dots x \in Thm_{T^{((M))}} \\ \text{“ist\_Formel,\_kein\_Theorem\_T”} & \dots x \in Fo_{T^{((M))}} \setminus Thm_{T^{((M))}} \\ \text{“ist\_keine\_Formel”} & \dots x \notin Fo_{T^{((M))}} \end{cases}$$

für $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ ins Spiel.

Mit diesen Setzungen können nun obere und untere Schranken für die Entscheidungskomplexität von entscheidbaren logischen Theorien so definiert werden:

Definition 1.5.1. Obere und untere Schranken für die Entscheidungskomplexität einer Theorie T bzgl. IOTM-Komplexitätsklassen.

T sei eine entscheidbare Theorie, $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ die Theorie als formales System mit informatisch-sinnvoller Formelsyntax; $t, s : \mathbb{N}_0 \to \mathbb{N}_0$ Funktionen.

(i) **$t(n)$** *ist eine* **obere Schranke für die Entscheidungskomplexität von T bzgl. deterministischer [nichtdeterministischer][28] IOTM-Rechenzeit** *:* $\Longleftrightarrow$

$\Longleftrightarrow$ $THM_{T^{((M))}} \in DFTime(t(n))$
$[Thm_{T^{((M))}} \in NTime(t(n))$ & co$-Thm_{T^{((M))}} \in NTime(t(n))]$;

$s(n)$ *ist eine* **obere Schranke für die Entscheidungskomplexität von T bzgl. deterministischem [nichtdeterministischem] IOTM-Speicherplatz***:* $\Longleftrightarrow$

$\Longleftrightarrow$ $THM_{T^{((M))}} \in DFSpace(s(n))$
$[Thm_{T^{((M))}} \in NSpace(s(n))$ & co$-Thm_{T^{((M))}} \in NSpace(s(n))]$.

Analog können Paare **$(t(n), s(n))$** *als* **obere Schranken der Entscheidungskomplexität von T bzgl. det. [nichtdet.] IOTM-Rechenzeit und** *gleichzeitig betrachtetem* **det. [nichtdet.] IOTM-Speicherplatz** *unter Verwendung der Klasse $DFTimeSpace(t(n), s(n))$ $[NTimeSpace(t(n), s(n))]$ definiert werden.*

[28] Diese Definition ist an verschiedenen Stellen jeweils zweimal zu lesen, einmal ohne den Einschluß [...] in eckigen Klammern und dann noch einmal damit bei gleichzeitiger Weglassung des unmittelbar davorstehendes Ausdrucks (eines Wortes bzw. einer formalen Aussage).

(ii) $\boldsymbol{t(n)}$ *ist eine* **untere Schranke für die Entscheidungskomplexität von** T **bzgl. deterministischer** [**nichtdeterministischer**] **IOTM-Rechenzeit***:* $\Longleftrightarrow$

$$\Longleftrightarrow \quad THM_{T^{((M))}} \notin DFTime(t(n))$$
$$[Thm_{T^{((M))}} \notin NTime(t(n)) \ \vee \ \text{co}-Thm_{T^{((M))}} \notin NTime(t(n))];$$

$\boldsymbol{s(n)}$ *ist eine* **untere Schranke für die Entscheidungskomplexität von** T **bzgl. deterministischem** [**nichtdeterministischem**] **IOTM-Speicherplatz***:* $\Longleftrightarrow$

$$\Longleftrightarrow \quad THM_{T^{((M))}} \notin DFSpace(s(n))$$
$$[Thm_{T^{((M))}} \notin NSpace(s(n)) \ \vee \ \text{co}-Thm_{T^{((M))}} \notin NSpace(s(n))].$$

Erneut können Paare $\boldsymbol{(t(n), s(n))}$ *als* **untere Schranken für die Entscheidungskomplexität von** T **bzgl.** *gleichzeitig betrachteten Komplixitätsmaßen* **IOTM-Rechenzeit und IOTM-Speicherplatz***bedarf analog definiert werden.*

Zur unterschiedlichen Art, in der hier obere und untere Schranken für die Entscheidungskomplexität bezüglich deterministischer bzw. bezüglich nichtdeterministischen Turing- bzw. IOTM-Komplexitätsmaßen definiert wurden, sei hier als Erklärung noch folgende Überlegung nachgestellt: Es wäre in den Fällen, in denen die Entscheidungskomplexität bzgl. der Verwendung nichtdeterministischer IOTM's betrachtet wird, durchaus auch möglich gewesen, die früher angedeuteten Komplexitätsklassen $NFTime(t(n))$, $NFSpace(t(n))$ bzw. $NFTimeSpace(t(n), s(n))$ zu verwenden und im Fall (i) beispielsweise zu setzen:

$$\begin{aligned} &t(n) \text{ ist obere Schranke für die Entscheidungskomplexität} \\ &\text{bzgl. nichtdet. IOTM-Rechenzeit } :\Longleftrightarrow \\ &\Longleftrightarrow \quad THM_{T^{((M))}} \in NFTime(t(n)) \end{aligned} \tag{1.6}$$

Dies wurde hier jedoch v.a. aus dem schon früher erwähnten Grund umgangen, daß diese nichtdeterministische Komplexitätsklassen für die Berechnung von Funktionen in der Komplexitätstheorie keineswegs standardisiert sind. Da jedoch leicht einzusehen ist, daß für alle $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ und Funktionen $t\colon \mathbb{N}_0 \to \mathbb{R}_0^+$

$$\begin{aligned} THM_{T^{((M))}} \in NFTime(t(n)) \ \Longleftrightarrow \ & Thm_{T^{((M))}} \in NTime(t(n)) \ \& \\ & \& \ \text{co}-Thm_{T^{((M))}} \in NTime(t(n)) \end{aligned} \tag{1.7}$$

gilt[29], ist klar, daß eine Festsetzung wie in (1.6) zur entsprechenden Aussage in Definition 1.5.1, (i), äquivalent ist. (Eine analoge Überlegung läßt sich sofort auch für jedes andere

[29](Aus einer (nichtdeterministischen) IOTM M, die $THM_{T^{((M))}}$ mit Rechenzeitschranke $t(n)$ entlang von (1.4) berechnet, lassen sich leicht zwei (nichtdeterministische) Turingmaschinen M_1 und M_2 gewinnen, die $Thm_{T^{((M))}}$ bzw. $\text{co}-Thm_{T^{((M))}}$ mit Rechenzeitschranke $t(n)$ akzeptieren und umgekehrt lassen sich zwei (nichtdeterministische) Turingmaschinen M_1 und M_2, die $Thm_{T^{((M))}}$ bzw. $\text{co}-Thm_{T^{((M))}}$ jeweils mit Rechenzeitschranke $t(n)$ akzeptieren, einfach zur Konstruktion einer (nichtdeterministischen) IOTM M nutzen, die $THM_{T^{((M))}}$ entlang von (1.4) mit Rechenzeitschranke $t(n)$ berechnet.)

Entscheidungs-Problem im Bezug zu dessen Lösung mit Hilfe von nichtdeterministischen IOTM's anstellen.)

Umgekehrt hätten in Definition 1.5.1 im Fall der bezüglich deterministischer IOTM's betrachteten Entscheidungskomplexität statt der Charakterisierung des Aufwands zur Berechnung von $THM_{T((M))}$ wie im nichtdeterministischen Fall auch der Aufwand für die Erkennung von $Thm_{T((M))}$ und von co$-Thm_{T((M))}$ zur Definition verwendet werden können (da (1.7) auch in Beziehung zu den Komplexitätsklassen $DFTime(t(n))$ und $DTime(t(n))$ gilt). Die solcherart abgeänderten Definitionen wären den in Definition 1.5.1 dafür schon erfolgten aber gleichwertig bzw. zu diesen äquivalent.

Obere und untere Schranken für die Entscheidungskomplexität logischer Theorien durch IOTM's sind in Definition 1.5.1 so definiert worden, daß sich die Eigenschaften, obere bzw. untere Schranke zu sein, gegenseitig ausschließen und sogar entgegengesetzte Begriffe sind. Die Aussage, daß eine Funktion $t(n)$ untere Schranke für die Entscheidungskomplexität einer Theorie T ist, daß also $THM_{T((M))} \notin DFTime(t(n))$ gilt, impliziert, daß

$$\begin{array}{l}(\forall M \text{ IOTM, } M \text{ berechnet } THM_{T((M))}) \\ \quad (\exists\ \infty\text{-viele } n \in \mathbb{N}_0 \text{ und } x \in \Sigma_{T((M))}) \\ \qquad \big(|x| = n \ \&\ Min{-}RZ_M(x) > t(n)\big)\end{array} \tag{1.8}$$

gilt, und ist damit etwa mit der früher dargestellten Aussage (1.3) in Verbindung zu bringen.

Die Klassifizierung der Entscheidungskomplexität einer entscheidbaren Theorie T kann mit Hilfe dieser Begriffe nun im Rahmen von IOTM-Komplexitätsklassen geschehen. Es stellt sich dabei aber heraus, daß schon die einfachsten logischen Probleme eine inhärente Komplexität von solcher Größenordnung besitzen, daß die Lösung des Problems auf realen Computern außer für sehr kleine Probleminstanzen aus wahrscheinlich sehr grundsätzlichen Gründen praktisch unmöglich ist. In noch höherem Ausmaß und mit beweisbarer Gewißheit trifft das jedoch für viele entscheidbare Theorien zu.

Nun besteht jene Komplexitätsklasse von Turingmaschinen, die Spracherkennungs-Probleme erfaßt, von denen im mindesten die Hoffnung besteht, daß diese in vernünftigem Maßstab auch von Computern halbwegs effizient bearbeitet und gelöst werden können, in der Klasse $\boldsymbol{\mathcal{P}} := DTime(POL)$ aller Sprachen, die von einer Turingmaschine in polynomial-beschränkter Rechenzeit akzeptiert werden können. (Hierbei ist aber einzuräumen, daß sich ein Verfahren, dessen Rechenzeitaufwand z.B. nur durch eine Funktion aus $O(n^{59})$ beschränkt werden kann, wohl kaum zum effizienten Einsatz auf einem realen Computer eignet; dennoch sind die meisten interessanten Spracherkennungsprobleme in $\mathcal{P}$ von Turingmaschinen erkennbar, deren Rechenzeit sich durch ein Polynom niedrigen Grades begrenzen läßt.)

Daß ein Problem auch durch tatsächlichen Computereinsatz gelöst werden kann, wird oft als die Eigenschaft des Problems, „*behandelbar*“ oder *effizient behandelbar* zu sein,

ausgedrückt ("tractable problems"), im Gegensatz zu „*unbehandelbaren*" oder „*schwerbehandelbaren*" Problemen ("intractable problems"). Eine Grenzziehung zwischen diesen beiden Begriffen kann aber—aus verschiedenen, einigen bereits auch angedeuteten Gründen—nicht durch eine exakte Definition erfolgen.

Eine $\mathcal{P}$ sehr wahrscheinlich echt umfassende, interessante Klasse ist die Klasse $\boldsymbol{\mathcal{NP}} := NTime(POL)$ von allen Sprachen, deren Erkennung auf einer nichtdeterministischen Turingmaschine in polynomial beschränkter Rechenzeit erfolgen kann. Die Sprachen L, die dieser Klasse angehören, zeichnen sich dadurch aus, daß ein Polynom $p(n)$ existiert, sodaß zu jedem $x \in L$ durch einen „Beweis" der Länge $p(|x|)$ der Nachweis geführt werden kann, daß x tatsächlich der Sprache L angehört (für $x \notin L$ muß ein so kurzer „Beweis" nicht existieren). $\mathcal{NP}$ enthält eine Reihe von Problemen, die vermutlich „*unbehandelbar*" sind, z.B. AUSSAGENLOGISCHE ERFÜLLBARKEIT. Die Vermutung, daß dieses Problem (und viele andere, wie das Problem des Handlungsreisenden ("Travelling Salesman Problem") nicht in $\mathcal{P}$ liegt, wird dadurch unterstützt, daß bewiesen werden kann, daß es mindestens ebenso schwierig zu lösen ist wie jedes andere Problem in $\mathcal{NP}$; es ist „$\mathcal{NP}$*-vollständig*". Die genaue Definition diese Begriffes erfordert die Definitionen von Reduzierbarkeiten zwischen verschiedenen Sprachen.

Definition 1.5.2. Reduzierbarkeiten zwischen Sprachen.
Δ, Σ *seien endliche Alphabete.*

(i) *Sei* $f\colon \Sigma^* \to \Delta^*$ *eine Funktion.*
f *heißt* **linear-beschränkt***:* $\iff (\exists c \in \mathbb{N})(\forall x \in \Sigma^*)\ (|f(x)| \leq c \cdot |x|)$.

(ii) $\boldsymbol{POLYLIN} := DFTimeSpace(POL, LIN)$;
$\boldsymbol{DFLOGSPACE} := DFSpace(LOG)$.

(iii) *Seien* $A \subseteq \Sigma^*$, $B \subseteq \Delta^*$ *Sprachen.*

Dann heißt A **poly-lin-reduzierbar** *auf* B $(A \leq_{pl} B)$*:* $\iff$
$\iff$ $(\exists f\colon \Sigma^* \to \Delta^*$ *Funktion*$)$
$\big(f$ *ist linear beschränkt* $\&\ f \in POLYLIN\ \&$
$\&\ (\forall x \in \Sigma^*)\ (x \in A \leftrightarrow f(x) \in B)\big)$;

A *heißt* **logspace-lin-reduzierbar** *auf* B $(A \leq_{log-lin} B)$*:* $\iff$
$\iff$ $(\exists f\colon \Sigma^* \to \Delta^*$ *Funktion*$)$
$\big(f$ *ist linear beschränkt* $\&\ f \in DFLOGSPACE\ \&$
$\&\ (\forall x \in \Sigma^*)\ (x \in A \leftrightarrow f(x) \in B)\big)$;

A *heißt* **polynomial-Zeit-reduzierbar** *auf* B $(A \leq_p B)$*:* $\iff$
$\iff$ $(\exists f\colon \Sigma^* \to \Delta^*$ *Funktion*$)$
$\big(f \in \mathcal{P}(= DFTime(POL))\ \&\ (\forall x \in \Sigma^*)\ (x \in A \leftrightarrow f(x) \in B)\big)$;

A *heißt* **logspace-reduzierbar** *auf* B $(A \leq_{logspace} B)$: $\iff$
$\iff$ $(\exists f\colon \Sigma^* \to \Delta^*$ *Funktion*)
$\big(f \in DFLOGSPACE \;\&\; (\forall x \in \Sigma^*)\,(x \in A \leftrightarrow f(x) \in B)\big)$.

poly-lin- bzw. logspace-Reduktionen spielen erst in Kapitel 2 und Kapitel 3 bei der feineren Untersuchung der Entscheidungskomplexität entscheidbarer Theorien eine Rolle.

Definition 1.5.3. $\mathcal{NP}$**-vollständige Sprachen.**
Σ *ein Alphabet,* $L \subseteq \Sigma^*$ *eine Sprache.*
L *ist* $\mathcal{NP}$**-vollständig unter** $\leq_p$**-Reduktionen** : $\iff$
$\iff$ $L \in \mathcal{NP}\;\&\;(\forall L' \in \mathcal{NP})\,(L' \leq_p L)$;
L *ist* $\mathcal{NP}$**-vollständig unter** $\leq_{logspace}$**-Reduktionen** : $\iff$
$\iff$ $L \in \mathcal{NP}\;\&\;(\forall L' \in \mathcal{NP})\,(L' \leq_{logspace} L)$.

Hierbei ist $\mathcal{NP}$-Vollständigkeit bzgl. $\leq_{logspace}$-Reduktionen der eingeschränktere Begriff, obwohl nicht bekannt ist, ob er wirklich enger ist als der Begriff der $\mathcal{NP}$-Vollständigkeit unter $\leq_p$-Reduktionen.

Es ist nun leicht einzusehen, daß für 2 Sprachen L_1, L_2 gilt: $L_1 \leq_p L_2 \;\&\; L_2 \in \mathcal{P} \;\Rightarrow$
$\Rightarrow\; L_1 \in \mathcal{P}$. Damit könnte, falls für eine bezgl. $\leq_p$ $\mathcal{NP}$-vollständige Sprache L nachgewiesen werden würde, daß $L \in \mathcal{P}$ gilt, folgen[30]: $\mathcal{P} = \mathcal{NP}$. Da es jedoch über 150 $\mathcal{NP}$-vollständige Probleme gibt, für die bisher trotz vieler Anstrengungen keine deterministischen polynomial-Zeit-Algorithmen gefunden worden sind, liegt die Vermutung nahe, daß sehr wahrscheinlich $\mathcal{P} \neq \mathcal{NP}$ gilt und es tatsächlich (eine Vielzahl von) schwer-behandelbaren Problemen in $\mathcal{NP}$ gibt. Zu diesen würde dann auch AUSSAGENLOGISCHE ERFÜLLBARKEIT gehören und damit das wohl einfachste Entscheidungs-Problem der formalen Logik.

Für viele entscheidbare logische Theorien kann jedoch bewiesen werden, daß das Problem der Entscheidung von Formeln in diesen Theorien tatsächlich „schwer-behandelbar" ist, d.h. daß diese Theorien selbst „*schwer-entscheidbar*" sind. Das kann dadurch geschehen, daß untere Schranken für die Entscheidungskomplexität dieser Theorien gefunden werden, die schneller als jedes Polynom, beispielsweise exponentiell, wachsen.

Das trifft z.B. auf die Theorie $RA = Th(\langle \mathbb{R}; 0, 1, + \rangle)$ der Addition reeller Zahlen zu, die von A. Tarski als entscheidbar erkannt worden ist, und für die M. Fischer und M. Rabin eine untere Schranke der Gestalt 2^{cn}, für ein $c > 0$, bezüglich nichtdeterministischer Turing-Rechenzeit ermittelt haben. In diesem Fall spricht man davon, daß $Th(\langle \mathbb{R}; 0, 1, + \rangle)$ von „*exponentiell-linearer* (nichtdeterministischer Rechenzeit-)*Komplexität*" ist. In noch höherem Ausmaß trifft die „*Schwer-Entscheidbarkeit*" auf Theorien der Presburger Arithmetik wie $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ zu, für die M. Fischer und M. Rabin (vgl. Kapitel 3) bewiesen haben, daß für ein $c > 0$ die Funktion $2^{2^{cn}}$ eine untere Schranke ihrer Entscheidungskomplexität bezüglich nichtdeterministischer Turing-Rechenzeit ist; diese Theorie ist von

[30] Für $\mathcal{NP}$-vollständige Sprachen bzgl. $\leq_{logspace}$-Reduktionen kann ebenso argumentiert werden.

„*doppelt-exponentiell-linearer* (nichtdeterministischer Rechenzeit-)*Komplexität*“ und ist also (in wirklicher Allgemeinheit der zu entscheidenden Formeln) einer praktischen Behandlung auf einem Computer wohl unzugänglich. Eine noch höhere untere Schranke besteht für die Theorie $Th(\langle \mathbb{N}_0; . \rangle)$, nämlich eine von dreifach-exponentiell-linearer Gestalt $2^{2^{2^{cn}}}$ für ein $c > 0$.

Als ein in diesem Zusammenhang zu nennender Extremfall an Schwer-Entscheidbarkeit sind hier z.B. Theorien $Th(\mathcal{C})$ von nichtleeren Klassen $\mathcal{C}$ von „*P-Strukturen*“ zu nennen; eine P-Struktur ist dabei eine Struktur $\langle \mathbb{N}_0; \rho \rangle$, wobei $\rho : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ eine „Paarungsfunktion“ ist, d.h. eine injektive Funktion der angegebenen Gestalt. Solche Theorien $Th(\mathcal{C})$, wobei $\mathcal{C}$ eine nichtleere Klasse von P-Strukturen ist, sind im allgemeinen unentscheidbar. Insbesondere ist $Th(\mathcal{C})$, wenn $\mathcal{C}$ für die Klasse aller P-Strukturen steht, unentscheidbar. Es gibt jedoch einzelne P-Strukturen, sodaß $Th(\mathcal{C})$ entscheidbar ist. – [FeRa79] weisen nun nach, daß es jedoch in keinem Fall eine elementar-rekursive[31] untere Schranke für die Entscheidungskomplexität einer solchen Theorie geben kann, d.h. genau, daß mit $f(n) := \left. 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \right\}$ (Höhe n) für alle Klassen $\mathcal{C}$ von P-Strukturen

$$Thm_{Th(\mathcal{C})} \notin NTime(f(cn)) \text{ (für ein } c \in \mathbb{R},\ c > 0) \tag{1.9}$$

gilt. (Falls $Th(\mathcal{C})$ unentscheidbar ist, ist (1.9) auf triviale Weise deshalb gültig, weil es dann für keine $Thm_{Th(\mathcal{C})}$-akzeptierende Turingmaschine M eine (total-)rekursive Rechenzeitschranke (für das Akzeptieren dieser Sprache) geben kann[32]. – Das ist auch der Grund dafür, warum es für $Th(\mathcal{C})$ mit $\mathcal{C}$ der Klasse aller P-Strukturen keine ((total-)rekursive) *obere* Schranke für die Entscheidungskomplexität geben kann, da $Th(\mathcal{C})$ dann ja unentscheidbar ist). Die Entscheidungskomplexität solcher Theorien sprengt also auch im Fall, daß die Theorie entscheidbar ist, alle n-fach-exponentiellen Limitierungen ($n \in \mathbb{N}$).

[31] Eine *elementar-rekursive* Funktion $f : \mathbb{N}_0 \to \mathbb{N}_0$ bzw. $f : \Delta^* \to \Sigma^*$ (Δ, Σ zwei Alphabete) ist eine Funktion, die von einer IOTM mit einer Rechenzeitschranke, die eine fixierte Komposition von exponentiellen Funktionen ist, berechnet werden kann. – Diese Charakterisierung elementar-rekursiver Funktionen ist (nach Beweisen von [Cob64] und [Rit63]) äquivalent zur rekursionstheoretischen Definition solcher Funktionen nach Kalmár (vgl. hierzu etwa [Pet67]) [diese Zitate sind [FeRa79], p. 5 entnommen].

[32] Es ist nämlich leicht einzusehen, daß umgekehrt für jede, als System $T = (\Sigma_T, Fo_T, Thm_T)$ aufgefaßte logische Theorie T ausgehend von einer (eventuell nichtdeterministischen oder sogar alternierenden) Turingmaschine M und einer (total-)rekursiven Schrankenfunktion $\tilde{f}(n)$, derart, daß M (die Sprache) Thm_T ($\subseteq \Sigma_T^*$) mit Rechenzeitschranke $\tilde{f}(n)$ akzeptiert, eine deterministische IOTM M' konstruiert werden kann, die THM_T berechnet (und die also Formeln von T wirklich zu *entscheiden* gestattet) [jedenfalls unter der sinnvollen—und eigentlich fraglosen—Voraussetzung, daß $Fo_T \subseteq \Sigma_T^*$ entscheidbar ist].

1.6 Praktische Bedeutung von oberen und unteren Schranken für die Entscheidungskomplexität einer entscheidbaren Theorie

Für diese für die Entscheidungskomplexität von entscheidbaren Theorien erzielten theoretischen Resulate (der Schwer-Entscheidbarkeit) stellen sich natürlich auch Fragen nach deren praktischer Bedeutung, d.h. die Fragen, ob sich daraus überhaupt Folgerungen für auf realen Computern implementierte Entscheidungsalgorithmen für eine dieser Theorien ergeben und dann, wie solche Folgerungen präzisiert werden könnten. – Die Darstellung der folgenden hierzu angestellten Überlegungen folgt im wesentlichen [FeRa79].

Gegen die auch reale Bedeutung von für die Entscheidungskomplexität entscheidbarer Theorien erzielten unteren Schranken könnten eine Reihe von Einwänden erhoben werden, auf die hier näher eingegangen werden soll. – Als Beispiel sei hier eine—bereits erwähnte—untere Schranke für die Entscheidungskomplexität einer Theorie $PreAN$ der Presburger Arithmetik natürlicher Zahlen (vgl. Kapitel 2, Abschnitt 2.3; diese Theorie 1. Ordnung ist zu $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ äquivalent) der Gestalt

$$Thm_{PreAN^{((M))}} \notin NTime(2^{2^{cn}}) \text{ (füer ein } c \in \mathbb{R},\ c > 0) \tag{1.10}$$

betrachtet, die von M. Fischer und M. Rabin in [FiR74] erzielt worden ist (vgl. Aufarbeitung dieser Arbeit in Kapitel 3). (1.10) ist zu

$$\begin{aligned} &(\exists\, c \in \mathbb{R},\ c > 0)\ (\forall\, M \text{ IOTM},\ L(M) = Thm_{PreAN^{((M))}}) \\ &\quad (\exists\, \infty\text{-viele } n \in \mathbb{N} \text{ und } \mathbf{A} \in Thm_{PreAN^{((M))}}) \\ &\qquad \left(|\mathbf{A}| = n \ \&\ Min\text{-}RZ_M(\mathbf{A}) > 2^{2^{cn}}\right) \end{aligned} \tag{1.11}$$

äquivalent (vgl. die ähnliche Aussage (1.3) früher) und besagt auf jeden Fall, daß die Entscheidung von $PreAN$ in allgemeiner Weise mit Hilfe von IOTM-Turingmaschinen im worst-case (dem Aufwand im schlimmsten Fall) sehr schwierig ist.

Es könnte aber darauf hingewiesen werden, daß in (1.10) und (1.11) ein spezieller Wert von $c \in \mathbb{R}$, $c > 0$, für den diese Aussagen gelten, nicht angegeben worden ist und daß damit das genaue quantitative Ausmaß der Schwer-Entscheidbarkeit dieser Theorie noch nicht feststeht. – Ein entsprechendes $c \in \mathbb{R}$, $c > 0$ kann jedoch durch eine genaue Analyse der Komplexitätsbeweise in [FiR74] (nach einer genauen Festlegung einer Syntax für diese Theorie) sehr wohl auf konstruktive Weise gefunden und angegeben werden.

Es könnte weiters argumentiert werden, daß man im Fall eines auf einem realen Computer installierten Entscheidungsalgorithmus wegen durch die Systemgröße vorgegebenen oder verursachten Limitierungen immer nur am für die Entscheidung von Formeln aus einer *endlichen* Menge von möglichen Eingaben entstehenden Aufwands interessiert sein

kann, daß demgegenüber aber die Qualität z.B. der Aussage (1.11) gerade im Rechenzeitverhalten *für unendlich viele* Eingabeformeln liegt. Damit im Zusammenhang steht ein grundlegender Unterschied zwischen der Klasse der Turingmaschinen und der Klasse (oder Menge ?) möglicher realer Computer:

So kann beispielsweise zu jeder Turingmaschine (oBdA: IOTM) M mit akzeptierter Sprache $L(M) = L$ und jeder endlichen Menge $E \subseteq (\Sigma(M))^*$ von möglichen Eingabewörtern von M eine Turingmaschine M' konstruiert werden, die M simuliert und die auf allen Eingabewörtern $w \in E$ sehr schnell arbeitet, d.h. für diese nur $|w|$ Schritte Rechenzeit und keinen Speicherplatz auf Arbeitsbändern benötigt, d.h. solche Wörter nur zu lesen braucht (deren Entscheidung dabei durch das Absuchen einer in den Programmcode der Maschine übernommenen (endlichen) Liste dieser Wörter $w \in E$ und symbolweise interne Fallunterscheidungen vornimmt), und auf allen anderen Eingabewörtern $w \in (\Sigma(M))^* \setminus E$ fast genau so schnell wie M operiert, d.h. dafür nur ca. $2\,|w| + 2$ Schritte Rechenzeit zusätzlich braucht (diese Wörter nur einmal umsonst gelesen haben muß). Die dafür nötige Konstruktion erhöht die Zustände von M und ist für den Bau wirklicher Computer keine sinnvoll-vorstellbare Möglichkeit. – Daneben gibt es noch andere, keine realen Entsprechungen besitzende Eigenschaften der Klasse von Turingmaschinen, die gerade aus der Abstraktheit dieses Berechnungsmodelles resultieren.

Es stellt sich aber heraus, daß die zur Erzielung unterer Schranken geführten Komplexitätsbeweise meistens mehr an Information enthalten und in eine direktere Beziehung zu realen Anwendungssituationen gebracht werden können. Dies deshalb, weil wirkliche Computer von Turingmaschinen simuliert werden können, wenngleich nur unter großem Effizienzverlust. Dennoch können solche präzis (oder angenähert-präzis) gemachten Simulationen der Ausgangspunkt für die Übertragung von unteren Schranken zu Entsprechungen dafür auf tatsächlich verwendeten Rechenmaschinen sein. Als ein auf diese Art erzieltes Beispiel einer solchen Aussage über das wirkliche Rechenzeitverhalten eines auf einem realen Computer operierenden Entscheidungsverfahrens beziehen sich [FeRa79] auf die enorm schwer-entscheidbaren Theorien $Th(\mathcal{C})$ von P-Strukturen und wagen sich dabei an folgende Behauptung heran:

Theorem. *$\mathcal{C}$ sei eine nichtleere Klasse von P-Strukturen, C sei ein realer Computer bzw. ein auf einem realen Computer installiertes Entscheidungsverfahren für $Th(\mathcal{C})$, das in der Lage ist, Formeln der Theorie 1. Ordnung $Th(\mathcal{C})$ bis mindestens der Symbollänge 1000 zu entscheiden (nach Zugrundelegung einer informatisch-sinnvollen Formelsyntax).*

Dann existiert jedenfalls eine Formel $\mathbf{A}$ von $Th(\mathcal{C})$ mit $\left|\mathbf{A}^{((M))}\right| \leq 1000$, zu deren Entscheidung C mindestens 10^9 (1 Milliarde) Jahre benötigt.

Diese Aussage konnte sich zum Zeitpunkt ihrer Veröffentlichung (1979) aber sicher nur auf sequentielle Computer und die damals herstellbaren Rechnerleistungen beziehen; schon aus diesem Grund müßte die Größe „10^9 Jahre“ mittlerweile wohl um einiges nach unten

revidiert werden. Weiters soll darauf hingewiesen werden, daß sich ähnlich-gestaltige Aussagen in der Kryptographie aus den 70-er Jahren auch schon als falsch herausgestellt haben (obzwar die unter wenig gesicherten Grundannahmen getroffen worden sein müssen)[33] und daß solchen Abschätzungen gegenüber aus einer Reihe von Gründen eine gewisse Vorsicht angebracht ist. Es sollte aber nicht in Zweifel gezogen werden, daß sich für feststehende reale Systeme und für beliebige schwer-entscheidbare Theorien Aussagen von ähnlicher Gestalt und vergleichbaren beteiligten Größen trotzdem finden lassen, denen jeweils einzeln wirklich praktisch wirksame Gültigkeit zukommt. Für weniger schwer-entscheidbare Theorien als einer Theorie von $P-Strukturen$ werden natürlich nur erheblich schwächere, auf reale Gegebenheiten verweisende entsprechende Aussagen als oben erzielbar sein.

Ein weiterer möglicher Einwand gegen die Bedeutung von (mindestens exponentiellen) unteren Schranken für die Entscheidungskomplexität einer Theorie T könnte darin bestehen, daß die Vermutung geäußert würde, in praktischen Zusammenhängen (:wie immer die konkret gedacht werden müßten) wäre man vielleicht nicht so sehr an der Entscheidung *aller* Formeln von T interessiert als vielmehr nur an der Entscheidung von den einer *eingeschränkten* Formelmenge angehörenden Formeln. Und daß der dafür nötige Aufwand u.U. merkbar niedriger sein könnte als der im schlimmsten allgemeinen Fall zu erwartende. – Damit im Zusammenhang könnte auch die denkbare Möglichkeit stehen, daß die in den Beweisen unterer Schranken auftretenden, zu Entscheidungsturingmaschinen konstruierten Formeln, von diesen nur mit einem die Schranke übersteigenden Aufwand zu entscheidenden Formeln immer von seltener, (bezüglich des zu ihrer Entscheidung nötigen Aufwandes) extremer Gestalt wären und damit praktisch wohl kaum vorkommen würden. (Damit ist

[33] Z.B.: 1977 wurde von maßgeblichen Experten in der Kryptographie (vgl. die im folgenden angegebene Quelle) behauptet, daß die Faktorisierung einer 125-stelligen Zahl durchschnittlich $40 \cdot 10^{12}$ Jahre dauern würde. Demgegenüber wurde 1994 eine (keineswegs speziell-konstruierte oder speziell-gestaltige, sondern kryptographisch interessante) 129-stellige Zahl in 8 Monaten durch die Benutzung der freien Rechenzeit von 1600 Rechnern auf der ganzen Welt faktorisiert (zitiert aus: `sci.crypt-item, From: schneier@chinet.chinet.com (Bruce Schneier); Subject: Factoring -- State of the Art and Predictions; Date: Sun, 12 Feb 1995, 23:29:16 GMT` ; derzeit z.B. erhaeltlich unter: `http://www.cs.hut.fi/crypto/rsa-key-length-recommendations`). – Ein erwähnenswerter wichtiger Unterschied zwischen der hier mitgeteilten (und mittlerweile falsifizierten) Behauptung über die praktische Schwer-Entscheidbarkeit des Faktorisierungs-Problems und der oben aus [FeRa79] zitierten Aussage dürfte aber doch darin bestehen, daß diese nicht auf der Basis einer theoretisch erzielten unteren Schranke für das Faktorisieren von Zahlen gemacht werden konnte (eine hinreichend präzise untere Schranke dafür dürfte noch nicht erzielt worden sein, die Vermutungen über das Wachstumsverhalten des zum Faktorisieren einer Zahl $n \in \mathbb{N}$ notwendigen deterministischen Rechenzeitaufwands bewegen sich in der Größenordnung von einer Funktion aus $O(e^{c \cdot \sqrt{\ln n \cdot \ln \ln n}})$ (mit $c = 1$ für die schnellsten Algorithmen) [vgl. [Riv90], p. 724]). Und in der seit der erwähnten Behauptung vergangenen Zeit sind aber sowohl durch das Finden neuer und die Verbesserung bekannter Faktorisierungsmethoden als auch v.a. durch die Einführung neuer Computerarchitekturen und die dadurch erhöhten Rechnergeschwindigkeiten und -kapazitäten und weiters noch durch neue Methoden zur Optimierung des Zusammenspiels zwischen Algorithmen und hardware große Fortschritte bei der praktischen Lösung dieses Problems für über 100-stellige Zahlen erzielt worden.

dann allerdings auch die Frage nach einer Charakterisierung der Entscheidungskomplexität von T etwa im average-case-Sinn (dem Entscheidungsaufwand im durchschnittlichen Fall) gestellt. – Und solche Fragen sind in der Komplexitätstheorie bisher allerdings wohl eher noch wenig erforscht worden.)

Obzwar sich solche Vermutungen einfach aussprechen lassen, könnten diese tatsächlich nur durch die konkrete Definition einer eingeschränkten Formelmenge für T und die Erzielung einer nun niedrigeren oberen Schranke für die Entscheidungskomplexität der dieser Menge angehörenden Formeln bestätigt werden. In den meisten Fällen lassen es jedoch auch die für untere Schranken geführten Komplexitätsbeweise wenig wahrscheinlich erscheinen, daß wesentliche und natürliche eingeschränkte Mengen von Formeln mit geringerer Entscheidungskomplexität gefunden werden könnten. Dies deswegen, weil in diese Beweise oft sehr grundlegende Begriffe und Ausdrucksmöglichkeiten dieser Theorien eingehen, die bei der Definition einer eingeschränkten Formelmenge ausgeschlossen werden müßten, wenn verhindert werden soll, daß jene Beweise oder angepaßte Modifikationen davon auch dann noch geführt werden können. Und weil danach fraglich ist, ob für solche Einschränkungen der Formelmenge zuletzt andere als triviale oder bekannte Sonderfälle übrig bleiben können.

Eine gewisse praktische Bedeutung von für die Entscheidungskomplexität einer Theorie erzielten oberen Schranken kann selbst im Fall, daß diese von 1-fach-, 2-fach- oder mehrfach-exponentieller Gestalt sind, darin liegen, daß die entsprechenden Beweise Entscheidungsalgorithmen beinhalten, zugleich mit genauen Aufwandsschranken dafür. Diese Verfahren könnten nämlich auf Computern installiert werden und darauf jedenfalls zur Entscheidung von kurzen (oder „hinreichend kurzen“) Formeln auch tatsächlich eingesetzt werden.

Aus logischer Sicht könnte eine wesentliche Bedeutung oberer und unterer Schranken für die Entscheidungskomplexität einer Theorie T darin liegen, daß man, falls diese Schranken einander hinreichend weit (etwa bis auf Lücken, denen bislang ungelöste automatentheoretische Probleme zugrundeliegen oder entsprechen) angenähert worden sind, davon sprechen könnte, daß dann die *Ausdrucksstärke* von T gut verstanden wird. In besonderem Maß ist das wohl immer dann der Fall, wenn der Entscheidungskomplexität einer Theorie eine bestimmte Komplexitätsklasse eindeutig zugeordnet werden konnte, wie das zum Beispiel für die Theorien 1. Ordnung RA und $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ in Beziehung zu den Komplexitätsklassen $ATimeAlter(EXL, LIN)$ bzw. $ATimeAlter(EEXL, LIN)$ bezüglich alternierender Turingmaschinen erfolgt ist (diese Theorien sind in der entsprechenden Komplexitätsklasse $\leq_{pl}$- bzw. $\leq_p$-vollständig (vgl. Abschnitt 2.6) d.h. daß ihr Entscheidungs-Problem zu den schwierigsten dieser jeweiligen Klassen gehört und daß dadurch diese Komplexitätsklassen selbst auch umgekehrt durch die Entscheidungskomplexität dieser Theorien genau charakterisiert werden können). – Allgemein erweitern Resultate über die Entscheidungskomplexität einer Theorie T natürlich das schon vorhandene logische Wissen über T.

Es ist weiters noch von großem logischen Interesse, daß für die Entscheidungskomplexität einer Theorie erzielte untere Schranken von mindestens exponentieller Gestalt bzgl. nichtdeterministischer (Turing-)Rechenzeit ziemlich unmittelbar auch auf ebensogestaltige untere Schranken für die Längen der kürzesten Beweise in allen „einfach"-angebbaren, d.h. näher, in $\mathcal{P}$-erkennbaren [34] Axiomatisierungen dieser Theorien führen.

Solche Aussagen über die Längen kürzester Beweise in einer Theorie haben natürlich auch zur Folge, daß diese Theorien mit automatischen Beweismethoden ebenfalls nur in sehr beschränktem Ausmaß praktisch zugänglich sein können.

Die allgemeine Bedeutung ihrer für die Theorien RA und $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ erzielten exponentiell-linearen und doppelt-exponentiell-linearen unteren Schranken für deren Entscheidungskomplexität (bzgl. nichtdeterministischer Turing-Rechenzeit) fassen [FiR74] mit folgenden, die hier angesprochenen Fragen betreffenden, allgemeinen Worten zusammen:

> "The fact that decision and proof procedures for such simple theories are exponentially complex is of significance to the problem of theorem proving on the one hand, and to the more general issue of what is knowable in mathematics on the other hand."[35]

[34] Damit ist gemeint, daß die zu solchen Axiomatisierungen gehörige Axiomenmenge in $\mathcal{P}$ oder in $\mathcal{NP}$ liegt.

[35] [Hierbei ist " ... of what is knowable in mathematics" wohl etwa in der Bedeutung von „in welchem Ausmaß mathematisches Wissen algorithmisch zugänglich ist" zu verstehen, C.G.]

Kapitel 2

Presburger Arithmetik

In diesem Kapitel werden im wesentlichen drei verschiedene Theorien der Additionsarithmetik ganzer bzw. natürlicher Zahlen behandelt, die alle eng mit dem bekannten Vollständigkeits- und Entscheidbarkeitsergebnis von M. Presburger für prädikatenlogische Systeme der Arithmetik ganzer Zahlen aus den Jahren 1928, 1929 verbunden sind. Dabei sind die hier betrachteten formal-logischen Theorien heute eher verwendete, neuere Entsprechungen zu den von Presburger verwendeten Systemen.

Bei diesen Theorien handelt es sich um die zuerst von Presburger als vollständig und entscheidbar erkannte Theorie TAZ („Theorie der Addition ganzer Zahlen"), sowie um eine Theorie $PreAZ$[1] („Presburger Arithmetik ganzer Zahlen"), auf die Presburger seine Beweisführung ausdehnen konnte, und um die Theorie $PreAN$[1] („Presburger Arithmetik natürlicher Zahlen"), die ebenfalls als vollständig und entscheidbar erkannt werden kann.

In den Abschnitten 1, 2 und 3 werden diese Theorien durch Axiomatisierungen vorgestellt, diese werden untersucht und Quantoreneliminationsverfahren für diese Theorien werden beschrieben oder wenigstens wird auf solche verwiesen. Im Abschnitt 4 wird der inhaltlich recht anschauliche Zusammenhang zwischen $PreAZ$ und $PreAN$ auf seinen formal-logischen Charakter hin analysiert.

Im Abschnitt 5 soll eine Verbindung von der Presburger Arithmetik natürlicher Zahlen $PreAN$ zur Peano-Arithmetik PeA[1] hergestellt werden. Zuletzt sollen in Abschnitt 6 die wichtigsten Komplexitätsresulate für Theorien der Presburger Arithmetik versammelt werden.

[1] Die etwas aufwendige symbolische Namensgebung für diese Theorien hier will v.a. Bezeichnungskonflikte vermeiden, wie sie sonst häufig zwischen Theorien der Presburger Arithmetik, der Peano-Arithmetik und etwa der häufig mit PRA bezeichneten primitiv-rekursiven Arithmetik entstehen können.

2.1 Die Theorie TAZ

M. Presburger[2] löste 1928 (siehe [Pre29]) ein von A. Tarski im selben Jahr gestelltes Problem[3]: Er zeigte die Vollständigkeit und die Entscheidbarkeit einer Theorie 1. Ordnung

> „eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt."

(vgl. die Einleitung in [Pre29].) Und zwar tat er das dadurch, daß er die Methode der Quantorenelimination (bzgl. der Presburger auf Th. Skolem und C.H. Langford verweist, die diese schon früher benutzt haben) in dem von ihm benutzten formal-logischen System arithmetischer Aussagen zur Konstruktion eines effektiven Verfahrens für die Entscheidung von formalen Aussagen dieses Systems *und* (damit gleichzeitig für die Entscheidung über) deren arithmetischer Gültigkeit nutzen konnte. In Presburgers Worten (vgl. [Pre29]):

> „Der [unten] skizzierte Vollständigkeitsbeweis gibt zugleich, infolge seines effektiven Charakters ein Verfahren, das bei einer vorgelegten Aussage des von uns betrachteten Gebietes die Entscheidung darüber erlaubt, ob sie einen arithmetischen Satz vorstellt."

Er erzielte damit zugleich eine der ersten Entscheidbarkeitsaussagen für prädikatenlogische Theorien.

Das von Presburger betrachtete formale System arithmetischer Aussagen ist nun wie folgt als logische Theorie 1. Ordnung TAZ („Theorie der Addition auf den ganzen Zahlen $\mathbb{Z}$") (in der hier und im folgenden benutzten Formalisierung dieses Begriffs durch [Shoe67]) aufzufassen:

[2] Mojżesz Presburger (1904-1943(?)), polnischer Mathematiker (die Lebensdaten in dieser Form sind aus [Th95] übernommen).

[3] (Presburger verweist in [Pre29] auf [Tar28].)

Definition 2.1.1. Die Theorie TAZ.

Sei L_{TAZ} die Sprache einer Theorie 1. Ordnung, die als einzige nichtlogische Symbole die Konstantensymbole 0,1 und das 2-stellige Funktionssymbol + aufweist [4]*. Dann ist TAZ jene Theorie, die als nichtlogische Axiome einzig TAZ.1., TAZ.2., TAZ.3., TAZ.4., sowie weiters noch Formeln, die einem der Schemata TAZ.S1., TAZ.S2., TAZ.S3. angehören, besitzt:* [5]

TAZ.1.	$x + (y + z) = (x + y) + z$
TAZ.2.	$x + 0 = x$
TAZ.3.	$\exists\, y\,(\, x + y = 0\,)$
TAZ.4.	$x + y = y + x$
TAZ.S1.	$\{\ \underline{n}\, x = \underline{n}\, y \to x = y\ \}_{n\in\mathbb{N},\, n\geq 2}$
TAZ.S2.	$\{\ \exists\, y\,(\,\underline{n}\, y = x\ \vee\ \underline{n}\, y + 1 = x\ \vee\ \ldots\ \vee\ \underline{n}\, y + \underline{\underline{n-1}} = x\,)\ \}_{n\in\mathbb{N},\, n\geq 2}$
TAZ.S3.	$\{\ \neg\, \underline{n}\, x + 1 = 0\ \}_{n\in\mathbb{N},\, n\geq 2}\,.$

Hierbei wurden die folgenden abkürzenden Schreibweisen verwendet:

- *Die Mengenklammern in den obigen Darstellungen der Axiomenschemata TAZ.S1., TAZ.S2. und TAZ.S3. geben gemeinsam mit der Indizierung die Axiome des Schemas in Familiennotation an; TAZ.S3. z.B. beschreibt auf diese Weise also gerade alle Formeln $\neg\, \underline{2}\, x + 1 = 0$, $\neg\, \underline{3}\, x + 1 = 0$, $\neg\, \underline{4}\, x + 1 = 0$, ...*

- *Für $n \in \mathbb{N}_0$ und Terme $\mathbf{a}$ seien hier und im folgenden die abgekürzten Schreibweisen $\underline{n}\,\mathbf{a}$ sowie $\underline{\underline{n}}$ wie folgt zu verstehen:*

[4] Im hier benutzten Formalismus bzw. Kalkül der „Theorie 1. Ordnung“ aus [Shoe67] enthält eine Sprache einer Theorie 1. Ordnung immer das Gleichheitssymbol = als *logisches* Symbol.

[5] Es handelt sich bei diesen Axiomen genau um die von Presburger in [Pre29] für sein System angegebenen, wenn man davon absieht, daß (1) in [Pre29] für TAZ.4. das Axiom $\exists y\,(\, x + y = z\,)$ verwendet wird, (2) dort zusätzlich noch vorkommt: $x + z = y + z \to x = y$, das aber im Anhang als überflüssig erkannt wird, (3) Axiome bezüglich der Gleichheit = (nämlich $x = x$ und $x = y \to x = z \to y = z$) und $x = z \to x + z = y + z$ (also Identitäts- und Gleichheitsaxiome im Sinne von [Shoe67]), sowie weiters noch aussagenlogische Axiome von Lukasiewicz (die Axiome $(\mathbf{A} \to \mathbf{B}) \to (\mathbf{B} \to \mathbf{C}) \to (\mathbf{A} \to \mathbf{C})$, $(\neg\, \mathbf{A} \to \mathbf{A}) \to \mathbf{A}$, $\mathbf{A} \to (\neg\, \mathbf{A} \to \mathbf{B})$) verwendet werden, die hier unnötig sind, weil sie durch das logische System der „Theorie 1. Ordnung“ von [Shoe67] erfaßt sind, d.h. darin in jeder Theorie beweisbar sind. (Als Regelsystem benutzte Presburger ein Regelsystem von A. Tarski: (1) Aus $\mathbf{A}$ ist $\mathbf{A}_{\mathfrak{a}}[\mathbf{a}]$ herleitbar, (2) aus $\mathbf{A}$ und $\mathbf{A} \to \mathbf{B}$ ist $\mathbf{B}$ herleitbar, (3) aus $\exists \mathbf{x}\, \mathbf{A} \to \mathbf{B}$ ist $\mathbf{A} \to \mathbf{B}$ herleitbar und (4) aus $\mathbf{A} \to \mathbf{B}$ die Formel $\exists \mathbf{x}\, \mathbf{A} \to \mathbf{B}$, sofern $\mathbf{x}$ in $\mathbf{A}$ vorkommt, nicht aber in $\mathbf{B}$.)

$$\underline{n}\,\mathbf{a} := \begin{cases} 0 & \dots\ n = 0 \\ \underbrace{\mathbf{a} + \mathbf{a} + \dots + \mathbf{a}}_{n} & \dots\ n \geq 1 \end{cases} ; \qquad \underline{\underline{n}} := \begin{cases} 0 & \dots\ n = 0 \\ \underbrace{1 + 1 + \dots + 1}_{n} & \dots\ n \geq 1 \end{cases} .$$

Hierbei ist noch zu bemerken, daß hier und im folgenden öfter auf die Klammerung der Terme bezüglich + verzichtet wird, was in den betrachteten arithmetischen Theorien immer wegen der Gültigkeit des Assoziativgesetzes bezüglich der Addition (das hier in TAZ.1. ausgedrückt ist) berechtigt ist. Um $\underline{n}\,\mathbf{a}$ *bzw.* $\underline{\underline{n}}$ *jedoch eindeutig festzulegen, kann hier z.B. für* $n \in \mathbb{N}_0$, $n \geq 2$ *immer als gleich* $\mathbf{a} + (\mathbf{a} + (\dots + (\mathbf{a} + \mathbf{a}) \dots))$ *bzw.* $\underline{\underline{n}}$ *gleich* $1 + (1 + (\dots + (1 + 1) \dots))$ *gesetzt werden (Rechtsbündigkeit der Klammerung).*

Formal betrachtet handelt es sich bei den Axiomen von TAZ um die Axiome für eine abelsche Gruppe (TAZ.1.–TAZ.4.), zu denen noch Eindeutigkeitseigenschaften der Teilbarkeitsrelationen (TAZ.S1.), sowie eine gewisse Diskretheitseigenschaft (TAZ.S3.) und die Möglichkeit von Kongruenzenbildung (TAZ.S2.) hinzukommen.

Es ist sofort einzusehen, daß es sich bei den Axiomen von TAZ um in der Arithmetik ganzer Zahlen gültige Formeln handelt, d.h. genauer, um Formeln, die im Modell $\mathfrak{Z} := \langle \mathbb{Z}; 0, 1, + \rangle$ [6] wahr sind. In diesem Sinn handelt es sich bei TAZ um eine Axiomatisierung der semantisch definierten Theorie $Th(\langle \mathbb{Z}; 0, 1, + \rangle)$, d.h., um eine Theorie, die (die per definitionem vollständige Theorie) $Th(\langle \mathbb{Z}; 0, 1, + \rangle)$ als Erweiterung besitzt.

Daß TAZ auch eine *vollständige* Axiomatisierung von $Th(\langle \mathbb{Z}; 0, 1, + \rangle)$ darstellt (d.h., daß TAZ und $Th(\langle \mathbb{Z}; 0, 1, + \rangle)$ äquivalent sind, die gleichen Theoreme besitzen) ist eine Folge davon, daß das Ergebnis von Presburger es erlaubt, die Theorie TAZ als vollständig zu erkennen. (Presburger drückt das in [Pre29] so aus:

[6] Diese Bezeichnungsweise von Strukturen und Modellen weicht von der Symbolik in [Shoe67] ab, ist hauptsächlich [FeRa79] entlehnt, und gibt eine Struktur $\mathfrak{A}$ für eine Sprache L in der Form $\langle |\mathfrak{A}|; f_1, \dots, p_1, \dots \rangle$ an, also durch Auflistung des Universums $|\mathfrak{A}|$ von $\mathfrak{A}$ und der den nichtlogischen Symbolen von L auf $|\mathfrak{A}|$ entsprechenden Funktionen und Prädikaten der Struktur $\mathfrak{A}$. Diese Bezeichnungsweise, die im folgenden oft verwendet wird, ist v.a. dann sehr nützlich, wenn damit Standardmodelle von Theorien bezeichnet werden, in welchen die Bedeutung aufgelisteter Symbole für Funktionen und Prädikate eindeutig festgelegt und unmißverständlich ist. Das ist bei den hier untersuchten vollständigen Theorien weitgehend immer der Fall. – Im Gegensatz zur Verwendung dieser Schreibweise in [FeRa79] wird hier bezüglich einer Sprache L und einer Struktur $\mathfrak{A}$ für L ein Gleichheitsprädikat $=$ auf $|\mathfrak{A}|$ nicht zusammen mit den weiteren Funktions- und Prädikatssymbolen von $\mathfrak{A}$ aufgelistet, da das Gleichheitssymbol $=$ im Formalismus von [Shoe67] in L immer schon als logisches Symbol enthalten ist und dessen Semantik bezüglich Formeln über L unabhängig von einem (explizit definierten) Gleichheitsprädikat auf $\mathfrak{A}$ festgelegt ist. (Demgegenüber setzen [FeRa79] das Vorhandensein eines Gleichheitssymbols in einer betrachteten Sprache 1. Ordnung *nicht* voraus und betrachten weiters ausschließlich Sprachen L von Theorien 1. Ordnung, die keine Funktionssymbole enthalten.)

„Es ist aus der gegebenen Beweisführung leicht einzusehen, [...] daß *in dem auf die Menge $\mathfrak{A}_x$ beschränkten Gebiete der Arithmetik ganzer Zahlen*[7] *keine unentschiedenen Probleme mehr existieren*“ [8])

Das Ergebnis von Presburger beruht nun im wesentlichen darauf, daß eine Erweiterung von TAZ um die definitorische Einführung von Kongruenzensymbolen $\equiv_n$ ($n \in \mathbb{N}$, $n \geq 2$) die Quantorenelimination zuläßt (und zwar im Unterschied zur nicht erweiterten Theorie TAZ).

Diese im folgenden darzustellende Erweiterungstheorie TAZ', die eine Erweiterung von TAZ um die gleichzeitige definitorische Einführung aller Kongruenzensymbole $\equiv_n$ ($n \in \mathbb{N}$, $n \geq 2$) ist, übersteigt um ein Geringes den Begriff der „definitorischen Erweiterung“ von Theorien in [Shoe67]. Und zwar insofern, als dort nur Erweiterungen um die definitorische Einführung von endlich vielen neuen nichtlogischen Symbolen den Namen „definitorische Erweiterung“ tragen[9]. Dieser Begriff könnte jedoch unter Erhaltung der mit ihm verknüpften wesentlichen Aussagen deutlich erweitert werden. Für die Verwendung hier reicht folgende Verallgemeinerung:

Definition 2.1.2. Definitorische Erweiterungen.
Seien T und T' Theorien 1. Ordnung, L_T und $L_{T'}$ die zugehörigen Sprachen.

(i) *Sei $\mathbf{p}$ ein n-stelliges Prädikatensymbol, das in L_T nicht vorkommt. Seien $\mathbf{x}_1, \ldots, \mathbf{x}_n$ verschiedene Variable. Sei $\mathbf{D}$ eine Formel in T, in der keine anderen Variablen außer $\mathbf{x}_1, \ldots, \mathbf{x}_n$ frei vorkommen.*

T' heißt **definitorische Erweiterung** *von T* **um die Einführung des Prädikatensymbols $\mathbf{p}$**, *genau dann, wenn $L_{T'}$ aus L_T durch die Hinzunahme des Symbols $\mathbf{p}$ entsteht und T' aus T durch die Hinzunahme des neuen nichtlogischen Axioms*

$$\mathbf{p}\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D} \qquad (\text{„definierendes Axiom für } \mathbf{p}\text{“})$$

zu den Axiomen von T hervorgeht.

(ii) *Sei $\mathbf{f}$ ein n-stelliges Funktionssymbol, das in T nicht vorkommt, seien die Variablen $\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y}, \mathbf{y}'$ paarweise verschieden, sei $\mathbf{D}$ eine Formel, in der keine Variablen*

[7] [und das hieße bezüglich des hier zugrundegelegten formal-logischen Systems: in dem auf die Theorie TAZ beschränkten Gebiet der formalisierten Arithmetik, C.G.]

[8] [Hervorhebung im Original, C.G.]

[9] Ein Grund dafür, warum [Shoe67] nur definitorische Erweiterungen um die Einführung endlich vieler neuer nichtlogischer Symbole betrachtet, liegt vielleicht darin, daß bezüglich des von diesem Begriff abhängigen, auf p. 134 definierten Begriffs der „definitorischen Erweiterung eines Modells“ in den Beweis eines Lemmas auf p. 134 in [Shoe67] die Einschränkung auf diese Art von definitorischen Erweiterungen explizit und in wesentlichem Ausmaß eingeht (im Zusammenhang mit dem dort untersuchten Begriff der „starken Unentscheidbarkeit“ von Modellen).

außer $\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y}$ *frei vorkommen und für die in* T *die Formeln*

$$\exists \mathbf{y}\, \mathbf{D} \qquad (\text{„Existenzbedingung für } \mathbf{f}\text{“}),$$
$$\mathbf{D} \,\&\, \mathbf{D}_{\boldsymbol{y}}[\mathbf{y}'] \to \mathbf{y} = \mathbf{y}' \qquad (\text{„Eindeutigkeitsbedingung für } \mathbf{f}\text{“})$$

beweisbar sind. Dann heißt T' **definitorische Erweiterung** *von* T **um die Einführung des Funktionssymbols** $\mathbf{f}$*, genau dann, wenn* $L_{T'}$ *aus* L_T *durch die Hinzunahme des Symbols* $\mathbf{f}$ *zu den Symbolen von* L_T *entsteht, sowie* T' *aus* T *durch die Hinzunahme des neuen nichtlogischen Axioms*

$$\mathbf{y} = \mathbf{f}\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D} \qquad (\text{„definierendes Axiom für } \mathbf{f}\text{“})$$

zu den Axiomen von T *hervorgeht.*

(iii) *Sei* $\{\mathbf{p}_i\}_{i\in A}$ *eine Familie von* n*-stelligen Prädikatssymbolen (*$n \in \mathbb{N}$*,* A *eine Indexmenge), die in* T *nicht vorkommen. Seien* $\mathbf{x}_1, \ldots, \mathbf{x}_n$ *verschiedene Variablen, seien* $\{\mathbf{D}^{(i)}\}_{i\in A}$ *eine Familie von Formeln von* T*, in denen keine Variablen außer* $\mathbf{x}_1, \ldots, \mathbf{x}_n$ *frei vorkommen.*

Dann heißt T' **definitorische Erweiterung** *von* T **um die Einführung von Prädikatensymbolen der Familie** $\{\mathbf{p}_i\}_{i\in A}$*, wenn* $L_{T'}$ *aus* L_T *durch die Hinzunahme aller Symbole von* $\{\mathbf{p}_i\}_{i\in A}$ *zu den Symbolen von* L_T *und* T' *aus* T *durch die Hinzunahme aller definierender Axiome des Axiomenschemas*

$$\left\{\ \mathbf{p}_i\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}^{(i)}\ \right\}_{i\in A} \qquad (\text{„definierende Axiome für } \mathbf{p}_i\text{“ } (i \in A))$$

entsteht.

(iv) *Sei* $\{\mathbf{f}_i\}_{i\in A}$ *eine Familie von* n*-stelligen Funktionssymbolen (*A *eine Indexmenge,* $n \in \mathbb{N}_0$*), die in* L_T *nicht vorkommen. Seien* $\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y}, \mathbf{y}'$ *verschiedene Variablen, sei* $\{\mathbf{D}^{(i)}\}_{i\in A}$ *eine Familie von Formeln in* T*, in denen nur* $\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y}$ *frei vorkommen und für die in* T *die Formeln*

$$\exists \mathbf{y}\, \mathbf{D}^{(i)} \qquad (i \in A),$$
$$\mathbf{D}^{(i)} \,\&\, \mathbf{D}^{(i)}_{\boldsymbol{y}}[\mathbf{y}'] \to \mathbf{y} = \mathbf{y}' \qquad (i \in A),$$

die Existenz- bzw. die Eindeutigkeitsbedingungen für $\mathbf{f}_i$ *(*$i \in A$*) beweisbar sind. Dann heißt* T **definitorische Erweiterung** *von* T' **um die Einführung von Funktionssymbolen, die der Familie** $\{\mathbf{f}_i\}_{i\in A}$ **angehören***, genau dann, wenn* $L_{T'}$ *eine Erweiterung von* L_T *um die Funktionssymbole* $\mathbf{f}_i$ *(für alle* $i \in A$*) und* T' *eine Erweiterung von* T *um die nichtlogischen, definierenden Axiome des Axiomenschemas*

$$\left\{\ \mathbf{y} = \mathbf{f}_i\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}^{(i)}\ \right\}_{i\in A} \qquad (\text{„definierende Axiome für } \mathbf{f}_i\text{“ } (i \in A))$$

ist.

(v) Weiters heißt nun T' eine **definitorische Erweiterung** *von T, wenn T' aus T durch endlich viele nacheinandergereihte Erweiterungsschritte vom Typ (i), (ii), (iii) oder (iv) aus T hervorgeht.*

Die wesentlichen Eigenschaften von definitorischen Erweiterungen, die wie in [Shoe67] aus endlich vielen Erweiterungsschritten der Typen (i) und (ii) in 2.1.2 bestehen, bleiben bei definitorischen Erweiterungen der hier definierten Form erhalten. Und zwar, daß zu jeder Formel $\mathbf{A}$ der erweiterten Theorie eine „Translation“ $\mathbf{A}^*$ von $\mathbf{A}$ in T existiert und daß die erweiterte Theorie T' eine konservative Erweiterung der ursprünglichen Theorie ist.

Satz 2.1.3. *T' sei definitorische Erweiterung von T. Dann gilt:*

(a) T' ist konservative Erweiterung von T (d.h. für alle Formeln $\mathbf{A}$ von T gilt: $\vdash_{T'} \mathbf{A} \Rightarrow \vdash_T \mathbf{A}$) ;

(b) Zu jeder Formel $\mathbf{A}$ von T' ist eine Formel $\mathbf{A}^*$ von T konstruierbar, die „Translation von $\mathbf{A}$ nach T“*, für die gilt:*

$$\vdash_{T'} \mathbf{A} \leftrightarrow \mathbf{A}^* ,$$
$$\vdash_{T'} \mathbf{A} \Leftrightarrow \vdash_T \mathbf{A}^* \qquad \textit{und}$$
$$\text{Ist } \mathbf{A} \text{ Formel von } T, \text{ so ist } \mathbf{A}^* \text{ gleich } \mathbf{A} .$$

Beweis. Diese Eigenschaften von definitorischen Erweiterungen werden in [Shoe67] für den Fall von Typ-(i)- und Typ-(ii)-Erweiterungen von Definition 2.1.2 gezeigt. Die dort dargestellten Beweise reichen im wesentlichen auch für die hier zusätzlich betrachteten allgemeineren Fälle aus. Hier wird auf die Beweise dort verwiesen und nur zusätzlich nötige Schritte werden ausführlich dargestellt.

(1) Um den Satz zu zeigen, reicht es aus, die Aussage für definitorische Erweiterungen T' von T zu beweisen, die aus einem einfachen Erweiterungsschritt vom Typ (iii) oder (iv) in Definition 2.1.2 aus T entstehen: Denn (α) wird diese Aussage für einfache Erweiterungsschritte vom Typ (i) und (ii) in Definition 2.1.2 in [Shoe67] gezeigt, und (β) ergibt sich die Aussage des Satzes für beliebige definitorische Erweiterungen T' von T (mehr oder weniger) sofort aus einem Induktionsbeweis über die Anzahl der definitorischen Erweiterungsschritte von T zu T'.

(2) Weiters recht es aus, für definitorische Erweiterungen T' von T, die aus einem einfachen Erweiterungsschritt vom Typ (iii) oder (iv) bestehen, zu zeigen, daß zu jeder Formel $\mathbf{A}$ von T' eine Formel $\mathbf{A}^*$ von T konstruiert werden kann mit

$$\vdash_{T'} \mathbf{A} \leftrightarrow \mathbf{A}^*, \tag{2.1}$$
$$\vdash_{T'} \mathbf{A} \Rightarrow \vdash_T \mathbf{A}^* \qquad \text{und} \tag{2.2}$$
$$\text{ist } \mathbf{A} \text{ Formel von } T, \text{ so ist } \mathbf{A}^* \text{ gleich } \mathbf{A} . \tag{2.3}$$

Dies ist deswegen ausreichend, weil damit dann auch folgt: (α) Für jede Formel $\mathbf{A}$ von T gilt:
$\vdash_{T'} \mathbf{A} \underset{(2.2)}{\Rightarrow} \vdash_T \mathbf{A}^* \underset{(2.3)}{\Rightarrow} \vdash_T \mathbf{A}$; T' ist also konservative Erweiterung von T.
Und: (β) $\vdash_T \mathbf{A}^* \underset{(T' \text{ ist Erw. von } T)}{\Longrightarrow} \vdash_T \mathbf{A}^* \underset{(2.1)}{\Rightarrow} \vdash_T \mathbf{A}$ (für alle Formeln $\mathbf{A}$ von T).

(3) Sei nun T' eine definitorische Erweiterung von T um einen Erweiterungsschritt vom Typ (iii) in Definition 2.1.2, d.h. T' entsteht aus T durch definitorische Einführung von n-stelligen Prädikatensymbolen $\mathbf{p}_i$ der Familie $\{\mathbf{p}_i\}_{i\in A}$ vermittels des Schemas $\left\{ \mathbf{p}_i\mathbf{x}_1 \dots \mathbf{x}_n \leftrightarrow \mathbf{D}^{(i)} \right\}_{i\in A}$ von definierenden Axiomen für $\mathbf{p}_i$, wobei $\mathbf{A}$ eine Indexmenge ist und $\mathbf{D}^{(i)}$ für alle $i \in A$ Formeln von T sind.

Dann kann $\mathbf{A}^*$ für eine beliebige Formel $\mathbf{A}$ über $L_{T'}$ analog wie im Fall (i) definiert bzw. gefunden werden: $\mathbf{A}^*$ entsteht aus $\mathbf{A}$ durch die Ersetzung aller in $\mathbf{A}$ vorkommenden atomaren Formeln $\mathbf{p}_i\mathbf{a}_1 \dots \mathbf{a}_n$ ($i \in A$) durch Formeln $\mathbf{D}^{(i)\prime}_{\boldsymbol{x}_1,\dots,\boldsymbol{x}_n}[\mathbf{a}_1, \dots, \mathbf{a}_n]$, wobei $\mathbf{D}^{(i)\prime}$ aus $\mathbf{D}^{(i)}$ jeweils durch Umbenennung gebundener Variablen so entsteht, daß in $\mathbf{D}^{(i)\prime}$ schließlich keine der in $\mathbf{a}_1, \dots, \mathbf{a}_n$ vorkommenden Variablen mehr als gebundene Variable auftritt.

Durch Einsetzung in definierende Axiome ergibt sich unter diesen Bedingungen dann immer $\vdash_{T'} \mathbf{p}_i\mathbf{a}_1 \dots \mathbf{a}_n \leftrightarrow \mathbf{D}^{(i)\prime}_{\boldsymbol{x}_1,\dots,\boldsymbol{x}_n}[\mathbf{a}_1, \dots, \mathbf{a}_n]$ und daraus ergibt sich $\vdash_{T'} \mathbf{A} \leftrightarrow \mathbf{A}^*$, d.h. (2.1), unter schrittweiser Anwendung des "Equivalence Theorems" in [Shoe67] für die einzelnen Ersetzungsschritte.

Ist $\mathbf{A}$ eine Formel auch von T, so finden zur Konstruktion von $\mathbf{A}^*$ keine Ersetzungen statt, d.h. $\mathbf{A}^*$ ist gleich $\mathbf{A}$, also gilt (2.3).

Bezüglich des Beweises von (2.2), d.h. von $\vdash_{T'} \mathbf{A} \Rightarrow \vdash_T \mathbf{A}^*$ für beliebige Formeln $\mathbf{A}$ von T', kann vollinhaltlich auf [Shoe67] verwiesen werden; der dort für den Fall von Typ-(i)-Erweiterungen geführte induktive Beweis über die Theoreme von T' kann hierher formal übernommen werden.

(4) Sei T' eine definitorische Erweiterung von T um einen Erweiterungsschritt vom Typ (iv) in Definition 2.1.2, d.h. also um die definitorische Einführung von n-stelligen ($n \in \mathbb{N}_0$) Funktionssymbolen $\mathbf{f}_i$ der Familie $\{\mathbf{f}_i\}_{i\in A}$ (A eine Indexmenge) vermittels des Schemas von definierenden Axiomen $\left\{ \mathbf{y} = \mathbf{f}_i\mathbf{x}_1 \dots \mathbf{x}_n \leftrightarrow \mathbf{D}^{(i)} \right\}_{i\in A}$, wobei $\mathbf{D}^{(i)}$ für alle $i \in A$ Formeln von T sind.

Dann kann $\mathbf{A}^*$ analog zu Typ-(ii)-Erweiterungen definiert werden (vgl. [Shoe67]): In dieser Definition reicht es aus, atomare Formeln $\mathbf{A}$ zu betrachten und in diesen schrittweise die Anzahl der vorkommenden Symbole $\mathbf{f}_i$ zu verringern: $\mathbf{A}$ sei $\mathbf{B}_{\boldsymbol{z}}[\mathbf{f}_i\mathbf{a}_1 \dots \mathbf{a}_n]$, wobei in $\mathbf{a}_1, \dots, \mathbf{a}_n$ kein Symbol $\mathbf{f}_j$ ($j \in A$) mehr vorkommt und $\mathbf{z}$

in $\mathbf{a}_1, \ldots, \mathbf{a}_n$ nicht vorkommt. Dann sei $\mathbf{A}^*$ induktiv als

$$\exists \mathbf{z} \left(\mathbf{D}^{(i)\prime}_{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n,\boldsymbol{y}}[\mathbf{a}_1, \ldots, \mathbf{a}_n, \mathbf{z}] \;\&\; \mathbf{B}^* \right)$$

definiert, wobei $\mathbf{D}^{(i)\prime}$ aus $\mathbf{D}^{(i)}$ erneut durch Umbenennung gebundener Variablen so entsteht, daß die obige Substitution möglich wird.

$\vdash_{T'} \mathbf{A} \leftrightarrow \mathbf{A}^*$ für atomares $\mathbf{A}$ kann nun wie in [Shoe67] gezeigt werden (nämlich induktiv über Ersetzungen der obigen Art, daß für $\mathbf{A}$ gleich $\mathbf{B}_{\boldsymbol{z}}[\mathbf{f}_i \mathbf{a}_1 \ldots \mathbf{a}_n]$, $\mathbf{a}_1, \ldots, \mathbf{a}_n$ enthalten kein $\mathbf{f}_j$ $(j \in A)$, $\mathbf{z}$ kommt in $\mathbf{a}_1, \ldots, \mathbf{a}_n$ nicht vor, unter der Annahme $\vdash_{T'} \mathbf{B} \leftrightarrow \mathbf{B}^*$ folgt, daß

$$\vdash_{T'} \exists \mathbf{z} \left(\mathbf{D}^{(i)\prime}_{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n,\boldsymbol{y}}[\mathbf{a}_1, \ldots, \mathbf{a}_n, \mathbf{z}] \;\&\; \mathbf{B}^* \right) \leftrightarrow \mathbf{A}$$

also $\vdash_{T'} \mathbf{A} \leftrightarrow \mathbf{A}^*$; der Beweis dafür kann von dort übernommen werden).

Für allgemeine Formeln $\mathbf{A}$ von T folgt $\vdash_{T'} \mathbf{A} \leftrightarrow \mathbf{A}^*$, d.h. (2.1), wegen des "Equivalence Theorems" aus der oben eingesehenen Einschränkung dieser Aussage auf atomare Formeln.

Ist $\mathbf{A}$ Formel von T, so finden in der Konstruktion von $\mathbf{A}^*$ keine Ersetzungen statt, d.h. $\mathbf{A}^*$ ist gleich $\mathbf{A}$, also gilt (2.3).

Damit bleibt nun übrig, zu zeigen, daß T' konservative Erweiterung von T ist (denn damit folgt für Formeln $\mathbf{A}$ von T' die Aussage (2.2):
$\vdash_{T'} \mathbf{A} \underset{(2.3)}{\Rightarrow} \vdash_T \mathbf{A}^* \underset{(T' \text{ ist kons. Erw. von } T)}{\Longrightarrow} \vdash_T \mathbf{A}^*$, also (2.2)) :

Analog zum Beweis für Typ (ii)-Erweiterungen in [Shoe67] sei T'' eine Erweiterung von T, deren Sprache $L_{T''}$ gleich $L_{T'}$ ist (gegenüber T also auch genau die zusätzlichen Funktionssymbole $\mathbf{f}_i$ $(i \in A)$ besitzt), und die als zusätzliche Axiome genau alle Formeln des Schemas $\left\{ \mathbf{D}^{(i)}_{\boldsymbol{y}}[\mathbf{f}\mathbf{x}_1 \ldots \mathbf{x}_n] \right\}_{i \in A}$ besitzt.

Nun ist T'' aber zu T' äquivalent: Wie in [Shoe67] kann gezeigt werden, daß für alle $i \in A$ gilt, daß $T\left[\mathbf{y} = \mathbf{f}_i \mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}^{(i)}\right]$ zu $T\left[\mathbf{D}^{(i)}_{\boldsymbol{y}}[\mathbf{f}_i \mathbf{x}_1 \ldots \mathbf{x}_n]\right]$ äquivalent ist, d.h. also, daß die definierenden Axiome von T' und die ihnen jeweils entsprechenden neuen Axiome von T'' mit den Mitteln von T wechselseitig auseinander herleitbar sind. Daraus folgt die Äquivalenz von T' und T''.

T'' ist nun aber konservative Erweiterung von T, was sich aus dem Theorem über funktionale Erweiterungen in [Shoe67] ("Theorem on Functional Extensions") so herleiten läßt: Ist $\mathbf{A}$ Formel von T und gilt $\vdash_{T''} \mathbf{A}$, so gilt wegen des "Compactness Theorems" jedenfalls $\vdash_{T[\mathbf{E}_{i_1},\ldots,\mathbf{E}_{i_m}]} \mathbf{A}$, für ein $m \in \mathbb{N}_0$ und $i_1, \ldots, i_m \in A$ und wobei damit $\mathbf{E}_{i_j}$ gleich $\mathbf{D}^{(i_j)}_{\boldsymbol{y}}[\mathbf{f}_{i_j} \mathbf{x}_1, \ldots, \mathbf{x}_n]$ (für $j \in \{1, \ldots, m\}$) ist (die Formeln $\mathbf{E}_{i_j}$ sind also bestimmte neue Axiome in T''). Nun ist $T[\mathbf{E}_{i_1}, \ldots, \mathbf{E}_{i_m}]$ aber konservative Erweiterung von T (denn nach dem "Theorem on Functional Extensions" sind $T[\mathbf{E}_{i_1}]$,

$T[\mathbf{E}_{i_1}][\mathbf{E}_{i_2}]$, ... , $T[\mathbf{E}_{i_1}]\ldots[\mathbf{E}_{i_m}]$ jeweils konservative Erweiterungen (und eine endliche Reihe von konservativen Erweiterungen über einer Grundtheorie ist natürlich selbst auch konservative Erweiterung über der Ausgangstheorie)). Da $\mathbf{A}$ Formel von T ist, folgt also auch $\vdash_T \mathbf{A}$.

Da T' und T'' äquivalent sind, ist damit auch gezeigt, daß T' konservative Erweiterung von T ist.

□

Definition 2.1.4. Die Theorie TAZ'.

TAZ' ist die definitorische Erweiterung von TAZ um die Prädikate der Kongruenzenfamilie $\{\equiv_n\}_{n\in\mathbb{N},\, n\geq 2}$ vermittels der definierenden Axiome des Schemas D.KON.S. :

$$\textbf{D.KON.S.} \qquad \left\{\ x \equiv_n y \leftrightarrow \exists\, z\, \left(x + \underline{n}\, z = y\right)\ \right\}_{n\in\mathbb{N},\, n\geq 2}.$$

Lemma 2.1.5. *TAZ' läßt die Quantorenelimination zu.*

Es gibt darüber hinaus ein genau beschreibbares, deterministisches (QE-) Verfahren, das zu einer vorgelegten Formel $\mathbf{A}$ von TAZ' in endlich vielen Schritten eine dazu in TAZ' äquivalente, offene Formel $\mathbf{B}$ herstellt, in der außerdem keine Variablen frei vorkommen, die nicht auch in $\mathbf{A}$ frei vorkommen.

(Es ließe sich grob abkürzend auch sagen: TAZ' läßt die QE auf eine effektive Weise zu.)

Beweis. Dieser erfolgt hier im Sinne einer Schilderung der wesentlichen Schritte des in [Pre29] vorgestellten Verfahrens:

(1) Allgemein kann ein effektives QE-Verfahren für eine Theorie T dann als vollständig gegeben angesehen werden, wenn eine genaue Beschreibung eines Verfahrens vorliegt, das es gestattet, zu jeder offenen Formel $\mathbf{A}'$ von T und jeder Variablen $\mathbf{x}$ eine offene Formel $\mathbf{B}'$ von T mit

$$\vdash_T \exists \mathbf{x}\mathbf{A}' \leftrightarrow \mathbf{B}'$$

effektiv zu konstruieren. Denn:

(i) Es ist dann auch möglich, zu jeder offenen Formel $\mathbf{A}''$ von T und jeder Variablen $\mathbf{x}$ eine offene Formel $\mathbf{B}''$ von T mit

$$\vdash_T \forall \mathbf{x}\mathbf{A}'' \leftrightarrow \mathbf{B}''$$

zu konstruieren:

Denn: Seien $\mathbf{A}''$ offen, $\mathbf{x}$ eine Variable, gegeben. Dann ist auch $\neg\,\mathbf{A}''$ offen und nach Annahme ist $\mathbf{B}_0''$ offen mit

$$\vdash_T \exists\mathbf{x}\neg\,\mathbf{A}'' \leftrightarrow \mathbf{B}_0''$$

aus $\exists\mathbf{x}\neg\,\mathbf{A}''$ effektiv konstruierbar. Daraus folgt aber sofort

$$\vdash_T \neg\,\exists\mathbf{x}\neg\,\mathbf{A}'' \leftrightarrow \neg\,\mathbf{B}_0''$$

was mit $\vdash_T \forall\mathbf{x}\,\mathbf{A}'' \leftrightarrow \mathbf{B}_0''$ gleichbedeutend ist, wenn man $\forall$ wie [Shoe67] als definiertes Symbol ansieht, oder woraus diese Aussage sofort logisch folgt. Hiermit ist aber nun eine gesuchte Formel $\mathbf{B}''$ in $\neg\,\mathbf{B}_0''$ gefunden worden.

(ii) Um zu einer Formel $\mathbf{A}$ von T eine in T äquivalente offene Formel $\mathbf{B}$ effektiv zu finden, kann man nun so vorgehen:

Ist $\mathbf{A}$ selbst offen, so bleibt nichts mehr zu tun. Man wählt $\mathbf{A}$ für $\mathbf{B}$.

Enthält $\mathbf{A}$ aber Quantoren, so formt man $\mathbf{A}$ durch Pränex-Operationen äquivalent zu einer Formel der Gestalt $(Q_1\mathbf{x}_1)\ldots(Q_n\mathbf{x}_n)\,\mathbf{A}'$ um, wobei Q_i $(1 \leq i \leq n)$ hierin für Quantifikationen $\exists$ oder $\forall$ stehen, $\mathbf{A}'$ offen ist und $n \in \mathbb{N}$ gilt, und eliminiert dann nacheinander von innen beginnend die einzelnen Quantoren. D.h. genau:

Unter Benutzung des in der Annahme vorausgesetzten Verfahrens sowie des in (i) beschriebenen konstruiert man von $(Q_1\mathbf{x}_1)\ldots(Q_n\mathbf{x}_n)\mathbf{A}'$ ausgehend nacheinander effektiv offene Formeln $\mathbf{B}_1,\ldots,\mathbf{B}_n$ von T mit:

$$\begin{aligned}
&\vdash_T (Q_n\mathbf{x}_n)\,\mathbf{A}' \leftrightarrow \mathbf{B}_1\,,\\
&\vdash_T (Q_{n-1}\mathbf{x}_{n-1})\,\mathbf{B}_1 \leftrightarrow \mathbf{B}_2\,,\\
&\quad\vdots\\
&\vdash_T (Q_1\mathbf{x}_1)\,\mathbf{B}_{n-1} \leftrightarrow \mathbf{B}_n\,.
\end{aligned}$$

Hieraus folgt für $\mathbf{B}_n$ ($(n-1)$-malige Anwendung des "Equivalence Theorem"s aus [Shoe67]) jedoch

$$\vdash_T (Q_1\mathbf{x}_1)\ldots(Q_n\mathbf{x}_n)\mathbf{A}' \leftrightarrow \mathbf{B}_n\,,$$

woraus mit $\vdash_T \mathbf{A} \leftrightarrow (Q_1\mathbf{x}_1)\ldots(Q_n\mathbf{x}_n)\mathbf{A}'$ (wegen Pränex-Operationen) sofort folgt:

$$\vdash_T \mathbf{A} \leftrightarrow \mathbf{B}_n\,.$$

Die zu $\mathbf{A}$ gesuchte, in T äquivalente offene Formel $\mathbf{B}$ wurde also dann in $\mathbf{B}_n$ effektiv gefunden.

(2) Ist nun für eine Theorie T ein Verfahren gegeben, um zu einer Formel $\exists \mathbf{x}\mathbf{A}'$, $\mathbf{A}$' offen, eine in T äquivalente Formel $\mathbf{B}$' mit der weiteren Eigenschaft, daß in $\mathbf{B}$' keine Variablen frei vorkommen, die nicht auch in $\exists \mathbf{x}\mathbf{A}'$ frei vorkommen, zu konstruieren, so besitzt die in (1) beschriebene Ausdehnung dieses Verfahrens auf alle Formeln $\mathbf{A}$ von T ebenfalls diese Eigenschaft, daß in der entsprechenden, zu $\mathbf{A}$ in T äquivalenten, quantorenfreien Formel $\mathbf{B}$ gegenüber der Ausgangsformel $\mathbf{A}$ keine neuen freien Variablen vorkommen.

(Im folgenden wird die Bezeichnung $\mathbf{A}$ jedoch auch für offene Formeln verwendet werden, auf die in den Verfahrensbeschreibungen bisher immer mit $\mathbf{A}'$ verwiesen worden ist.)

(3) Im weiteren reicht es nun aus, ein Verfahren anzugeben, wie zu einer Formel $\exists \mathbf{x}\mathbf{A}$, $\mathbf{A}$ offen und in Negationsnormalform (NNF) (d.h. $\mathbf{A}$ solcherart, daß darin Negationssymbole nur unmittelbar vor atomaren Formeln stehen), eine in T äquivalente Formel $\mathbf{B}$ gefunden werden kann, in der gegenüber $\exists \mathbf{x}\mathbf{A}$ keine neuen freien Variablen auftreten:

Dies deswegen, weil eine beliebige Formel $\mathbf{A}$ durch aussagenlogische Umformungen leicht auf diese entsprechende Gestalt in äquivalenter Weise gebracht werden kann (d.h., in dem Negationszeichen ganz nach innen gebracht und dann weiters jeweils zwei aufeinanderfolgende Negationszeichen eliminiert werden).

(4) Im Fall von TAZ' kann nun die Menge der Ausgangsformeln $\exists \mathbf{x}\,\mathbf{A}$, wobei $\mathbf{A}$ offen und wie in (3), eines anzugebenden Verfahrens weiters noch dahingehend eingeschränkt werden, daß sich bei Ausgangsformeln der verkleinerten Menge $\neg$ auch nicht auf atomare Formeln mit Prädikatssymbolen $\equiv_n$ ($n \in \mathbb{N}$, $n \geq 2$) bezieht:

Dies deshalb, weil in einer Ausgangsformel $\exists \mathbf{x}\,\mathbf{A}$ ($\mathbf{A}$ wie in (3) gefordert) eventuell auftretende Teilformeln der Gestalt $\neg\, \mathbf{a} \equiv_n \mathbf{b}$ ($n \in \mathbb{N}$, $n \geq 2$, $\mathbf{a}, \mathbf{b}$ Terme von TAZ) durch Formeln

$$\mathbf{a} + 1 \equiv_n \mathbf{b} \;\vee\; \mathbf{a} + \underline{\underline{2}} \equiv_n \mathbf{b} \;\vee\; \ldots \;\vee\; \mathbf{a} + \underline{\underline{n-1}} \equiv_n \mathbf{b}$$

äquivalent ersetzt werden können und die dann entstehende Formel nach solchen Ersetzungen wieder in DNF-Gestalt, wobei gleichzeitig erneut auch NNF-Gestalt erreicht wird, gebracht werden kann, sodaß darin dann keine verneinten atomaren Formeln mit Prädikatssymbol $\equiv_n$ ($n \in \mathbb{N}$, $n \geq 2$) mehr vorkommen. – Diese hierbei verwendeten Ersetzungen sind wegen

$$\vdash_{TAZ'} \neg\, x \equiv_n y \;\leftrightarrow\; x + 1 \equiv_n y \;\vee\; x + \underline{\underline{2}} \equiv_n y \;\vee\; \ldots \;\vee\; x + \underline{\underline{n-1}} \equiv_n y$$

und dem "Equivalence Theorem" in [Shoe67] tatsächlich äquivalente Umformungen (in TAZ').

(5) In [Pre29] wird nun die QE lediglich für Formeln $\exists \mathbf{x}\, \mathbf{A}$, $\mathbf{A}$ offen, $\mathbf{A}$ ist eine *Konjunktion* von atomaren Formeln mit Prädikatssymbol $=$ oder $\equiv_n$ ($n \in \mathbb{N}$, $n \geq 2$) (: Gleichungen und Kongruenzen) oder verneinten atomaren Formeln mit Prädikatssymbol $=$ (: verneinte Gleichungen) geschildert:

Dies ist deswegen berechtigt, weil zu einer Ausgangsformel $\exists \mathbf{x}\, \mathbf{A}$, $\mathbf{A}$ wie in (4), $\mathbf{A}$ durch aussagenlogische Umformungen auf eine disjunktive Normalform $\mathbf{A}_1 \vee \mathbf{A}_2 \vee \ldots \vee \mathbf{A}_n$ gebracht werden kann, wobei die $\mathbf{A}_i$ gerade Konjunktionen von der hier betrachteten Form sind und weil insgesamt dann gilt:

$$\begin{aligned} \vdash \exists \mathbf{x}\, \mathbf{A} &\leftrightarrow \exists \mathbf{x} \left(\mathbf{A}_1 \vee \mathbf{A}_2 \vee \ldots \vee \mathbf{A}_n \right) \\ &\leftrightarrow \exists \mathbf{x}\, \mathbf{A}_1 \vee \exists \mathbf{x}\, \mathbf{A}_2 \vee \ldots \vee \exists \mathbf{x}\, \mathbf{A}_n \end{aligned}$$

(Dies gilt für allgemeine Konjunktionen $\mathbf{A}$ gleich $\mathbf{A}_1 \vee \mathbf{A}_2 \vee \ldots \vee \mathbf{A}_n$ in jeder Theorie.)

(6) Nun können die atomaren Formeln von TAZ' bezüglich einer Variablen $\mathbf{x}$ immer äquivalent durch atomare Formeln der Gestalt $\underline{\alpha}\, \mathbf{x} + \mathbf{a} = \mathbf{b}$, $\underline{\alpha}\, \mathbf{x} + \mathbf{a} \equiv_n \mathbf{b}$, $\mathbf{a} = \mathbf{b}$ oder $\mathbf{a} \equiv_n \mathbf{b}$ ($\alpha \in \mathbb{N}$, $n \in \mathbb{N}$, $n \geq 2$, $\mathbf{a}, \mathbf{b}$ Terme, in denen $\mathbf{x}$ nicht vorkommt) ersetzt werden.

Eine atomare Formel, in der $\mathbf{x}$ vorkommt, ist nämlich zuerst durch assoziative und kommutative Umformungen auf eine Gestalt $\underline{\alpha_1}\, \mathbf{x} + \mathbf{a} = \underline{\alpha_2}\, \mathbf{x} + \mathbf{b}$ bzw. $\underline{\alpha_1}\, \mathbf{x} + \mathbf{a} \equiv_n \underline{\alpha_2}\, \mathbf{x} + \mathbf{b}$ ($\alpha_1, \alpha_2 \in \mathbb{N}_0$, $\alpha_1 + \alpha_2 > 0$, $n \in \mathbb{N}$, $n \geq 2$, $\mathbf{a}, \mathbf{b}$ Terme ohne $\mathbf{x}$) umformbar und dann wegen TAZ.3. zu Formeln der Gestalt $\underline{\alpha}\, \mathbf{x} + \mathbf{a} = \mathbf{b}$, $\underline{\alpha}\, \mathbf{x} + \mathbf{a} \equiv_n \mathbf{b}$ bzw. $\mathbf{a} = \mathbf{b}$ oder $\mathbf{a} \equiv_n \mathbf{b}$ äquivalent ($\alpha \in \mathbb{N}$, n, $\mathbf{a}$ und $\mathbf{b}$ wie oben).

Im weiteren werden folgende Abkürzungen für den Typ von solcherart umgeformten atomaren Formeln und bestimmten negierten entsprechenden Formeln verwendet:

$\underline{\alpha}\, \mathbf{x} + \mathbf{a} = \mathbf{b}$	... „vom Typ $\boldsymbol{GL}(\mathbf{x})$“	(„Gleichung in $\mathbf{x}$“)
$\underline{\alpha}\, \mathbf{x} + \mathbf{a} \equiv_n \mathbf{b}$	... „vom Typ $\boldsymbol{K}(\mathbf{x})$“	(„Kongruenz in $\mathbf{x}$“)
$\neg\, \underline{\alpha}\, \mathbf{x} + \mathbf{a} = \mathbf{b}$	... „vom Typ $\boldsymbol{NGL}(\mathbf{x})$“	(„Negierte Gleichung in $\mathbf{x}$“)
$\mathbf{a} = \mathbf{b}$	... „vom Typ $\boldsymbol{GL}_{\boldsymbol{x}}$“	(„Gleichung ohne $\mathbf{x}$“)
$\mathbf{a} \equiv_n \mathbf{b}$	... „vom Typ $\boldsymbol{K}_{\boldsymbol{x}}$“	(„Kongruenz ohne $\mathbf{x}$“)
$\neg\, \mathbf{a} = \mathbf{b}$	... „vom Typ $\boldsymbol{NGL}_{\boldsymbol{x}}$“	(„Negierte Gleichung ohne $\mathbf{x}$“)

(wobei $\alpha \in \mathbb{N}$ und $\mathbf{a}, \mathbf{b}$ Terme ohne $\mathbf{x}$, $n \in \mathbb{N}$, $n \geq 2$).

(7) Um nun den $\exists$-Quantor in einer Formel $\exists \mathbf{x}\, \mathbf{A}$ von TAZ', $\mathbf{A}$ offen, $\mathbf{A}$ ist eine Konjunktion von Gleichungen, negierten Gleichungen und Kongruenzen, zu eliminieren,

benutzte Presburger eine Vorgangsweise entsprechend dem folgenden Ersetzungsregelschema bezüglich beliebiger Variablen $\mathbf{x}$:

R1. $\boldsymbol{GL}(\mathbf{x})\ \&\ \boldsymbol{GL}(\mathbf{x}) \quad \twoheadrightarrow \quad \boldsymbol{GL}(\mathbf{x})\ \&\ \boldsymbol{GL}_{\boldsymbol{x}}$

R2. $\boldsymbol{GL}(\mathbf{x})\ \&\ \boldsymbol{NGL}(\mathbf{x}) \twoheadrightarrow \quad \boldsymbol{GL}(\mathbf{x})\ \&\ \boldsymbol{NGL}_{\boldsymbol{x}}$

R3. $\boldsymbol{GL}(\mathbf{x})\ \&\ \boldsymbol{K}(\mathbf{x}) \quad \twoheadrightarrow \quad \boldsymbol{GL}(\mathbf{x})\ \&\ \boldsymbol{K}_{\boldsymbol{x}}$

R4. $\boldsymbol{K}(\mathbf{x})\ \&\ \boldsymbol{K}(\mathbf{x}) \quad \twoheadrightarrow \quad \boldsymbol{K}(\mathbf{x})\ \&\ \boldsymbol{K}_{\boldsymbol{x}}$

R5. $\exists\,\mathbf{x}\,(\,\boldsymbol{GL}(\mathbf{x})\,) \quad \twoheadrightarrow \quad \boldsymbol{K}_{\boldsymbol{x}}$ bzw. $0 = 0$

R6. $\exists\,\mathbf{x}\,(\,\boldsymbol{K}(\mathbf{x})\,) \quad \twoheadrightarrow \quad \boldsymbol{K}_{\boldsymbol{x}}$ bzw. $0 = 0$

R7. $\exists\,\mathbf{x}\,\big(\,\boldsymbol{K}(\mathbf{x})\ \&\ \boldsymbol{NGL}(\mathbf{x})\ \&\ \ldots\ \&\ \boldsymbol{NGL}(\mathbf{x})\,\big) \twoheadrightarrow \quad \boldsymbol{K}_{\boldsymbol{x}}$ bzw. $0 = 0$

R8. $\exists\,\mathbf{x}\,\big(\,\boldsymbol{K}(\mathbf{x})\ \&\ \boldsymbol{NGL}(\mathbf{x})\ \&\ \ldots\ \&\ \boldsymbol{NGL}(\mathbf{x})\,\big) \twoheadrightarrow \quad 0 = 0\ .$

Hierbei sollen Ersetzungsregeln dieses Schemas als Verfahren betrachtet werden, die es ermöglichen, zu einer Formel von TAZ', die vom Formeltyp der linken Seite einer Regel ist, eine in TAZ' äquivalente Formel vom Typ der rechten Regelseite effektiv zu finden; weiters sollen bei diesen Umformungen von Formeln gegenüber der Ausgangsformel keine neuen freien Variablen in der Ergebnisformel entstehen und die Variable $\mathbf{x}$ soll jeweils nur mehr in jenen Formeln auftreten, deren Typ das zuläßt.

Die Ersetzungsregeln R1.–R4. werden im weiteren dazu dienen, ausgehend von einer Formel $\exists\,\mathbf{x}\,\mathbf{A}$ von TAZ', $\mathbf{A}$ offen, $\mathbf{A}$ ist eine Konjunktion von Formeln der Typen $\boldsymbol{GL}(\mathbf{x})$, $\boldsymbol{NGL}(\mathbf{x})$, $\boldsymbol{K}(\mathbf{x})$, $\boldsymbol{GL}_{\boldsymbol{x}}$, $\boldsymbol{NGL}_{\boldsymbol{x}}$, $\boldsymbol{K}_{\boldsymbol{x}}$ innerhalb von $\mathbf{A}$ die Anzahl der $\mathbf{x}$ enthaltenden Konjunktionsformeln weitgehend und durch schrittweise Ersetzungen zu verringern; soweit, daß $\mathbf{A}$ durch $\mathbf{B}_1\ \&\ \mathbf{B}_2$ äquivalent ersetzt werden kann, wobei $\mathbf{B}_2$ $\mathbf{x}$ nicht mehr enthält und schließlich eine zu $\exists\mathbf{x}\,\mathbf{A}$ äquivalente offene Formel $\mathbf{B}$ gefunden werden kann, indem mittels der Regeln R5.–R8. eine zu $\exists\mathbf{x}\,\mathbf{B}_1$ äquivalente offene Formel $\mathbf{B}'_1$ gefunden wird und $\mathbf{B}$ gleich $\mathbf{B}'_1\ \&\ \mathbf{B}_2$ gesetzt wird (vgl. Schritt (7)).

Im folgenden seien nun solche Verfahren an einigen Beispielen beschrieben und begündet: Zuerst sei dabei hier R3. betrachtet:

Sei eine Formel $\mathbf{C}$ vom Typ $\boldsymbol{GL}(\mathbf{x})\ \&\ \boldsymbol{K}(\mathbf{x})$ gegeben, d.h. eine Formel $\mathbf{C}$ gleich $\mathbf{C}_1\ \&\ \mathbf{C}_2$, wobei $\mathbf{C}_1$ vom Typ $\boldsymbol{GL}(\mathbf{x})$ und $\mathbf{C}_2$ vom Typ $\boldsymbol{K}(\mathbf{x})$ ist. Dann ist $\mathbf{C}_1$ von der Gestalt $\underline{\alpha}\,\mathbf{x} + \mathbf{a} = \mathbf{b}$ und $\mathbf{C}_2$ von der Gestalt $\underline{\alpha'}\,\mathbf{x} + \mathbf{a}' \equiv_n \mathbf{b}'$ (für $\alpha, \alpha' \in \mathbb{N}$, und Terme $\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}'$ in T, in denen $\mathbf{x}$ nicht vorkommt, sowie für $n \in \mathbb{N}$, $n \geq 2$). Nun kann in TAZ' begründet werden, daß $\underline{\alpha}\,\mathbf{x} + \mathbf{a} = \mathbf{b}\ \&\ \underline{\alpha'}\,\mathbf{x} + \mathbf{a}' \equiv_n \mathbf{b}'$ durch $\underline{\alpha\,\alpha'}\,\mathbf{x} + \underline{\alpha'}\,\mathbf{a} = \underline{\alpha'}\,\mathbf{b}\ \&\ \underline{\alpha\,\alpha'}\,\mathbf{x} + \underline{\alpha}\,\mathbf{a}' \equiv_{\alpha\,n} \underline{\alpha}\,\mathbf{b}'$ ersetzt werden kann und also durch eine Formel der Gestalt $\underline{\gamma}\,\mathbf{x} + \mathbf{c} = \mathbf{d}\ \&\ \underline{\gamma}\,\mathbf{x} + \mathbf{c}' \equiv_m \mathbf{d}'$ ($\gamma \in \mathbb{N}$, $\mathbf{c}, \mathbf{c}', \mathbf{d}, \mathbf{d}'$ Terme in T, in denen $\mathbf{x}$ nicht vorkommt, $m \in \mathbb{N}$, $m \geq 2$). Diese wiederum kann durch $\underline{\gamma}\,\mathbf{x} + \mathbf{c} = \mathbf{d}\ \&\ \mathbf{c}' + \mathbf{d} \equiv_m \mathbf{c} + \mathbf{d}'$ ersetzt werden, das sei die Formel $\mathbf{D}$. Insgesamt gilt für entsprechende $\alpha, \alpha', \gamma \in \mathbb{N}$, $n, m \in \mathbb{N}$, $n, m \geq 2$, und Terme $\mathbf{a}, \mathbf{a}', \mathbf{b}, \mathbf{b}', \mathbf{c}, \mathbf{c}'\ \mathbf{d}, \mathbf{d}'$,

in denen $\mathbf{x}$ nicht vorkommt:

$$\begin{aligned}
\vdash_{TAZ'} \mathbf{C} &\leftrightarrow \mathbf{C}_1 \ \&\ \mathbf{C}_2 \\
&\leftrightarrow \underline{\alpha}\,\mathbf{x} + \mathbf{a} = \mathbf{b} \ \&\ \underline{\alpha}\,\mathbf{x} + \mathbf{a}' \equiv_n \mathbf{b}' \\
&\leftrightarrow \underline{\alpha\,\alpha'}\,\mathbf{x} + \underline{\alpha'}\,\mathbf{a} = \underline{\alpha'}\,\mathbf{b} \ \&\ \underline{\alpha\,\alpha'}\,\mathbf{x} + \underline{\alpha}\,\mathbf{a}' \equiv_{\alpha\,n} \underline{\alpha}\,\mathbf{b}' \\
&\leftrightarrow \underline{\gamma}\,\mathbf{x} + \mathbf{c} = \mathbf{d} \ \&\ \underline{\gamma}\,\mathbf{x} + \mathbf{c}' \equiv_m \mathbf{d}' \\
&\leftrightarrow \underline{\gamma}\,\mathbf{x} + \mathbf{c} = \mathbf{d} \ \&\ \mathbf{c}' + \mathbf{d} \equiv_m \mathbf{c} + \mathbf{d}' \\
&\leftrightarrow \mathbf{D}
\end{aligned}$$

(Dabei sind hier und häufig auch im folgenden Darstellungen von Äquivalenzumformungen in einer Theorie T von Formeln $\mathbf{A}$ zu Formeln $\mathbf{B}$ wie

$$\begin{aligned}
\vdash_T \mathbf{A} &\leftrightarrow \mathbf{A}_1 \\
&\leftrightarrow \mathbf{A}_2 \\
&\ \ \vdots \\
&\leftrightarrow \mathbf{A}_n \\
&\leftrightarrow \mathbf{B}
\end{aligned}$$

als abgekürzte Schreibweisen für die Gültigkeit der Kette von Aussagen

$$\vdash_T \mathbf{A} \leftrightarrow \mathbf{A}_1\,, \quad \vdash_T \mathbf{A}_1 \leftrightarrow \mathbf{A}_2\,, \quad \ldots\,, \vdash_T \mathbf{A}_{n-1} \leftrightarrow \mathbf{A}_n\,, \quad \vdash_T \mathbf{A}_n \leftrightarrow \mathbf{B}\,,$$

die die Beweisbarkeit der einzelnen Schritte der oben vereinfacht angeschriebenen, (in T) äquivalenten Umformung von $\mathbf{A}$ zu $\mathbf{B}$ ausdrücken, zu verstehen.)

Auf diesem Weg ist also hiermit auf effektive Weise zu einer offenen Formel $\mathbf{C}$ vom Typ $\boldsymbol{GL}(\mathbf{x})$ & $\boldsymbol{K}(\mathbf{x})$ eine äquivalente offene Formel $\mathbf{D}$ vom Typ $\boldsymbol{GL}(\mathbf{x})$ & $\boldsymbol{K}_{\boldsymbol{x}}$ gewonnen werden.

Die Einzelschritte in dieser logischen Umformung in TAZ' ergeben sich hier beispielsweise unter ausschließlicher Benützung der Axiome TAZ.1. und TAZ.4., sowie von solchen des Schemas TAZ.S3. .

R5. ist so zu begründen: Sei $\mathbf{C}$ eine offene Formel vom Typ $\boldsymbol{GL}(\mathbf{x})$. Es gibt also $\alpha \in \mathbb{N}$, $\mathbf{a}, \mathbf{b}$ Terme ohne $\mathbf{x}$, sodaß $\mathbf{C}$ gleich $\underline{\alpha}\,\mathbf{x} + \mathbf{a} = \mathbf{b}$ ist. Nun ist jedoch klar, daß $\exists\,\mathbf{x}\,(\,\underline{\alpha}\,\mathbf{x} + \mathbf{a} = \mathbf{b}\,)$ im Fall $\alpha = 1$ wegen TAZ.4. (der Existenz inverser Elemente bezüglich $+$) immer beweisbar ist bzw. im Fall $\alpha \neq 1$ wegen D.KON.S. zu $\mathbf{a} \equiv_\alpha \mathbf{b}$ äquivalent ist. Im Fall $\alpha \neq 1$ gilt z.B. also insgesamt mit $\mathbf{D}$ gleich $\mathbf{a} \equiv_\alpha \mathbf{b}$:

$$\begin{aligned}
\vdash_{TAZ'} \exists\,\mathbf{x}\mathbf{C} &\leftrightarrow \exists\,\mathbf{x}\,(\,\underline{\alpha}\,\mathbf{x} + \mathbf{a} = \mathbf{b}\,) \\
&\leftrightarrow \mathbf{a} \equiv_\alpha \mathbf{b} \\
&\leftrightarrow \mathbf{D}
\end{aligned}$$

Insgesamt ist damit klar, wie eine Formel vom Typ $\exists\,\mathbf{x}\,\boldsymbol{GL}(\mathbf{x})$ äquivalent entweder durch die offene Formel $0=0$ oder eine $\mathbf{x}$ nicht mehr enthaltende (und keine neuen freien Variablen enthaltende) Formel vom Typ $\boldsymbol{K}_{\boldsymbol{x}}$ ersetzt werden kann. (Für die hier beteiligten Umformungen benötigte nichtlogische Axiome von TAZ': TAZ.1., TAZ.2., TAZ.3., TAZ.4., D.KON.S. .)

R6. ist so einzusehen: Es sei eine Formel $\mathbf{C}$ vom Typ $\boldsymbol{K}(\mathbf{x})$ gegeben. $\mathbf{C}$ ist also für bestimmte $\alpha\in\mathbb{N}$, $n\in\mathbb{N}$, $n\geq 2$, $\mathbf{a},\mathbf{b}$ Terme ohne $\mathbf{x}$ gleich $\underline{\alpha}\,\mathbf{x}+\mathbf{a}\equiv_n\mathbf{b}$. Sei nun $c:=\mathrm{ggT}(\alpha,n)$ und sei $c\neq 1$ (im Fall $c=1$, so ist $\mathbf{C}$ ja zu $\mathbf{D}$ gleich $0=0$ äquivalent). Dann gilt mit $\mathbf{D}$ gleich $\mathbf{a}\equiv_c\mathbf{b}$, falls $\mathbf{y}$ eine neue Variable $\mathbf{x}$ ist, noch in $\mathbf{a}$ oder $\mathbf{b}$ vorkommt:

$$\begin{aligned}
\vdash_{TAZ'}\exists\,\mathbf{x}\,\mathbf{C} &\leftrightarrow \exists\,\mathbf{x}\,(\,\underline{\alpha}\,\mathbf{x}+\mathbf{a}\equiv_n\mathbf{b}\,)\\
&\leftrightarrow \exists\,\mathbf{x}\,\exists\,\mathbf{y}\,(\,\underline{\alpha}\,\mathbf{x}+\underline{n}\,\mathbf{y}+\mathbf{a}\equiv_n\mathbf{b}\,)\\
&\leftrightarrow \exists\,\mathbf{x}\,\exists\,\mathbf{y}\,\big(\,\underline{c}\,\big(\,\underline{\tfrac{\alpha}{c}}\,\mathbf{x}+\underline{\tfrac{n}{c}}\,\mathbf{y}\,\big)+\mathbf{a}=\mathbf{b}\,\big)\\
&\leftrightarrow \exists\,\mathbf{x}\,(\,\underline{c}\,\mathbf{x}+\mathbf{a}\equiv_n\mathbf{b}\,)\\
&\leftrightarrow \mathbf{a}\equiv_c\mathbf{b}\\
&\leftrightarrow \mathbf{D}
\end{aligned}$$

Hierbei ergibt sich der Teilschritt

$$\vdash_{TAZ'}\exists\,\mathbf{x}\,(\,\underline{c}\,\mathbf{x}+\mathbf{a}\equiv_n\mathbf{b}\,)\rightarrow\exists\,\mathbf{x}\,\exists\,\mathbf{y}\,\big(\,\underline{c}\,\big(\,\underline{\tfrac{\alpha}{c}}\,\mathbf{x}+\underline{\tfrac{n}{c}}\,\mathbf{y}\,\big)+\mathbf{a}=\mathbf{b}\,\big)\tag{2.4}$$

in folgender Weise:

Da $c=\mathrm{ggT}(\alpha,n)$ existieren natürliche Zahlen x^*, y^* so, daß $c=\alpha\,x^*-n\,y^*$. In TAZ' ist dann jedenfalls $\vdash_{TAZ'}\underline{c}\,\mathbf{x}+\underline{n\,y^*}\,\mathbf{x}=\underline{\alpha\,x^*}\,\mathbf{x}$ beweisbar. Damit ist nun leicht zu beweisen:

$$\vdash_{TAZ'}\exists\,\mathbf{x}\,(\,\underline{c}\,\mathbf{x}+\mathbf{a}\equiv_n\mathbf{b}\,)\rightarrow\exists\,\mathbf{x}\,(\,\underline{\alpha\,x^*}\,\mathbf{x}+\mathbf{a}\equiv_n\mathbf{b}+\underline{n\,y^*}\,\mathbf{x}\,)\,.\tag{2.5}$$

Sowie im weiteren

$$\vdash_{TAZ'}\exists\,\mathbf{x}\,(\,\underline{\alpha\,x^*}\,\mathbf{x}+\mathbf{a}\equiv_n\mathbf{b}+\underline{n\,y^*}\,\mathbf{x}\,)\rightarrow\exists\,\mathbf{x}\,\exists\,\mathbf{y}\,(\,\underline{\alpha}\,\mathbf{x}+\mathbf{a}=\mathbf{b}+\underline{n}\,\mathbf{y}\,)\tag{2.6}$$

und

$$\vdash_{TAZ'}\exists\,\mathbf{x}\,\exists\,\mathbf{y}\,(\,\underline{\alpha}\,\mathbf{x}+\mathbf{a}=\mathbf{b}+\underline{n}\,\mathbf{y}\,)\rightarrow\exists\,\mathbf{x}\,\exists\,\mathbf{y}\,\big(\,\underline{c}\,\big(\,\underline{\tfrac{\alpha}{c}}\,\mathbf{x}+\underline{\tfrac{n}{c}}\,\mathbf{y}\,\big)+\mathbf{a}=\mathbf{b}\,\big)\tag{2.7}$$

(2.4) folgt nun aus (2.5), (2.6) und (2.7). (Für diesen Schritt benötigte nichtlogische Axiome von TAZ': TAZ.1., TAZ.2., TAZ.3., TAZ.4., D.KON.S. .)

Bis auf R4., das etwas schwieriger zu begründen ist, sind die restlichen Regeln leicht einzusehen. Bemerkenswert ist dabei vielleicht, daß die Schemata TAZ.S2. und

TAZ.S3. an keiner Stelle in die Begründung der Regeln eingehen und in das Verfahren nur zur Rechtfertigung der Ersetzungsschritte von Formeln der Gestalt $\neg\, \mathbf{a} \equiv_n \mathbf{b}$ ($n \in \mathbb{N}$, $n \geq 2$) durch Formeln $\mathbf{a}+1 \equiv_n \mathbf{b} \vee \mathbf{a}+\underline{2} \equiv_n \mathbf{b} \vee \ldots \vee \mathbf{a}+\underline{\underline{n-1}} \equiv_n \mathbf{b}$, also zur Begründung von

$$\vdash_{TAZ'} \neg\, x \equiv_n y \leftrightarrow x+1 \equiv_n y \vee x+\underline{2} \equiv_n y \vee \ldots \vee x+\underline{\underline{n-1}} \equiv_n y$$

gemeinsam eingehen[10].

Die exakte Zurückführung der Umformungsschritte auf in TAZ' beweisbare Aussagen ist umständlich und geschieht hier ebensowenig wie in [Pre29], man kann sich in jedem einzelnen Fall jedoch rasch davon überzeugen, daß das immer möglich ist.

(8) Das in (7) vorgestellte und teilweise begründete Ersetzungsregelschema für einfache Konjunktionsformeln von TAZ' kann nun in folgender Weise zur Elimination des $\exists$-Quantors in Formeln $\exists\, \mathbf{x}\, \mathbf{A}$ ($\mathbf{A}$ offen, wie in (5) gefordert) verwendet werden:

Sei $\mathbf{A}$ also eine offene Formel in TAZ', $\mathbf{x}$ eine Variable, $\mathbf{A}$ ist eine Konjunktion von Formeln der möglichen Typen $\boldsymbol{GL}(\mathbf{x})$, $\boldsymbol{K}(\mathbf{x})$, $\boldsymbol{NGL}(\mathbf{x})$, $\boldsymbol{GL_x}$, $\boldsymbol{K_x}$, $\boldsymbol{NGL_x}$. Eine zu $\exists\, \mathbf{x}\, \mathbf{A}$ in TAZ' äquivalente offene Formel $\mathbf{B}$, in der gegenüber $\mathbf{A}$ keine neuen freien Variablen (und auch $\mathbf{x}$ nicht mehr) auftreten, kann nun mit Hilfe der Vorgangsweisen in den einzelnen Fällen der folgenden Fallunterscheidungen gefunden werden:

Fall 1: $\mathbf{A}$ enthält eine Konjunktionsformel vom Typ $\boldsymbol{GL}(\mathbf{x})$:

Durch fortgesetztes Anwenden der Ersetzungsregeln R1., R2. und R3. auf verschiedene Konjunktionsformeln von $\mathbf{A}$ kann (jeweils durch Ersetzung von Formelpaaren durch ein davon abgeleitetes Paar) die Zahl der Konjunktionen $\boldsymbol{K}(\mathbf{x})$ und negierten Gleichungen $\boldsymbol{NGL}(\mathbf{x})$ auf 0 und dann die Zahl der Gleichungen $\boldsymbol{GL}(\mathbf{x})$ auf 1 reduziert werden. $\mathbf{A}$ kann insgesamt durch $\mathbf{C}_1$ mit $\mathbf{C}_1$ vom Typ $\boldsymbol{GL}(\mathbf{x})$ ($\mathbf{A}$ bestand schon ursprünglich nur aus einer Gleichung in $\mathbf{x}$) oder durch $\mathbf{C}_1$ & $\mathbf{C}_2$ mit $\mathbf{C}_1$ vom Typ $\boldsymbol{GL}(\mathbf{x})$ und $\mathbf{C}_2$ eine Konjunktion von Formeln, in denen $\mathbf{x}$ nicht mehr auftritt ($\mathbf{C}_2$ ist eine Konjunktion von Formeln der Typen $\boldsymbol{GL_x}$, $\boldsymbol{K_x}$, $\boldsymbol{NGL_x}$), ersetzt werden. Mit Hilfe von R5. kann nun eine zu $\exists\, \mathbf{x}\, \mathbf{C}_1$ äquivalente offene Formel $\mathbf{C}_1'$ gefunden werden. Die gesuchte offene Formel $\mathbf{B}$ ist dann $\mathbf{C}_1'$ bzw. $\mathbf{C}_1'$ & $\mathbf{C}_2$.

Denn im ersten Fall:

$$\begin{aligned} \vdash_{TAZ'} \exists\, \mathbf{x}\, \mathbf{A}' &\leftrightarrow \exists\, \mathbf{x}\, \mathbf{C}_1 \\ &\leftrightarrow \mathbf{B}\,, \end{aligned}$$

Im zweiten Fall:

$$\begin{aligned} \vdash_{TAZ'} \exists\, \mathbf{x}\, \mathbf{A}' &\leftrightarrow \exists\, \mathbf{x}\, (\, \mathbf{C}_1 \,\&\, \mathbf{C}_2\,) \\ &\leftrightarrow (\, \exists\, \mathbf{x}\, \mathbf{C}_1\,) \,\&\, \mathbf{C}_2 \\ &\leftrightarrow \mathbf{C}_1' \,\&\, \mathbf{C}_2 \\ &\leftrightarrow \mathbf{B}\,. \end{aligned}$$

[10] Diese für seinen Beweis benutzte Vereinfachung schreibt M. Presburger A. Lindenbaum zu.

Fall 2: $\mathbf{A}$ enthält keine Konjunktionsformel vom Typ $\boldsymbol{GL}(\mathbf{x})$, jedoch mindestens eine vom Typ $\boldsymbol{K}(\mathbf{x})$:

Durch wiederholtes Anwenden der Ersetzungsregel R4. gelingt es, die Zahl der von $\mathbf{x}$ abhängigen Kongruenzformeln in Konjunktionen von $\mathbf{A}$ auf 1 zu reduzieren, d.h. $\mathbf{A}$ insgesamt durch $\mathbf{C}_1$ oder durch $\mathbf{C}_1$ & $\mathbf{C}_2$ oder durch $\mathbf{C}_1$ & $\mathbf{C}_3$ oder durch $\mathbf{C}_1$ & $\mathbf{C}_2$ & $\mathbf{C}_3$ zu ersetzen, wobei $\mathbf{C}_1$ vom Typ $\boldsymbol{K}(\mathbf{x})$, $\mathbf{C}_2$ vom Typ $\boldsymbol{NGL}(\mathbf{x})$ & ... & $\boldsymbol{NGL}(\mathbf{x})$ und $\mathbf{C}_3$ $\mathbf{x}$ nicht enthält.

Im ersten und dritten Fall wird nun entsprechend R6. eine zu $\exists\,\mathbf{x}\,\mathbf{C}_1$ äquivalente offene Formel $\mathbf{C}_1'$ gefunden, im zweiten und im vierten Fall eine zu $\exists\,\mathbf{x}\,(\,\mathbf{C}_1$ & $\mathbf{C}_2\,)$ äquivalente Formel $\mathbf{C}_2'$ mit Hilfe von R7. .

Die gesuchte Formel $\mathbf{B}$ ist dann in $\mathbf{C}_1$ bzw. in $\mathbf{C}_2'$ bzw. in $\mathbf{C}_1'$ & $\mathbf{C}_3$ bzw in $\mathbf{C}_2'$ & $\mathbf{C}_3$ gefunden.

Denn z.B. im vierten Fall gilt:

$$\begin{aligned}\vdash_T \exists\,\mathbf{x}\,\mathbf{A} &\leftrightarrow \exists\,\mathbf{x}\,(\,\mathbf{C}_1 \,\&\, \mathbf{C}_2 \,\&\, \mathbf{C}_3\,)\\ &\leftrightarrow \exists\,\mathbf{x}\,(\,\mathbf{C}_1 \,\&\, \mathbf{C}_2\,) \,\&\, \mathbf{C}_3\\ &\leftrightarrow \mathbf{C}_2' \,\&\, \mathbf{C}_3\\ &\leftrightarrow \mathbf{B}\,.\end{aligned}$$

Wie sich aus den Bedingungen an die Ersetzungsregeln (bzw. an die damit verbundenen effektiven Verfahren) ergibt, ist in $\mathbf{B}$ schließlich gegenüber $\mathbf{A}$ keine neue Variable frei und kommt darin $\mathbf{x}$ ebenfalls nicht mehr vor.

Fall 3: $\mathbf{A}$ enthält keine Konjunktionsformeln vom Typ $\boldsymbol{GL}(\mathbf{x})$ oder $\boldsymbol{K}(\mathbf{x})$, hingegen schon solche vom Typ $\boldsymbol{NGL}(\mathbf{x})$:

$\mathbf{A}$ kann als $\mathbf{C}_1$ bzw. als $\mathbf{C}_1$ & $\mathbf{C}_2$ aufgefaßt werden, wobei $\mathbf{C}_1$ vom Typ $\boldsymbol{NGL}(\mathbf{x})$ & ... & $\boldsymbol{NGL}(\mathbf{x})$ ist und in $\mathbf{C}_2$ $\mathbf{x}$ nicht vorkommt. Vermittels R8. kann eingesehen werden, daß $\mathbf{C}_1$ in TAZ' zur variablenfreien Formel $0 = 0$ äquivalent ist, woraus sofort folgt, daß $\exists\,\mathbf{x}\,\mathbf{A}$ (im ersten Fall) zu $0 = 0$, bzw. zu $\mathbf{C}_2$ (im zweiten Fall) äquivalent ist. $\mathbf{B}$ sei also $0 = 0$ bzw. $\mathbf{C}_2$.

Im zweiten Fall:

$$\begin{aligned}\vdash_T \exists\,\mathbf{x}\,\mathbf{A} &\leftrightarrow \exists\,\mathbf{x}\,(\,\mathbf{C}_1 \,\&\, \mathbf{C}_2\,)\\ &\leftrightarrow (\,\exists\,\mathbf{x}\,\mathbf{C}_1\,) \,\&\, \mathbf{C}_2\\ &\leftrightarrow 0 = 0 \,\&\, \mathbf{C}_2\\ &\leftrightarrow \mathbf{C}_2\\ &\leftrightarrow \mathbf{B}\,.\end{aligned}$$

Fall 4: $\mathbf{A}$ enthält $\mathbf{x}$ nicht:

Dann ist $\exists\,\mathbf{x}\,\mathbf{A}$ selbstverständlich zur offenen Formel $\mathbf{A}$ äquivalent. $\mathbf{B}$ kann als $\mathbf{A}$ gewählt werden.

Hiermit ist die Beschreibung eines effektiven QE-Verfahrens für TAZ' abgeschlossen. Das hier geschilderte Verfahren entspricht dem in [Pre29] dargestellten bis auf die Durchführung der Entscheidung von variablenfreien Formeln von TAZ', die dort Teil des Verfahrens ist. Dieser Schritt ist nicht eigentlich Teil der *Quantorenelimination* in Formeln von TAZ' (falls dieser Begriff wörtlich—wie z.B. in [Shoe67]—verstanden wird) und wird hier im folgenden erst im Beweis zu Satz 2.1.6 behandelt. □

Eine unmittelbare Folgerung davon, daß TAZ' die QE zuläßt, ist die Vollständigkeit von TAZ (die Vollständigkeit einer Theorie, die die Quantorenelimination zuläßt, folgt allgemein jedenfalls immer dann, wenn T eine Konstante enthält und wenn variablenfreie Formeln in T entscheidbar sind). Die Entscheidbarkeit von TAZ ist im wesentlichen eine Folgerung davon, daß die QE in TAZ' auf eine effektive Weise (die oben beschrieben worden ist) durchgeführt werden kann.

Satz 2.1.6. *TAZ ist vollständig und entscheidbar.*

Beweis. (1) TAZ ist vollständig:

„Vollständigkeit“ einer Theorie im Sinne von [Shoe67] meint: Konsistenz *und* jede geschlossene Formel ist entscheidbar (d.h. zusammen: Für jede geschlossene Formel $\mathbf{A}$ ist genau eine der beiden Formeln $\mathbf{A}$ oder $\neg\,\mathbf{A}$ ein Theorem).

- Die Konsistenz kann semantisch durch das Modell $\langle\mathbb{Z};0,1,+\rangle$ für TAZ eingesehen werden.
- Um zu zeigen, daß jede geschlossene Formel von TAZ entscheidbar ist, genügt es, das für die konservative (weil definitorische) Erweiterung TAZ' von TAZ zu zeigen.
  - Nun muß zuerst begründet werden, warum in TAZ' jede variablenfreie Formel $\mathbf{A}$ von TAZ' entscheidbar ist, d.h. selbst beweisbar oder in negierter Form beweisbar ist:
    Hierfür reicht es aus, zu zeigen, daß atomare Formeln von TAZ entscheidbar sind; denn die Entscheidung einer beliebigen variablenfreien Formel kann nach der Klärung der Entscheidbarkeit jeder in der Formel vorkommenden atomaren Formel dann auf aussagenlogischem Weg geschehen.
    Atomare, variablenfreie Formeln von TAZ' können nach die Gruppeneigenschaft in TAZ bezüglich $+$ benutzenden Umformungen als $\underline{\underline{a}} = 0$ oder $\underline{\underline{b}} \equiv_n 0$ $(a, b \in \mathbb{N}_0,\ n \in \mathbb{N},\ n \geq 2)$ geschrieben werden.
    Für solche Formeln gilt aber:

Fall 1: $a = 0$. Dann gilt $\vdash_{TAZ'} \underline{a} = 0$:
Das folgt durch Substitution aus einem Identitätsaxiom $x = x$.

Fall 2: $a \neq 0$. Dann gilt $\vdash_{TAZ'} \neg \underline{a} = 0$:
Zuerst gilt $\vdash_{TAZ'} \neg\, 1 = 0$, da $\vdash_{TAZ'} 1 = 0 \to \underline{2} = 1$ (wegen Gleichheitsaxiomen und TAZ.2.) und $\vdash_{TAZ'} \neg\, \underline{2}\, 1 = 1$ (wegen TAZ.S3. und weil $\underline{2}\, 1$ in TAZ gleich $\underline{2}$ ist). Nun gilt weiters $\vdash_{TAZ'} \underline{a}\, 1 = \underbrace{\underline{a}\, 0}_{=0} \to 1 = 0$ (wegen $a \neq 0$ und TAZ.S1.). Insgesamt folgt aussagenlogisch: $\vdash_{TAZ'} \neg \underline{a} = 0$.

Fall 3: $n \mid b$. Dann gilt $\vdash_{TAZ'} \underline{b} \equiv_n 0$:
Wegen $n \mid b$ existiert ein $c \in \mathbb{N}_0$ mit $n\, c = b$. Damit gilt $\vdash_{TAZ'} \underline{n}\, \underline{c} = \underline{b}$, wegen TAZ.1. dann auch $\vdash_{TAZ'} \underline{n}\, \underline{c} = \underline{b}$. Mit einem Substitutionsaxiom ist daraus $\vdash_{TAZ'} \exists z\, (\, \underline{n}\, z = \underline{b}\,)$ herleitbar, also auch $\vdash_{TAZ'} \exists z\, (\, \underline{b} = \underline{n}\, z\,)$, mithin (wegen D.KON.S. und TAZ.2.) $\vdash_{TAZ'} \underline{b} \equiv_n 0$.

Fall 4: $n \nmid b$. Dann gilt $\vdash_{TAZ'} \neg \underline{b} \equiv_n 0$:
Wegen $\vdash_{TAZ'} \underline{b} \equiv_n 0 \to \underline{b} + \underline{n}\, z \equiv_n 0$ reicht es, $\vdash_{TAZ'} \neg \underline{b} \equiv_n 0$ für $0 < b < n$ zu zeigen.
Weiters reicht es aus, für $0 < b < n$ $\vdash_{TAZ'} \neg\, \underline{n}\, x = \underline{b}$ zu zeigen: Denn daraus folgt ("Generalization Rule") $\vdash_{TAZ'} \forall x\, (\, \neg\, \underline{n}\, x = \underline{b}\,)$, also $\vdash_{TAZ'} \neg\, \exists x\, (\, \underline{n}\, x = \underline{b}\,)$. Wegen

$$\begin{aligned}
\vdash_{TAZ'} \exists x\, (\, \underline{n}\, x = \underline{b}\,) &\leftrightarrow \exists x\, \big(\, \underline{n}\, x = \underline{b} \;\&\; \exists z\, (\, x + z = 0\,)\,\big) \\
&\leftrightarrow \exists x\, \exists z\, \big(\, \underline{n}\, x = \underline{b} \;\&\; \underline{n}\, x + \underline{n}\, z = 0\,\big) \\
&\leftrightarrow \exists x\, \exists z\, \big(\, 0 = \underline{b} + \underline{n}\, z\,\big) \\
&\leftrightarrow \exists z\, (\, \underline{b} + \underline{n}\, z = 0\,) \\
&\leftrightarrow \underline{b} \equiv_n 0
\end{aligned}$$

(benutzte nichtlogische Axiome: TAZ.1., TAZ.2., TAZ.3., TAZ.4., TAZ.S1., D.KON.S) folgt also $\vdash_{TAZ'} \neg\, \underline{b} \equiv_n 0$.
Im letzten Beweisreduktionsschritt reicht es dann aus, $\vdash_{TAZ'} \neg\, \underline{n}\, x = \underline{b}$ nur für $b \in \mathbb{N}$, $n \in \mathbb{N}$, $n \geq 2$ mit $0 < b < n$ und b, n teilerfremd zu zeigen; denn mit $c := \mathrm{ggT}(b, n)$ gilt: $\vdash_{TAZ'} \underline{n}\, x = \underline{c}\, \big(\, \underline{\tfrac{n}{c}}\, x\big)$, $\vdash_{TAZ'} \underline{b} = \underline{c}\, \underline{\tfrac{b}{c}}$ wegen TAZ.1., $\vdash_{TAZ'} \underline{c}\, \underline{\tfrac{n}{c}}\, x = \underline{c}\, \underline{\tfrac{b}{c}} \to \underline{\tfrac{n}{c}}\, x = \underline{\tfrac{b}{c}}$ wegen TAZ.S1., insgesamt also $\vdash_{TAZ'} \underline{n}\, x = \underline{b} \to \underline{\tfrac{n}{c}}\, x = \underline{\tfrac{b}{c}}$ und $\mathrm{ggT}(\tfrac{n}{c}, \tfrac{b}{c}) = 1$.
Seien nun $n, b \in \mathbb{N}$ teilerfremd mit $0 < b < n$. Dann gibt es $x^*, y^* \in \mathbb{N}$ so, daß $-n\, x^* + b\, y^* = 1$. Also gilt $\vdash_{TAZ'} \underline{b\, y^*} = 1 + \underline{n\, x^*}$; daraus folgt $\vdash_{TAZ'} \underline{y^*}\, \underline{b} = 1 + \underline{n}\, \underline{x^*}$ (wegen TAZ.1.). Weiters gilt $\vdash_{TAZ'} \underline{n}\, x = \underline{b} \to \underline{y^*}\, (\, \underline{n}\, x\,) = \underline{y^*}\, \underline{b}$ wegen Gleichheitsaxiomen bezüglich $+$. Daraus folgt mit dem zuvor hergeleiteten

$\vdash_{TAZ'} \underline{n}\, x = \underline{\underline{b}} \rightarrow \underline{y^*}\,(\,\underline{n}\, x\,) = 1 + \underline{n}\,\underline{\underline{x^*}}$ erneut mit TAZ.1. . Wegen TAZ.3. folgt daraus (ähnlich einem zuvor ausführlich gezeigten Schritt): $\vdash_{TAZ'} \underline{n}\, x = \underline{\underline{b}} \rightarrow \exists\, z\,(\,\underline{n}\, z = 1\,)$. Nun gilt aber $\vdash_{TAZ'} \neg\, \underline{n}\, z = 1$ wegen TAZ.S3. (nach Annahme ist $n \geq 2$), woraus durch "Generalization Rule" sofort $\vdash_{TAZ'} \neg\, \exists\, z\,(\,\underline{n}\, z = 1\,)$ folgt; letzteres führt nun aber von $\underline{n}\, x = \underline{\underline{b}} \rightarrow \exists\, z\,(\,\underline{n}\, z = 1\,)$ auf $\vdash_{TAZ'} \neg\, \underline{n}\, x = \underline{\underline{b}}$.

– Ist nun $\mathbf{A}$ eine beliebige geschlossene Formel von TAZ', so ist $\mathbf{A}$ entscheidbar:
Mit Hilfe des in Lemma 2.1.5 dargestellten QE-Verfahrens für TAZ' kann zu $\mathbf{A}$ effektiv eine offene Formel $\mathbf{B}$ mit

$$\vdash_{TAZ'} \mathbf{A} \leftrightarrow \mathbf{B} \tag{2.8}$$

gefunden werden, wobei $\mathbf{B}$ offen und variablenfrei ist (weil wegen der zusätzlichen Eigenschaft des QE-Verfahrens in $\mathbf{B}$ keine Variablen frei vorkommen, die in $\mathbf{A}$ nicht frei sind; und $\mathbf{A}$ hier geschlossen ist). Wegen dem oben gezeigten gilt nun aber, da $\mathbf{B}$ offen und variablenfrei, genau entweder $\vdash_{TAZ'} \mathbf{B}$ oder $\vdash_{TAZ'} \neg\, \mathbf{B}$, was zudem effektiv entschieden werden kann. Im ersten Fall folgt daraus mit (2.8) sofort $\vdash_{TAZ'} \mathbf{A}$, im zweiten $\vdash_{TAZ'} \neg\, \mathbf{A}$, mithin wegen der (offensichtlichen) Konsistenz von TAZ' dann also $\nvdash_{TAZ'} \mathbf{A}$.

(2) TAZ ist entscheidbar:

Folgt sofort aus dem oben skizzierten effektiven Vollständigkeitsbeweis, in dem ja eine durchführbare Methode angegeben wurde, wie von einer geschlossenen Formel $\mathbf{A}$ von TAZ' festgestellt werden kann, ob $\mathbf{A}$ ein Theorem von TAZ' ist. Damit ist TAZ' entscheidbar und, da TAZ' konservative Erweiterung von TAZ ist (und damit die Anwendung eines Entscheidungsverfahrens für TAZ' auf eine Formel $\mathbf{A}$ von TAZ auch über die Beweisbarkeit von $\mathbf{A}$ in TAZ entscheidet), gilt das auch für TAZ.

□

Eine weitere unmittelbare Folgerung der Vollständigkeit von TAZ ist nun aber die Tatsache, daß TAZ und $Th(\langle \mathbb{Z}; 0, 1, + \rangle)$ äquivalent sind bzw. daß nun schließlich TAZ auch als vollständige Axiomatisierung von $Th(\langle \mathbb{Z}; 0, 1, + \rangle)$ erkannt werden kann. Anders ausgedrückt heißt das, daß für eine Formel $\mathbf{A}$ von L_{TAZ} die Aussagen „$\mathbf{A}$ ist in TAZ beweisbar“ und „$\mathbf{A}$ ist in $\langle \mathbb{Z}; 0, 1, + \rangle$ gültig“ immer den selben Wahrheitswert besitzen, d.h. daß nun *Beweisbarkeit* in TAZ mit *Gültigkeit* in $\langle \mathbb{Z}; 0, 1, + \rangle$ identifiziert werden kann.

Hierzu ist für eine Formel $\mathbf{A}$ in TAZ nur zu zeigen, daß

$$\mathbf{A} \text{ ist gültig in } \langle \mathbb{Z}; 0, 1, + \rangle \;\; \Rightarrow \;\; \vdash_{TAZ} \mathbf{A}$$

gilt, bzw. daß (als meta-sprachliche Aussage:) äquivalent dazu die Kontraposition dieser Folgerung für alle Formeln $\mathbf{A}$ in TAZ gilt, nämlich

$$\nvdash_{TAZ} \mathbf{A} \quad \Rightarrow \quad \mathbf{A} \text{ ist in } \langle \mathbb{Z}; 0, 1, + \rangle \text{ nicht gültig .}$$

Sei dazu nun $\mathbf{A}$ dazu eine Formel von TAZ, und es sei weiters angenommen, daß $\nvdash_{TAZ}$ $\mathbf{A}$ gilt. Bezeichnet nun $\mathbf{A}^c$ den Abschluß von $\mathbf{A}$, so muß dann auch $\nvdash_{TAZ} \mathbf{A}^c$ gelten (da immer $\vdash \mathbf{A}^c \to \mathbf{A}$ gilt („Substitution Theorem“ in [Shoe67])). Wegen der Vollständigkeit von TAZ muß dann aber $\vdash_{TAZ} \neg \mathbf{A}^c$ gelten. Da $\langle \mathbb{Z}; 0, 1, + \rangle$ ein Modell von TAZ ist, folgt, daß $\neg \mathbf{A}^c$ in diesem Modell gültig, $\mathbf{A}^c$ also nicht gültig ist. Hieraus folgt aber die Nicht-Gültigkeit von $\mathbf{A}$ in $\langle \mathbb{Z}; 0, 1, + \rangle$ (da die Gültigkeit von $\mathbf{A}$ immer die Gültigkeit von $\mathbf{A}^c$ nach sich zieht).

Lemma 2.1.7. *Die definitorische Einführung eines einzelnen nichtlogischen Symbols bzw. einer einzelnen Familie von nichtlogischen Symbolen in einer Theorie kann (wenn sie überhaupt erfolgen kann) schon in einem einzigen definitorischen Erweiterungsschritt geschehen.*

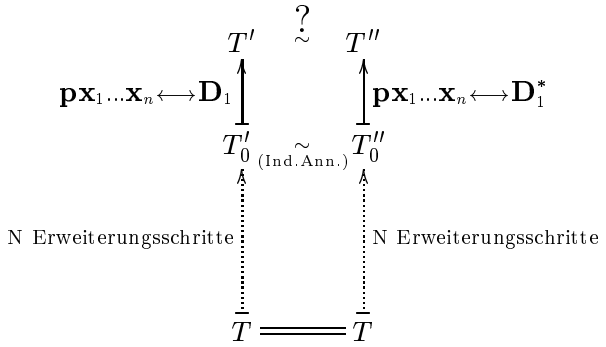
Präzisierung. Sei T' eine definitorische Erweiterung von T, die im Sinne von Definition 2.1.2 aus endlich vielen aufeinanderfolgenden Erweiterungsschritten hervorgeht und bei der einer dieser Erweiterungsschritte vom Typ (i)–(iv) in Definition 2.1.2 in der Einführung eines neuen nichtlogischen Symbols $\mathbf{p}$ bzw. $\mathbf{f}$ bzw. von neuen Symbolen einer Familie $\{\mathbf{p}_i\}_{i \in A}$ bzw. $\{\mathbf{f}_i\}_{i \in A}$ besteht. Dann existiert eine definitorische Erweiterung T'' von T um einen einfachen Erweiterungsschritt der definitorischen Einführung von $\mathbf{p}$ bzw. $\mathbf{f}$ bzw. der Symbole der Familie $\{\mathbf{p}_i\}_{i \in A}$ bzw. $\{\mathbf{f}_i\}_{i \in A}$ in T, für die dann weiters auch gilt, daß T' konservative Erweiterung von T'' ist. (D.h. also, daß die definitorische Einführung von einzelnen neuen nichtlogischen Symbolen bzw. Symbolen einzelner Symbolfamilien in einer Theorie, wenn diese überhaupt möglich ist, im selben Ausmaß schon in einem einzigen definitorischen Erweiterungsschritt möglich ist, wobei „im selben Ausmaß“ hier ist als „dabei dieselbe inhaltliche und formale Ausdruckskraft der definierten Symbole erzielend“ zu verstehen ist.)

Beweis. (1) Zuerst sei folgendes gezeigt: Ist T' eine definitorische Erweiterung von T, so existiert eine definitorische Erweiterung T'' von T, die zu T' äquivalent ist, die aber (möglicherweise im Unterschied zu T') als in ihren definierenden Axiomen auftretende Definitionsformeln $\mathbf{D}$ nur solche besitzt, die ausschließlich schon mit mit den (logischen und nichtlogischen) Symbolen von T gebildet werden können:

Das kann durch Induktion über die Anzahl N der definitorischen Erweiterungsschritte von T' gezeigt werden.

$N = 0$: Es bleibt nichts zu zeigen.

Diagramm 2.1.1 Für den Induktionsschritt in (1) im Beweis von Lemma 2.1.7 zu betrachtende Situation; dabei wird das Zeichen $\sim$ für die Symbolisierung der nach der Induktionsannahme bestehenden bzw. nun zu zeigenden Äquivalenz der entsprechenden, damit symbolisch verbundenen Theorien verwendet.



$N \to N+1$: T' entstehe aus T_0' z.B. durch die definitorische Einführung des n-stelligen Prädikatensymbols $\mathbf{p}$ vermittels des definierenden Axioms $\mathbf{p}\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}_1$, T_0' sei definitorische Erweiterung von T.

Nach der Induktionshypothese existiert eine definitorische Erweiterung T_0'' von T, in der die in definierenden Axiomen auftretenden Definitionsformeln $\mathbf{D}$ allesamt schon über L_T gebildet werden können und die zu T_0' äquivalent ist.

Sei nun $\mathbf{D}_1^*$ die Translation von $\mathbf{D}_1$ nach T, d.h. also: $\mathbf{D}_1^*$ besitzt nur Symbole von L_T und es gilt

$$\vdash_{T_0'} \mathbf{D}_1 \leftrightarrow \mathbf{D}_1^* \,. \tag{2.9}$$

Da T_0' und T_0'' äquivalent sind, gilt damit auch

$$\vdash_{T_0''} \mathbf{D}_1 \leftrightarrow \mathbf{D}_1^* \,. \tag{2.10}$$

Sei nun T'' jene definitorische Erweiterung von T_0'', die aus der definitorischen Einführung von $\mathbf{p}$ in T_0'' vermittels des definierenden Axioms $\mathbf{p}\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}_1^*$ aus T_0' entsteht (vgl. diese in Diagramm 2.1.1 dargestellte Situation).

T'' erfüllt nun damit weiterhin die an die Definitionsformeln $\mathbf{D}$ der definierenden Axiome gerichtete Forderung (: als Formeln schon über L_T gebildet werden zu können), und ist außerdem zu T' äquivalent:

T' und T'' haben dieselbe Sprache ($L_{T'}$) und entstehen aus den äquivalenten Theorien T_0' bzw. T_0'' durch definitorische Einführung des selben Symbols, jedoch auf unterschiedliche Weise, nämlich vermittels $\mathbf{p}\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}_1$ als definierendes Axiom für $\mathbf{p}$ in T'' und $\mathbf{p}\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}_1^*$ als definierendes Axiom für

$\mathbf{p}$ in T''. Es bleibt also zu zeigen, daß das jeweilige definierende Axiom in der einen Theorie in der jeweils anderen beweisbar ist:

(a) $\vdash_{T''} \mathbf{p}\mathbf{x}_1 \dots \mathbf{x}_n \leftrightarrow \mathbf{D}_1$: Folgt wegen $\vdash_{T''} \mathbf{p}\mathbf{x}_1 \dots \mathbf{x}_n \leftrightarrow \mathbf{D}_1^*$ (def. Ax. in T'') und $\vdash_{T_0''} \mathbf{D}_1 \leftrightarrow \mathbf{D}_1^*$ ((2.10), sowie: T'' ist Erweiterung von T_0'') als aussagenlogische Folgerung („tautological consequence“ in [Shoe67]).

(b) $\vdash_{T'} \mathbf{p}\mathbf{x}_1 \dots \mathbf{x}_n \leftrightarrow \mathbf{D}_1^*$: Dies folgt sofort aus dem definierenden Axiom $\vdash_{T''} \mathbf{p}\mathbf{x}_1 \dots \mathbf{x}_n \leftrightarrow \mathbf{D}_1$ von $\mathbf{p}$ in T' sowie aus $\vdash_{T'} \mathbf{D}_1 \leftrightarrow \mathbf{D}_1^*$ ((2.9), sowie T' ist Erweiterung von T_0') wiederum als aussagenlogische Folgerung.

(Im Falle von definitorischen Erweiterungen von T_0' zu T' um ein Funktionssymbol oder eine Familie von Symbolen kann analog argumentiert werden; für die Äquivalenz der betrachteten definitorischen Erweiterungen reicht es, im Falle von Symbolfamilien die wechselseitige Ableitbarkeit der definierenden Axiome jedes einzelnen Symbols in den erweiterten Theorien T', T'' zu zeigen.)

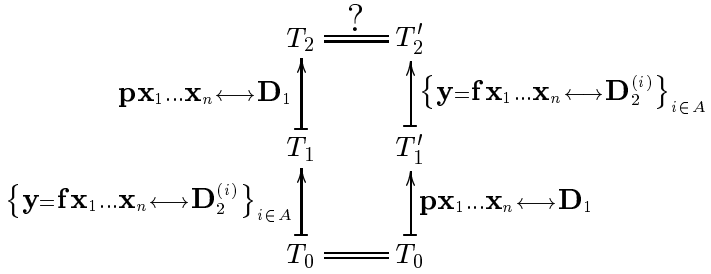
(2) Ist nun T' eine definitorische Erweiterung von T, in der die in den definierenden Axiomen auftretenden Definitionsformeln alle die Eigenschaft haben, schon über L_T gebildet werden zu können, so kommt es bei der Bildung von T' aus T auf die Reihenfolge der einzelnen definitorischen Erweiterungsschritt nicht mehr an, diese kann beliebig (im Sinne von Permutationen der einzelnen Schritte) verändert werden:

Hierfür reicht es offenbar, einzusehen, daß unter den obigen Bedingungen an die definierenden Axiome zwei aufeinanderfolgende definitorische Erweiterungsschritte vertauscht werden können, d.h. auf beide Wege zur selben definitorischen Erweiterung führen. (Durch solche Vertauschungen aufeinanderfolgender Schritte können leicht Abänderungen der Gesamtreihenfolge der Erweiterungsschritte, die beliebigen Transpositionen von Schritten entsprechen, aufgebaut werden; Permutationen von Schritten können dann mit Hilfe endlich vieler entsprechender Transpositionen hergestellt werden.)

Sei nun zum Beispiel die Theorie T_1 eine definitorische Erweiterung von T_0 um die Einführung eines n-stelligen Prädikatssymbols $\mathbf{p}$ unter der Verwendung des definierenden Axioms $\mathbf{p}\mathbf{x}_1 \dots \mathbf{x}_n \leftrightarrow \mathbf{D}_1$ und T_2 definitorische Erweiterung von T_1 um die Einführung der Funktionssymbolfamilie $\{\mathbf{f}_i\}_{i \in A}$ ($\mathbf{f}_i$ n-stellige Funktionssymbole) vermittels $\mathbf{y} = \mathbf{f}_i\mathbf{x}_1 \dots \mathbf{x}_n \leftrightarrow \mathbf{D}_2^{(i)}$, wobei sowohl $\mathbf{D}_1$ als auch alle $\mathbf{D}_2^{(i)}$ ($i \in A$) Formeln über L_{T_0} sind.

Nun sei T_1' definitorische Erweiterung von T_0 um die Einführung von $\mathbf{p}$ (das ist möglich, denn $\mathbf{D}_1$ enthält nach Annahme nur nichtlogische Symbole aus L_{T_0}, die Definition von $\mathbf{p}$ setzt also in keiner Weise die (beim Aufbau von T_2) vorher erfolgte Definition aller $\mathbf{f}_i$ voraus); sei weiters T_2' definitorische Erweiterung von T_1 um die Einführung von allen Funktionssymbolen der Familie $\{\mathbf{f}_i\}_{i \in A}$ (das ist zulässig, da die

Diagramm 2.1.2 Ist die Vertauschung von zwei Erweiterungsschritten bei der definitorischen Erweiterung einer Theorie T_0 zulässig, d.h. sind die dadurch entstehenden Theorien T_2 und T_2' äquivalent? – (Das Diagramm zeigt einen der hierfür in (2) im Beweis von Lemma 2.1.7 zu untersuchenden Fälle bzgl. verschiedener Typen von Theorieerweiterungen, nämlich den einer Erweiterung um einen Schritt von Typ (i) und um einen Schritt vom Typ (iv).)



Existenz und Eindeutigkeitsbedingungen für die $\mathbf{f}_i$, die ursprünglich in T_0 beweisbar sein mußten, selbstverständlich auch in der (definitorischen) Erweiterung T_1' von T_0 beweisbar sind). – Die gesamte hier betrachtete Situation ist in Diagramm 2.1.2 bildlich dargestellt.

Dann sind T_2 und T_2' in dem Sinne gleich, daß sie dieselbe Sprache und dieselben nichtlogischen Axiome haben (und dadurch ist eine Theorie im Sinne von [Shoe67] eindeutig bestimmt).

Sollte der Vertauschungsschritt von definitorischen Erweiterungen im oben betrachteten Fall in die umgekehrte Richtung durchgeführt und in seiner Zulässigkeit begründet werden, d.h. wären die definitorischen Erweiterungen T_1' um $\mathbf{p}$ aus T_0 und T_2' um $\{\mathbf{f}_i\}_{i \in A}$ aus T_1' gegeben, so müßte so argumentiert werden: Eine definitorische Erweiterung T_1 um die Einführung von $\{\mathbf{f}_i\}_{i \in A}$ in T_0 vermittels $\mathbf{y} = \mathbf{f}_i\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}_2^{(i)}$ ist deshalb möglich, weil (a) $\mathbf{D}_2^{(i)}$ $(i \in A)$ nach Annahme schon Formeln über L_{T_0} (und nicht erst über L_{T_1}) sind und weil (b) die Existenz- und Eindeutigkeitsbedingungen für die $\mathbf{f}_i$ schon in T_0 beweisbar sind (und nicht erst in T_1'; dies deswegen, weil diese Bedingungen nach Annahme Formeln über L_{T_0} sind, die Theoreme von $L_{T_1'}$ sind (nach Annahme, daß T_2' definitorische Erweiterung von T_1' um $\{\mathbf{f}_i\}_{i \in A}$ ist), und—da T_1' (als definitorische Erweiterung) konservative Erweiterung von T_0 ist—auch Theorem von T_0). – Die nach T_1 gereihte Erweiterung um $\mathbf{p}$ zu T_2 ist dann völlig unproblematisch.

Weiters ist leicht einzusehen, daß eine solche Vertauschung von definitorischen Erweiterungsschritten unter den hier angenommenen Bedingungen an die definierenden

Axiome auch in allen anderen Fällen von Typen von Erweiterungsschritten erlaubt ist.

(3) Beweis der Aussage des Lemmas: Wegen (1) und (2) kann man zu einer definitorischen Erweiterung T' von T, in der z.B. (u.a.) ein n-stelliges Prädikatssymbol $\mathbf{p}$ (vermittels definierendem Axiom $\mathbf{p}\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D}$ in irgend einem definitorischen Erweiterungsschritt) gegenüber T definitorisch eingeführt wurde, eine äquivalente definitorische Erweiterung T''' von T betrachten, bei der die definitorische Einführung von $\mathbf{p}$ bereits im ersten Erweiterungsschritt geschieht (vermittels definierendem Axiom $\mathbf{p}\mathbf{x}_1 \ldots \mathbf{x}_n \leftrightarrow \mathbf{D^*}$, $\mathbf{D^*}$ die Translation in T' von $\mathbf{D}$ nach T).

Sei nun T'' jene einfache definitorsche Erweiterung von T um die Einführung von $\mathbf{p}$, die dem ersten Erweiterungsschritt im Aufbau von T''' entspricht (vgl. Darstellung dieser Situation in Diagramm 2.1.3).

Für die Aussage des Lemmas bleibt nun noch zu zeigen, daß T' konservative Erweiterung von T'' ist:

(a) T' ist Erweiterung von T'': Da T''' Erweiterung von T'' ist (T'' ist der erste definitorische Erweiterungsschritt von T zu T''') und T' und T''' äquivalent sind.

(b) T' ist konservative Erweiterung von T'': Sei $\mathbf{A}$ eine Formel von T' über der Sprache $L_{T''}$ (also mit Symbolen von T und zusätzlich vielleicht noch mit dem Symbol $\mathbf{p}$ gebildet), angenommen, es gilt: $\vdash_{T'} \mathbf{A}$. Dann gilt (da T' und T''' äquivalent sind) auch $\vdash_{T'''} \mathbf{A}$. Hieraus folgt aber auch $\vdash_{T''} \mathbf{A}$ (da T''' konservative Erweiterung über seinem ersten Erweiterungsschritt ist).

Dieser Beweisteil verläuft völlig analog für definitorische Erweiterungsschritte vom Typ (ii), (iii), (iv) in Definition 2.1.2, also für Erweiterungsschritte um die Einführung von Funktionssymbolen oder ganzen Symbolfamilien.

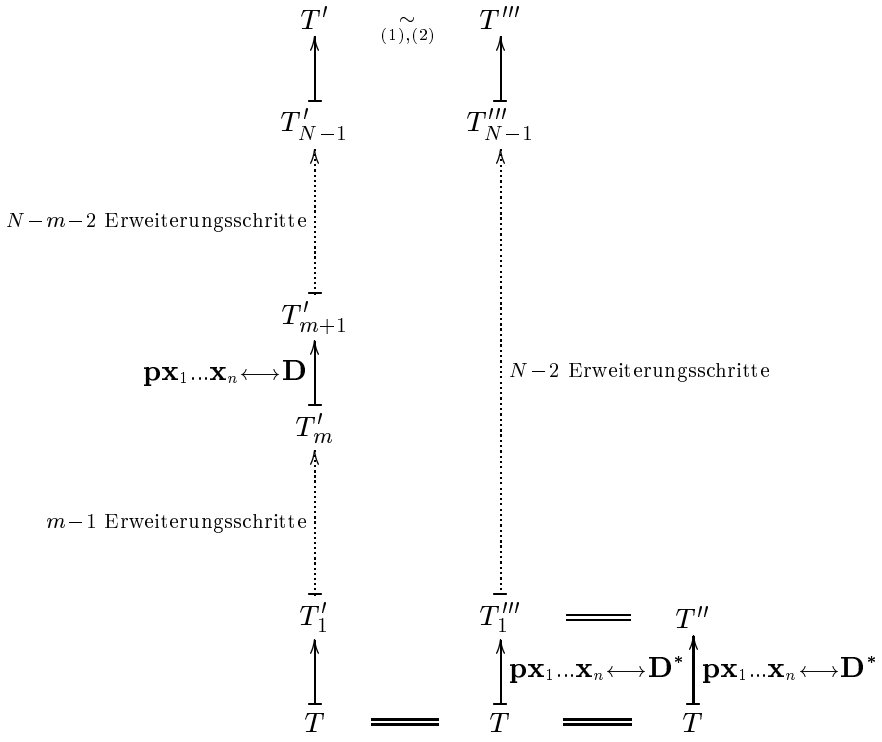
□

Satz 2.1.8. *TAZ' ist auf definitorischem Weg nicht zu einer Theorie der Additionsarithmetik ganzer Zahlen mit Ordnungssymbol erweiterbar*[11].

Präzisierung. Es gibt keine definitorische Erweiterung TAZ^* von TAZ, deren Sprache L_{TAZ^*} das Ordnungssymbol $<$ enthält und die ein Modell $\langle \mathbb{Z}; \mathbf{0}, \mathbf{1}, +, <, \ldots \rangle$ über den ganzen Zahlen besitzt, wobei die Entsprechungsrelation $<$ über $\mathbb{Z}$ für $<$ im aufgeführten Modell die übliche Bedeutung dieses Symbols über den ganzen Zahlen haben soll (die Punkte in der Modelldarstellung sollen Entsprechungen für etwaig in TAZ^* noch weiter

[11] [Den Hinweis auf diese Aussage und eine Erläuterung des dem Beweis zugrundeliegenden Hauptgedankens verdanke ich Herrn M. Baaz, Wien; C.G.]

Diagramm 2.1.3 In (3) im Beweis von Lemma 2.1.7 zu untersuchende Situation, wobei gezeigt werden soll, daß T' konservative Erweiterung von T'' ist. (Im Diagramm gilt: $m \in \mathbb{N}_0$, $N \in \mathbb{N}$, $\mathbf{D}$ ist eine Formel von $L_{T'_m}$ bzw. von T'_m und T', $\mathbf{D}^*$ ist die Translation von $\mathbf{D}$ nach T.)



definitorisch eingeführte nichtlogische Symbole im Modell der ganzen Zahlen andeuten). Weiters soll diese Aussage auch für die Symbole $\leq$, $>$, bzw. $\geq$ in der Beziehung zu den dafür über $\mathbb{Z}$ gewöhnlich verwendeten Entsprechungsrelationen $\leq$, $>$, $\geq$ gelten.

Beweis. (1) Zunächst ist leicht einsehbar, daß der Satz nur bezüglich des Ordnungssymbols $<$ gezeigt zu werden braucht: Gäbe es nämlich eine definitorische Erweiterung TAZ_1 von TAZ, in der $\leq$ (bzw. $>$ bzw. $\geq$) so eingeführt worden wäre, daß TAZ_1 ein Modell über den ganzen Zahlen mit den Entsprechungen $\mathbf{0}$, $\mathbf{1}$, $+$ und $\leq$ (bzw. $>$ bzw. $\geq$) in deren jeweils üblicher Bedeutung über $\mathbb{Z}$ für die nichtlogischen Symbole 0, 1, $+$ und $\leq$ (bzw. $>$ bzw. $\geq$) von TAZ_1 besäße, so würde das natürlich sofort auch für eine definitorische Erweiterung TAZ^* von TAZ_1 gelten, in der $<$ vermittels des definierenden Axioms

$$x < y \;\leftrightarrow\; x \leq y \,\&\, \neg\, x = y$$
$$(\text{ bzw. } \quad x < y \;\leftrightarrow\; y > x\,, \quad \text{ bzw. } \quad x < y \;\leftrightarrow\; y \geq x \,\&\, \neg\, x = y\,)$$

eingeführt worden wäre.

(2) Weiters wird es im folgenden ausreichen, zu zeigen, daß $<$ in TAZ nicht mittels einer definitorischen Erweiterung von TAZ, die durch einen einfachen Erweiterungsschritt aus TAZ vermittels eines definierenden Axioms für $<$ hervorgeht, in dessen üblicher Bedeutung für ganze Zahlen eingeführt werden kann:

Wäre nämlich TAZ^{**} eine aus TAZ in mehreren definitorische Erweiterungsschritten entstandene definitorische Erweiterung, in der $<$ in entsprechender Weise eingeführt worden wäre, so gäbe es wegen Lemma 2.1.7 auch eine definitorische Erweiterung TAZ^* von TAZ um die direkte Einführung von $<$ in einem einfachen Erweiterungsschritt, deren Sprache L_{TAZ^*} genau $0, 1, +$ sowie $>$ enthält und für die TAZ^{**} eine konservative Erweiterung darstellt. D.h., daß alle mit den Symbolen von L_{TAZ^*} gebildeten Formeln, die Theoreme von TAZ^{**} sind, auch schon Theoreme der einfachen definitorischen Erweiterung TAZ^* von TAZ sind. Auf diese Weise wäre dann eine definitorische Erweiterung TAZ^* von TAZ gefunden, in der $<$ so eingeführt worden wäre, daß TAZ^* über $\mathbb{Z}$ mit der natürlichen Entsprechung $<$ für $<$ interpretierbar wäre (in der Sprache von [Shoe67] präzis: ein Modell mit den Entsprechungen $\mathbf{0}$, $\mathbf{1}$, $+$, $<$ für die Symbole $0, 1, +, <$ von TAZ über Universum $\mathbb{Z}$ besäße). (– Dies wird aber in den folgenden Beweisschritten ausgeschlossen werden).

(3) Mehr noch, es darf im folgenden angenommen werden, daß es zu zeigen ausreicht, daß $<$ nicht in einer einfachen definitorischen Erweiterung TAZ'^* von TAZ' auf entsprechende, hier behandelte Weise eingeführt werden kann:

Wegen (2) darf angenommen werden, daß es zu zeigen ausreicht, daß es keine einfache definitorische Erweiterung TAZ^* von TAZ um $<$ mit der damit verbundenen

gewöhnlichen Bedeutung der Entsprechungsrelation für $<$ bei einer Interpretation über $\mathbb{Z}$ gibt. Gäbe es im Widerspruch dazu aber nun dennoch eine solche definitorische Erweiterung TAZ^*, so würde die definitorische Erweiterung $TAZ^{*\prime}$ von TAZ^* um die zusätzliche Einführung der Kongruenzsymbole äquivalent zu TAZ'^* (der Einführung zuerst von $\{\equiv\}_{n\in\mathbb{N},\, n\geq 2}$ und danach folgend der von $<$) sein und damit dann auch eine einfache definitorische Erweiterung um $<$ von TAZ' in entsprechender Weise darstellen. (Daß $TAZ^{*\prime}$ und TAZ'^* äquivalent sind, folgt aus dem Beweisschritt (2) im Beweis von Lemma 2.1.7).

Hiermit ist die behauptete Beweisreduktion gezeigt.

(4) Nun kann aber unter Zuhilfenahme des im Beweis zu Lemma 2.1.5 geschilderten QE-Verfahrens für TAZ auf folgende Weise eingesehen werden, daß eine entsprechende Erweiterung TAZ'^* um die Einführung von $<$ in TAZ' unmöglich ist:

Angenommen, TAZ'^* entsteht aus TAZ' durch Erweiterung der Sprache $L_{TAZ'}$ von TAZ' um das 2-stellige Prädikatssymbol $<$ zur Sprache $L_{TAZ'^*}$ und durch die Hinzunahme des (neuen nichtlogischen) definierenden Axioms

$$x < y \leftrightarrow \mathbf{D} \tag{2.11}$$

(wobei $\mathbf{D}$ eine Formel der Sprache $L_{TAZ'}$ ist, in der nur x und y frei vorkommen) für $<$ zu den Axiomen von TAZ' *so, daß* $\mathfrak{Z}^* := \langle \mathbb{Z}; \mathbf{0}, \mathbf{1}, =, \equiv_{\mathbf{2}}, \equiv_{\mathbf{3}}, \ldots, \equiv_{\boldsymbol{n}}, \ldots, < \rangle$ (übliche Bedeutung der hierin über $\mathbb{Z}$ in Gebrauch stehenden Symbole) ein Modell von TAZ'^* ist.

Dann folgt aus dem definierenden Axiom (2.11) in TAZ'^* durch Substitution

$$\vdash_{TAZ'^*} 0 < x \leftrightarrow \mathbf{D}'_{x,y}[0, x]\ , \tag{2.12}$$

wobei $\mathbf{D}'$ aus $\mathbf{D}$ durch—eventuelle nötige—Umbenennung von gebundenen Variablen in $\mathbf{D}$ entsteht (also Variante von $\mathbf{D}$ ist). $\mathbf{D}'_{x,y}[0, x]$ sei nun die Formel $\mathbf{E}$; $\mathbf{E}$ ist ebenfalls eine mit Symbolen von $L_{TAZ'}$ gebildete Formel.

Da nach Lemma 2.1.5 TAZ' die QE zuläßt, gibt es eine in TAZ' zu $\mathbf{E}$ äquivalente offene Formel $\mathbf{F}$, d.h. eine Formel $\mathbf{F}$ mit

$$\vdash_{TAZ'} \mathbf{E} \leftrightarrow \mathbf{F}\ , \tag{2.13}$$

wobei wegen des im Beweis zu Lemma 2.1.5 geschilderten QE-Verfahrens angenommen werden kann, daß in $\mathbf{F}$ nur noch die Variable x vorkommt.

Sei nun weiters $\mathbf{F}'$ eine disjunktive Normalform von $\mathbf{F}$. Sei weiters $\mathbf{F}''$ eine aus $\mathbf{F}'$ durch Ersetzung von negierten Kongruenzen entsprechend Schritt (4) im Beweis von Lemma 2.1.5 aus $\mathbf{F}'$ und durch Entscheidung und Ersetzung von variablenfreien

Formeln von $\mathbf{F}'$ durch $0 = 0$ oder $0 = 1$ (vgl. hierbei den Beweis zu Satz 2.1.6) und zugleich deren weitestgehender Weglassung (so das aussagenlogisch in den Verknüpfungen von $\mathbf{F}'$ wegen $\vdash_{TAZ'} 0 = 0$ und $\vdash_{TAZ'} \neg 0 = 1$ in TAZ' als äquivalente Formelersetzung möglich ist) entsteht.

Sei nun $\mathbf{F}'''$ erneut eine disjunktive Normalform von $\mathbf{F}''$. $\mathbf{F}'''$ hat dann die Gestalt $\mathbf{F}_1 \vee \ldots \vee \mathbf{F}_n$ ($n \in \mathbb{N}$), wobei die $\mathbf{F}_i$ Konjunktionen von Formeln der Typen $\boldsymbol{GL}(x)$, $\boldsymbol{NGL}(x)$, $\boldsymbol{K}(x)$ bzw. $0 = 0$ sind oder $\mathbf{F}'''$ selbst die Formel $0 = 1$ ist.

Nun kann aber jedoch eine Formel $\mathbf{F}_i$, die eine Konjunktion von Formeln der Typen $\boldsymbol{GL}(x)$, $\boldsymbol{K}(x)$, $\boldsymbol{NGL}(x)$ ist und in der nur x frei vorkommt, entsprechend Umformungen gemäß den Regeln R1.–R4. des Ersetzungsregelschemas in Schritt (7) im Beweis von Lemma 2.1.5 und nachheriger Entscheidung und weitgehender Weglassung von entstandenen variablenfreien Teilformeln in den Konjunktionen $\mathbf{F}_i$ in TAZ' äquivalent durch eine Formel $\mathbf{G}_i$ ersetzt werden, wobei $\mathbf{G}_i$ eine Formel von TAZ' ist, die vom Typ $\boldsymbol{GL}(x)$, $\boldsymbol{K}(x)$, $\boldsymbol{K}(x)$ & $\boldsymbol{NGL}(x)$ & $\ldots$ & $\boldsymbol{NGL}(x)$ oder $\boldsymbol{NGL}(x)$ & $\ldots$ & $\boldsymbol{NGL}(x)$ oder $0 = 1$ ist.

$\mathbf{F}'''$ kann also durch eine Formel $\mathbf{G}$ in TAZ' äquivalent ersetzt werden, wobei $\mathbf{B}$ entweder $0 = 0$ oder $0 = 1$ oder eine Disjunktion $\mathbf{G}_1 \vee \ldots \vee \mathbf{G}_n$ ist, wobei die Formeln $\mathbf{G}_i$ ($1 \leq i \leq n$) Disjunktionen von Formeln von TAZ', in denen nur x vorkommt und die vom Typ $\boldsymbol{GL}(x)$, $\boldsymbol{K}(x)$, $\boldsymbol{K}(x)$ & $\boldsymbol{NGL}(x)$ & $\ldots$ & $\boldsymbol{NGL}(x)$ oder $\boldsymbol{NGL}(x)$ & $\ldots$ & $\boldsymbol{NGL}(x)$ sind.

Insgesamt (über die Gesamtlänge der Umformungen bisher) (v.a. wegen (2.11), (2.12), (2.13)) und wegen der Tatsache, daß es sich (dabei) immer um äquivalente Umformungen bzw. Ersetzungen in TAZ' (bzw. damit auch in TAZ'^*) gehandelt hat, gilt nun für die offene Formel $\mathbf{G}$, in der nur mehr die Variable $\mathbf{x}$ vorkommt,

$$\vdash_{TAZ'^*} 0 < x \leftrightarrow \mathbf{G}$$

bzw.

$$\vdash_{TAZ'^*} \forall x(\, 0 < x \leftrightarrow \mathbf{G}\,)\,. \tag{2.14}$$

Nun kann aber die vorhin festgelegte Struktur $\mathfrak{Z}^*$ im Widerspruch zur obigen Annahme kein Modell von TAZ'^* sein, denn:

Fall 1: $\mathbf{G}$ ist $0 = 1$ oder $0 = 0$:

Dann gilt $\mathfrak{Z}^*(\,\forall x(\,0 < x \leftrightarrow \mathbf{G}\,)\,)$=F (da $\mathfrak{Z}^*(\,0 = 1\,)$=F, es aber doch positive Zahlen in $\mathbb{Z}$ gibt; bzw. da $\mathfrak{Z}^*(\,0 = 0\,)$=T und aber z.B. $\mathfrak{Z}^*(\,0 < 0\,)$=F gilt).

Das ist aber nun wegen (2.14) ein Widerspruch dazu, daß $\mathfrak{Z}^*$ ein Modell für TAZ'^* ist.

Fall 2: $\mathbf{G}$ ist von der Gestalt $\mathbf{G}_1 \vee \mathbf{G}_2 \vee \ldots \mathbf{G}_n$ ($n \in \mathbb{N}$) und es existiert ein $i \in \{1, \ldots, n\}$, sodaß $\mathbf{G}_i$ vom Typ $\boldsymbol{K}(x)$ ist:

$\mathbf{G}_i$ ist dann äquivalent zu $\underline{\alpha}\, x + \underline{\underline{a}} \equiv_n \underline{\underline{b}}$ (für bestimmte $\alpha \in \mathbb{N}$, $a, b \in \mathbb{N}_0$, $n \in \mathbb{N}$, $n \geq 2$); diese Formel ist weiter äquivalent zu einer Formel der Gestalt $\underline{\alpha}\, x \equiv_n \underline{\underline{c}}$ ($\alpha \in \mathbb{N}$, $c \in \mathbb{N}_0$, $n \in \mathbb{N}$, $n \geq 2$), und diese Formel ist (Auflösung einer linearen Kongruenz, d.h. einer diophantischen Gleichung) zu einer Formel der Gestalt $x \equiv_n \underline{\underline{d}}$ äquivalent, falls $\mathrm{ggT}(\alpha, n) \mid c$ (bezüglich einer Lösung $d \in \mathbb{N}_0$ von $\alpha\, x + n\, y = c$ nach x), oder sonst zu $0 = 1$.

$\mathbf{G}_i'$ sei nun diese jeweilige letzte Formel der Umformung von $\mathbf{G}_i$.

Falls G_i' gleich $0 = 1$ ist, kann G_i aus $\mathbf{G}_1 \vee \mathbf{G}_2 \vee \ldots \vee \mathbf{G}_n$ entfernt werden und eine Beweisreduktion ist insofern erzielt, als weiter dann nur noch eine Disjunktion $\mathbf{G}'$ mit weniger Gliedern als $\mathbf{G}$ betrachtet werden und nach den Fällen 1–5 untersucht werden muß.

Falls $\mathbf{G}_i'$ von der Gestalt $x \equiv_n \underline{\underline{d}}$ ist, so gilt jedenfalls $\mathfrak{Z}^*(\,\forall x(\,\mathbf{G}_i' \to 0 < x\,)\,)$=F (da es immer auch negative Zahlen gibt, die einer Kongruenz genügen), woarus wegen der Äquivalenz von $\mathbf{G}_i$ und $\mathbf{G}_i'$ folgt: $\mathfrak{Z}^*(\,\forall x(\,\mathbf{G}_i \to 0 < x\,)\,)$=F. Hieraus folgt aber $\mathfrak{Z}^*(\,\forall x(\,\mathbf{G} \to 0 < x\,)\,)$=F und somit $\mathfrak{Z}^*(\,\forall x(\,\mathbf{G} \leftrightarrow 0 < x\,)\,)$=F, was erneut im Widerspruch zu (2.14) und der Annahme, daß $\mathfrak{Z}^*$ ein Modell für TAZ'^* ist, steht.

Fall 3: $\mathbf{G}$ ist von der Gestalt $\mathbf{G}_1 \vee \mathbf{G}_2 \vee \ldots \vee \mathbf{G}_n$ und es existiert ein $i \in \{1, \ldots, n\}$ so, daß $\mathbf{G}_i$ vom Typ $\boldsymbol{K}(x)$ & $\boldsymbol{NGL}(x)$ & $\ldots$ & $\boldsymbol{NGL}(x)$ ist:

$\mathbf{G}_i$ ist also zu $\mathbf{H}\,\&\,\mathbf{H}_1'\,\&\,\ldots\,\&\,\mathbf{H}_n'$ äquivalent, wobei $\mathbf{H}$ von der Gestalt $\underline{\alpha}\, x \equiv_n \underline{\underline{a}}$ ist und die $\mathbf{H}_i$ von der Gestalt $\neg\, x + \underline{\underline{b_i}} = 0$, $\neg\, x = \underline{\underline{b_i}}$ oder $0 = 0$ sind ($\alpha \in \mathbb{N}_0$, $n \in \mathbb{N}$, $n \geq 2$, $a \in \mathbb{N}$, $b_i \in \mathbb{N}_0$). Wie im Fall 2 ist $\mathbf{H}$ entweder zu einer Formel der Gestalt $x \equiv_m \underline{\underline{c}}$ ($c \in \mathbb{N}_0$, $m \in \mathbb{N}$, $m \geq 2$) oder zu $0 = 1$ äquivalent.

Im ersten Fall gilt aber jedenfalls

$$\mathfrak{Z}^*\big(\forall x\,\big(\,x \equiv_m \underline{\underline{c}}\,\&\,\mathbf{H}_1'\,\&\,\ldots\,\&\,\mathbf{H}_n' \to 0 < x\,\big)\,\big) = \mathrm{F}$$

(da für hinreichend große, die Kongruenz erfüllende, negative Zahlen alle verneinten Gleichungen wahr sind), woraus auch $\mathfrak{Z}^*(\,\forall x\,(\,\mathbf{G} \to 0 < x\,)\,)$=F und also auch $\mathfrak{Z}^*(\,\forall x\,(\,\mathbf{G} \to 0 < x\,)\,)$=F folgt, wegen (2.14) wiederum im Widerspruch zur Annahme, daß $\mathfrak{Z}^*$ ein Modell von $TAZ^{*\prime}$ ist.

Im zweiten Fall ($\mathbf{H}$ ist zu $0 = 1$ äquivalent) kann $\mathbf{G}_i$ aus $\mathbf{G}$ gestrichen werden und es ist dann damit erneut eine Beweisreduktion insofern erzielt worden, als weiter nur noch eine Disjunktion mit weniger (aus entsprechenden Konjunktionen bestehenden) Gliedern als $\mathbf{G}$ betrachtet und nach den Fällen 1–5 untersucht werden muß.

Fall 4: $\mathbf{G}$ ist von der Gestalt $\mathbf{G}_1 \vee \mathbf{G}_2 \vee \ldots \vee \mathbf{G}_n$ und es existiert ein $i \in \{1, \ldots, n\}$ so, daß $\mathbf{G}_i$ vom Typ $\boldsymbol{NGL}(x)$ & $\ldots$ & $\boldsymbol{NGL}(x)$ ist.
Hier gilt erneut $\mathfrak{Z}^*(\,\forall x\,(\,\mathbf{G} \to 0 < x\,)\,)$=F (da mit endlich vielen Ungleichungen nicht alle negativen Zahlen ausgeschlossen werden können) und es kann wie in den vorigen Fällen einen Widerspruch zur Annahme geschlossen werden.

Fall 5: $\mathbf{G}$ ist von der Gestalt $\mathbf{G}_1 \vee \mathbf{G}_2 \vee \ldots \vee \mathbf{G}_n$ und alle $\mathbf{G}_i$ sind vom Typ $\boldsymbol{GL}(x)$: Gleichungen $\underline{\alpha}\, x + \mathbf{a} = \mathbf{b}$ ($\alpha \in \mathbb{N}$, $\mathbf{a}, \mathbf{b}$ variablenfreie Terme) können durch Umformungen auf eine der Formen $x + \underline{\underline{c}} = 0$, $x = \underline{\underline{c}}$ oder $0 = 1$ gebracht werden ($c \in \mathbb{N}_0$). Nun ist $\mathbf{G}$ also selbst entweder mit $0 = 1$ äquivalent oder zu einer Formel der Gestalt

$$x + \underline{\underline{a_1}} = 0 \;\vee\; x + \underline{\underline{a_2}} = 0 \;\vee\; \ldots \;\vee\; x + \underline{\underline{a_m}} = 0$$
$$\vee\; x = \underline{\underline{a'_1}} \;\vee\; x = \underline{\underline{a'_2}} \;\vee\; \ldots \;\vee\; x = \underline{\underline{a'_{m'}}}\ ,$$

(wobei $a_1, \ldots, a_m, a'_1, \ldots, a'_{m'} \in \mathbb{N}_0$). Im ersten Fall kann auf Fall 1 verwiesen werden. Im zweiten Fall gilt aber jedenfalls $\mathfrak{Z}^*(\,\forall x\,(\,0 < x \to \mathbf{G}\,)\,)$=F (da mit endlich vielen Gleichungen nicht alle positiven Zahlen erfaßbar sind), woraus wie in den vorigen Fällen sofort ein Widerspruch zur Annahme entsteht.

Es ist hiermit insgesamt also gezeigt worden, daß die obige Annahme über die definitorische Erweiterung TAZ'^* von TAZ', $\mathfrak{Z}^*$ als Modell zu besitzen, verworfen werden muß.

Hiermit ist nun aber der letzte für den Gesamtbeweis des Satzes noch nötige Beweisschritt abgeschlossen worden.

□

Die Aussage von Satz 2.1.8 bleibt allerdings in dem Fall nicht mehr erhalten, wenn statt TAZ bzw. $Th(\langle\mathbb{Z}; 0, 1, +\rangle)$ die umfassendere, jedoch unentscheidbare Theorie $VZZ := Th(\langle\mathbb{Z}; 0, 1, +, .\rangle)$ betrachtet wird, deren Sprache also noch zusätzlich das Multiplikationssymbol . enthält. Denn das Ordnungssymbol $<$ ist in einer definitorischen Erweiterung von VZZ (und eigentlich auch schon in einer von $Th(\langle\mathbb{Z}; +, .\rangle)$) definierbar: Und zwar kann dies[12] unter Verwendung des Satzes von Lagrange (: Jede natürliche Zahl läßt sich als Summe von 4 Quadratzahlen darstellen, d.h. als Summe von 4 Quadraten ganzer Zahlen (oder Quadraten von Zahlen aus $\mathbb{N}_0$).) in einer definitorischen Erweiterung von $Th(\langle\mathbb{Z}; +, .\rangle)$ um das einstellige Prädikat $\mathbf{nn}$ ("natural number") vermittels

$$\mathbf{nn}(x) \;\leftrightarrow\; \neg\, x = 0 \,\&\, \exists\, y\, \exists\, z\, \exists\, y'\, \exists\, z'\,(\, x = y.y + z.z + y'.y' + z'.z'\,)\ ,$$

[12] (worauf [Shoe67] hinweist)

und dann um $<$ mittels

$$x < y \;\leftrightarrow\; \exists z(\,\mathbf{nn}(x)\;\&\;x + z = y\,)$$

erfolgen.

2.2 Die Presburger Arithmetik ganzer Zahlen $PreAZ$

In einem Anhang zu seiner Arbeit [Pre29], „Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in dem ... “, teilte M. Presburger mit:

> „Das Ergebnis der Vollständigkeit läßt sich erweitern auf die Arithmetik ganzer Zahlen, die auf den primitiven Begriffen „0“, „1“, „+“, „>“ gebaut ist.“ [13]

Bei der für dieses System im folgenden betrachteten Entsprechung handelt es sich um die—hier so bezeichnete—Theorie $PreAZ$ („Presburger Arithmetik ganzer Zahlen“), die eine Erweiterung von TAZ um die zusätzliche Verwendung des Ordnungssymbols $<$ darstellt. Allerdings muß es sich bei dieser Erweiterung von TAZ zu $PreAZ$ um eine nichtdefinitorische Einführung von $<$ [14] handeln, damit $PreAZ$ eine Axiomatisierung von $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ sein kann (vgl. Satz 2.1.8).

Definition 2.2.1. Die Theorien $PreAZ$, $PreAZ'$.

(i) Sei L_{PreAZ} eine (Sprache einer Theorie 1. Ordnung und eine) Erweiterung von L_{TAZ} um das 2-stellige Prädikatssymbol $<$. Dann ist $PreAZ$ jene Theorie mit Sprache L_{PreAZ}, die als nichtlogische Axiome genau die im folgenden mit PreAZ.1., PreAZ.2., ... , PreAZ.9., sowie weiters noch alle aus dem Axiomenschema PreAZ.S. stammenden Formeln besitzt:

PreAZ.1. $x + (y + z) = (x + y) + z$

PreAZ.2. $x + 0 = x$

PreAZ.3. $\exists\, y\,(\, x + y = 0\,)$

PreAZ.4. $x + y = y + x$

PreAZ.5. $\neg\,(\, x < x\,)$

PreAZ.6. $x < y \to y < z \to x < z$

PreAZ.7. $x < y \;\vee\; x = y \;\vee\; y < x$

PreAZ.8. $x < y \to x + z < y + z$

PreAZ.9. $x < y + 1 \;\leftrightarrow\; x = y \;\vee\; x < y$

PreAZ.S. $\left\{\; \exists\, y\,\left(\underline{n}\,y = x \;\vee\; \underline{n}\,y + 1 = x \;\vee\; \ldots \;\vee\; \underline{n}\,y + \underline{\underline{n-1}} = x\right)\;\right\}_{n\in\mathbb{N},\, n\geq 2}$.

[13] (Vgl. [Pre29], S. 395)

[14] Daß hier im Unterschied zu [Pre29] eine Erweiterung um die Einführung von $<$ anstatt von $>$ betrachtet wird, führt natürlich nur auf eine geringfügig syntaktisch und symbolisch anders organisierte Theorie, weil ja $>$ sofort aus $<$ vermittels $x > y \leftrightarrow y < x$ definiert werden kann. Die „Ausdrucksstärken“ der betrachteten Erweiterungen von TAZ um $<$ bzw. um $>$ unterscheiden sich also nicht; die Einführung von Ordnungssymbolen geschieht heute üblicherweise eher für $<$ bzw. für $\leq$.

(Wie schon bei der Definition von TAZ sind auch hier abkürzende Schreibweisen verwendet worden, die in Definition 2.1.1 erklärt sind: Mengenklammern zur Darstellung des Axiomenschemas PreAZ.S., Weglassung der Klammerung bzgl. $+$, Ersetzung von n-fach-Termen bzgl. der Addition durch kompakter geschriebene, jedoch immer als genau definierte Ausdrücke zu verstehende Terme von $PreAZ$.)

(ii) $PreAZ'$ sei die definitorische Erweiterung von $PreAZ$ um die Einführung der 2-stelligen Kongruenzsymbole der Familie $\{\equiv_n\}_{n\in\mathbb{N},\, n\geq 2}$ vermittels des Schemas D.KON.S. von definierenden Axiomen (vgl. Definition 2.1.4).

$PreAZ$ ist eine Erweiterung von TAZ um Axiome, die eine lineare Ordnung beschreiben (d.h., die es möglich machen, daß eine solche Ordnung $\leq$ aus $<$ mittels $x \leq y \leftrightarrow x = y \vee x < y$ definiert werden kann), es sind dies PreAZ.5., PreAZ.6., PreAZ.7., sowie um ein Axiom PreAZ.8., das eine Eigenschaft der Verträglichkeit von $+$ mit $<$ beschreibt, und um das Axiom PreAZ.9., das wesentlich die Eigenschaft der Diskretheit der aus $<$ definierbaren Ordnung $\leq$ enthält (d.h. genau etwa das, was noch fehlt, wenn man zu den bisherigen Axiomen für PreAZ noch die Axiome der Diskretheit einer Ordnung $\leq$ (mit eindeutig bestimmten Vorgänger- und eindeutig bestimmter Nachfolgereigenschaft bzgl. hier: „Nachfolger“ entspricht „Addition + 1“) hinzunimmt).

PreAZ.S. steht hier wieder für die Möglichkeit von Kongruenzenbildung und könnte in der Erweiterung $PreAZ'$ von $PreAZ$ auch als Schema der Gestalt

$$\left\{\ x \equiv_n 0 \ \vee\ x \equiv_n 1 \ \vee\ \ldots\ \vee\ x \equiv_n \underline{\underline{n-1}}\ \right\}_{n\in\mathbb{N},\, n\geq 2}$$

betrachtet werden. PreAZ.S.(=TAZ.S2.) ist nicht von den übrigen Axiomen von $PreAZ$ abhängig (vgl. [KrKr72], S. 57) und kann dort daher nicht wie die Schemata TAZ.S1. und TAZ.S3., die das schon sind (was leicht beweisbar ist), in der Definition von $PreAZ$ unberücksichtigt bleiben.

Eine von $PreAZ$ etwas verschiedene Art, die Presburger Arithmetik ganzer Zahlen (und damit ist gemeint: eine Theorie der Addition ganzer Zahlen mit Ordnungssymbol) zu axiomatisieren, geschieht in [KrKr72]. Dort wird für die Axiomatisierung einer (hier so bezeichneten) Theorie $PreAZ^{\mathrm{KrKr}}$ neben den nichtlogischen Symbolen $0, 1, +$ noch das einstellige Funktionssymbol $-$ („minus“) und als Ordnungssymbol das einstellige Relationssymbol $\underline{\geq 0}$ („größer als 0“) verwendet; zusätzlich zu diesen Symbolen werden in der Axiomatisierung von $PreAZ^{\mathrm{KrKr}}$ noch einstellige Prädikatssymbole $\underline{n|}$ („n teilt ... “) (für $n \in \mathbb{N}$, $n \geq 2$) verwendet. Diese Symbole übernehmen in $PreAZ^{\mathrm{KrKr}}$ (im Verein mit $+$ und $-$) die Rolle der Kongruenzsymbole $\equiv_n$ ($n \in \mathbb{N}$, $n \geq 2$) in $PreAZ'$. Dabei werden diese Symbole $\underline{n|}$ in [KrKr72] nicht (wie in $PreAZ'$) erst definitorisch über einer Grundtheorie eingeführt (was (wie auch für das Symbol $-$) möglich wäre), sondern sind dann in der definierten Theorie sofort verfügbar (d.h. die definitorischen Erweiterungen einer zu-

grundeliegenden Theorie, die nicht mehr definitorische Erweiterung einer weniger Symbole enthaltenden Theorie ist, sind in der vorgestellten Theorie $PreAZ^{\mathrm{KrKr}}$ schon beinhaltet).

Definition 2.2.2. Die Theorie $PreAZ^{\mathrm{KrKr}}$.

Sei $L_{PreAZ^{\mathrm{KrKr}}}$ eine Sprache einer Theorie 1. Ordnung, die als nichtlogische Symbole enthält: Die Konstantensymbole 0,1, das einstellige Funktionssymbol $+$ und die einstelligen Relationssymbole $\underline{\geq 0}$ und $\underline{n|}$ (für alle $n \in \mathbb{N}$, $n \geq 2$). Dann ist $PreAZ^{\mathrm{KrKr}}$ jene Theorie, die als Axiome alle im folgenden mit $PreAZ^{\mathrm{KrKr}}.1., \ldots, PreAZ^{\mathrm{KrKr}}.8.$ bezeichneten, sowie weiters noch alle einem der Axiomenschemata $PreAZ^{\mathrm{KrKr}}.S1.$ oder $PreAZ^{\mathrm{KrKr}}.S2.$ angehörenden Formeln besitzt:

PreAZ$^{\mathrm{KrKr}}$.1.	$x + (y + z) = (x + y) + z$
PreAZ$^{\mathrm{KrKr}}$.2.	$x + y = y + x$
PreAZ$^{\mathrm{KrKr}}$.3.	$x + 0 = x$
PreAZ$^{\mathrm{KrKr}}$.4.	$x + (-x) = 0$
PreAZ$^{\mathrm{KrKr}}$.5.	$x \underline{\geq 0} \rightarrow y \underline{\geq 0} \rightarrow x + y \underline{\geq 0}$
PreAZ$^{\mathrm{KrKr}}$.6.	$\neg\,(\, x \underline{\geq 0} \;\&\; -x \underline{\geq 0}\,)$
PreAZ$^{\mathrm{KrKr}}$.7.	$x = 0 \;\vee\; x \underline{\geq 0} \;\vee\; -x \underline{\geq 0}$
PreAZ$^{\mathrm{KrKr}}$.8.	$x \underline{\geq 0} \;\leftrightarrow\; x = 1 \;\vee\; x + (-1) \underline{\geq 0}$
PreAZ$^{\mathrm{KrKr}}$.S1.	$\{\; \underline{n|}\, x \;\leftrightarrow\; \exists y\,(\, x = \underline{n}\, y\,)\;\}_{n \in \mathbb{N},\, n \geq 2}$
PreAZ$^{\mathrm{KrKr}}$.S2.	$\{\; \underline{n|}\, x \;\vee\; \underline{n|}\, x + 1 \;\vee\; \ldots \;\vee\; \underline{n|}\, x + \underline{\underline{n-1}}\;\}_{n \in \mathbb{N},\, n \geq 2}$.

(Für die Darstellung von $PreAZ^{\mathrm{KrKr}}.S1.$ und $PreAZ^{\mathrm{KrKr}}.S2.$ wurden wieder abkürzende Schreibweisen aus Definition 2.1.1 verwendet.)

PreAZ$^{\mathrm{KrKr}}$.1., ..., PreAZ$^{\mathrm{KrKr}}$.4. beschreiben erneut die Struktur einer kommutativen Gruppe, PreAZ$^{\mathrm{KrKr}}$.5., ..., PreAZ$^{\mathrm{KrKr}}$.8. definieren nun implizit eine erneut diskrete (: das ist wesentlich in PreAZ$^{\mathrm{KrKr}}$.8. formuliert) lineare Ordnung, die mit $+$ verträglich ist (PreAZ$^{\mathrm{KrKr}}$.5.). Die beiden Axiomenschemata in $PreAZ^{\mathrm{KrKr}}$ ermöglichen die Kongruenzenbildung (in der hier möglichen formalen Ausgestaltung) (PreAZ$^{\mathrm{KrKr}}$.S2.) und die Verwendung der Teilbarkeitssymbole $\underline{n|}$ (PreAZ$^{\mathrm{KrKr}}$.S1.).

Insgesamt scheint die Axiomatisierung von $PreAZ$ etwas durchsichtiger zu sein, die Struktur von $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ wird dadurch vielleicht deutlicher aufgehellt. Es sollte hier aber klar gemacht werden, daß $PreAZ$ nicht die einzige mögliche Axiomatisierung ist, sondern andere bündige Möglichkeiten durchaus ebenso existieren.

$PreAZ$ und $PreAZ^{\mathrm{KrKr}}$ sind nun in dem Sinn verschiedene, aber gleichwertige Wege der Axiomatisierung der Presburger Arithmetik ganzer Zahlen, als von den beiden Theorien auf einfache Weise zu zwei definitorischen Erweiterungen übergegangen werden kann,

die als Theorien äquivalent sind. Zwei Theorien mit dieser Eigenschaft werden von [Shoe67] als „schwach äquivalent“ bezeichnet.

Definition 2.2.3. Schwache Äquivalenz von Theorien.

Seien T_1 und T_2 zwei Theorien. T_1 und T_2 heißen **schwach äquivalent**, *wenn es definitorische Erweiterungen T_1' und T_2' von T_1 bzw. von T_2 gibt, die äquivalent sind.*

Satz 2.2.4. *$PreAZ$ und $PreAZ^{\mathrm{KrKr}}$ sind schwach äquivalent.*

Beweisskizze. Man erweitert $PreAZ$ definitorisch zu $PreAZ'$ und weiter durch die definitorische Einführung von $-$ vermittels $y = -x \leftrightarrow y + x = 0$ und von $\underline{\geq 0}$ vermittels $x \underline{\geq 0} \leftrightarrow x > 0$ und um die Familie $\{\underline{n|}\}_{n\in\mathbb{N},\, n\geq 2}$ mit Hilfe von $\{\underline{n|}\, x \leftrightarrow x \equiv_n 0\}_{n\in\mathbb{N},\, n\geq 2}$ zur Theorie $PreAZ''$; andererseits erweitert man $PreAZ^{\mathrm{KrKr}}$ um die Einführung von $<$ durch $x < y \leftrightarrow y + (-x) \underline{\geq 0}$ und von $\{\equiv_n\}_{n\in\mathbb{N},\, n\geq 2}$ vermittels des Schemas $\{\, x \equiv_n y \leftrightarrow \underline{n|}\,(\, x_1 + (-x_2)\,)\,\}_{n\in\mathbb{N},\, n\geq 2}$ von definierenden Axiomen zur Theorie $PreAZ_1^{\mathrm{KrKr}}$. Schließlich zeigt man, daß alle Axiome von $PreAZ_1^{\mathrm{KrKr}}$ in $PreAZ''$ beweisbar sind und alle Axiome von $PreAZ''$ in $PreAZ_1^{\mathrm{KrKr}}$ (das ist mühsam, birgt aber keine grundsätzlichen Schwierigkeiten). Daraus folgt die Äquivalenz von $PreAZ''$ und von $PreAZ_1^{\mathrm{KrKr}}$. $\diamondsuit$

Satz 2.2.5. *$PreAZ'$ läßt die QE auf eine effektive Weise zu. Alle variablenfreien Formeln von $PreAZ'$ sind entscheidbar. $PreAZ$ ist vollständig und entscheidbar.*

Beweisskizze. Wie im Beweis zu Satz 2.1.6 anhand von TAZ' nachgewiesen, so folgen auch hier die Vollständigkeit und die Entscheidbarkeit von $PreAZ$ dann unmittelbar, wenn ein effektives QE-Verfahren für $PreAZ'$ angegeben werden kann und außerdem nachgewiesen wird, daß alle variablenfreien Formeln von $PreAZ'$ entscheidbar sind.

Der Nachweis davon, daß in $PreAZ'$ alle variablenfreien Formeln entscheidbar sind, erfordert über den für TAZ' diesbezüglich schon erfolgten Beweis in Satz 2.1.6 hinaus lediglich noch die Einsicht in die Richtigkeit von $\vdash_{PreAZ'} \underline{\underline{a}} < \underline{\underline{b}}$ für $a, b \in \mathbb{N}_0$, $a < b$, sowie von $\vdash_{PreAZ'} \neg\, \underline{\underline{a}} < \underline{\underline{b}}$ für $a, b \in \mathbb{N}_0$, $b \leq a$, und in die Tatsache, daß $PreAZ$ wirklich Erweiterung von TAZ ist (daß also die in der Axiomatisierung von $PreAZ$ gegenüber der von TAZ fehlenden Schemata TAZ.S1. und TAZ.S3. in $PreAZ$ beweisbar sind). – Diese Aussagen sind aber schnell zu überprüfen (ein ausführlicher Nachweis unterbleibt hier).

Bezüglich eines effektiven Quantoreneliminationsverfahrens für $PreAZ'$ sei hier auf [BoJe74] verwiesen. Das dort vorgestellte Verfahren ist nicht so sehr eine direkte Erweiterung des ursprünglich von Presburger vorgestellten Verfahrens für TAZ' [15] (das hier im

[15] Als eine direkte Erweiterung des ursprünglichen Presburgerschen Beweises ist am ehesten ein in [HiBe68] für eine Theorie, die der in Abschnitt 3 behandelten Theorie $PreAN'$ entspricht, dargestelltes Verfahren zu betrachten. Dieses könnte auf einfache Weise auch zu einem für $PreAZ'$ anwendbaren umgebildet werden.

wesentlichen im Beweis zu Lemma 2.1.5 beschrieben worden ist), als vielmehr eine elegant dargestellte Variante eines erweiterten und verbesserten Verfahrens.

Allerdings wird in [BoJe74] nicht eine $PreAZ'$ unmittelbar entsprechende Theorie (mit den nichtlogischen Symbolen 0, 1, $+$, $<$, $\equiv_2$, $\equiv_3$, ...) betrachtet, sondern eine schwach äquivalente Theorie dazu, die als nichtlogische Symbole neben 0, 1 und $+$ noch das einstellige Funktionssymbol $-$ („minus“) und die einstelligen Prädikatssymbole $\mathbf{D}_m$ („m teilt ... “) ($m \in \mathbb{N}$, $m \geq 2$) besitzt.

Um nun von dem in [BoJe74] für eine Theorie der Addition ganzer Zahlen mit diesen nichtlogischen Symbolen dargestellten QE-Verfahren zu einem für $PreAZ'$ zu gelangen, sind zwei Wege möglich: (1) Entweder man überzeugt sich (was leicht möglich ist), daß das in [BoJe74] beschriebene Verfahren direkt umgebildet werden kann zu einem, das auf Formeln von $PreAZ'$ operiert und in diesen zur Quantorenelimination führt, oder (2) man betrachtet eine definitorische Erweiterung $PreAZ'^*$ von $PreAZ'$ um die definitorische Einführung von $-$ vermittels $y = -x \leftrightarrow x + y = 0$ und von $\{\mathbf{D}_m\}_{m\in\mathbb{N},\, m\geq 2}$ vermittels $\{\, \mathbf{D}_m\, x \leftrightarrow x \equiv_m 0 \,\}_{m\in\mathbb{N},\, m\geq 2}$, und gelangt dann für eine Formel $\mathbf{A}$ von $PreAZ'$ auf folgende Weise zu einer äquivalenten offenen Formel $\mathbf{B}$: (a) Man bildet $\mathbf{A}$ so zu $\mathbf{A}^*$ um, daß man in $\mathbf{A}$ alle Terme $\mathbf{a} \equiv_n \mathbf{b}$ ($n \in \mathbb{N}$, $n \geq 2$) durch $\mathbf{D}_n(\mathbf{b} + (-\mathbf{a}))$ ersetzt; dann gilt $\vdash_{PreAZ'^*} \mathbf{A} \leftrightarrow \mathbf{A}^*$; (b) dann wendet man auf $\mathbf{A}^*$ das in [BoJe74] beschriebene QE-Verfahren an und gelangt damit schließlich zu einer offenen Formel $\mathbf{B}^*$ mit $\vdash_{PreAZ'^*} \mathbf{A}^* \leftrightarrow \mathbf{B}^*$; (c) man ersetzt in $\mathbf{B}^*$ auftretende atomare Formeln, die das Symbol $-$ oder Symbole $\mathbf{D}_m$ enthalten, wieder durch äquivalente atomare Formeln, die höchstens $+$, 0, 1 und Symbole $\equiv_n$ ($n \in \mathbb{N}$, $n \geq 2$) enthalten (das ist immer möglich und wird noch dadurch vereinfacht, daß die durch die Quantorenelimination neu entstehenden Kongruenzformeln dieses Verfahrens immer von der einfachen Gestalt $\mathbf{D}_m\big(\,(\mathbf{a} + \underline{\underline{i}}) - \underline{\underline{j}}\,\big)$ sind, die sofort durch $\mathbf{a} + \underline{\underline{i}} \equiv_m \underline{\underline{j}}$ ersetzt werden können) und gelangt damit zu einer offenen Formel $\mathbf{B}$. – Insgesamt wurde dann eine offene Formel $\mathbf{B}$ mit $\vdash_{PreAZ'^*} \mathbf{A} \leftrightarrow \mathbf{B}$ effektiv gefunden und es gilt dann auch $\vdash_{PreAZ'} \mathbf{A} \leftrightarrow \mathbf{B}$, da $PreAZ'^*$ definitorische (und also konservative) Erweiterung von $PreAZ'$ ist.

Der letzte Schritt in einem (wie oben in (1) angedeutet) umgebildeten Verfahren für $PreAZ'$ besteht im allgemeinsten Fall aus der Elimination des $\exists$-Quantors bezüglich einer Variablen $\mathbf{x}$ in einer Formel der Gestalt

$$\exists\, \mathbf{x}\, \big(\, \mathbf{x} \equiv_m \underline{\underline{i}}\, \&\, \mathbf{a} < \underline{\alpha}\, \mathbf{x} + \mathbf{b}\, \&\, \underline{\alpha'}\mathbf{x} + \mathbf{b}' < \mathbf{a}' \,\big)\,, \tag{2.15}$$

wobei $m \in \mathbb{N}$, $m \geq 2$, $i \in \mathbb{N}_0$, $i < m$, $\alpha, \alpha' \in \mathbb{N}$, $\mathbf{a}, \mathbf{b}, \mathbf{a}', \mathbf{b}'$ Terme ohne $\mathbf{x}$.

Die dafür nötigen Umformungen sollen hier exemplarisch dargestellt werden, auch, weil dieser Schritt in einer noch etwas weiter abgeänderten Form in Abschnitt 3 für die Theorie $PreAN'$ nötig sein wird.

Von (2.15) ausgehend ergibt eine erste äquivalente Umformung

$$\exists\, \mathbf{x}\, \big(\, \underline{\alpha\, \alpha'}\mathbf{x} \equiv_{\alpha\, \alpha'\, m} \underline{\alpha\, \alpha'}\, \underline{\underline{i}}\, \&\, \underline{\alpha'}\, \mathbf{a} < \underline{\alpha\, \alpha'}\, \mathbf{x} + \underline{\alpha'}\mathbf{b}\, \&\, \underline{\alpha\, \alpha'}\, \mathbf{x} + \underline{\alpha}\, \mathbf{b}' < \underline{\alpha}\, \mathbf{a}' \,\big)\,.$$

Daraus ergeben sich äquivalent in der Folge

$$\exists\, \mathbf{x}\, \big(\, \mathbf{x} \equiv_{\alpha\, \alpha'\, m} \underline{\alpha\, \alpha'\, \underline{\underline{i}}} \;\;\&\;\; \underline{\alpha'}\, \mathbf{a} < \mathbf{x} + \underline{\alpha'}\, \mathbf{b} \;\;\&\;\; \mathbf{x} + \underline{\alpha}\, \mathbf{b}' < \underline{\alpha}\, \mathbf{a}' \,\big)$$

und

$$\begin{aligned} \exists\, \mathbf{x}\, \big(\, & \mathbf{x} \equiv_{\alpha\, \alpha'\, m} \underline{\alpha\, \alpha'\, \underline{\underline{i}}} \\ & \&\;\; \underline{\alpha'}\, \mathbf{a} + \underline{\alpha}\, \mathbf{b}' < \mathbf{x} + \underline{\alpha'}\, \mathbf{b} + \underline{\alpha}\, \mathbf{b}' \;\;\&\;\; \mathbf{x} + \underline{\alpha}\, \mathbf{b}' + \underline{\alpha'}\, \mathbf{b} < \underline{\alpha}\, \mathbf{a}' + \underline{\alpha'}\, \mathbf{b} \,\big) \end{aligned} \tag{2.16}$$

(2.16) ist nun aber von der Gestalt

$$\exists\, \mathbf{x}\, \big(\, \mathbf{x} \equiv_{\tilde{m}} \underline{\underline{j}} \;\;\&\;\; \mathbf{d} < \mathbf{x} + \mathbf{c} \;\;\&\;\; \mathbf{x} + \mathbf{c} < \mathbf{d}' \,\big)\,,$$

wobei $\tilde{m} \in \mathbb{N}$, $\tilde{m} \geq 2$, $j \in \mathbb{N}_0$ $j < \tilde{m}$, $\mathbf{c}, \mathbf{d}, \mathbf{d}'$ Terme ohne $\mathbf{x}$. Es folgt nun äquivalent

$$\exists\, \mathbf{x}\, \big(\, \mathbf{x} \equiv_{\tilde{m}} \underline{\underline{j}} + \mathbf{c} \;\;\&\;\; \mathbf{d} < \mathbf{x} \;\;\&\;\; \mathbf{x} < \mathbf{d}' \,\big)\,; \tag{2.17}$$

(2.17) ist nun aber äquivalent zur quantorenfreien Formel

$$\begin{aligned} & \mathbf{d} + 1 \equiv_{\tilde{m}} \underline{\underline{j}} + \mathbf{c} \;\;\&\;\; \mathbf{d} + 1 < \mathbf{d}' \;\;\vee\;\; \mathbf{d} + \underline{\underline{2}} \equiv_{\tilde{m}} \underline{\underline{j}} + \mathbf{c} \;\;\&\;\; \mathbf{d} + \underline{\underline{2}} < \mathbf{d}' \;\;\vee\;\; \ldots \\ & \quad \ldots \;\;\vee\;\; \mathbf{d} + \underline{\underline{\tilde{m}}} \equiv_{\tilde{m}} \underline{\underline{j}} + \mathbf{c} \;\;\&\;\; \mathbf{d} + \underline{\underline{\tilde{m}}} < \mathbf{d}'\,. \end{aligned}$$

Weiters muß betont werden, daß ausführlich überprüft werden kann, daß für das (wie oben in (1) vorgeschlagene) bezüglich Formeln von $PreAZ'$ abgeänderte Verfahren von [BoJe74] dessen einzelne Umformungsschritte wirklich Ersetzungs- bzw. Überführungsschritte[16] für Formeln von $PreAZ'$ sind. Eine solche ausführliche Überprüfung der Beweisbarkeit dieser Schritte in $PreAZ'$ ist nötig, um die Aussage von Satz 2.2.5 im selben Ausmaß für $PreAZ'$ bzw. $PreAZ$ wie für $Th(\langle \mathbb{Z}; 0, 1, +, <, \equiv_2, \equiv_3, \ldots \rangle)$ bzw. $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ nachzuweisen[17] (denn die Gültigkeit der Umformungsschritte über $\mathbb{Z}$ ist meistens ganz offensichtlich).

Es ist natürlich auch möglich, das in [KrKr72] für $PreAZ^{\mathrm{KrKr}}$ angegebene QE-Verfahren (und sogar auch das in [HiBe68] für die im nächsten Kapitel behandelten Theorien der Presburger Arithmetik natürlicher Zahlen) zur Quantorenelimination in und zur Entscheidung von Formeln von $PreAZ'$ auf ähnliche Weise (und d.h. über die oben angedeuteten zwei Wege entweder des Umbaus des Verfahrens oder der Verwendung des Verfahrens zuzüglich Hin- und Rückübersetzung von Formeln) nutzbar zu machen. Alle diese Verfahren unterscheiden sich methodisch nicht grundlegend. $\diamondsuit$

[16] [HiBe68] sprechen in diesem Zusammenhang von der (äquivalenten) „Überführbarkeit“ von Formeln.

[17] Eine solche ausführliche Überprüfung ist letztlich die wesentliche Stütze dafür, daß $PreAZ$ wirklich eine vollständige Axiomatisierung von $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ ist und lag der Definition und Darstellung von $PreAZ$ hier natürlich zugrunde.

Es gibt dennoch auch noch andere Möglichkeiten zur Entscheidung von $PreAZ'$, z.B. benutzten [FeRa73] ein Quantoreneliminationsverfahren von [Coo72] für die der Theorie $PreAZ'$ (im Lichte von Satz 2.2.5) entsprechende, d.h. dazu äquivalente Theorie $Th(\langle \mathbb{Z}; 0, 1, +, <, \equiv_2, \equiv_3, \ldots \rangle)$ und eine Komplexitätsanalyse dieses Verfahrens durch D. Oppen in [Opp73] zur Konstruktion eines Ehrenfeucht-game-Entscheidungsverfahrens. Eine Darstellung dieses Verfahrens findet sich in [FeRa79]. Dieses bildet die Grundlage für eine deterministische obere Rechenzeitschranke für die Entscheidungskomplexität von $PreAZ$ (vgl. Abschnitt 6), die von J. Ferrante und Ch. Rackoff schon in [FeRa73] vorgestellt wurde.

Im Zusammenhang mit dem oben erwähnte QE-Verfahren für $PreAZ'$ und für verwandte Theorien sei noch erwähnt, daß [KrKr72] darauf aufmerksam machen, daß eine Theorie, die aus der Weglassung des Schemas $\mathrm{PreAZ}^{\mathrm{KrKr}}$.S2. aus $PreAZ^{\mathrm{KrKr}}$ als Theorie mit derselben Sprache entsteht, die QE nicht mehr zuläßt. Diese Aussage trifft auch auf eine aus $PreAZ'$ durch Weglassung von PreAZ.S. entstehende Theorie mit gleicher Sprache wie $PreAZ'$ zu. Und zwar läßt sich das unter Verwendung einer Argumentation wie bei Weg (2) der Quantorenelimination für $PreAZ'$ im Beweis zu Satz 2.2.5 einsehen, wenn man beachtet, daß die beiden durch Weglassung der Kongruenzenschemata aus $PreAZ^{\mathrm{KrKr}}$ bzw. aus $PreAZ'$ entstehenden Theorien immer noch schwach äquivalent sind.

2.3 Die Presburger Arithmetik ganzer Zahlen $PreAN$

Der dritte Typ von Theorien der Additionsarithmetik, der oft auch ebenso wie die in Abschnitt 2 behandelten Theorien unterschiedslos als „Presburger Arithmetik“ bezeichnet wird, besteht aus einer Gruppe von Theorien der Arithmetik natürlicher Zahlen. Dabei handelt es sich hier—wie schon im Fall von $PreAZ$, $PreAZ'$ und z.B von $Th(\langle\mathbb{Z}; 0, 1, +, <\rangle)$—um unterschiedlich definierte Theorien, jedoch—wie sich herausstellt—um Theorien von gleicher Aussagekraft (womit gemeint ist, daß diese sich immer durch einfache definitorische Erweiterungen zu Theorien erweitern lassen, die schließlich als äquivalent erkannt werden können).

Dem unscharfen Sprachgebrauch in der Verwendung der Bezeichnung „Presburger Arithmetik“ sowohl für Theorien der Addition ganzer Zahlen als auch für Theorien der Addition natürlicher Zahlen kann schließlich wieder eine bestimmte Berechtigung zugesprochen werden (weil wirklich eine nahe Verwandtschaft zwischen diesen beiden Gruppen von Theorien herstellbar ist, vgl. Abschnitt 4). Für eine genaue Behandlung der formalaxiomatischen Unterscheidung und der herzustellenden Beziehung ist es jedoch nötig, beide Gruppen von Theorien formal getrennt betrachten zu können.

Das Vollständigkeits- und Entscheidbarkeitsresultat von Presburger wird sich auch auf die hier betrachteten Theorien übertragen lassen, sodaß die Berechtigung der namentlichen Bezeichnung „Presburger Arithmetik natürlicher Zahlen“ daraufhin eingesehen wird können.

Die Axiomatisierung der hier im folgenden nun zuerst betrachteten Theorie $PreAN$ erfolgte in der Bemühung, die Axiomatisierung von $PreAZ$ möglichst direkt zu einer Axiomatisierung der Additionsarithmetik natürlicher Zahlen umzubilden.

Definition 2.3.1. Die Theorien $PreAN$, $PreAN'$.

(i) *$PreAN$ sei jene Theorie 1. Ordnung, deren Sprache L_{PreAN} gleich der Sprache L_{PreAZ} von $PreAZ$ ist (und welche somit genau die Symbole 0, 1, $+$, $<$ als nichtlogische Symbole enthält) und die als nichtlogische Axiome genau die Axiome PreAN.1., PreAN.2., ... , PreAN.10. besitzt, sowie zusätzlich noch alle jene Formeln, die dem Schema PreAN.S. angehören, wobei:*

PreAN.1. $x + (y + z) = (x + y) + z$

PreAN.2. $x + 0 = x$

PreAN.3. $x + y = y + x$

PreAN.4. $\exists\, z\,(\, x + z = y \;\vee\; x = y + z\,)$

PreAN.5. $\neg\,(\, x < x\,)$

PreAN.6. $x < y \to y < z \to x < z$

PreAN.7. $x < y \;\vee\; x = y \;\vee\; y < x$

PreAN.8. $0 = x \;\vee\; 0 < x$

PreAN.9. $x < y + 1 \;\leftrightarrow\; x = y \;\vee\; x < y$

PreAN.10. $x < y \to x + z < y + z$

PreAN.S. $\left\{\; \exists\, y\,\big(x = \underline{n}\, y \;\vee\; x = \underline{n}\, y + 1 \;\vee\; \ldots \;\vee\; x = \underline{n}\, y + \underline{\underline{n-1}}\big) \;\right\}_{n\in\mathbb{N},\, n\geq 2}$.

(Für die in PreAN.S. dabei verwendeten abkürzenden Schreibweisen vgl. erneut Definition 2.1.1.)

(ii) *$PreAN'$ sei die definitorische Erweiterung von $PreAN$ um die Einführung der 2-stelligen Prädikatssymbole $\equiv_n^{\mathrm{N}}$ ($n \in \mathbb{N}$, $n \geq 2$) der Familie $\left\{\equiv_n^{\mathrm{N}}\right\}_{n\in\mathbb{N},\, n\geq 2}$ von Kongruenzsymbolen mittels des Schemas D.KON.N.S. von definierenden Axiomen, wobei:*

D.KON.N.S. $\left\{\; x \equiv_n^{\mathrm{N}} y \leftrightarrow \exists\, z\,\big(x = y + \underline{n}\, z \;\vee\; x + \underline{n}\, z = y\big) \;\right\}_{n\in\mathbb{N},\, n\geq 2}$.

Wie bereits erwähnt, wurde die Axiomatisierung von $PreAN$ v.a. im Hinblick darauf gewählt, schon dadurch und darin die nahe Verwandtschaft von $PreAN$ mit $PreAZ$ deutlich zu machen.

Es handelt sich bei $PreAN$ also nicht mehr wie bei $PreAZ$ um die Axiomatisierung einer kommutativen Gruppe, sondern nur noch um die eines kommutativen Monoids, in welchem aber auf die durch PreAN.4. beschriebene Weise immerhin noch Differenzenbildungen zwischen Elementen möglich sind.

Dieses Axiom PreAN.4. ist allerdings stark mit den Ordnungsaxiomen verknüpft, auf präzisierte Weise etwa in dem Sinn, daß eine Theorie, die aus $PreAN$ durch Weglassung von PreAN.4. und PreAN.10, jedoch durch gleichzeitige Hinzunahme eines neuen Axioms $x < y \leftrightarrow \exists z\,(\neg z = 0 \,\&\, y = x + z\,)$ entsteht, zu $PreAN$ äquivalent ist.

PreAN.5., PreAN.6. und PreAN.7. beschreiben wieder den Charakter von $<$, eine lineare Ordnung $\leq$ zu bestimmen, PreAN.9. wieder die Diskretheit der Ordnung $<$ bezüglich der arithmetischen Vorgänger- und Nachfolgereigenschaft zwischen natürlichen Zahlen und PreAN.10. fordert erneut die Verträglichkeit der Addition $+$ mit der durch $<$ induzierten Ordnung.

Hinzu tritt hier aber PreAN.8., das die Konstante 0 als das kleinste Element einer durch $<$ bestimmten Ordnung $\leq$ festsetzt. Die die Ordnung betreffenden Axiome in $PreAN$ fordern also jedenfalls (würde von $<$ zu $\leq$ definitorisch übergegangen) eine lineare, diskrete, mit $+$ verträgliche Ordnung $\leq$, die ein kleinstes Element (nämlich 0) besitzt.

In ihren nichtlogischen Axiomen unterscheidet sich die Theorie $PreAN$ also genau in PreAN.4., das eine Abschwächung von PreAZ.3. darstellt und in PreAN.8., dem kein nichtlogisches Axiom von $PreAZ$ entspricht; alle anderen nichtlogischen Axiome von $PreAN$ sind auch Axiome von $PreAZ$.

In der Definition dieser Theorie hätte auch der Weg beschritten werden können, die Ordnungssymbole sämtlich aus allen Axiomen zu eliminieren (mit Hilfe der schon erwähnten, in $PreAN$ beweisbaren Formel $x < y \leftrightarrow \exists z\,(\neg z = 0 \,\&\, y = x + z\,)$) und die Axiomatisierung lediglich auf Formeln zu stützen, in denen als nichtlogische Symbole nur 0, 1 und $+$ vorkommen (woraus dann durch die definitorische Einführung von $<$ erneut vermittels $x < y \leftrightarrow \ldots$ sofort wieder eine zu $PreAN$ äquivalente Theorie entstünde). Diese Überlegung führt auf die im folgenden definierte Theorie $PreAN_1$.

Definition 2.3.2. Die Theorien $PreAN_0$, $PreAN_1$.

(i) Sei L_{PreAN_1} die Sprache einer Theorie 1. Ordnung, die als nichtlogische Symbole lediglich 0, 1 *und* $+$ *enthält; dann ist $PreAN_1$ jene Theorie, die als nichtlogische Axiome genau besitzt:*

PreAN$_1$.1. $x + (y + z) = (x + y) + z$

PreAN$_1$.2. $x + 0 = x$

PreAN$_1$.3. $x + y = y + x$

PreAN$_1$.4. $\exists\, z\,(\, x + z = y \;\vee\; x = y + z\,)$

PreAN$_1$.5. $x + z = y + z \to x = y$

PreAN$_1$.6. $x + y = 0 \to x = 0$

PreAN$_1$.7. $\neg\, x + 1 = 0$

PreAN$_1$.8. $\neg\, x = 0 \to \exists\, y\,(\, x = y + 1\,)$

PreAN$_1$.S. $\Big\{\;\exists\, y\,\big(\, x = \underline{n}\, y \;\vee\; x = \underline{n}\, y + 1 \;\vee\; \ldots \;\vee\; x = \underline{n}\, y + \underline{\underline{n-1}}\,\big)\;\Big\}_{n\in\mathbb{N},\, n\geq 2}$.

(ii) L_{PreAN_0} *sei die Sprache einer Theorie erster Ordnung, die nur das 2-stellige Funktionssymbol* $+$ *besitzt,* $\mathbf{A}$ *sei die Formel* $\forall\, x\,(\, x + z = x\,)$, $\mathbf{B}$ *sei die Formel*

$$\mathbf{A} \to \neg\, w = z \;\&\; \forall\, x\,\big(\,\neg\, x = z \to \exists\, y'\,(\, x = y' + w\,)\,\big)\ .$$

Dann ist $PreAN_0$ *jene Theorie mit Sprache* L_{PreAN_0}*, die als nichtlogische Axiome die im folgenden aufgeführten Formeln* $PreAN_0.1.$*,* $\ldots$ *,* $PreAN_0.8.$*, sowie weiters noch alle Formeln, die dem nachstehenden Schema* $PreAN_0.S.$ *angehören, besitzt:*

PreAN$_0$.1. $x + (y + z) = (x + y) + z$

PreAN$_0$.2. $\exists\, z\, \mathbf{A}$

PreAN$_0$.3. $x + y = y + x$

PreAN$_0$.4. $\exists z\,(\, x + z = y \;\vee\; x = y + z\,)$

PreAN$_0$.5. $x + z = y + z \to x = y$

PreAN$_0$.6. $\mathbf{A} \to x + y = z \to x = z$

PreAN$_0$.7. $\mathbf{A} \to \mathbf{B} \to \neg\, x + w = z$

PreAN$_0$.8. $\exists\, w\, \mathbf{B}$

PreAN$_0$.S. $\Big\{\;\mathbf{B} \to \exists y\,\big(\, x = \underline{n}\, y \;\vee\; x = \underline{n}\, y + w \;\vee\; \ldots$
$\ldots \;\vee\; x = \underline{n}\, y + \underline{n-1}\, w\,\big)\;\Big\}_{n\in\mathbb{N},\, n\geq 2}$.

(Bei der Darstellung von $PreAN_1.S.$ *und* $PreAN_0.S.$ *wurden wieder abkürzende Schreibweisen aus Definition 2.1.1 verwendet.)*

$PreAN_0$ entsteht aus $PreAN_1$ dadurch, daß noch die Konstanten 0 und 1 entfernt werden unter Zuhilfenahme der sie in $PreAN_1$ eindeutig charakterisierenden Formeln $\mathbf{A}$

und $\mathbf{B}$ [18]; „entfernt werden“ jedoch in dem Sinn, daß die entstehende Theorie $PreAN_0$ noch die gleiche Aussagestärke wie $PreAN_1$ (und dann wie $PreAN$) besitzt: $PreAN_0$ kann durch eine definitorische Erweiterung um die Einführung von 0 vermittels $y = 0 \leftrightarrow \mathbf{A}_z[y]$ und der darauffolgenden definitorischen Erweiterung um die Einführung von 1 vermittels $y = 1 \leftrightarrow \mathbf{B}_{z,w}[0, y]$ nämlich wieder zu einer zu $PreAN_1$ äquivalenten Theorie erweitert werden[19].

$PreAN_0$ ist hier deshalb noch ausdrücklich eingeführt und definiert worden (obwohl die dafür verwendete formale Axiomatisierung wie schon im Fall von $PreAN_1$ die grundlegenden Begriffe, auf die diese Theorien gebaut sind, eher verschleiert, jedenfalls im Vergleich zu und mit $PreAN$), weil oftmals auch eine semantisch definierte Entsprechung für diese Theorie (nämlich $Th(\langle \mathbb{N}_0; + \rangle)$) mit der Bezeichnung „Presburger Arithmetik“ identifiziert wird und dargelegt werden wollte, daß dennoch eine leicht zugängliche Axiomatisierung dieser Theorie angegeben werden kann.

Satz 2.3.3. *$PreAN'$ läßt die QE auf eine effektive Weise zu. Alle variablenfreien Formeln von $PreAN'$ sind entscheidbar. $PreAN'$ ist vollständig und entscheidbar.*

Beweisskizze. Vollständigkeit und Entscheidbarkeit von $PreAN$ folgen wieder aus der Existenz eines effektiven QE-Verfahrens für $PreAN'$ und der Tatsache, daß alle variablenfreien Formeln von $PreAN'$ entscheidbar sind.

Letzteres kann wieder—analog wie im Beweis zu Satz 2.1.6—ausführlich überprüft werden.

Ein effektives QE-Verfahren laßt sich ziemlich unmittelbar aus einem für $PreAZ$ anwendbaren gewinnen, beispielsweise aus dem in [BoJe74], Chapt. 21 angegebenen. Es sind dafür in der Hauptsache nur geringfügige Änderungen dahingehend nötig, als dieses Verfahren konsequent zu einem entsprechenden umgebaut werden muß, das nur mit Formeln der Sprache $L_{PreAN'}$ operiert und nicht mit den Symbolen 0, 1, $+$, $-$, $<$, $\mathbf{D}_m$ ($m \in \mathbb{N}$, $n \geq 2$) wie das in [BoJe74] beschriebene; das ist aber (auf recht direkte Weise) möglich.

Eine etwas gewichtigere Änderung ergibt sich bezüglich des letzten Schritts des dort in [BoJe74] dargestellten Verfahrens, an der Stelle, wo ein eine Variable $\mathbf{x}$ bindender Quantor, der sich dann nur mehr auf eine Konjunktion bestehend aus höchstens einer Kongruenz, höchstens einer Ungleichung mit $\mathbf{x}$ auf der rechten Seite und höchstens einer Ungleichung mit $\mathbf{x}$ auf der linken Seite bezieht, wirklich eliminiert wird. Im folgenden wird dieser Schritt (der in ganz ähnlicher Form schon in der Beweisskizze von Satz 2.2.5, ausgehend von (2.15) für die Quantorenelimination in $PreAZ$ beschrieben wurde) dargestellt:

[18] Das ist in dem Sinn zu verstehen, daß die Eindeutigkeitsbedingungen $\mathbf{A}$ & $\mathbf{A}_z[z'] \rightarrow z = z'$ und $\mathbf{B}_z[0]$ & $\mathbf{B}_{z,w}[0, w'] \rightarrow w = w'$ bei der im folgenden geschilderten Wieder-Einführung des Konstantensymbols 0 und der darauffolgenden des Konstantensymbols 1 in $PreAN_0$ bzw. in der um 0 schon erweiterten Theorie jeweils beweisbar sind.

[19] Die Existenzbedingungen für diese aufeinanderfolgenden Einführungen der Konstantensymbole 0 und 1 bestehen gerade in $\exists\, y\mathbf{A}_z[y]$ bzw. in $\exists\, y\mathbf{B}_{z,w}[0, y]$ und folgen unmittelbar aus den Axiomen $\mathrm{PreAN}_0.2.$ und $\mathrm{PreAN}_0.8.$.

Ausgangspunkt für diesen Schritt ist eine Formel der Gestalt

$$\exists\, \mathbf{x}\, \big(\, \mathbf{x} \equiv^{\mathrm{N}}_{m} \underline{\underline{i}} \;\&\; \mathbf{a} < \underline{\alpha}\, \mathbf{x} + \mathbf{b} \;\&\; \underline{\alpha'} \mathbf{x} + \mathbf{b}' < \mathbf{a}' \,\big)\ ,$$

wobei $\mathbf{x}$ eine beliebige Variable ist und außerdem gilt: $m \in \mathbb{N}$, $m \geq 2$, $i \in \mathbb{N}$, $\alpha, \alpha' \in \mathbb{N}$, $\mathbf{a}, \mathbf{b}, \mathbf{a}', \mathbf{b}'$ Terme ohne $\mathbf{x}$. Eine erste äquivalente Umformung ergibt

$$\exists\, \mathbf{x}\, \big(\, \underline{\alpha\, \alpha'} \mathbf{x} \equiv^{\mathrm{N}}_{\alpha\, \alpha'\, m} \underline{\alpha\, \alpha'}\, \underline{\underline{i}} \;\&\; \underline{\alpha'}\, \mathbf{a} < \underline{\alpha\, \alpha'}\, \mathbf{x} + \underline{\alpha'} \mathbf{b} \;\&\; \underline{\alpha\, \alpha'}\, \mathbf{x} + \underline{\alpha}\, \mathbf{b}' < \underline{\alpha}\, \mathbf{a}' \,\big)\ .$$

Daraus ist äquivalent

$$\exists\, \mathbf{x}\, \big(\, \mathbf{x} \equiv^{\mathrm{N}}_{\alpha\, \alpha'\, m} \underline{\alpha\, \alpha'}\, \underline{\underline{i}} \;\;\&\;\; \underline{\alpha'}\, \mathbf{a} < \mathbf{x} + \underline{\alpha'}\, \mathbf{b} \;\;\&\;\; \mathbf{x} + \underline{\alpha}\, \mathbf{b}' < \underline{\alpha}\, \mathbf{a}' \,\big)$$

herleitbar; hieraus weiters

$$\begin{aligned} \exists\, \mathbf{x}\, \big(\, & \mathbf{x} \equiv^{\mathrm{N}}_{\alpha\, \alpha'\, m} \underline{\alpha\, \alpha'}\, \underline{\underline{i}} \\ & \;\&\;\; \underline{\alpha'}\, \mathbf{a} + \underline{\alpha}\, \mathbf{b}' < \mathbf{x} + \underline{\alpha'}\, \mathbf{b} + \underline{\alpha}\, \mathbf{b}' \;\;\&\;\; \mathbf{x} + \underline{\alpha}\, \mathbf{b}' + \underline{\alpha'}\, \mathbf{b} < \underline{\alpha}\, \mathbf{a}' + \underline{\alpha'}\, \mathbf{b} \,\big)\ . \end{aligned}$$

Diese Formel ist aber von der Gestalt

$$\exists\, \mathbf{x}\, \big(\, \mathbf{x} \equiv^{\mathrm{N}}_{\tilde{m}} \underline{\underline{j}} \;\;\&\;\; \mathbf{d} < \mathbf{x} + \mathbf{c} \;\;\&\;\; \mathbf{x} + \mathbf{c} < \mathbf{d}' \,\big)\ ,$$

mit $\tilde{m} \in \mathbb{N}$, $\tilde{m} \geq 2$, $j \in \mathbb{N}_0$ $j < \tilde{m}$, $\mathbf{c}, \mathbf{d}, \mathbf{d}'$ Terme ohne $\mathbf{x}$. Es folgt

$$\exists\, \mathbf{x}\, \big(\, \mathbf{x} \equiv^{\mathrm{N}}_{\tilde{m}} \underline{\underline{j}} + \mathbf{c} \;\;\&\;\; (\, \mathbf{c} = \mathbf{x} \;\vee\; \mathbf{c} < \mathbf{x}\,) \;\;\&\;\; \mathbf{d} < \mathbf{x} \;\;\&\;\; \mathbf{x} < \mathbf{d}' \,\big)\ .$$

Setzt man nun noch $\mathbf{e}$ gleich $\underline{\underline{j}} + \mathbf{c}$, so kann nun der Quantor eliminiert werden und es ergibt sich

$$\begin{aligned} & \mathbf{d} + 1 < \mathbf{c} \;\&\; \mathbf{e} < \mathbf{d}' \\ & \vee\; \mathbf{c} < \mathbf{d} + \underline{\underline{2}} \;\&\; \big(\, \mathbf{d} + 1 \equiv^{\mathrm{N}}_{\tilde{m}} \mathbf{e} \;\&\; \mathbf{d} + 1 < \mathbf{d}' \;\vee\; \mathbf{d} + \underline{\underline{2}} \equiv^{\mathrm{N}}_{\tilde{m}} \mathbf{e} \;\&\; \mathbf{d} + \underline{\underline{2}} < \mathbf{d}' \;\vee\; \ldots \\ & \qquad\qquad \ldots \;\vee\; \mathbf{d} + \underline{\underline{\tilde{m}}} \equiv^{\mathrm{N}}_{\tilde{m}} \mathbf{e} \;\&\; \mathbf{d} + \underline{\underline{\tilde{m}}} < \mathbf{d}' \,\big)\ . \end{aligned}$$

Diese Änderung im Verfahren (die für $\exists$-quantifizierte Formeln, die als Matrix nur eine Konjunktion von einer oder zwei der oben betrachteten Konjunktionsformeln besitzen, zu vergleichbaren, aber geringfügigeren Änderungen führt) wird wesentlich von der Beschränktheit der mittels $<$ bestimmten Ordnung $\leq$ nach unten durch 0 verursacht.

Weiters läßt sich ausführlich überprüfen, daß in dem der Sprache von $PreAN'$ angepaßten und wie beschrieben leicht abgeänderten QE-Verfahren in [BoJe74] für $PreAN'$ die einzelnen Umformungsschritte wirklich Ersetzungen von Formeln von $PreAN'$ sind,

d.h. daß diesen Schritten jeweils Theoreme von $PreAN'$ zugrundeliegen (und diese Umformungen nicht nur in $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ äquivalente Formelersetzungen sind, was zumeist augenscheinlich ist)[20].

Es sei hier noch ausdrücklich auf [HiBe68] hingewiesen, wo ein QE-Verfahren direkt für eine $PreAN'$ entsprechende Theorie (einer Erweiterung um die Kongruenzsymbole für $\mathbb{N}_0$ des dort mit (D) bezeichneten Systems der additiven Zahlentheorie AZ, die in Abschnitt 5 definiert wird) beschrieben wird. Das dort beschriebene Verfahren entspricht auch ziemlich gut einer Ausdehnung des ursprünglichen Presburgerschen Verfahrens für TAZ', die nötig ist, um davon ausgehend zu einem QE-Verfahren für $PreAZ'$ zu gelangen. Das für (die Entsprechung (D) für) $PreAN$ in [HiBe68] beschriebene Verfahren muß allerdings noch zusätzlich auf die Eigenschaft der Beschränktheit der durch $<$ bestimmten Ordnung $\leq$ nach unten in $PreAN$ Bedacht nehmen. $\diamondsuit$

Da $PreAN$ als Axiomatisierung von $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ aufgebaut wurde, erlaubt nun Satz 2.3.3 einzusehen, daß $PreAN$ auch eine vollständige Axiomatisierung von $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ ist. Daraus ergibt sich die Berechtigung der Namensgebung „Presburger Arithmetik natürlicher Zahlen“ für $PreAN$, (1) weil es sich bei $PreAN$ erneut um eine vollständige und entscheidbare Theorie der Additionsarithmetik (hier von natürlichen Zahlen) handelt und v.a. (2) weil die Entscheidung von Formeln von $PreAN$ relativ direkt durch Verwendung eines Entscheidungsverfahrens (eines QE-Verfahrens) für $PreAZ$ erfolgen kann, womit eine enge Beziehung zu $PreAZ$ entsteht.

Im Zusammenhang mit Satz 2.3.3 sei noch auf ein Ergebnis verwiesen, auf das [Ra77] hinweist: Und zwar gelang J.R. Büchi und C.C. Elgot die Zurückführung der Entscheidbarkeit von $PreAN$ (bzw. genau: von $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$) auf die Entscheidbarkeit einer logischen Theorie $WS1S := Th_w(\langle \mathbb{N}_0; S \rangle)$ von *„schwacher zweiter Ordnung“* (womit eine Theorie gemeint ist, in deren Formeln Variablen für endliche Mengen vorkommen können; S steht dabei in $WS1S$ für das Nachfolgerprädikat auf $\mathbb{N}_0$). Und zwar gaben sie eine Möglichkeit an, wie eine Interpretation (vgl. Definition 2.4.3) von $PreAN$ (bzw. von $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$) in der von ihnen als entscheidbar erkannten Theorie WS1S gefunden werden kann (vgl. [Ra77], p. 617).

In [Ra77] wird außerdem die Durchführbarkeit der Quantorenelimination nicht in $PreAN'$ betrachtet, sondern in einer (hier nun so bezeichneten) Theorie $PreAN''$, die der definitorischen Erweiterung von $PreAN$ um Symbole $<_n$ der Familie $\{<_n\}_{n \in \mathbb{N},\, n \geq 2}$ vermittels definierender Axiome $\left\{ x <_n y \leftrightarrow x < y \,\&\, \exists z \, (y = x + \underline{n} z) \right\}_{n \in \mathbb{N},\, n \geq 2}$ entspricht. Diese Theorie $PreAN''$ ist aber zu $PreAN'$ schwach äquivalent und das Ergebnis, daß

[20] Eine solche ausführliche Überprüfung mußte der Darstellung von $PreAN$ hier insofern zugrundeliegen, als nur dadurch Gewißheit erlangt werden konnte, daß $PreAN$ in der Tat eine vollständige Axiomatisierung von $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ ist. [„Nur dadurch“ ist jedoch insofern auch unrichtig, als ursprünglich noch ein anderer formal-logischer Weg gegangen wurde, um eine vollständige Axiomatisierung von $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ aus einer von $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ zu rechtfertigen, C.G.].

$PreAN''$ ebenfalls die QE zuläßt, läßt sich sofort aus Satz 2.3.3 (d.h. der Tatsache, daß $PreAN'$ die QE zuläßt) gewinnen, wenn man beachtet, daß in einer definitorischen Erweiterung $PreAN'''$ von $PreAN$ um die Einführung der Symbole der Familien $\{\equiv_n^{\mathbb{N}}\}_{n\in\mathbb{N},\, n\geq 2}$ und $\{<_n\}_{n\in\mathbb{N},\, n\geq 2}$ mittels der entsprechenden, zugehörigen Schemata dann die Aussagen $x \equiv_n^{\mathbb{N}} y \leftrightarrow x <_n y \vee x = y \vee y <_n x$ und $x <_n y \leftrightarrow x \equiv_n^{\mathbb{N}} y \,\&\, x < y$ (jeweils für alle $n \in \mathbb{N}$, $n \geq 2$) beweisbar sind.

2.4 Der Zusammenhang zwischen $PreAZ$ und $PreAN$

Wie in den letzten beiden Abschnitten dargestellt, handelt es sich bei $PreAZ$ und $PreAN$ um vollständige und entscheidbare logische Theorien 1. Ordnung mit den nichtlogischen Symbolen 0, 1, + und <, die Axiomatisierungen der Additionsarithmetik ganzer bzw. natürlicher Zahlen sind. (Wobei als Unterschied vielleicht schon hier festgehalten werden sollte, daß $<$ in $Th(\langle\mathbb{Z};0,1,+\rangle)$ nicht auf definitorische Weise (verbunden mit der gewöhnlichen Bedeutung dieses Symbols über $\mathbb{Z}$) eingeführt werden kann, das dagegen in $Th(\langle\mathbb{N}_0;0,1,+\rangle)$ schon möglich ist.)

Es ist weiters schon darauf hingewiesen worden, daß sich QE-Verfahren für eine dieser beiden Theorien (d.h. genauer: QE-Verfahren für definitorische Erweiterungen dieser Theorien um die Einführung von Kongruenzensymbolen) öfter auf einfache Weise zu QE-Verfahren für die jeweils andere Theorie (bzw. eine jeweils entsprechende definitorische Erweiterung davon) umbilden und verwenden lassen, sodaß sich darin schon eine sehr enge Verbindung von $PreAZ$ und $PreAN$ andeutet. Näheres Hinsehen kann außerdem auch zeigen, daß sich ein QE-Verfahren für $PreAN'$ wahrscheinlich viel leichter und direkter aus einem QE-Verfahren für $PreAZ'$ gewinnen läßt, als umgekehrt eines für $PreAZ'$ aus einem für $PreAN'$.

Obwohl $PreAZ$ eigentlich Axiomatisierung einer spezielleren algebraischen Struktur als $PreAN$ ist, nämlich die der Gruppe $\langle\mathbb{Z};+\rangle$ (unter Beachtung zusätzlicher Eigenschaften dieser Gruppe bezüglich der gewöhnlichen Ordnung auf $\mathbb{Z}$), gegenüber $PreAN$, das wesentlich eine Axiomatisierung des Monoids $\langle\mathbb{N}_0;+\rangle$ ist, und obwohl in einer Gruppe Umformungen von Aussagen gewöhnlich viel einfacher und eleganter erfolgen können (wegen der möglichen Bildung von inversen Elementen) als in einem Monoid, scheint es im vorliegenden Fall so zu sein, daß die Entscheidung von Formeln von $PreAN$ keineswegs *erheblich* mehr Aufwand erfordert als die Entscheidung von Formeln von $PreAZ$. Sowie weiters, daß die Existenz des (mit einer Ordnungsrelation in einfacher Verbindung stehenden) Symbols $<$ in $PreAZ$ es erlaubt, das Problem der Entscheidung von Formeln von $PreAN$ auch in einem praktischen Sinn in das Problem der Entscheidung von Formeln von $PreAZ$ „einzubetten“ (d.h. im „praktischen“ oder „praktisch-beobachtbaren“ Sinn der Konstruktion bzw. bei der Konstruktion eines QE-Verfahrens für $PreAN'$ aus einem gegebenen QE-Verfahren für $PreAZ'$).

Es läßt sich nun aber auch ein formal-logischer Grund dafür angeben, warum sich mit einigem Recht sagen läßt, daß die Entscheidung von $PreAZ$ grundlegender und die Entscheidung von $PreAN$ im wesentlichen ein Spezialfall davon ist: Denn die Mittel von $PreAZ$ zur Formulierung von Aussagen über ganze Zahlen reichen auch aus, um alle jene Aussagen über natürliche Zahlen, die in $PreAN$ ausgedrückt werden können, auch als Aussagen in $PreAZ$ mit derselben inhaltlichen Bedeutung zu formulieren. Genau ist das so zu verstehen: Eine geschlossene Formel $\mathbf{A}$ von $PreAN$ kann zu einer in $PreAZ$ (der Bedeutung nach:) äquivalenten Formel $\mathbf{A}^{QR}$ so umgeformt werden, daß in $\mathbf{A}$ alle

Quantifikationen $\exists\,\mathbf{x}\,(\,\ldots\,)$ durch die Formel $0 = \mathbf{x} \vee 0 < \mathbf{x}$ *„relativiert“* werden, d.h. durch Quantifikationen $\exists\,\mathbf{x}\,\big(\,(\,0 = \mathbf{x} \vee 0 < \mathbf{x}\,)\;\&\;\ldots\big)$ ersetzt werden. Für eine nicht geschlossene Formel $\mathbf{A}$ von $PreAN$ ist eine über $\langle\mathbb{Z};0,1,+,<\rangle$ dazu inhaltlich äquivalente Formel $\mathbf{A}^R$ weiters in

$$0 = \mathbf{x}_1 \;\vee\; 0 < \mathbf{x}_1 \;\rightarrow\; 0 = \mathbf{x}_2 \;\vee\; 0 < \mathbf{x}_2 \;\rightarrow\; \ldots \;\rightarrow\; 0 = \mathbf{x}_n \;\vee\; 0 < \mathbf{x}_n \;\rightarrow\; \mathbf{A}^{QR}$$

(wobei $\mathbf{x}_1,\ldots,\mathbf{x}_n$ die in $\mathbf{A}$ frei vorkommenden Variablen sind) zu finden, also durch *Relativierung*[21] des Geltungsbereiches der freien und gebundenen Variablen von $\mathbf{A}$. (Dieses Vorgehen wird in Definition 2.4.1 präzisiert.)

Ein solches inhaltlich motivierte Vorgehen führt unmittelbar auf die Reduktion des Entscheidungsproblems für $PreAN$ auf das für $PreAZ$. Wegen $\vdash_{PreAN} \mathbf{A} \Leftrightarrow$ $\Leftrightarrow \vdash_{PreAZ} \mathbf{A}^R$ (was unter Zuhilfenahme der Standardmodelle für $PreAN$ und $PreAZ$ und der Vollständigkeit dieser Theorien unmittelbar einzusehen ist) kann eine Formel $\mathbf{A}$ von $PreAN$ in $PreAZ$ dadurch entschieden werden, indem aus $\mathbf{A}$ zuerst die Formel $\mathbf{A}^R$ konstruiert und dann $\mathbf{A}^R$ in $PreAZ$ entschieden wird.

In formal-logischen Begriffen ausgedrückt, liegt einem solchen Vorgehen zugrunde, daß $PreAN$ in $PreAZ$ „interpretiert“ werden kann, oder auch, daß das Modell $\langle\mathbb{N}_0;0,1,+,<\rangle$ im Modell $\langle\mathbb{Z};0,1,+,<\rangle$ definiert werden kann. Das soll unter Verwendung der exakten Definitionen in [Shoe67] dafür im weiteren präzis gemacht werden.

Es wird sich nun aber auch zeigen lassen, daß umgekehrt $PreAZ$ ebenfalls in $PreAN$ interpretiert werden kann, wenngleich keineswegs auf eine ähnlich natürliche Weise. Insgesamt ist die Tatsache, daß sich $PreAN$ auf offensichtliche Weise in $PreAZ$ interpretieren läßt, das aber umgekehrt für $PreAZ$ bezüglich $PreAN$ nicht im selben Maß gilt, ein starker Hinweis darauf, daß das Entscheidungsproblem für $PreAZ$ das grundlegendere ist.

Trotzdem läßt sich aber mit Hilfe der erwähnten Interpretation von $PreAZ$ in $PreAN$ die Entscheidbarkeit von $PreAZ$ auch auf die von $PreAN$ zurückführen, zwar mit etwas größerem Aufwand als in umgekehrter Richtung, dennoch aber einfach genug (vgl. Abschnitt 6, Lemma 2.6.3), sodaß eingesehen werden kann, daß die Entscheidungskomplexität von $PreAN$ und die von $PreAZ$ von der selben (zwischen 2-fach- und 3-fach-exponentiell-linearen) Größenordung (bezüglich der *Rechenzeit* deterministischer oder nichtdeterministischer Turingmaschinen) sind.

Alle erwähnten Gemeinsamkeiten und Beziehungen zwischen $PreAZ$ und $PreAN$ (oder den ihnen entsprechenden, d.h. zu diesen äquivalenten Theorien $Th(\langle\mathbb{Z};0,1,+,<\rangle)$ bzw. $Th(\langle\mathbb{N}_0;0,1,+,<\rangle)$) rechtfertigen die Bezeichnung von $PreAN$ als „Presburger Arithmetik natürlicher Zahlen“ wie weiters auch den verbreiteten unscharfen Sprachgebrauch in der Bezeichnung „Presburger Arithmetik“ sowohl für Theorien der Additionsarithmetik ganzer wie natürlicher Zahlen in bestimmtem Ausmaß. Trotzdem ist das Festhalten der

[21] (dieser Ausdruck stammt aus [BoJe74])

Unterschiede zwischen $PreAN$ und $PreAZ$ z.B. auch für Komplexitätsuntersuchungen vorerst wesentlich.

Definition 2.4.1. Bezüglich $0 = \mathbf{x} \vee 0 < \mathbf{x}$ relativierte Formeln $\mathbf{A}^R$ in $PreAZ$.

(i) Für eine Formel $\mathbf{A}$ über der Sprache L_{PreAN} (bzw. L_{PreAZ}) sei zunächst eine Formel A^{QR} definiert: Ist $\mathbf{A}$ atomare Formel, so ist $\mathbf{A}^{QR}$ gleich $\mathbf{A}$, ist $\mathbf{A}$ gleich $\neg\mathbf{B}$, so ist $\mathbf{A}^{QR}$ gleich $\neg\mathbf{B}^{QR}$; ist $\mathbf{A}$ gleich $\mathbf{B} \vee \mathbf{C}$, so ist $\mathbf{A}^{QR}$ gleich $\mathbf{B}^{QR} \vee \mathbf{C}^{QR}$, und ist $\mathbf{A}$ gleich $\exists\,\mathbf{x}\,\mathbf{B}$, so ist $\mathbf{A}^{QR}$ gleich $\exists\,\mathbf{x}\,\big(\,(\,0 = \mathbf{x} \vee 0 < \mathbf{x}\,)\,\&\,\mathbf{B}^{QR}\,\big)$.

(ii) Kommen in einer Formel $\mathbf{A}$ über der Sprache L_{PreAZ} genau die verschiedenen Variablen $\mathbf{x}_1, \ldots, \mathbf{x}_n$ frei vor und entspricht diese Reihenfolge der Variablen genau der lexikographischen Reihenfolge der Zeichenketten, die sie darstellen, dann ist $\mathbf{A}^R$ die Formel $0 = \mathbf{x}_1 \vee 0 < \mathbf{x}_1 \to \ldots \to 0 = \mathbf{x}_n \vee 0 < \mathbf{x}_n \to \mathbf{A}^{QR}$.

Lemma 2.4.2. *Für jede Formel $\mathbf{A}$ über L_{PreAN} gilt:*

$$\vdash_{PreAN} \mathbf{A} \quad \Rightarrow \quad \vdash_{PreAZ} \mathbf{A}^R\,.$$

Beweisskizze. Der Beweis kann dadurch geschehen, daß die Aussage durch Induktion über die Theoreme von $PreAN$ gezeigt wird; unter Verwendung des "Interpretation Theorems" in [Shoe67] reicht es allerdings, die Aussage nur für alle nichtlogischen Axiome von $PreAN$ zu zeigen. $\diamondsuit$

Da es sich bei $PreAN$ und bei $PreAZ$ um vollständige Theorien handelt, ist auch die Umkehrung in Lemma 2.4.2 richtig, wie sofort wieder unter Verwendung der Vertauschbarkeit der Begriffe „Beweisbarkeit" und „Gültigkeit in einem Modell" in einer vollständigen Theorie eingesehen werden kann, bzw. mit Hilfe der Tatsache, daß vollständige Theorien für geschlossene Formeln $\mathbf{A}$ das *tertium non datur* bezüglich Beweisbarkeit von $\mathbf{A}$ und Beweisbarkeit von $\neg\,\mathbf{A}$ erfüllen[22].

[22] Die Umkehrung von Lemma 2.4.2 wäre verletzt, wenn es eine Formel $\mathbf{A}'$ über L_{PreAN} gäbe, für die $\vdash_{PreAZ} (\,\mathbf{A}'\,)^R$, jedoch gleichzeitig $\nvdash_{PreAN} \mathbf{A}'$ gelten würde. – Die Existenz einer solchen Formel $\mathbf{A}'$ steht nun aber im Widerspruch zur Gültigkeit der Kontraposition $\nvdash_{PreAN} \mathbf{A} \Rightarrow \nvdash_{PreAZ} \mathbf{A}^R$ zur Umkehrung von Lemma 2.4.2, welche man (: die Gültigkeit dieser Kontraposition zu ...) wie folgt einsehen kann (unter dabei wesentlichem Rückgriff auf das Wissen um die Vollständigkeit dieser beiden Theorien):

Angenommen, es gilt $\nvdash_{PreAN} \mathbf{A}$. Dann gilt $\nvdash_{PreAN} \mathbf{A}^c$, wobei $\mathbf{A}^c$ der Abschluß von $\mathbf{A}$ ist ("Closure Theorem"). Wegen der (hier vorausgesetzten, in Abschnitt 3 (in einem wesentlichen Schritt) gezeigten) Vollständigkeit von $PreAN$ folgt dann $\vdash_{PreAN} \neg\,\mathbf{A}^c$. Daraus folgt mit Lemma 2.4.2 $\vdash_{PreAZ} (\,\neg\,\mathbf{A}^c\,)^R$, also auch $\vdash_{PreAZ} \neg\,(\,\mathbf{A}^c\,)^R$ (dies wegen: $(\,\neg\,\mathbf{A}^c\,)^R$ ist gleich $(\,\neg\,\mathbf{A}^c\,)^{QR}$, dies ist gleich $\neg\,(\,\mathbf{A}^c\,)^{QR}$ und weiter gleich $\neg\,(\,\mathbf{A}^c\,)^R$; vgl. hierbei Definition 2.4.1). Wegen der Konsistenz von $PreAZ$ folgt daraus $\nvdash_{PreAZ} (\,\mathbf{A}^c\,)^R$. Daraus folgt wegen $\vdash_{PreAZ} (\,\mathbf{A}^c\,)^R \leftrightarrow (\,\mathbf{A}^R\,)^c$ {dies gilt nämlich wegen: falls in $\mathbf{A}$ genau $\mathbf{x}_1, \ldots, \mathbf{x}_n$ frei vorkommen und dies die lexikographische Ordnung dieser Variablen ist, so ist $(\,\mathbf{A}^c\,)^R$ von der Gestalt

$$\forall\,\mathbf{x}_1\,\big(\,(\,0 = \mathbf{x}_1 \vee 0 < \mathbf{x}_1\,)\,\&\,\forall\,\mathbf{x}_2\,\big(\ldots\,\&\,\forall\,\mathbf{x}_n\,\big(\,(\,0 = \mathbf{x}_n \vee 0 < \mathbf{x}_n\,) \to \mathbf{A}^{QR}\,\big)\ldots\big)\big)\,,$$

Auf einem konstruktiven, Beweise erhaltenden (=findenden) Weg ist diese Umkehrung hier nicht direkt zu gewinnen.

Die Konstruktion von $\mathbf{A}^R$ gibt einen Weg an, wie eine Formel $\mathbf{A}$, die als Aussage über natürliche Zahlen verstanden wird, über den ganzen Zahlen so „interpretiert“ werden kann, daß die Aussage $\mathbf{A}$ und ihre Entsprechung $\mathbf{A}^R$ in den dann unterschiedlichen Modellen natürlicher bzw. ganzer Zahlen inhaltlich dasselbe ausdrücken.

Die Interpretation I einer Theorie T in einer Theorie T' nach [Shoe67] besteht nun aus einer Möglichkeit, die Formeln $\mathbf{A}$ von $L(T)$ (der Sprache von T) u.a. durch Ersetzung von nichtlogischen Symbolen von $L(T)$ durch Symbole von $L(T')$ (der Sprache von T') als Formeln $\mathbf{A}^{(I)}$ von T' so audrücken zu können, daß immer aus $\vdash_T \mathbf{A}$ folgt: $\vdash_{T'} \mathbf{A}^{(I)}$. Eine Interpretation I von T in T' bietet also eine Möglichkeit, die in T formulierbaren Formeln $\mathbf{A}$ als Formeln $\mathbf{A}^{(I)}$ von T' zu betrachten, wobei eine Formel $\mathbf{A}^{(I)}$ in T' jedenfalls immer dann beweisbar sein soll, wenn $\mathbf{A}$ in T beweisbar ist. (Eine Interpretation I von T in T', für die immer $\vdash_T \mathbf{A} \Leftrightarrow \vdash_{T'} \mathbf{A}^{(I)}$ gilt, wird von [Shoe67] *faithful*[23] genannt.)

Definition 2.4.3. Interpretationen.
Seien L und L' Sprachen von Theorien 1. Ordnung. Seien T und T' Theorien 1. Ordnung mit $L = L(T)$ und $L' = L(T')$.

(i) Eine **Interpretation I der Sprache L in der Sprache L'** *besteht aus*

- *(a) einem 1-stelligen Prädikatssymbol U_I von L', dem* **Universum** *von I;*
- *(b) einem n-stelligen Funktionssymbol $\mathbf{f}_I$ von L' für jedes n-stellige Funktionssymbol $\mathbf{f}$ von L;*
- *(c) einem n-stelligen Prädikatssymbol $\mathbf{p}_I$ von L' für jedes n-stellige Prädikatssymbol $\mathbf{p}$ von T, das von $=$ verschieden ist.*

(ii) Eine **Interpretation I der Sprache L in der Theorie T'** *ist eine Interpretation von L in L', für die noch zusätzlich*

$$\vdash_{T'} \exists \mathbf{x} U_I \mathbf{x}$$

und

$$\vdash_{T'} U_I \mathbf{x}_1 \to \ldots \to U_I \mathbf{x}_n \to U_I \mathbf{f}_I \mathbf{x}_1 \ldots \mathbf{x}_n$$

(für jedes n-stellige Funktionssymbol $\mathbf{f}$ von L) gelten.

---

und das ist äquivalent (vermittels Pränexoperationen einzusehen) zu

$$\forall \mathbf{x}_1 \ldots \forall \mathbf{x}_n \left(0 = \mathbf{x}_1 \vee 0 < \mathbf{x}_1 \to \ldots \to 0 = \mathbf{x}_n \vee 0 < \mathbf{x}_n \to \mathbf{A}^{QR} \right)$$

mithin zu $(\mathbf{A}^R)^c$ } ... weiters $\nvdash_{PreAZ} (\mathbf{A}^R)^c$ und (wegen dem “Closure Theorem”) $\nvdash_{PreAZ} \mathbf{A}^R$.

[23] [Ich schaudere davor zurück, diesen Begriff mit einem Wort wie „glaubwürdig“ oder „treu“ zu übersetzen, C.G.]

(iii) *Ist I eine Interpretation von L in L', dann sei zu einer Formel $\mathbf{A}$ von L die Formel $\mathbf{A}^{(I)}$ wie folgt definiert:*

Zuerst entstehe aus $\mathbf{A}$ eine Formel $\mathbf{A}_I$ so: (a) Durch Ersetzung aller nichtlogischen Symbole $\mathbf{u}$ in $\mathbf{A}$ durch Symbole $\mathbf{u}_I$ (entsprechend der Interpretation von L in L'), und (b) durch schrittweise 1-malige Ersetzung jeder Teilformel $\exists\,\mathbf{x}\,\mathbf{B}$ in $\mathbf{A}$ durch $\exists\,\mathbf{x}\,(\,U_I\mathbf{x}\,\&\,\mathbf{B}\,)$.

Danach sei $\mathbf{A}^{(I)}$ durch

$$U_I\mathbf{x}_1 \to \ldots \to U_I\mathbf{x}_n \to \mathbf{A}_I$$

festgesetzt, wobei $\mathbf{x}_1, \ldots, \mathbf{x}_n$ die in $\mathbf{A}$ (sowie in $\mathbf{A}_I$) freien Variablen sind, von denen außerdem angenommen sei, daß sie in der angeschriebenen Reihenfolge lexikographisch geordnet sind.

(iv) *Eine* **Interpretation I einer Theorie T in einer Theorie T'** *besteht aus einer Interpretation I von L in T', für die $\vdash_{T'} \mathbf{A}^{(I)}$ für jedes nichtlogische Axiom $\mathbf{A}$ von T gilt.*

(v) *T heißt* **in T' interpretierbar**, *falls es eine definitorische Erweiterung T'' von T' und eine Interpretation I von T in T'' gibt.*

Die Aussage des "Interpretation Theorems" in [Shoe67] ist nun, daß, wenn I eine Interpretation von T in T' ist, $\vdash_{T'} \mathbf{A}^{(I)}$ für alle Theoreme $\mathbf{A}$ von T gilt (und nicht nur für alle nichtlogischen Axiome $\mathbf{A}$ von T, wie nach Definition 2.4.3, (iv), guarantiert ist). Daraus folgt in diesem Fall unmittelbar weiters, daß sich die Konsistenz von T auf jene von T' zurückführen läßt.

Falls I Interpretation von T in T' ist, so läßt sich die Entscheidbarkeit von T auf jene von T' allerdings nur in dem Fall unmittelbar zurückführen, wenn die Interpretation *faithful* ist, d.h. wenn $\vdash_T \mathbf{A} \Leftrightarrow \vdash_{T'} \mathbf{A}^{(I)}$ für alle Formeln $\mathbf{A}$ von T gilt; denn in diesem Fall genügt es, um $\mathbf{A}$ in T zu entscheiden, $\mathbf{A}^{(I)}$ effektiv zu konstruieren (was entlang Definition 2.4.3, (iii), auf algorithmischem Weg erfolgen kann) und dann in T' zu entscheiden.

Satz 2.4.4. *$PreAN$ ist in $PreAZ$ interpretierbar.*

Beweis. Sei $PreAZ^{(INZ)}$ definitorische Erweiterung von $PreAZ$ um das 1-stellige Prädikatssymbol U_{INZ} vermittels $U_{INZ}\,x \leftrightarrow 0 = x \vee 0 < x$.

Nun sei INZ jene Interpretation von L_{PreAN} in $L(PreAZ^{(INZ)})$, die als Universumssymbol das Symbol U_{INZ} besitzt, für die 0_{INZ} gleich 0, 1_{INZ} gleich 1, $+_{INZ}$ gleich + und $<_{INZ}$ gleich < ist.

Dann gilt $\vdash_{PreAN} \mathbf{A} \Rightarrow \vdash_{PreAZ} \mathbf{A}^{(INZ)}$ für jedes nichtlogische Axiom von $PreAN$ (das folgt sofort aus Lemma 2.4.2 und dem definierenden Axiom von U_{INZ}) und damit ist INZ eine Interpretation von $PreAN$ in $PreAZ^{(INZ)}$. □

Daß es sich bei INZ um eine Interpretation handelt, die *faithful* ist, folgt unter Zuhilfenahme der Vollständigkeit von $PreAN$ wie die Umkehrung von Lemma 2.4.2. Da aber die Vollständigkeit von $PreAN$ erst durch die Konstruktion eines QE-Verfahrens für $PreAN$ und also im weiteren erst durch die Entscheidbarkeit von $PreAN$ eingesehen werden konnte, bietet so ein Argument nicht die Möglichkeit, die Entscheidbarkeit von $PreAN$ mittels Satz 2.4.4 auf die Entscheidbarkeit von $PreAZ$ zu stützen.

Das wäre aber für $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ im Bezug zu $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ schon möglich, wenn (was inhaltlich sofort evident ist) eingesehen wird, daß $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ in der Theorie $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ interpretierbar ist, vermittels der auch als Interpretation von $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ in $Th(\langle \mathbb{Z}; 0, 1, +, <, U_{INZ} \rangle)$ auffaßbaren Interpretation INZ; denn $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ ist per def. vollständig.

Es sei hier darauf hingewiesen, daß eine Formel $\mathbf{A}^{(INZ)}$, die die Interpretation einer Formel $\mathbf{A}$ von $PreAN$ in $PreAZ^{(INZ)}$ ist (bezüglich der Interpretation INZ im Beweis von Satz 2.4.4), unmittelbar auch als $\mathbf{A}^R$ entsprechend angesehen werden kann, in dem Sinn, daß $\mathbf{A}^R$ die Translation von $\mathbf{A}^{(INZ)}$ von $PreAZ^{(INZ)}$ nach $PreAZ$ ist.

Für die Untersuchung des Zusammenhangs der Entscheidungskomplexität von $PreAZ$ und der von $PreAN$ ist weiters noch die Tatsache von bestimmter Bedeutung, daß auch $PreAZ$ in $PreAN$ interpretiert werden kann. Denn dadurch kann man auch eine Möglichkeit gewinnen, aus einem Entscheidungsverfahren für $PreAN$ eines für $PreAZ$ zu konstruieren.

Satz 2.4.5. *$PreAZ$ ist in $PreAN$ interpretierbar.*

Beweis. Der Beweis beruht darauf, daß es möglich ist, mit den Mitteln von $PreAN$ eine Verknüpfung $\oplus$ so zu definieren, daß $\oplus$ die Addition von in die natürlichen Zahlen $\mathbb{N}_0$ kodierten ganzen Zahlen formalisiert. Die dabei benutzte Kodierung von $\mathbb{Z}$ in $\mathbb{N}_0$ weist den positiven ganzen Zahlen $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$ die geraden natürlichen Zahlen $\mathbb{N}_g = \{2, 4, 6, \dots\}$, den negativen ganzen Zahlen $\mathbb{Z}^- = \{-1, -2, -3, \dots\}$ die ungeraden natürlichen Zahlen $\mathbb{N}_u = \{1, 3, 5, \dots\}$ und der ganzen Zahl 0 wiederum die Zahl 0 in $\mathbb{N}_0$ zu.

Sei nun $PreAN^{(IZN)}$ die definitorische Erweiterung von $PreAN'$ um die Einführung des 1-stelligen Symbols U_{IZN}, des Konstantensymbols ① und des 2-stelligen Prädikatssymbols $\lessgtr$ vermittels

$$
\begin{aligned}
U_{IZN}\, x &\leftrightarrow 0 = 0\,; \\
y = ① &\leftrightarrow y = 1 + 1\,; \\
y = x_1 \oplus x_2 &\leftrightarrow \dots \qquad \text{(Vgl. Formel 2.4.1)}\,; \\
x_1 \lessgtr x_2 &\leftrightarrow x_1 \equiv_2^{\mathrm{N}} 0 \;\&\; x_2 \equiv_2^{\mathrm{N}} 0 \;\&\; x_1 < x_2 \\
&\qquad \vee\; x_1 \equiv_2^{\mathrm{N}} 1 \;\&\; x_2 \equiv_2^{\mathrm{N}} 1 \;\&\; x_2 < x_1 \\
&\qquad \vee\; x_1 \equiv_2^{\mathrm{N}} 1 \;\&\; x_2 \equiv_2^{\mathrm{N}} 0\,.
\end{aligned}
$$

Formel 2.4.1 Definierendes Axiom für $\oplus$ in $PreAN^{(IZN)}$:

$$
\begin{aligned}
y = x_1 \oplus x_2 \quad \leftrightarrow \quad & x_1 \equiv_2^{\mathrm{N}} 0 \;\&\; x_2 \equiv_2^{\mathrm{N}} 0 \;\&\; y = x_1 + x_2 \\
& \vee\; x_1 \equiv_2^{\mathrm{N}} 1 \;\&\; x_2 \equiv_2^{\mathrm{N}} 1 \;\&\; y = x_1 + x_2 + 1 \\
& \vee\; \exists\, x_{10}\, \exists\, x_{20}\, \exists\, w \\
& \qquad \{\, [\, x_1 = x_{10} + x_{10} \;\&\; x_2 + 1 = x_{20} + x_{20} \\
& \qquad\quad \&\; (\, x_{10} = x_{20} + w \;\&\; y = w + w \\
& \qquad\qquad \vee\; x_{20} = x_{10} + w \;\&\; \neg\, w = 0 \;\&\; y + 1 = w + w \,)\,] \\
& \qquad \vee\; [\, x_1 + 1 = x_{10} + x_{10} \;\&\; x_2 = x_{20} + x_{20} \\
& \qquad\quad \&\; (\, x_{10} = x_{20} + w \;\&\; \neg\, w = 0 \;\&\; y + 1 = w + w \\
& \qquad\qquad \vee\; x_{20} = x_{10} + w \;\&\; y = w + w \,)\,] \,\}\,.
\end{aligned}
$$

Sei nun IZN jene Interpretation von L_{PreAZ} in $PreAZ^{(IZN)}$, die als Universumsymbol U_{IZN} besitzt, für die 0_{IZN} gleich 0, 1_{IZN} gleich ①, $+_{IZN}$ gleich $\oplus$ und $<_{IZN}$ gleich $\circledless$ ist.

Dann gilt $\vdash_{PreAZ} \mathbf{A} \quad \Rightarrow \quad \vdash_{PreAN^{(IZN)}} \mathbf{A}^{(IZN)}$ für jedes nichtlogische Axiom $\mathbf{A}$ von $PreAZ$ (das kann *theoretisch* auch ausführlich gezeigt werden; wegen der Vollständigkeit von $PreAN$ und der anschaulich einsehbaren Tatsache, daß $\oplus$ und $\circledless$ in $PreAN$ wirklich die Symbole + und < von $PreAZ$ bezüglich—wie beschrieben—kodierten ganzen Zahlen „interpretieren“ (: hier als inhaltliche Entsprechung zu verstehen) ist diese Folgerung aber ausreichend begründet).

Damit ist IZN eine Interpretation von $PreAZ$ in $PreAN^{(IZN)}$ [24]. □

Erneut sei hier darauf hingewiesen, daß die Tatsache, daß IZN eine Interpretation ist, die *faithful* ist, nur unter Zuhilfenahme der Vollständigkeit von $PreAZ$ und der Konsistenz von $PreAN$ unmittelbar einzusehen ist, daß also eine *direkte* (gemeint ist: eine unmittelbar einzusehende) theoretische Zurückführung der Entscheidbarkeit von $PreAZ$ auf die von $PreAN$ mit den Mitteln von IZN (ohne das erwähnte zusätzliche Wissen) nicht gelingt. Wiederum wäre jedoch eine Stützung der Entscheidbarkeit der per definitionem vollständigen Theorie $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ auf die Entscheidbarkeit von $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ durch die Interpretation IZN, die auch als Interpretation von $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ in $Th(\langle \mathbb{N}_0; 0, 1, +, <, U_{IZN}, ①, \oplus, \circledless \rangle)$ aufgefaßt werden kann, unmit-

[24] Die hier betrachtete Interpretation von $PreAN$ in $PreAZ^{(IZN)}$ beruht nicht auf einer Eigenart additiver Theorien: IZN könnte z.B. durch die zusätzliche (ebenfalls leicht und analog konstruierbare) definitorische Einführung von $\odot$ zu einer Interpretation der (unentscheidbaren) Theorie $Th(\langle \mathbb{Z}; 0, 1, +, ., < \rangle)$ in der Theorie $Th(\langle \mathbb{N}_0; 0, 1, +, ., <, U_{IZN}, ①, \oplus, \odot \rangle)$ erweitert werden.

telbar möglich. (Hierbei geht ein, daß die Entscheidbarkeit der definitorischen Erweiterung $Th(\langle \mathbb{N}_0; 0, 1, +, <, U_{IZN}, \textcircled{1}, \oplus, \textcircled{\leq} \rangle)$ von $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ aus der Entscheidbarkeit von $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ folgt.)

Die Zurückführung der Entscheidbarkeit der Theorie $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ auf die von $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$ mit Hilfe der Interpretation INZ, und insbesondere, daß es sich bei INZ um eine Interpretation, die *faithful* ist, handelt, könnte auch besonders einfach mit Hilfe eines Begriffs aus [Shoe67], sect. 6.9, behandelt und ausführlich begründet werden, nämlich damit, daß die Struktur $\langle \mathbb{N}_0; 0, 1, +, < \rangle$ in der Struktur $\langle \mathbb{Z}; 0, 1, +, < \rangle$ *definierbar*[25] ist.

[25] Dabei nennt [Shoe67] eine Struktur $\mathfrak{A}$ in einer Struktur $\mathfrak{B}$ *definierbar*, wenn $|\mathfrak{A}|$ Teilmenge von $|\mathfrak{B}|$ ist und wenn es eine Struktur $\mathfrak{C}$ gibt, die Modell einer definitorischen Erweiterung (: im eingeschränkteren, in [Shoe67] festgesetzten und gebrauchten Sinn dieses Begriffs) $Th(\mathfrak{C})$ von $Th(\mathfrak{B})$ ist, die einerseits das der Teilmenge $|\mathfrak{A}|$ von $|\mathfrak{B}|$ (gleich $|\mathfrak{C}|$) entsprechende Prädikat enthält und für die weiters jede Funktion $\mathbf{f}_{\mathfrak{A}}$ und jedes Prädikat $\mathbf{p}_{\mathfrak{A}}$ von $\mathfrak{A}$ Einschränkung einer Funktion $\mathbf{f}'_{\mathfrak{C}}$ bzw. eines Prädikats $\mathbf{p}'_{\mathfrak{C}}$ von $\mathfrak{C}$ auf $|\mathfrak{A}|$ ist. – Unter diesen Bedingungen gibt es immer eine (offensichtliche) Interpretation von $Th(\mathfrak{A})$ in $Th(\mathfrak{C})$, die *faithful* ist (das ist im Rahmen des von [Shoe67] auf p. 132 dargestellten sofort ausführlich zu beweisen). Ist nun $Th(\mathfrak{B})$ entscheidbar, so trifft das auch auf die definitorische Erweiterung $Th(\mathfrak{C})$ davon zu (: statt $\mathbf{A}$ in $Th(\mathfrak{C})$ entscheide man die Translation $\mathbf{A}^*$ von $Th(\mathfrak{C})$ nach $Th(\mathfrak{B})$) und weiters auch auf $Th(\mathfrak{A})$ (denn: statt $\mathbf{A}$ in $Th(\mathfrak{A})$ entscheide man nun $\left(\mathbf{A}^{(I)}\right)^*$ in $Th(\mathfrak{B})$).

2.5 Die Presburger Arithmetik natürlicher Zahlen im Kontext der Peano-Arithmetik und anderer zahlentheoretischer Theorien 1. Ordnung

Wie in Abschnitt 3 behandelt, sind die dort beschriebenen Theorien $PreAN$, $PreAN_1$ sowie $PreAN_0$ vollständig und als Theorien der Additionsarithmetik natürlicher Zahlen daher auch vollständige Axiomatisierungen der semantisch definierten Theorien $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ bzw. $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ bzw. $Th(\langle \mathbb{N}_0; + \rangle)$. Es ist nun klar, daß es sich bei der „vollständigen Zahlentheorie“ $VZ = Th(\langle \mathbb{N}_0; 0, S, +, . \rangle)$ (wobei S die 1-stellige Nachfolgerfunktion bezüglich Zahlen in $\mathbb{N}_0$ bezeichnet) jedenfalls eine Erweiterung von $PreAN_0$ handelt (und eigentlich—würde man VZ definitorisch um 1 und $<$ bzw. um 1 erweitern—auch um eine Erweiterung von $PreAN$ und $PreAN_1$).

Eine zugängliche[26] Axiomatisierung von VZ ist die *Peano-Arithmetik* PeA, die aber, wie K. Gödel 1931 bewiesen hat, unvollständig ist und keine konsistente, axiomatisierbare[27] Erweiterung besitzt, die vollständig ist. PeA ist, wie A. Church 1936 nach einer genauen Präzisierung des Begriffs der Entscheidbarkeit bewiesen hat, auch unentscheidbar.

VZ ist also eine echte Erweiterung der unvollständigen Theorie PeA. Dennoch läßt sich ein enger Zusammenhang zwischen PeA und den vollständigen Theorien der Presburger Arithmetik natürlicher Zahlen herstellen. PeA enthält (wie gezeigt werden kann) nämlich jedenfalls alle in $\langle \mathbb{N}_0; 0, S, +, . \rangle$ gültigen Formeln, in denen das Multiplikationssymbol . nicht vorkommt; PeA umfaßt (d.h. erweitert) also sicher $PreAN_0$ und kann leicht zu definitorischen Erweiterungen ausgebaut werden, die $PreAN$ und $PreAN_0$ enthalten (d.h. Erweiterungen dieser Theorien darstellen).

[26] Hiermit ist gemeint, daß jedenfalls die semantische Definition von VZ als $VZ = Th(\langle \mathbb{N}_0; 0, S, +, . \rangle)$ keine Möglichkeit bietet, die „Axiome“ dieser Theorie (formal sind es im Sinne von [Shoe67] tatsächlich Axiome) einzeln und erschöpfend in einer verfahrensmäßigen Weise anzugeben oder aufzuführen (das ist im Lichte der Sätze von Gödel und Church über PeA auch gar nicht möglich).

[27] „Axiomatisierbar“ heißt präzisiert etwa: Die Gödelzahlen der Axiome sind eine rekursive Menge.

Definition 2.5.1. Die Theorien PeA, VZ, AZ, Q, NA, SkA.

(a) L_{PeA} *sei eine Sprache einer Theorie 1. Ordnung, die genau das Konstantensymbol* 0, *das 1-stellige Prädikatssymbol* S *und die 2-stelligen Funktionssymbole* $+$ *und* $.$ *enthält. Die* **Peano-Arithmetik**[28] PeA *ist jene Theorie mit Sprache* L_{PeA}, *die als nichtlogische Axiome genau die im folgenden mit PeA.1., ... , PeA.6. bezeichneten und weiters noch alle aus dem Axiomenschema PeA.S. (dem Schema der „Induktionsaxiome" in* PeA*) stammenden Formeln besitzt:*

PeA.1.	$\neg\, Sx = 0$
PeA.2.	$Sx = Sy \to x = y$
PeA.3.	$x + 0 = x$
PeA.4.	$x + Sy = S(x + y)$
PeA.5.	$x \,.\, 0 = 0$
PeA.6.	$x \,.\, Sy = (x \,.\, y) + x$
PeA.S.	$\mathbf{A}_{\boldsymbol{x}}[0] \,\&\, \forall\, \mathbf{x}\,(\,\mathbf{A} \to \mathbf{A}_{\boldsymbol{x}}[S\mathbf{x}]\,) \to \mathbf{A}$.

(PeA.S. ist dabei als jenes Axiomenschema aufzufassen, das aus allen zu beliebigen Formeln $\mathbf{A}$ *von* L_{PeA} *und beliebigen Variablen* $\mathbf{x}$ *wie in PeA.S. angegeben gebildeten Formeln besteht.)*

(b) Die **vollständige Zahlentheorie** VZ *besitzt als Sprache* L_{VZ} *dieselbe Sprache* L_{PeA} *wie* PeA *und ist semantisch als* $VZ := Th(\langle \mathbb{N}_0; 0, S, +, . \rangle)$ *definiert.*

(c) Sei L_{AZ} *die Einschränkung der Sprache* L_{PeA} *auf die Symbole* 0, S, $+$; *dann ist die* **additive Zahlentheorie** AZ *jene Theorie mit Sprache* L_{AZ}, *die als nichtlogische Axiome gerade PeA.1., ... , PeA.4. besitzt, sowie weiters genau noch alle jene aus dem Schema PeA.S. stammenden Induktionsaxiome, die sich bezüglich Formeln* $\mathbf{A}$ *bilden lassen, die schon über* L_{AZ} *formuliert werden können.*

(d) Sei L_Q *gleich* L_{PeA}; *die* **Robinson-Arithmetik** Q [29] *besitzt die Sprache* L_Q *(die gleiche wie* PeA*) und als nichtlogische Axiome wie* PeA *ebenfalls PeA.1.,*

[28] Diese Theorie wird oft auch *Elementare Peano-Arithmetik* genannt, da das Peanosche Induktionsaxiom „Besitzt die natürliche Zahl 1 eine Eigenschaft P und besitzt für jede natürliche Zahl n, die die Eigenschaft P besitzt, auch deren Nachfolger Sn die Eigenschaft P, so besitzt jede natürliche Zahl die Eigenschaft P" in einer logischen Theorie 1. Ordnung nicht (d.h. genauer: nicht vollständig) formuliert werden kann und statt dessen für den Zweck der Formulierung einer möglichst umfassenden, entsprechenden Theorie 1. Ordnung durch ein Schema von Induktionsaxiomen (das im folgenden mit PeA.S. bezeichnet wird) mit insgesamt schwächerer Wirkung ersetzt werden muß; in diesem Schema von Induktionsaxiomen werden die vom Peanoschen Induktionsaxiom betrachteten Eigenschaften natürlicher Zahlen auf gerade alle solchen eingeschränkt, die sich auch als Formeln der betrachteten Sprache 1. Ordnung formulieren lassen.

[29] Die Robinson-Arithmetik Q wird oft auch mit PRA (primitiv-rekursive Arithmetik) abgekürzt, wobei

... , PeA.6., nicht jedoch das Induktionsschema PeA.S., an dessen statt hingegen noch das folgende Axiom Q.7. :

$$\textbf{Q.7.} \qquad \neg\, x = 0 \rightarrow \exists\, y\,(\, x = Sy\,)\,.$$

(e) Die **Nachfolger-Arithmetik** *NA besitzt als Sprache L_{NA} die Einschränkung der Sprache L_{PeA} auf die Symbole 0 und S und als nichtlogische Axiome nur PeA.1., PeA.2. und alle dem Schema PeA.S. angehörenden Induktionsaxiome, die zu Formeln* **A**, *die schon mit Symbolen von L_{NA} gebildet werden können, gehören.*

(f) Sei L_{SkA} die Einschränkung von L_{PeA} auf das Multiplikationssymbol . als einziges nichtlogisches Symbol; dann ist die **Skolem-Arithmetik** *SkA die semantisch definierte Theorie $Th(\langle \mathbb{N}_0; . \rangle)$.*

PeA ist nun, wie bereits erwähnt, unentscheidbar und unvollständig und läßt sich auf axiomatisierbare Weise nicht zu einer vollständigen Theorie erweitern, also kann auch VZ nicht axiomatisierbar oder entscheidbar sein. PeA ist weiters nicht endlich axiomatisierbar (Ryll-Nardzewski, 1952).

Die Robinson-Arithmetik Q ist (per def.) endlich axiomatisierbar und als Teiltheorie von PeA natürlich unvollständig, jedoch auch unentscheidbar (Tarski, Mostowski und Robinson, 1953). Die Theorie Q hat die interessante Eigenschaft, daß die in ihr darstellbaren[30] Funktionen genau die rekursiven Funktionen sind (vgl. [BoJe74], Chapt. 14). Q besitzt allerdings z.B. nicht die Formel $x + y = y + x$ als Theorem (vgl. ebenfalls [BoJe74], Chapt. 14). Q ist daher mit der Presburger Arithmetik natürlicher Zahlen nicht direkt in Verbindung zu setzen, da Q bezüglich einer Einschränkung ihrer Theoreme auf die in L_{PreAN_0} ausdrückbaren Formeln also weniger Theoreme als $PreAZ_0$ besitzt. Ebenso würde eine Weglassung der Axiome PeA.5. und PeA.6. (jener Axiome, die das Multiplikationszeichen enthalten) aus Q, verbunden mit der Einschränkung der Sprache auf die Sprache L_{PreAN_0}, natürlich nur auf eine echte Teiltheorie von $PreAZ_0$ und eine Theorie von geringerer Ausdrucksstärke führen.

Die Theorie NA ist vollständig und läßt die Quantorenelimination zu (vgl. [Ra77]), ist jedoch nicht endlich axiomatisierbar.

Die Skolem-Arithmetik SkA ist, wie Th. Skolem 1930 gezeigt hat (vgl. [Sko31]) vollständig und entscheidbar und läßt die QE zu. Diese Aussagen treffen aber (worauf [BoJe74] hinweist) nicht mehr auf eine Erweiterung von SkA um die semantisch-formale Einführung des Nachfolgersymbols S in der Theorie $Th(\langle \mathbb{N}_0; S, . \rangle)$ zu, denn diese Theorie ist stark genug, damit in ihr + auf definitorischem Weg (in der üblichen Bedeutung

diese letztere Bezeichnung der Grund dafür ist, warum hier bei der symbolischen Bezeichnung der Theorien der Presburger Arithmetik bzw. der Peano-Arithmetik der aufwendige aber vorsichtigere Weg über (z.B.:) $PreAZ$ bzw. über PeA beschritten wurde.

[30] Bezüglich einer genauen Definition von „darstellbaren Funktionen“ vgl. etwa [BoJe74], Chapt. 14.

von + bei der Interpretation über $\mathbb{N}_0$) eingeführt werden kann und zwar vermittels des definierenden Axioms

$$y = x_1 + x_2 \leftrightarrow \forall z_1 \forall z_2 \forall z_3 \\ \big[z_1 = Sx_1 \;\&\; z_2 = Sx_2 \;\&\; z_3 = S(Sy) \\ \rightarrow S(z_1 \,.\, z_3) \,.\, S(z_2 \,.\, z_3) = S\big(S(z_1 \,.\, z_2) \,.\, (z_3 \,.\, z_3) \big) \big] \;;$$

(es ist leicht nachzurechnen, daß diese Formel in der Struktur $\langle \mathbb{N}_0; \boldsymbol{S}, +, . \rangle$ gültig ist). $Th(\langle \mathbb{N}_0; S, . \rangle)$ ist daher schließlich zu VZ auf definitorischem Weg erweiterbar und daher unentscheidbar und nicht axiomatisierbar.

Die additive Zahlentheorie AZ ist nun jedoch eine nahe Entsprechung zur Presburger Arithmetik natürlicher Zahlen $PreAN$. Genau gilt nämlich, daß die (auf naheliegende Weise mögliche) definitorische Erweiterung von AZ um die Einführung von 0 und $<$ äquivalent ist zur definitorischen Erweiterung von $PreAN$ um die Einführung des Nachfolgersymbols S. – Theorien mit einer solchen Eigenschaft nennt [Shoe67] „schwach äquivalent“ (Vgl. Definition 2.2.3).

Satz 2.5.2. *$PreAN$ und AZ sind schwach äquivalent.*

Beweisskizze. Es genügt zu zeigen, daß die definitorische Erweiterung $PreAN^*$ von $PreAN$ um die Einführung des Symbols S vermittels $y = Sx \leftrightarrow y = x + 1$ und die definitorische Erweiterung AZ^* von AZ um 1 und $<$ vermittels $y = 1 \leftrightarrow y = S0$ bzw. $x < y \leftrightarrow \exists z \, (\neg z = 0 \;\&\; y = x + z \,)$ äquivalente Theorien sind.

(1) Daß AZ^* eine Erweiterung der Theorie $PreAN^*$ ist, läßt sich (relativ leicht, wenngleich ein bißchen mühsam) durch den ausführlichen Nachweis einsehen, daß alle nichtlogischen Axiome von $PreAN$ und auch das definierende Axiom für S in $PreAN^*$ nun ebenfalls in der Theorie AZ^* beweisbar sind; hierbei muß oftmals von der Existenz geeigneter Induktionsaxiome aus AZ (nun auch) in AZ^* Gebrauch gemacht werden.

(2) Die Aussage, daß $PreAN^*$ auch Erweiterung von AZ^* ist, läßt sich durch eine Bezugnahme auf das Standardmodell $\langle \mathbb{N}_0; 0, 1, S, +, < \rangle$ bzw. auf die damit semantisch zu definierende Theorie so begründen:

Aus der aus der Vollständigkeit von $PreAN$ folgenden Äquivalenz von $PreAN$ und $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ ergibt sich sofort auch die Äquivalenz der jeweiligen definitorischen Erweiterungen dieser Theorien um die Einführung von S, nämlich von $PreAN^*$ und von $Th(\langle \mathbb{N}_0; 0, 1, S, +, < \rangle)$. Da umgekehrt AZ^* jedoch unmittelbar als Axiomatisierung von $Th(\langle \mathbb{N}_0; 0, 1, S, +, < \rangle)$ zu erkennen ist, folgt, daß $PreAN^*$ auch Erweiterung von AZ^* ist. $\diamondsuit$

2.6 Entscheidungskomplexität der Theorien der Presburger Arithmetik

In diesem Abschnitt sollen die wichtigsten Aussagen über die Entscheidungskomplexität von Theorien der Presburger Arithmetik zusammengestellt und in Verbindung mit den hier formal-axiomatisch dargestellten Theorien TAZ, $PreAZ$ und $PreAN$ gebracht werden.

Um die Entscheidungskomplexität der in diesem Kapitel behandelten Theorien der Presburger Arithmetik auf exakte Art untersuchen zu können, ist es im Sinn von Kapitel 1 (z.B.) nötig, diese Theorien als Tripel $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$, also als auf Computern handhabbare Sprachsysteme auffassen zu können (mit Zeichenalphabet $\Sigma_{T^{((M))}}$, Formelsprache $Fo_{T^{((M))}} \subseteq \Sigma^*_{T^{((M))}}$ und Theoremsprache $Thm_{T^{((M))}} \subseteq Fo_{T^{((M))}}$).

Es ist hierbei natürlich auch wieder möglich und sinnvoll, die Gestalt von Formeln dieser Theorien (die im formalen System von [Shoe67] ja immer genau spezifizierte Zeichenketten-Objekte sind, wenngleich zum Zweck der Abkürzung oft informelle, aber genau definierte Schreibweisen verwendet werden) im wesentlichen beizubehalten (mit kleineren Änderungen).

Exakt kann dies beispielsweise unter Verwendung der in Grammatik 2.6.1 definierten LR(1)-Grammatik G_{PreA} geschehen, die als Terminalalphabet $\Sigma_{G_{PreA}}$

$$\begin{aligned}\Sigma_{G_{PreA}} := \{\ &\neg, \vee, \exists, \&, \rightarrow, \leftrightarrow, \forall, =, x, y, z, w, {}_0, {}_1, {}_2, \ldots, {}_9, \\ &0, 1, \ldots, 9, *, +, <, \leq, \equiv, \equiv^{\mathrm{N}}, U_{IZN}, ①, \oplus, \circledless\ \}\end{aligned}$$

besitzt, sowie die in Grammatik 2.6.1 aufgeführten Produktionen. G_{PreA} generiert eine Formelsprache $L(G_{PreA})$, welche die Formeln der in den bisherigen Abschnitten definierten Theorien der Additionsarithmetik TAZ, TAZ', (bzw. Theorien der Presburger Arithmetik) $PreAZ$, $PreAZ'$, $PreAN$, $PreAN'$, sowie $PreAN^{(IZN)}$ als Formelstrings (Wörter) dieser Sprache aufzufassen gestattet. Bei Verwendung dieser Formel-Grammatik kann die Theorie TAZ' beispielsweise als Tripel $TAZ'^{((M))}=(\Sigma_{TAZ'^{((M))}}, Fo_{TAZ'^{((M))}}, Thm_{TAZ'^{((M))}})$ mit

$$\begin{aligned}\Sigma_{TAZ'^{((M))}} &:= \Sigma_{G_{PreA}} \setminus \{ <, \leq, \equiv^{\mathrm{N}}, U_{IZN}, ①, \oplus, \circledless \}\ , \\ Fo_{TAZ'^{((M))}} &:= L(G_{PreA}) \mid_{\Sigma_{TAZ'^{((M))}}} \qquad \text{und} \\ Thm_{TAZ'^{((M))}} &:= \{\ \boldsymbol{\mathcal{A}} \in Fo_{TAZ'^{((M))}} / \vdash_{TAZ'} \mathbf{A}^{(\boldsymbol{\mathcal{A}})}\ \}\ ^{31}\end{aligned} \tag{2.18}$$

aufgefaßt werden.

Der Unterschied zwischen einer Formel $\mathbf{A}$ von TAZ' und einem $\mathbf{A}$ entsprechenden Formelstring $\mathbf{A}^{((M))}$ (ohne, daß eine diese Entsprechung hier ausführlich dargestellt wird, ist

Grammatik 2.6.1 Die LR(1)-Formelgrammatik G_{PreA} für Theorien der Presburger Arithmetik:

<formula>::= <at_formula>|¬<formula>|∨<formula><formula>
∃<variable><formula>|&<formula><formula>|
→<formula><formula>|↔<formula><formula>|
∀<variable><formula>

<at_formula>::= =<term><term>|<1_ary_pred_symb><term>|
<2_ary_pred_symb><term><term>

<1_ary_pred_symb>::= U_{IZN}

<2_ary_pred_symb>::= <|≤|≡<dec_ind_ge_2>|$\equiv^N$<dec_ind_ge_2>|⋦

<dec_ind_ge_2>::= $_2|_3|\ \ldots\ |_9|_0$<dec_ind_str>| ... |$_9$<dec_ind_str>

<dec_ind_str>::= $_0|_1|\ \ldots\ |_9|_0$<dec_ind_str>| ... |$_9$<dec_ind_str>

<term>::= <variable>|<const_symb>|<1_ary_funct_symb><term>
<2_ary_funct_symb><term><term>

<variable>::= $x|y|z|w|x$<dec_ind>|y<dec_ind>|z<dec_ind>|w<dec_ind>

<dec_ind>::= $_0|_1|\ \ldots\ |_9|_1$<dec_ind_str>| ... |$_9$<dec_ind_str>

<const_symb>::= $\mathbf{0}|\mathbf{1}|①|($<dec_num>$)$

<1_ary_funct_Symb>::= (<dec_num>) *

<2_ary_funct_Symb>::= $+|\oplus$

<dec_num>:= $\mathbf{0}|\mathbf{1}|\ \ldots\ |\mathbf{9}|\mathbf{1}$<dec_num_str>| ... |$\mathbf{9}$<dec_num_str>

<dec_num>:= $\mathbf{0}|\mathbf{1}|\ \ldots\ |\mathbf{9}|\mathbf{0}$<dec_num_str>| ... |$\mathbf{9}$<dec_num_str>

anschaulich klar, wie eine solche definierbar ist)[31] besteht nun (1) in der Tatsache, daß die Variablen in $\mathbf{A}^{((M))}$ nicht mehr wie in $\mathbf{A}$ unär, sondern dezimal indiziert sind, (2) darin, daß z.B. einem Kongruenzsymbol $\equiv_{79}$ nicht mehr wie in TAZ' ein einzelnes Zeichen entspricht (da ja Computer nicht auf einem unendlichen Zeichenalphabet operieren können), sondern eine Symbolkette $\equiv\ 7\ 9$ bestehend aus 3 Zeichen, (3) darin, daß die in Definition 2.1.1 für den Gebrauch in Formeln von TAZ eingeführten, abgekürzten Schreibweisen wie etwa $\underline{27}\underline{\underline{2}}$ oder $\underline{19}\,x''$ nun auch in $TAZ'^{((M))}$ in der Form von $(\ 2\ 7\ )\ *\ (\ 2\ )$ oder $(\ 1\ 9\ )\ *\ x_{\ 2}$ verwendet werden dürfen (die Konstruktion von möglichst guten Entscheidungsalgorithmen erfordert eine solche zusätzliche Verkürzung in der Schreibweise von Formeln, vgl. [FeRa73]), und (4) darin, daß gegenüber dem formalen System von [Shoe67] für Theorien 1. Ordnung in einem Formelstring hier der Quantor $\forall$ und die logischen Operatoren &, $\rightarrow$ und $\leftrightarrow$ explizit auftreten können, während in [Shoe67] Formeln, in denen diese Operatoren erscheinen, als abgekürzte Schreibweisen für Formeln, in denen diese logischen Symbole nicht mehr vorkommen (und die nur mit dem Quantor $\exists$ und den Junktoren $\vee$ und $\neg$ gebildet sind) angesehen und behandelt werden.

Es muß an dieser Stelle noch festgehalten werden, daß bei der Definition der Entscheidungskomplexität einer betrachteten, entscheidbaren Theorie die Art der formal-logischen Definition einer Theorie auf entweder festgelegt-axiomatische Weise (wie z.B. bei TAZ') oder auf semantische Weise (wie z.B. entsprechend bei $Th(\langle\mathbb{Z};0,1,+,\equiv_2,\equiv_3,\dots\rangle)$) keine Rolle mehr spielt, da die Entscheidungskomplexität als der zur Erkennung von Worten einer Theoremsprache nötige Aufwand definiert ist und diese Theoremsprachen in beiden Fällen gleich sind[32]. (In der Tat verschwindet ein solcher Unterschied in der Art der Axiomatisierung einer Theorie beispielsweise beim Übergang von TAZ' bzw. von $Th(\langle\mathbb{Z};0,1,+,\equiv_2,\equiv_3,\dots\rangle)$ zu $TAZ'^{((M))}$ bzw. zu $Th(\langle\mathbb{Z};0,1,+,\equiv_2,\equiv_3,\dots\rangle)^{((M))}$ entlang von (2.18) bzw. von ganz analog für die äquivalente, semantisch definierte Theorie erfolgenden Setzungen).

Deshalb kommt Resultaten über die Entscheidungskomplexität, in denen im folgenden oft auf bestimmte Weise axiomatisierte Theorien (wie z.B. TAZ oder $PreAN'$) vorkommen, auch die Bedeutung zu, in genau gleichem Ausmaß für alle anderen (konkreten oder vorstellbaren) Axiomatisierungen dieser Theorien (auf konstruktiv-axiomatische oder auf durch ein Modell fixierte, semantische Weise) ebenso gültig zu sein.

Die wichtigsten und bekanntesten Aussagen über die Entscheidungskomplexität von

[31] Hierbei bereitet die exakte Festlegung der einem Wort $\mathcal{A} \in Fo_{TAZ'^{((M))}}$ entsprechenden Formel $\mathbf{A}^{(\mathcal{A})}$ im Sinn von Kapitel 1, Abschnitt 1.3, keine Schwierigkeiten und soll auch nicht expliziter als anhand der folgenden Beispiele angedeutet werden: Variablen x_2, z_5 werden durch x'', z''''' ersetzt, $\equiv\ 7\ 5$ wird durch $\equiv_{75}$ ersetzt, Konstanten wie $(\ 5\ )$ werden durch $\underline{\underline{5}}$, und also durch $1+(1+(1+(1+1)))$, $(\ 4\ )\ *\ (\ 2\ )$ wird durch $\underline{4}\,\underline{\underline{2}}$ und also durch $(1+1)+((1+1)+((1+1)+(1+1)))$ ersetzt und $\forall\,\mathbf{x}\,\mathcal{A}$ durch $\neg\,\exists\,\mathbf{x}\,\neg\,\mathbf{A}^{(\mathcal{A})}$. Die umgekehrte Transformation einer Formel $\mathbf{A}$ über $L_{TAZ'}$ in einen Formelstring $\mathbf{A}^{((M))}$ ist völlig klar.

[32] Exakt ließe sich etwa sagen, daß der Begriff der „Entscheidungskomplexität“ einer Theorie (in dessen mannigfachen Präzisierungen) invariant unter der *Äquivalenz* von Theorien ist.

Theorien der Presburger Arithmetik bezüglich Komplexitätsklassen von *sequentiellen* Turingmaschinen bestehen in folgenden beiden Resultaten[33]:

Satz 2.6.1 (Ferrante, Rackoff, 1973). [34]
Es gibt ein $d_1 \in \mathbb{R}$, $d_1 > 0$, *so, daß* $PreAZ \in DSpace(2^{2^{d_1 n}})$.

Satz 2.6.2 (Fischer, Rabin, 1974). [35]
Es gibt ein $c_2 \in \mathbb{R}$, $c_2 > 0$, *so, daß* $PreAN \notin NTime(2^{2^{c_2 n}})$.
(Dieser Satz entspricht im wesentlichen der weiter präzisierten Aussage Satz 3.1.1 in Kapitel 3.)

Präzisierung dieser Aussagen. Betrachtet man die beiden Theorien $PreAZ$ und $PreAN$ in der oben für TAZ exakt festgelegten Weise als Tripel $PreAZ^{((M))} = (\Sigma_{PreAZ^{((M))}}, Fo_{PreAZ^{((M))}}, Thm_{PreAZ^{((M))}})$ bzw. als Tripel $PreAN^{((M))} = (\Sigma_{PreAN^{((M))}}, Fo_{PreAN^{((M))}}, Thm_{PreAN^{((M))}})$, so sollen die Aussagen von Satz 2.6.1 und von Satz 2.6.2 zuerst nur als die beiden präzisen Aussagen

„Es gibt ein $d_1 \in \mathbb{R}$, $d_1 > 0$ so, daß $Thm_{PreAZ^{((M))}} \in DSpace(2^{2^{d_1 n}})$ “,

bzw.

„Es gibt ein $c_2 \in \mathbb{R}$, $c_2 > 0$ so, daß $Thm_{PreAZ^{((M))}} \notin NTime(2^{2^{c_2 n}})$ “

aufgefaßt werden. Da diese Aussagen aber invariant unter $\leq_{pl}$-äquivalenten Formelschreibweisen, d.h. Formelsprachen $Fo_{T^{((M))}}$ (für verschiedene Festlegungen von $T^{((M))}$ in Rechenmaschinen-behandelbarer Form (für $T = PreAZ, PreAN$)) sind und da es außerdem wohl gerechtfertigt ist, anzunehmen, daß die in $\leq_{pl}$-Reduktionen von Formelsprachen *sinnvoller* Formelschreibweisen vorkommenden Parameter (Konstanten $c, d \in \mathbb{R}$, $c, d > 0$ und Polynome p) allesamt gemeinsam (geeignet) nach oben beschränkt werden können, deshalb gelten diese Aussagen auch in einer unrelativierten, von einer bestimmten (sinnvollen) Formelsprache für diese Theorien unabhängigen Form. Das ist die Begründung und die Bedeutung der in den Sätzen vorkommenden Gestalt der Behauptung über die Entscheidungskomplexität der jeweiligen Theorie, wobei darin auf die Theorien selbst und nicht auf bestimmte, dafür festgelegte Formel-(und Theorem-)sprachen Bezug genommen wird. (Diese dabei in den obigen Sätzen verwendete Schreibweise wird für die Darstellung von die Entscheidungskomplexität formal-logischer Theorien betreffenden Aussagen in der Literatur aber häufig in dieser prägnanten, jeoch unpräzisen Weise verwendet.)

Die hier mitgeteilte Behauptung, daß sich die beiden Aussagen „Es gibt ein $d \in \mathbb{R}$, $d > 0$, sodaß $L \in DSpace(2^{2^{dn}})$“ und „Es gibt ein $c \in \mathbb{R}$, $c > 0$, sodaß $L \notin NTime(2^{2^{cn}})$“

[33] Bei der Darstellung dieser Ergebnisse handelt es sich um sehr gebräuchliche abkürzende Schreibweisen, die im folgenden präzisiert werden.
[34] (Vgl. [FeRa73].)
[35] (Vgl. [FiR74] und das Kapitel 3 dieser Arbeit.)

für Sprachen $L \subseteq \Sigma$ (Σ ein Symbolalphabet) unter $\leq_{pl}$-äquivalenten Transformationen $L \equiv_{pl} L'$, $L \subseteq (\Sigma)^*$ (Σ ein Symbolalphabet) übertragen, wird implizit in Satz 2.6.4 bewiesen. (Für die oben ausgesprochene Behauptung über die Übertragbarkeit von Komplexitätsaussagen bezüglich verschiedener sinnvoller Formelsprachen für eine Theorie ist es außerdem nötig, von der (allerdings zumeist unmittelbar erreichbaren) Voraussetzung auszugehen, daß die betrachteten $POLYLIN$-Transformationen von Formelsprachen auch ebensolche Reduktionen bzw. Transformationen der beteiligten Theoremsprachen sind bzw. darauf definieren.)

Satz 2.6.1 gibt eine obere Schranke für die Entscheidungskomplexität von $PreAZ$ bezüglich deterministischem Turing-Speicherplatzbedarf an, die von doppelt-exponentiell-linearer Gestalt ist. Daraus folgt wegen $DSpace(f(n)) \subseteq NSpace(f(n)) \subseteq$ $\subseteq DTime(ExL(f(n))$ (für alle Funktionen $f(n)$) jedenfalls eine dreifach-exponentiell-lineare obere Schranke bezüglich deterministischer Turing-Rechenzeit. Satz 2.6.1 geht auf J. Ferrante und Ch. Rackoff zurück ([FeRa73]), die ein Quantoreneliminationsverfahren für $PreAZ$ von D. Cooper ([Coo72]) und eine Komplexitätsanalyse dieses Verfahrens durch D. Oppen ([Opp73]) dabei verwendet haben. (Eine weitere Darstellung dieses Verfahrens gaben Ferrante und Rackoff in der Form eines—ebenfalls auf den beiden anderen Arbeiten aufbauenden bzw. entsprechend konstruierten—Ehrenfeucht-game-Entscheidungsverfahrens für $PreAZ$ (bzw. für $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$) in [FeRa79]).

Satz 2.6.1 erfaßt das bekannte Resultat von M. Fischer und M. Rabin in [FiR74], das aussagt, daß $PreAN$ eine doppelt-exponentiell-lineare untere Schranke ihrer Entscheidungskomplexität bezüglich der Rechenzeit nichtdeterministischer Turingmaschinen besitzt. Eine Aufarbeitung von [FiR74] ist Gegenstand von Kapitel 3 dieser Arbeit.

Sieht man vorerst von der Tatsache ab, daß sich die obere Schranke in Satz 2.6.1 bzw. die untere Schranke in Satz 2.6.2 auf zwei verschiedene Theorien beziehen, so ist die zwischen diesen beiden Aussagen bestehende Lücke im wesentlichen eine zwischen den Klassen $NTime(EEXL)$ und (der diese umfassenden Klasse) $DSpace(EEXL)$ möglicherweise tatsächlich vorhandene Lücke. Wegen einer Aussage von A. Chandra, D. Kozen und L. Stockmeyer[36] gilt jedenfalls $NTime(EEXL) \subseteq DSpace(EEXL)$. Es ist jedoch nicht gewiß, daß zwischen diesen beiden Klassen wirklich eine strikte Inklusion besteht, daß also wirklich $NTime(EEXL) \subsetneqq DSpace(EEXL)$ gilt. Im Lichte dieser offenen Frage könnten nun eine untere Schranke aus $EEXL$ bezüglich nichtdeterministischer Turing-Rechenzeit und eine obere Schranke aus $EEXL$ bezüglich deterministischem Turing-Speicherplatzbedarf für die Entscheidungskomplexität einer Theorie T als einander bis auf die Lösung eines tief-liegenden komplexitätstheoretischen Problems genügend genähert

[36] Für jede Funktion mit $T(n) \geq n$ (für alle $n \in \mathbb{N}_0$) gilt: $ATime(T(n)) \subseteq DSpace(T(n)) \subseteq$ $\subseteq \bigcup_{c \in \mathbb{R},\, c>0} ATime(c\,(T(n))^2)$, vgl. [CKS81]. Weiters gilt natürlich auch die Aussagekette: $NTime(T(n)) =$ $= ATimeAlter(T(n), 1) \subseteq ATime(T(n))$.

betrachtet werden. Dies bezieht sich aber nur auf Komplexitätsklassen bezüglich sequentiellen Turingmaschinen und auch hier wären vielleicht noch Verfeinerungen bezüglich Komplexitätsklassen, die durch gleichzeitiges Betrachten von Rechenzeit und Speicherplatzbedarf definiert sind, vorstellbar.

Im Fall von ausschließlich betrachteter Rechenzeit läßt sich die Lücke, die zwischen Komplexitätsaussagen vom Typ von Satz 2.6.2 und von Satz 2.6.1 (sehr wahrscheinlich) besteht, als die zwischen $NTime(EEXL)$ und $DTime(EEEXL)$ (eher noch wahrscheinlicher) existierende darstellen (bzw. darauf erweitern). Diese läßt sich mit der ebenfalls noch ungeklärten Frage in Verbindung bringen, ob es Sprachen L gibt, für deren Erkennung durch eine deterministische Turingmaschine wirklich exponentieller Mehraufwand bezüglich benötigter Rechenzeit gegenüber der Erkennung von L durch eine nichtdeterministische Turingmaschine erforderlich ist.

Es stellt sich nun die Frage, ob die Situation einer solchen möglicherweise (vorerst) unausweichlichen Lücke bei der Charakterisierung des Entscheidungsaufwandes für $PreAN$ und $PreAZ$ mittels nichtdeterministischer Turing-Rechenzeit nach unten und deterministischem Turing-Speicherplatzbedarf nach oben hier tatsächlich vorliegen kann, d.h. ob sich die Komplexitätsaussagen aus Satz 2.6.1 und Satz 2.6.2 auf die jeweils andere Theorie übertragen lassen (mit Schrankenfunktionen vom selben Wachstumsverhalten). – Es wird gezeigt werden, daß solche Übertragungen möglich sind.

Dem dabei verwendeten Vorgehen liegt die folgende, hier speziell für $\leq_{pl}$-Reduktionen (die im kommenden die Hauptrolle spielen) angestellte Überlegung zugrunde, die aber typisch für die Verwendung von Reduzierbarkeiten in der Komplexitätstheorie ist:

Falls für zwei Sprachen A, B mit $A \subseteq \Sigma_1^*$, $B \subseteq \Sigma_2^*$ (Σ_1, Σ_2 endliche Alphabete) $A \leq_{pl} B$ via f mit $f\colon \Sigma_1^* \to \Sigma_2^*$ gilt, so kann zu jedem Entscheidungsverfahren M_B für B auf folgende Weise ein Entscheidungsverfahren M_A für A konstruiert werden: Ausgehend von $x \in \Sigma_1$ konstruiert M_A zuerst $f(x)$ (das ist wegen $f \in POLYLIN$ „praktisch durchführbar“) und setzt dann M_B zur Entscheidung von $f(x)$ ein.

Auf diese Weise kann (mit Hilfe einer genauen Aufwandsabschätzung zur Berechnung von f und einer Längenabschätzung für $f(x)$) jedenfalls immer eine obere Schranke für den zur Entscheidung von A nötigen Aufwand aus einer oberen Schranke für den Aufwand von B gewonnen werden. (Es ist dabei natürlich nicht sichergestellt, daß durch eine solche Übertragung immer eine brauchbare und möglichst niedrige obere Schranke für die Entscheidungskomplexität von A erzielt wird, auch wenn von einer Schranke mit dieser Eigenschaft für B ausgegangen wird).

Umgekehrt kann eine $\leq_{pl}$-Reduzierbarkeit $A \leq_{pl} B$ u.U. aber auch dazu dienen, aus einer unteren Schranke für die Entscheidungskomplexität von A eine untere Schranke für die Entscheidungskomplexität von B zu gewinnen. Und zwar dadurch, daß die Annahme der Existenz eines Entscheidungsverfahrens M_B für B mit einem bestimmten Aufwand auf einen Widerspruch zu einer für A (unabhängig) erzielten unteren Schranke geführt wird, damit, daß von M_B ausgehend wie oben durch die Verwendung der Reduzierbarkeit

$A \leq_{pl} B$ via einer Funktion f ein Entscheidungsverfahren M_A für A konstruiert wird, dessen (hypothetischer) Aufwand der unteren Schranke für A widerspricht.

Nun kann im Fall der Theorien $PreAN$ und $PreAZ$ die Aussage $\vdash_{PreAN} \mathbf{A} \Leftrightarrow \Leftrightarrow \vdash_{PreAZ} \mathbf{A}^R$ (Lemma 2.4.2 und dessen Umkehrung, die wegen der Vollständigkeit dieser Theorien gilt) dazu verwendet werden, um $PreAN \leq_{pl} PreAZ$, bzw. genauer, um $Thm_{PreAN} \leq_{pl} Thm_{PreAZ}$ einzusehen und nachzuweisen. Diese Reduzierbarkeit wird später in Satz 2.6.4 (in eher unausgesprochenem Sinn) auf die zuerst beschriebene zweifache Weise zur Übertragung von Schranken für die Entscheidungskomplexität zwischen $PreAN$ und $PreAZ$ verwendet. Und zwar zur Übertragung der oberen Schranke aus Satz 2.6.1 für $PreAZ$ zu einer analogen oberen Schranke Schranke für $PreAN$, sowie zur Übertragung der unteren Schranke für $PreAN$ aus Satz 2.6.2 zu einer gleich-gestaltigen und analogen unteren Schranke für $PreAZ$. (Es sollte hierbei aber angemerkt werden, daß die den Sätzen Satz 2.6.1 und Satz 2.6.2 zugrundeliegenden Arbeiten es auch ermöglichen würden, die entsprechenden Ergebnisse ebenfalls für die jeweils andere Theorie auszusprechen und mit geringem Mehraufwand zu beweisen.)

Vor der Darstellung der erwähnten Übertragungsaussage soll jedoch noch gezeigt werden, daß die Entscheidungskomplexität der beiden Theorien $PreAN$ und $PreAZ$ noch enger (als durch analog-gestaltige obere und untere Schranken) zusammenhängen bzw. gekoppelt sind. Die Reduzierbarkeit $PreAN \leq_{pl} PreAZ$ läßt nämlich die Möglichkeit offen, daß $PreAZ$ vielleicht deutlich schwieriger[37] zu entscheiden wäre als $PreAN$ (: „deutlich schwieriger“ im dafür später wegen der Ergebnisübertragung nur mehr in Frage kommenden, (etwa) durch $NTime(EEXL)$ nach unten und $DSpace(EEXL)$ nach oben eingegrenzten Bereich, in dem Thm_{PreAN} *und* Thm_{PreAZ} nach den Aussagen von Satz 2.6.1, Satz 2.6.2 und Satz 2.6.4 (aus dem folgenden) zugleich enthalten sind). – Es stellt sich aber heraus, daß dies nicht der Fall ist, da sich auch $PreAZ \leq_{pl} PreAN$ beweisen läßt.

Lemma 2.6.3. $PreAN \equiv_{pl} PreAZ$.

Präzisierung. Betrachtet man die in Abschnitt 2 und in Abschnitt 3 definierten Theorien $PreAZ$ und $PreAN$ im Rahmen der Untersuchung ihrer Entscheidungskomplexität als Tripel $PreAZ^{((M))}=\big(\Sigma, Fo, Thm_{PreAZ^{((M))}}\big)$ bzw. als Tripel $PreAN^{((M))}=\big(\Sigma, Fo, Thm_{PreAN^{((M))}}\big)$, mit

$$\begin{aligned} \Sigma &:= \Sigma_{G_{PreA}} \setminus \{ \leq, \equiv, \equiv^{\mathrm{N}}, U_{INZ}, ①, \oplus, \lessgtr \} , \\ Fo &:= L(G_{PreA}) \mid_{\Sigma} , \\ Thm_{T^{((M))}} &:= \{ \boldsymbol{\mathcal{A}} \in Fo_T / \vdash_T \mathbf{A}^{(\boldsymbol{\mathcal{A}})} \} \qquad (\text{für } T = PreAN, PreAZ) , \end{aligned}$$

[37] Diese Möglichkeit könnte—von vorne herein—ja auch von der am Anfang von Abschnitt 4 dargestellten, praktischen Beobachtung unterstützt sein, daß es einfacher zu sein scheint, ein QE-Verfahren für $PreAZ$ zur Entscheidung von Formeln von $PreAN$ zu nutzen (und damit auch ein solches QE-Verfahren für $PreAZ$ zu einem QE-Verfahren für $PreAN$ umzugestalten) als umgekehrt.

wobei G_{PreA} und Σ_{PreA} auf zu Beginn dieses Abschnitts erfolgte Festsetzungen verweisen, so soll die Aussage des Lemmas exakt als

$$Thm_{PreAN^{((M))}} \equiv_{pl} Thm_{PreAZ^{((M))}}$$

verstanden werden, d.h. als die Behauptung der Gültigkeit (der Konjunktion) der beiden Aussagen $Thm_{PreAN^{((M))}} \leq_{pl} Thm_{PreAZ^{((M))}}$ und $Thm_{PreAZ^{((M))}} \leq_{pl} Thm_{PreAN^{((M))}}$. – Nur in dieser präzis formulierten Gestalt wird der Beweis des Lemmas hier skizziert. In weniger präzisem Sinn kann das Lemma aber durchaus auch so verstanden werden, daß sich auf analoge, dem unten beschriebenen Beweisweg folgende Weise die gegenseitige $\leq_{pl}$-Reduzierbarkeit der beiden Theorien leicht auch bezüglich variierter Formelsyntax zeigen läßt (etwa für eine Syntax, die sich auf im Gegensatz zu den hier vorgestellten Formelgrammatiken, Grammatik 1.3.1 und Grammatik 2.6.1, auf die Schreibweise von Formeln in nicht-pränexer, sondern Klammerungsschreibweise gründet). Umgekehrt rührt diese (hier verwendete und vielerorts gebräuchliche) Schreibweise im Lemma auch davon her, daß die (behauptete) $\leq_{pl}$-Reduzierbarkeit der Theoremsprachen dieser Theorien als Schreibweise eng mit den in den Namen dieser Theorien steckenden allgemeinen Bezeichnungen von Theorien der Additionsarithmetik verknüpft und in einer von einer einzigen konkreten Formelsprache unabhängigen Form ausgedrückt werden sollte.

Beweisskizze. $PreAZ^{((M))}$, $PreAN^{((M))}$ und insbesondere auch Σ, Fo, $Thm_{PreAN^{((M))}}$ und $Thm_{PreAZ^{((M))}}$ seien wie in der Präzisierung des Lemmas.

(1) Die einfacher nachzuweisende Richtung in der Aussage des Lemmas besteht im Nachweis von $Thm_{PreAN^{((M))}} \leq_{pl} Thm_{PreAZ^{((M))}}$:

Hierfür ist eine $POLYLIN$-Funktion f mit der Eigenschaft

$$(\forall\, w \in \Sigma^*)\, \big(w \in Thm_{PreAN} \iff f(w) \in Thm_{PreAZ} \big) \tag{2.19}$$

anzugeben. Eine solche ist nun leicht mit Hilfe von Lemma 2.4.2 und dessen Umkehrung, insgesamt der Aussage

$$\vdash_{PreAN} \mathbf{A} \iff \vdash_{PreAZ} \mathbf{A}^R\,, \tag{2.20}$$

zu definieren: Und zwar durch

$$f\colon \Sigma^* \to \Sigma^*$$
$$w \mapsto \begin{cases} w & \ldots\ w \in \Sigma^* \setminus Fo \\ \boldsymbol{\mathcal{A}}^R & \ldots\ \text{es existiert ein } \boldsymbol{\mathcal{A}} \in Fo \text{ mit } w = \boldsymbol{\mathcal{A}} \end{cases}$$

(wobei $\boldsymbol{\mathcal{A}}^R$ für alle Formel-Wörter $\boldsymbol{\mathcal{A}} \in Fo$ analog zu Definition 2.4.1 definiert sei) erklärt. Nun läßt sich aber sowohl die Tatsache, daß f linear beschränkt ist (z.B.

mit multiplikativer Konstante 9), als auch $f \in POLYLIN$ einfach durch den in Definition 2.4.1 rekursiv festgelegten Zusammenhang zwischen den Formeln $\mathbf{A}$ und $\mathbf{A}^R$ einsehen bzw. beweisen. Ebenso ist durch die obige Definition von f die Gültigkeit von (2.19) durch den Verweis auf (2.20) (und die Tatsache, daß eine analoge entsprechende Aussage auch für Formel-Wörter $\mathcal{A}, \mathcal{A}^R \in Fo$, nämlich

$$\mathcal{A} \in Thm_{PreAN^{((M))}} \iff \mathcal{A}^R \in Thm_{PreAZ^{((M))}}$$

gilt) garantiert.

(2) $PreAZ \leq_{pl} PreAN$, d.h. genau: $Thm_{PreAZ^{((M))}} \leq_{pl} Thm_{PreAN^{((M))}}$ [38]:

In dieser Richtung des Lemmas (die nicht ebenso unmittelbar einsehbar ist) geht in entscheidender Weise ein, daß nicht nur $PreAN$ in $PreAZ$ interpretierbar ist (was vermittels der Interpretation INZ aus Satz 2.4.4 der Richtung (1) im Beweis entspricht), sondern, daß auch $PreAZ$ in $PreAN$ interpretierbar ist, nämlich mit Hilfe der Interpretation IZN von $PreAZ$ in $PreAN^{(IZN)}$ aus Satz 2.4.5.

Wegen dieser Interpretation IZN gibt es also zu jeder Formel $\mathbf{A}$ von $PreAZ$ eine Formel $\mathbf{A}^{(IZN)}$ von $PreAN^{(IZN)}$ mit

$$\vdash_{PreAZ} \mathbf{A} \iff \vdash_{PreAN^{(IZN)}} \mathbf{A}^{(IZN)} \tag{2.21}$$

(hierbei folgt „$\Rightarrow$“ aus der Aussage des “Interpretation Theorems”, da IZN Interpretation $PreAZ$ in $PreAN^{(IZN)}$ ist, und „$\Leftarrow$“, also, daß es sich dabei um eine Interpretation handelt, die *faithful* ist, unter Zuhilfenahme der Vollständigkeit dieser Theorien).

Da $PreAN^{(IZN)}$ definitorische Erweiterung von $PreAN$ ist, existiert natürlich für jede Formel $\mathbf{A}^{(IZN)}$ auch ihre Translation $(\mathbf{A}^{(IZN)})^*$ nach $PreAN$, für die jedenfalls auch gilt:

$$\vdash_{PreAN^{(IZN)}} \mathbf{A}^{(IZN)} \iff \vdash_{PreAN} (\mathbf{A}^{(IZN)})^* \,. \tag{2.22}$$

Insgesamt gilt damit wegen (2.21) und (2.22)

$$\vdash_{PreAZ} \mathbf{A} \iff \vdash_{PreAN} (\mathbf{A}^{(IZN)})^* \,, \tag{2.23}$$

und unter Zuhilfenahme dieser Aussage könnte ähnlich wie in (1) eine polynomial-Zeit-berechenbare Reduktionsfunktion von $Thm_{PreAZ^{((M))}}$ auf $Thm_{PreAN^{((M))}}$ definiert werden.

[38] Diese Richtung des Lemmas folgt (auf ganz anderem Weg) *auch* aus dem im folgenden in Satz 2.6.6 dargestellten Ergebnis von [Be80] der Vollständigkeit von $PreAN$ in der Klasse $ATimeAlter(EEXL, LIN)$ unter $\leq_{pl}$-Reduktionen zusammen mit $PreAZ \in ATimeAlter(EEXL, LIN)$, einer sich als Folgerung aus [FeRa73] und insbesondere aus [FeRa79] ergebenden Aussage.

Allerdings ist von einer so definierten Funktion nicht gesichert, daß sie linearbeschränkt ist und bei naiver (d.h. wie gebräuchlicher) Wahl von Translationsformeln ist diese Eigenschaft auch tatsächlich anhand vieler angebbarer Beispiele verletzt[39] Dennoch kann unter Verwendung spezieller Eigenschaften der Theorien der Presburger Arithmetik (etwa der Assoziativität und der Kommutativität von Termen bezüglich $+$) zu $\mathbf{A}^{(IZN)}$ immer eine Formel $(\mathbf{A}^{(IZN)})^{**}$ in $PreAN$ mit

$$\vdash_{PreAN^{(IZN)}} \mathbf{A}^{(IZN)} \quad \Longleftrightarrow \quad \vdash_{PreAN} (\mathbf{A}^{(IZN)})^{**}$$

und also auch mit

$$\vdash_{PreAZ} \mathbf{A} \quad \Longleftrightarrow \quad \vdash_{PreAN} (\mathbf{A}^{(IZN)})^{**} \,, \tag{2.24}$$

sowie der Eigenschaft

$$\begin{aligned} &(\,\exists\, c \in \mathbb{N}\,)\,(\,\forall\, \mathbf{A} \text{ Formel von } PreAZ\,) \\ &\qquad \big(\,\big|((\mathbf{A}^{(IZN)})^{**})^{((M))}\big| \leq c \cdot \big|\mathbf{A}^{((M))}\big|\,\big)\,, \end{aligned} \tag{2.25}$$

angegeben werden und dann auch immer in polynomialer Rechenzeit (und mit linearem Speicherplatzbedarf) berechnet werden.

Die Formel $(\mathbf{A}^{(IZN)})^{**})$ entsteht dabei aus $\mathbf{A}^{(IZN)}$ durch die Ausführung der folgender Schritte:

(S1) In $\mathbf{A}^{(IZN)}$ werden alle atomaren Formeln $U_{IZN}\mathbf{a}$ (die wegen des definierenden Axiomes $U_{IZN}\, x \leftrightarrow 0 = 0$ von U_{IZN} in $PreAN^{(IZN)}$ zur Entscheidung unwesentlich sind) weggelassen, und die Formel wird daraufhin aussagenlogisch weitestmöglich verkürzt (im Extremfall zu $0 = 0$ oder zu $0 = 1$).

Die resultierende Formel sei $\mathbf{C}$.

(S2) In $\mathbf{C}$ werden alle atomaren Formeln $\mathbf{a} = \mathbf{b}$ und $\mathbf{a} \lessgtr \mathbf{b}$ durch atomare Formeln $\mathbf{a}' = \mathbf{b}'$ bzw. $\mathbf{a}' \lessgtr \mathbf{b}'$ ersetzt, wobei die Terme $\mathbf{a}'$ bzw. $\mathbf{b}'$ jeweils von der Gestalt

$$\underline{\underline{a_0}} \oplus \underline{a_1}\,\mathbf{x}_1 \oplus \ldots \oplus \underline{a_n}\,\mathbf{x}_n \qquad \text{bzw.} \qquad \underline{\underline{b_0}} \oplus \underline{b_1}\,\mathbf{y}_1 \oplus \ldots \oplus \underline{b_m}\,\mathbf{y}_m$$

[39] Es scheint allgemein (gerade auch bei Zugrundelegung des formalen Systems von [Shoe67] und dem dort eingeschränkteren Begriff von definitorischen Erweiterungen) nicht möglich zu sein, in allen Fällen von definitorischen Erweiterungen T' einer Theorie 1. Ordnung T eine $\leq_{pl}$-Reduktion der Theoremsprache der erweiterten Theorie T' auf diejenige der Grundtheorie T vermittels Translationsformeln (in deren Wahl immer viele Freiheiten bestehen) zu finden. – In vielen Fällen sind solche $\leq_{pl}$-Reduktionen unter Verwendung spezieller formaler (: die Art der nichtlogischen Symbole in T, T' betreffender) und inhaltlicher (: die Beweisbarkeit von Formeln in T, T' betreffender) Eigenschaften von T und T' trotzdem konstruierbar sein.

$(n, m \in \mathbb{N}_0,\ a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathbb{N},\ \mathbf{x}_1, \ldots, \mathbf{x}_m$ und $\mathbf{y}_1, \ldots, \mathbf{y}_m$ jeweils verschiedene Variable) sind und $\vdash_{PreAN^{(IZN)}} \mathbf{a} = \mathbf{a}'$ sowie $\vdash_{PreAN^{(IZN)}} \mathbf{b} = \mathbf{b}'$ gilt (d.h. also, daß $\mathbf{a}'$ bzw. $\mathbf{b}'$ aus $\mathbf{a}$ bzw. $\mathbf{b}$ jeweils durch Umgruppierung bezüglich $\oplus$ und Zusammenfassen der jeweils darin vorkommenden Variablen entstehen). Die resultierende Formel sei $\mathbf{C}^*$.

(S3) Nun erst wird zu $\mathbf{C}^*$ eine Translationsformel $\mathbf{C}^{**}$ von $PreAN^{(IZN)}$ nach $PreAN$ auf genau präzisierte Weise gefunden. Hierfür werden die definierenden Axiome für $\oplus$ und $\bigotimes$ in $PreAN^{(IZN)}$ mit $y = x_1 \oplus x_2 \leftrightarrow \mathbf{D}_1$ und $x_1 \bigotimes x_2 \leftrightarrow \mathbf{D}_2$ (mit sich aus dem Beweis zu Satz 2.4.5 ergebenden Formeln $\mathbf{D}_1$ und $\mathbf{D}_2$ [40]) abgekürzt geschrieben.

$\mathbf{C}^{**}$ entstehe nun aus $\mathbf{C}^*$ durch Ersetzung jeder atomaren Teilformel in $\mathbf{C}^{**}$ der Gestalt

$$\underline{\underline{a_0}} \oplus \underline{a_1}\,\mathbf{x}_1 \oplus \ldots \oplus \underline{a_n}\,\mathbf{x}_n \ \bigotimes\ \underline{\underline{b_0}} \oplus \underline{b_1}\,\mathbf{y}_1 \oplus \ldots \oplus \underline{b_m}\,\mathbf{y}_m$$

durch

$$\begin{aligned}
&\exists\,\mathbf{z}_1\,\big(\mathbf{D}_1'[\underline{\underline{a_0}}, \underline{a_1}\,\mathbf{x}_1, \mathbf{z}_1]\ \&\ \exists\,\mathbf{z}_2\,\big(\mathbf{D}_1'[\mathbf{z}_1, \underline{a_2}\,\mathbf{x}_2, \mathbf{z}_2]\ \&\ \exists\,\mathbf{z}_1\,\big(\mathbf{D}_1'[\mathbf{z}_2, \underline{a_3}\,\mathbf{x}_3, \mathbf{z}_1]\ \&\ \ldots\\
&\qquad \ldots\ \&\ \exists\,\mathbf{z}_{1/2}\,\big(\mathbf{D}_1'[\mathbf{z}_{2/1}, \underline{a_n}\,\mathbf{x}_n, \mathbf{z}_{1/2}]\\
&\quad \&\ \exists\,\mathbf{w}_1\,\big(\mathbf{D}_1'[\underline{\underline{b_0}}, \underline{b_1}\,\mathbf{y}_1, \mathbf{w}_1]\ \&\ \exists\,\mathbf{w}_2\,\big(\mathbf{D}_1'[\mathbf{w}_1, \underline{b_2}\,\mathbf{y}_2, \mathbf{w}_2]\ \&\ \exists\,\mathbf{w}_1\,\big(\ldots\\
&\qquad \ldots\ \&\ \exists\,\mathbf{w}_{1/2}\,\big(\mathbf{D}_1'[\mathbf{w}_{2/1}, \underline{b_m}\,\mathbf{y}_m, \mathbf{w}_{1/2}]\\
&\qquad\qquad \&\ \mathbf{D}_2'[\mathbf{z}_{1/2}, \mathbf{w}_{1/2}]\big)\ \ldots\big)\big)\big)\big)\ldots\big)\big)\big)\,,
\end{aligned}$$

wobei $\mathbf{z}_1, \mathbf{z}_2, \mathbf{w}_1, \mathbf{w}_2$ jeweils von $\mathbf{x}_1, \ldots, \mathbf{x}_n$ und $\mathbf{y}_1, \ldots, \mathbf{y}_m$ verschiedene Variablen mit kleinstmöglichen Indizes sind, wobei weiters Formeln $\mathbf{D}_1[\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3]$ abgekürzte Schreibweisen für Formeln $(\mathbf{D}_1)_{\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{y}}, [\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3]$ darstellen, weiters $\mathbf{D}_1'$ aus $\mathbf{D}_1$ durch Umbenennung gebundener Variablen entsteht (und die neuen gebundenen Variablen kleinstmögliche Indizes haben :), sodaß alle Substitutionen sinnvoll möglich sind (das ist sicher dann der Fall, wenn in $\mathbf{D}_1'$ keine der Variablen $\mathbf{x}_1, \ldots, \mathbf{x}_n, \mathbf{y}_1, \ldots, \mathbf{y}_n, \mathbf{z}_1, \mathbf{z}_2, \mathbf{w}_1, \mathbf{w}_2$ mehr gebunden erscheinen), ebenso $\mathbf{D}_2'$ durch Umbenennung von gebundenen Variablen aus $\mathbf{D}_2$ entsteht, sodaß darin $\mathbf{z}_1, \mathbf{z}_2, \mathbf{w}_1, \mathbf{w}_2$ nicht gebunden vorkommen und $\mathbf{z}_{1/2}, \mathbf{z}_{2/1}, \mathbf{w}_{1/2}, \mathbf{w}_{2/1}$ für die Variablen $\mathbf{z}_2$ bzw. $\mathbf{z}_1$, $\mathbf{z}_1$ bzw. $\mathbf{z}_2$, $\mathbf{w}_2$ bzw. $\mathbf{w}_1$, $\mathbf{w}_1$ bzw. $\mathbf{w}_2$ stehen, abhängig davon, ob m und n jeweils gerade bzw. ungerade sind.

Weiters werden in $\mathbf{C}^*$ atomare Formeln mit Prädikatssymbol $=$ auf analoge (und sogar einfachere Weise) ersetzt.

[40] Hierbei werden die Definitionsformeln auf der rechten Seite der definierenden Axiomen für die Symbole $\oplus$ und $\bigotimes$ im Beweis zu Satz 2.4.5 durch das Ausdrücken von Kongruenzen mit Hilfe äquivalenter Formeln in $PreAN$ (Translationen von $PreAN'$ nach $PreAN$) neu angeschrieben.

Die insgesamt resultierende Formel $\mathbf{C}^{**}$ ist dann die gesuchte Translationsformel $(\mathbf{A}^{(IZN)})^{**}$.

Mit Hilfe der so erfolgten Festsetzung der Formel $(\mathbf{A}^{(IZN)})^{**}$ kann nun eine $POLYLIN$-Funktion $f\colon \Sigma^* \to \Sigma^*$, die die $\leq_{pl}$-Reduktion $Thm_{PreAZ^{((M))}} \leq_{pl} \leq_{pl} Thm_{PreAN^{((M))}}$ durchführt, durch eine Zuordnung der Gestalt $\mathbf{A} \mapsto (\mathbf{A}^{(IZN)})^{**}$ bestimmt werden, und zwar mit der Setzung

$$f\colon \Sigma^* \to \Sigma^*$$
$$w \mapsto \begin{cases} w & \dots\ w \in \Sigma^* \setminus Fo \\ (\boldsymbol{\mathcal{A}}^{(IZN)})^{**} & \dots\ \text{es existiert ein } \boldsymbol{\mathcal{A}} \in Fo \text{ mit } w = \boldsymbol{\mathcal{A}} \end{cases}$$

(wobei $(\boldsymbol{\mathcal{A}}^{(IZN)})^{**}$ für alle Formel-Wörter $\boldsymbol{\mathcal{A}} \in Fo$ analog wie $(\mathbf{A}^{(IZN)})^{**}$ in Beziehung zu $\mathbf{A}$ definiert sei). Die für $f \in POLYLIN$ notwendige (und für einen Beweis hier wesentliche) Eigenschaft von f, linear-beschränkt zu sein, läßt sich durch eine genaue Abschätzung der Länge von $(\mathbf{A}^{(IZN)})^{**}$ in Abhängigkeit von $|\mathbf{A}|$ (und insbesondere nur in Abhängigkeit von $\left|\mathbf{A}^{(IZN)}\right|$) einsehen bzw. beweisen.

$\diamondsuit$

Satz 2.6.4. *(i) Es gibt ein $d_2 \in \mathbb{R}$, $d_2 > 0$ so, daß $PreAN \in DSpace\left(2^{2^{d_2 n}}\right)$.*

(ii) Es gibt ein $c_1 \in \mathbb{R}$, $c_1 > 0$ so, daß $PreAZ \notin NTime\left(2^{2^{c_1 n}}\right)$.

Beweis. Seien $PreAZ^{((M))}$, $PreAN^{((M))}$ wie in der Präzisierung zu Lemma 2.6.3 (der Index $^{((M))}$ wird im Beweis hier der Kürze halber immer weggelassen); insbesondere sei Σ das dort festgelegte Formelalphabet dieser Theorien.

Zum Beweis wird die $\leq_{pl}$-Reduzierbarkeit $Thm_{PreAN} \leq_{pl} Thm_{PreAZ}$ aus Lemma 2.6.3 bei der Übertragung der oberen Schranke für $PreAZ$ aus Satz 2.6.1 zur oberen Schranke für $PreAN$ in Aussage (i) und bei der Übertragung der unteren Schranke für $PreAN$ aus Satz 2.6.2 zur unteren Schranke für $PreAZ$ in Aussage (ii) verwendet.

Wegen $Thm_{PreAN} \leq_{pl} Thm_{PreAZ}$ (vgl. dazu Lemma 2.6.3) existiert $g : \Sigma^* \to \Sigma^*$ so, daß $g \in POLYLIN$ und eine deterministische IOTM M, die g berechnet, sowie $C, D \in \mathbb{N}$ und $p \in \mathbb{N}_0[x]$ existieren, mit der Eigenschaft, daß für alle $x \in \Sigma^*$ gilt:

$$\begin{aligned} x \in Thm_{PreAN} \ &\Leftrightarrow\ g(x) \in Thm_{PreAZ}\ , \\ |g(x)| &\leq C \cdot |x|\ , \\ RZ_M(x) &\leq p(|x|)\ , \\ SP_M(x) &\leq D \cdot |x|\ . \end{aligned} \tag{2.26}$$

Seien g, M, C, D entsprechend gewählt.

ad (i): Wegen Satz 2.6.1 gibt es eine deterministische IOTM M_1 mit Eingabealphabet Σ, die für ein $d_1 \in \mathbb{R}$, $d_1 > 0$ die Sprache Thm_{PreAZ} mit Speicherplatzschranke $2^{2^{d_1 n}}$ akzeptiert; seien M_1 und d_1 entsprechend gewählt.

Wird nun mit Hilfe von M und M_1 eine deterministische IOTM M_2 mit Eingabealphabet Σ konstruiert, die im wesentlichen der Hintereinanderausführung $M_1 \circ M$ entspricht[41], so akzeptiert M_2 genau Thm_{PreAN}, es gilt dann nämlich für alle $x \in \Sigma^*$:

$$\begin{aligned} M_2 \text{ akzeptiert } x \quad &\Longleftrightarrow \\ &\Longleftrightarrow \quad M_1 \text{ akzeptiert } g(x) \\ &\Longleftrightarrow \quad g(x) \in Thm_{PreAZ} \\ &\Longleftrightarrow \quad x \in Thm_{PreAN} \ . \end{aligned} \tag{2.27}$$

(Wegen der Konstruktion von M_2, $L(M_1) = Thm_{PreAZ}$ und (2.26)). Der Speicherplatzbedarf von M_2 für Eingabewort $x \in Thm_{PreAN}$ kann nun auf folgende Weise abgeschätzt werden: Es gilt für alle $d_2 \in \mathbb{R}$, $d_2 > 0$ mit $d_2 > d_1 \cdot C$ und $D' := C + D$ [42] für $x \in Thm_{PreAN}$

$$\begin{aligned} SP_{M_2}(x) \leq \ & D' \cdot |x| + SP_{M_1}(g(x)) \leq_{\text{ae}} \\ \leq_{\text{ae}} & D' \cdot |x| + 2^{2^{d_1 |g(x)|}} \qquad \leq \\ \leq \ & D' \cdot |x| + 2^{2^{d_1 C |x|}} \qquad \leq_{\text{ae}} 2^{2^{d_2 |x|}} \end{aligned}$$

(wegen (2.26), der Konstruktion von M_2, der Annahme über die Speicherplatzschranke von M_1 zur Erkennung von Thm_{PreAZ} und einer einfachen Eigenschaft der verwendeten Exponentialfunktion).

Damit folgt aber zusammen mit (2.27), daß M_2 die Sprache Thm_{PreAN} mit Speicherplatzschranke $2^{2^{d_2|x|}}$ für $d_2 \in \mathbb{R}$, $d_2 > C \cdot d_1$ akzeptiert. Das bedeutet weiters für ein solches d_2, daß $Thm_{PreAN} \in DSpace(2^{2^{d_2 n}})$ gilt, was der Gültigkeit der hier immer so verstandenen Präzisierung von (i) entspricht.

ad (ii): Wegen Satz 2.6.2 existiert ein $c_2 \in \mathbb{R}$, $c_2 > 0$ so, daß

$$Thm_{PreAN} \notin NTime(2^{2^{c_2 n}}) \tag{2.28}$$

[41] Hiermit ist mit „im wesentlichen“ gemeint, daß M_2 so konstruiert wird: M_2 geht für Eingabewort $x \in \Sigma^*$ zur Berechnung von $f(x)$ zuerst wie M vor, schreibt $f(x)$ jedoch nicht auf das Ausgabeband, sondern auf ein dafür vorgesehenes leeres Arbeitsband und simuliert dann auf neuen, für den Ablauf von M bisher nicht benützten Arbeitsbändern M_1 so, daß jenes Arbeitsband, auf dem nun $f(x)$ steht, zum Zweck der Ausführung bzw. Simulation von M_1 als Eingabeband angesehen wird.

[42] Wegen der Konstruktion von M_2 muß nun die Länge der Ausgabe $f(x)$ von M in den von M_2 zur Erkennung von x benötigten Speicherplatz eingerechnet werden.

gilt; sei $c_2 \in \mathbb{R}$, $c_2 > 0$ entsprechend gewählt.

Werde im folgenden zeigen, daß die Annahme

$$Thm_{PreAZ} \in NTime(2^{2^{c_1 n}}) \ \& \ c_1 < \frac{c_2}{C} \ \& \ c_1 \in \mathbb{R} \tag{2.29}$$

für $c_1 \in \mathbb{R}$, $c_1 > 0$ auf einen Widerspruch zu (2.28) führt. Hierfür sei nun vorerst dazu also angenommen, daß (2.29) für ein $c_1 \in \mathbb{R}$, $c_1 > 0$ gilt.

Dann existiert eine nichtdeterministische IOTM M_1, die Thm_{PreAZ} mit Rechenzeitschranke $2^{2^{c_1 n}}$ akzeptiert. Durch eine analoge Vorgehensweise wie in (i) (mit dem Unterschied, daß es sich bei M_1 und M_2 nun um nichtdeterministische IOTM's handelt und hier Interesse an deren Rechenzeit besteht) kann zu M_1 mit Hilfe von M eine nichtdeterministische IOTM M_2 als Hintereinanderausführung von M_1 nach M konstruiert werden, die genau Thm_{PreAN} akzeptiert und für deren Rechenzeit für Eingabewörter $x \in Thm_{PreAN}$ gilt:

$$\begin{aligned} Min\text{-}RZ_{M_2}(x) \leq \quad & p(|x|) + Min\text{-}RZ_{M_1}(g(x)) \leq_{\text{ae}} \\ \leq_{\text{ae}} \ & p(|x|) + 2^{2^{c_1 |f(x)|}} \qquad\qquad \leq \\ \leq \quad & p(|x|) + 2^{2^{c_1 C |x|}} \qquad\qquad \leq_{\text{ae}} \ 2^{2^{c_2 |x|}} \end{aligned} \tag{2.30}$$

(wegen der Konstruktion von M_2 und (1), wegen der Rechenzeitschranke von M_1 zur Erkennung von Thm_{PreAZ}, wegen (1) und wegen erneut einer einfachen Eigenschaft der verwendeten Exponentialfunktion und $c_1 \cdot C < c_2$ (vgl. (2.29))).

Da M_2 die Sprache Thm_{PreAN} akzeptiert, muß aber wegen (2.28) andererseits

$$2^{2^{c_2 |x|}} <_{io} Min\text{-}RZ_{M_2}(x) \qquad (x \in Thm_{PreAN}) \tag{2.31}$$

gelten, was aber in offensichtlichem Widerspruch zu (2.30) steht.

Deshalb muß nun (2.29) verworfen werden, woraus

$$\left(c_1 < \frac{c_2}{C} \Rightarrow Thm_{PreAZ} \notin NTime(2^{2^{c_1 n}}) \right) \qquad \text{(für alle } c_1 \in \mathbb{R},\ c_1 > 0)$$

folgt. Hiermit ist nun aber die Existenz eines $c_1 \in \mathbb{R}$, $c_1 > 0$ mit $PreAZ \notin$ $\notin NTime(2^{2^{c_1 n}})$, also (ii), gezeigt, falls man darunter erneut präzisiert genau diese Existenz von $c_1 \in \mathbb{R}$, $c_1 > 0$ mit $Thm_{PreAZ} \notin NTime(2^{2^{c_1 n}})$ versteht.

□

Die im Beweis zu Satz 2.6.4 erfolgte Übertragung von unteren und oberen Schranken für die Entscheidungskomplexität von Theorien mit Hilfe von $\leq_{pl}$-Reduktionen ist ein Spezialfall des folgenden (in [FeRa79] ungefähr so dargestellten) Lemmas, das sich in allgemeinerer Weise auf Komplexitätsschranken und Komplexitätsklassen für Erkennung von formalen Sprachen bezieht.

Lemma 2.6.5. *Seien $L_1 \subseteq \Sigma_1^*$, $L_2 \subseteq \Sigma_2^*$ zwei Sprachen, für die $L_1 \leq_{pl} L_2$ [bzw. $L_1 \leq_{log-lin} L_2$] gilt. Sei $f\colon \mathbb{N}_0 \to \mathbb{N}_0$ monoton wachsend. Dann gilt:*

(i) Es gibt $c, d \in \mathbb{R}$, $c, d > 0$ und ein Polynom $p(n)$, so, daß

$$\begin{array}{lcl}
L_2 \in DTime(f(n)) & \Rightarrow & L_1 \in DTime(f(cn) + p(n)) \,; \\
L_2 \in DSpace(f(n)) & \Rightarrow & L_1 \in DSpace(f(cn) + dn) \\
 & & \quad [\ bzw.\ L_1 \in DSpace(f(cn) + d \log n)\ ] \,; \\
L_2 \in NTime(f(n)) & \Rightarrow & L_1 \in NTime(f(cn) + p(n)) \,; \\
L_2 \in NSpace(f(n)) & \Rightarrow & L_1 \in NSpace(f(cn) + dn) \\
 & & \quad [\ bzw.\ L_1 \in NSpace(f(cn) + d \log n)\ ] \,.
\end{array}$$

(ii) Umgekehrt gibt es ein Polynom $p(n)$ und Konstanten $c, d \in \mathbb{R}$, $c, d > 0$ so, daß:

$$\begin{array}{lcl}
L_1 \notin DTime(f(n) + p(n)) & \Rightarrow & L_2 \notin DTime(f(cn)) \,; \\
L_1 \notin DSpace(f(n) + dn) & & \\
\quad [\ bzw.\ L_1 \notin DSpace(f(n) + d \log n)\ ] & \Rightarrow & L_2 \notin DSpace(f(cn)) \,; \\
L_1 \notin NTime(f(n) + p(n)) & \Rightarrow & L_2 \notin NTime(f(cn)) \,; \\
L_1 \notin NSpace(f(n) + dn) & & \\
\quad [\ bzw.\ L_1 \notin NSpace(f(n) + d \log n)\ ] & \Rightarrow & L_2 \notin NSpace(f(cn)) \,.
\end{array}$$

Hinweis zum Beweis. Die Aussagen von (i) sind analog zu Satz 2.6.4, (i), die von (ii) analog zu Satz 2.6.4, (ii), zu zeigen. Der Beweis von Satz 2.6.4, (i), erforderte nämlich den Nachweis von

$$L_2 \in DSpace(f(n)) \quad \Rightarrow \quad L_1 \in DSpace(f(cn) + dn)$$

für $f(n) := 2^{2^{d_1 n}}$ (d_1 wie von Satz 2.6.4,(i), behauptet), für $L_1 := Thm_{PreAN}$ und $L_2 := Thm_{PreAZ}$ und unter der durch Lemma 2.6.3 abgestützten Voraussetzung $L_1 \leq_{pl} L_2$ zusammen mit wegen dieser Reduzierbarkeit existierenden, entsprechenden $c, d \in \mathbb{R}$, $c, d > 0$. Der Beweis von Satz 2.6.4, (ii), erforderte den Nachweis von

$$L_1 \notin NTime(f(n) + p(n)) \quad \Rightarrow \quad L_2 \notin NTime(f(cn))$$

mit L_1, L_2 wie oben, $f(n) := 2^{2^{c_2' n}}$ ($0 < c_2' < c_2$, c_2 wie von Satz 2.6.2 behauptet) und bestimmten, mit der $\leq_{pl}$-Reduktion $L_1 \leq_{pl} L_2$ in Zusammenhang stehenden $p \in \mathbb{N}_0[x]$ und $c \in \mathbb{R}$, $c > 0$ (c der Kehrwert der in der Forderung der linearen Beschränktheit der Übertragungsfunktion g (bzgl. $L_1 \leq_{pl} L_2$ *via* g) vorkommenden multiplikativen Konstanten). $\diamondsuit$

Die bislang wohl genaueste Klassifizierung der Entscheidungskomplexität von $PreAN$ und $PreAZ$ (bzw. der entsprechenden semantisch definierten Theorien $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$ und $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$) geht auf L. Berman ([Be80]) zurück und verweist auf eine Komplexitätsklasse bezüglich alternierender Turingmaschinen. Es ist dies die Klasse $ATimeAlter(EEXL, LIN)$ von Sprachen, die von solchen alternierenden Turingmaschinen akzeptiert werden können, deren Rechenzeit durch eine doppelt-exponentiell-lineare Funktion $2^{2^{dn}}$ $(d > 0)$ beschränkt ist und für die die Anzahl der Alternationen (ebenfalls in Abhängigkeit von der Eingabelänge) linear beschränkt ist. Für diese Klasse gilt (nach einem schon erwähnten Ergebnis in [CKS81])

$$\begin{aligned} DTime(EEXL) \subseteq NTime(EEXL) \subseteq ATimeAlter(EEXL, LIN) \subseteq \\ \subseteq DSpace(EEXL) \ , \end{aligned} \tag{2.32}$$

wobei es sich bei der Behauptung, daß jede der obigen Mengeninklusionen eine echte Inklusion $\subsetneq$ ist, zum aktuellen Zeitpunkt wohl immer noch um eine unbewiesenen Vermutung handeln dürfte.

Dasselbe dürfte im gleichen Ausmaß für die verwandte Kette

$$\begin{aligned} 2\text{-}EXPTIME \subseteq 2\text{-}NEXPTIME \subseteq 2\text{-}EH \subseteq ATimeAlter(EEXP, LIN) \subseteq \\ \subseteq 2\text{-}EXPSPACE = ATime(EEXP) \end{aligned} \tag{2.33}$$

gelten, wobei die Bezeichnungen

$$\begin{aligned} \mathbf{2\text{-}EXPTIME} &:= DTime(EEXP) \ , \\ \mathbf{2\text{-}NEXPTIME} &:= NTime(EEXP) \ , \\ \mathbf{2\text{-}EH} &:= ATimeAlter(EEXP, CON) \ , \\ \mathbf{2\text{-}EXPSPACE} &:= DSpace(EEXP) \ , \end{aligned}$$

gelten.

Das Ergebnis von Berman in [Be80] erlaubt es nun, die Komplexität der Entscheidung von $PreAN$ bzw. von $PreAZ$ mit den beiden Klassen $ATimeAlter(EEXL, LIN)$ und $ATimeAlter(EEXP, LIN)$ gleichermaßen zu identifizieren:

Satz 2.6.6 (Berman, 1979). *$PreAN$, $PreAZ$ [43] sind $ATimeAlter(EEXL, LIN)$-vollständig (bezüglich $\leq_{pl}$-Reduktionen) und $ATimeAlter(EEXP, LIN)$-vollständig (bezüglich $\leq_{pl}$- und $\leq_p$-Reduktionen).*

[43] Wird Satz 2.6.6 nur für eine der beiden Theorien $PreAN$, $PreAZ$ gezeigt, so ist wegen Lemma 2.6.3 klar, daß sich die Vollständigkeit in der betrachteten Klasse unter $\leq_{pl}$- und $\leq_p$-Reduktionen sofort auch auf die jeweils andere Theorie überträgt. – Da sich [Be80] auf $PreAN$ (bzw. auf $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$,

Es scheint also so zu sein, daß der Entscheidungskomplexität von $PreAN$ und $PreAZ$ eine im durch $NTime(EEXL)$ und $DSpace(EEXL)$ eingegrenzten Bereich liegende, eindeutig[44] bestimmte Komplexitätsklasse entspricht, die danach also zwischen jenen Klassen liegt, auf die von Satz 2.6.1 und Satz 2.6.2 beschriebenen unteren und oberen Schranken bezüglich sequentiellen Turingmaschinen verweisen.

Nach Satz 2.6.6 gilt die Vollständigkeit von $PreAN$ und $PreAZ$ weiters sogar auch bezüglich der größeren Klasse $ATimeAlter(EEXP, LIN)$ bezüglich $\leq_p$-Reduktionen[45]. Diese Klasse ist umgekehrt durch die Entscheidungskomplexität der beiden Theorien der Presburger Arithmetik zwischen $2-EH$ und $2-EXPSPACE$ wiederum weitgehend genau charakterisiert und bestimmt.

Es ist an dieser Stelle erwähnenswert und eine bemerkenswerte Tatsache, daß sich eine Exponentialstufe unterhalb der Entscheidungskomplexität von $PreAN$ und $PreAZ$, also im Bereich zwischen einfach-exponentiell-beschränkter (nichtdeterministischer Turing-) Rechenzeit und einfach-exponentiell-beschränktem (deterministischem oder nichtdeterministischem Turing-) Speicherplatzbedarf, eine völlig analoge Situation für die ebenfalls vollständige Theorie $RA := Th(\langle \mathbb{R}; 0, 1, + \rangle)$ der Additionsarithmetik reeller Zahlen zeigt (die Vollständigkeit von RA folgt aus der von A. Tarski (ungefähr um 1930) gezeigten Vollständigkeit der Theorie $RA := Th(\langle \mathbb{R}; 0, 1, +, . \rangle)$, der später so genannten *Tarski Algebra*). Die Entscheidungskomplexität dieser Theorie wird ebenfalls in den Arbeiten [FeRa73], [FiR74] und [Be80] (bzw. [BKR84]) behandelt und weitgehend genau ermittelt.

[FeRa73] erzielten ein Ergebnis der Gestalt $RA \in DSpace(2^{dn})$ für ein reelles $d > 0$, also die Existenz einer einfach-exponentiell-linearen oberen Schranke bezüglich deterministischem Turing-Speicherplatzbedarf. [FiR74] konnten die Existenz eines reellen $c > 0$ mit $RA \notin NTime(2^{cn})$ beweisen, also den Nachweis für das Vorhandensein einer einfach-exponentiell-linearen unteren Schranke bezüglich nichtdeterministischer Turing-Rechenzeit für RA erbringen. [Be80] wiederum konnte die Vollständigkeit von RA in

---

$Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$bzw. $Th(\langle \mathbb{N}_0; + \rangle)$) bezieht, reicht zur Übertragung dieses Ergebnisses für $PreAZ$ die Aussage $PreAN \leq_{pl} PreAZ$ aus, also die einfach einzusehende Richtung in Lemma 2.6.3.

Die in Lemma 2.6.3 auf logischem Weg (wobei spezielle Eigenschaften der betrachteten arithmetischen Theorien verwendet wurden) gezeigte Richtung $PreAZ \leq_{pl} PreAN$ folgt hingegen *auch* aus dem Ergebnis von Berman unter der Verwendung von $PreAZ \in ATime(EEXL, LIN)$, einer Aussage, die sich aus dem Beweis für Satz 2.6.1 in [FeRa79] ergibt und auf die sich auch [Be80] für seinen Beweis wesentlich bezieht (bzw. auf eine $PreAN$ betreffende analoge, daraus sofort folgende Aussage) (vgl. hierzu auch Fußnote 38). – Dabei wird eine $\leq_{pl}$-Reduktion von $PreAZ$ auf $PreAN$ allerdings tatsächlich nur auf sehr indirektem Weg garantiert (die aber freilich—jedenfalls theoretisch—dennoch auch explizit gemacht werden könnte).

[44](Eindeutig etwa als jene Klasse, die die formale Sprache $L = Thm_{PreAN}$ (bzw. die Sprache $L = Thm_{PreAZ}$) zugleich mit allen Sprachen L', für die $L' \leq_{pl} L$ gilt, enthält.)

[45]Die Übertragung der Vollständigkeit von $PreAN$ und von $PreAZ$ in $ATimeAlter(EEXL, LIN)$ unter $\leq_{pl}$-Reduktionen (und damit auch unter $\leq_p$-Reduktionen) zur Vollständigkeit in der Klasse $ATimeAlter(EEXP, LIN)$ bezüglich $\leq_p$-Reduktionen *dürfte* [hierbei interpretiere ich—ohne ein vielleicht nötiges, sehr viel näheres Verständnis—Passagen in [Jo90], C.G.] durch die Anwendung von "padding"-Methoden folgen.

der Klasse $ATimeAlter(EXL, LIN)$ (bezüglich $\leq_{pl}$-Reduktionen, und damit automatisch auch bezüglich $\leq_p$-Reduktionen) zeigen (eine weitere Darstellung dieses Ergebnisses findet sich in [BKR84]).

Insgesamt ergibt sich wieder ein zu (2.32) analoges Bild

$$\begin{aligned} DTime(EXL) \subseteq NTime(EXL) \subseteq ATimeAlter(EXL, LIN) \subseteq \\ \subseteq DSpace(EXL) \ , \end{aligned} \tag{2.34}$$

wobei erneut nicht bekannt ist, ob alle Inklusionen in dieser Kette—wie überwiegend angenommen wird—wirklich echte Inklusionen sind ($DTime(EXL) \neq NTime(EXL)$ würde z.B. aus $\mathcal{P} \neq \mathcal{NP}$ folgen, nach [Jo90] ist aber noch kein Beweis für einen solchen Schluß in umgekehrter Richtung gefunden worden). Die Entscheidungskomplexität von RA dürfte also wieder eine Komplexitätsklasse bezüglich alternierender Turingmaschinen zwischen $NTime(EXL)$ und $DSpace(EXL)$ (jenen Klassen, auf die die obere und die untere Schranke für RA bezüglich sequentiellen Turingmaschinen verweisen) eindeutig bestimmen.

Bezüglich einer Vergröberung (in etwa jeweils polynomialem Ausmaß) ergibt sich wieder eine zu (2.33) analoge Situation

$$\begin{aligned} EXPTIME \subseteq NEXPTIME \subseteq EH \subseteq ATimeAlter(EXP, LIN) \subseteq \\ \subseteq EXPSPACE = ATime(EXP) \end{aligned} \tag{2.35}$$

mit

$$\begin{aligned} \boldsymbol{EXPTIME} &:= DTime(EXP) \ , \\ \boldsymbol{NEXPTIME} &:= NTime(EXP) \ , \\ \boldsymbol{EH} &:= ATimeAlter(EXP, CON) \ , \\ \boldsymbol{EXPSPACE} &:= DSpace(EXP) \ , \end{aligned} \tag{2.36}$$

wobei die Theorie RA erneut auch in $ATimeAlter(EXP, LIN)$ (bezüglich $\leq_p$-Reduktionen) vollständig ist[46]. EH steht in (2.36) im übrigen für die „exponentielle Hierarchie“, eine zur polynomialen Hierarchie PH analog definierte Klasse (vgl. z.B. [Jo90]), die durch den Aufwand von alternierenden Turingmaschinen mit exponentieller Rechenzeit und endlich vielen Alternationen charakterisiert werden kann (d.h. es gilt: $EH = ATimeAlter(EXP, CON)$, vgl. z.B. [Jo90]).

Für die von M. Presburger ursprünglich betrachtete Theorie TAZ überträgt sich, da $PreAZ$ Erweiterung von TAZ ist und daher jedes Entscheidungsverfahren für $PreAZ$ auch

[46] Dies *dürfte* erneut aus der Vollständigkeit von RA in $ATimeAlter(EXL, LIN)$ bezüglich $\leq_p$-Reduktionen durch die Anwendung eines “padding”-Argumentes folgen [wenn ich dabei abermals (vgl. Fußnote 45) einem Zusammenhang in [Jo90] richtig folge, C.G.].

alle Formeln von TAZ entscheidet, die $PreAZ$ betreffende obere Schranke von zweifach-exponentiell-linearer Gestalt bezüglich deterministischer Turing-Rechenzeit sofort auch auf TAZ.

Andererseits ist durch die Arbeit [FiR74] von Fischer und Rabin noch nicht geklärt, ob eine zweifach-exponentiell-lineare untere Schranke auch für die Entscheidungskomplexität von TAZ bezüglich nichtdeterministischer Rechenzeit existiert. (Der von [FiR74] für $PreAN$ geführte Beweis läßt sich allerdings schnell auch auf $PreAZ$ übertragen, obwohl eine solche Beweisübertragung im Licht von Satz 2.6.4, (ii) unnötig ist). Fischer und Rabin haben sich mit dieser einfachsten Theorie der Additionsarithmetik nicht beschäftigt, ihre allgemeineren Ergebnisse würden für TAZ nur eine einfach-exponentiell-lineare untere Schranke bezüglich nichtdeterministischer Turing-Rechenzeit implizieren.

Dennoch gelingt es, das Ergebnis in [FiR74] für $PreAN$ auch auf TAZ mittels einer Variation[47] des dort für $PreAN$ bzw. für $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ geführten Beweises zu übertragen (vgl. Kapitel 3, Abschnitt 3.7).

Satz 2.6.7. *Es gibt ein $c_3 \in \mathbb{R}$, $c > 0$ so, daß $TAZ \notin NTime(2^{2^{c_3 n}})$.*

(Diese Aussage entspricht im wesentlichen Satz 3.7.1, Kapitel 3, und wird dort darin weitergehend präzisiert.)

Es sei an dieser Stelle als Gedanke zur möglichen Abrundung dieses Ergebnisses noch bemerkt: Der Beweis für die Vollständigkeit von $PreAN$ in $ATimeAlter(EXP, LIN)$ bzgl. $\leq_{pl}$-Reduktionen in [Be80] (bzw. dessen ungefähre Darstellung dort) legt [mir, C.G.] die Vermutung nahe, daß sich diese Vollständigkeitseigenschaft auch auf TAZ übertragen lassen *könnte*. Und zwar deshalb, weil sich [Be80] dabei in wesentlichem Ausmaß auf die in [FiR74] für $PreAN$ (bzw. für $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$) entwickelten Methoden bezieht, die—in etwas variierter Form—beim Beweis von der Satz 2.6.7 entsprechenden Aussage Satz 3.7.1 in Abschnitt 3.7, Kapitel 3, auch für TAZ angewendet werden konnten. – Diese Vermutung müßte jedoch ausführlich überprüft werden und würde als Folgerung die Existenz einer (aus rein logischer Sicht auf diese Theorien zuerst wohl recht unanschaulichen) $\leq_{pl}$-Reduktion von $PreAZ$, einer Theorie der Additionsarithmetik ganzer Zahlen mit Ordnungssymbol, auf TAZ, eine Theorie der Addition ganzer Zahlen, in der ein Ordnungssymbol substantiell fehlt, nach sich ziehen.

[47] Die Andeutung einer Beweisidee für $MULT := SkA = Th(\langle \mathbb{N}_0; . \rangle) \notin NTime\left(2^{2^{2^{c_4 n}}}\right)$ für ein reelles $c_4 > 0$ in [FiR74] legte [mir, C.G.] eine solche Variation nahe und andererseits die begründete Vermutung, [FiR74] hätten die Existenz der TAZ betreffenden unteren Schranke aus Satz 2.6.7 ebenfalls ausgesprochen, wenn ihnen dieses Problem vorgelegt worden bzw. vor Augen gestanden wäre.

Kapitel 3

Aufarbeitung der Arbeit [FiR74]

Im Mittelpunkt dieses Kapitels steht eine Aufarbeitung der Arbeit "Super-Exponential Complexity of Presburger Arithmetic" von M.J. Fischer und M.O. Rabin (vgl. [FiR74] und den Anhang A dieser Arbeit) aus dem Jahr 1974. Darin ist von den beiden Autoren als eines der ersten Ergebnisse über die logischen Theorien inhärente Entscheidungskomplexität die Schwer-Entscheidbarkeit von zwei bekannten entscheidbaren logischen Theorien nachgewiesen worden. Und zwar erfolgte das für die Theorie (1. Ordnung) $RA := Th(\langle \mathbb{R}; 0, 1, + \rangle)$ der Additionsarithmetik auf den reellen Zahlen (deren Entscheidbarkeit aus einem weitergehenden Ergebnis von A. Tarski aus den 30er-Jahren folgt) und für die Theorie (1. Ordnung) $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ der Presburger Arithmetik natürlicher Zahlen (die zu der axiomatisierten Theorie $PreAN_1$ äquivalent ist, vgl. Abschnitt 2.3, und deren Entscheidbarkeit auf den in Kapitel 2 behandelten Resultaten von M. Presburger, 1928/29, beruht). Die dabei von [FiR74] erzielten unteren Schranken für die Entscheidungskomplexität dieser Theorien gelten bezüglich nichtdeterministischer Turing-Rechenzeit und sind im Fall von RA von einfach-exponentiell-linearer Gestalt 2^{cn} (für ein reelles $c > 0$) und im Fall von $PreAN_1$ bzw. $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ bzw. $PreAN$ (auf diese Theorie kann das Ergebnis sofort auch erweitert werden) von doppelt-exponentiell-linearer Gestalt $2^{2^{cn}}$ (für ein reelles $c > 0$).

Aus diesen Schwer-Entscheidbarkeits-Aussagen konnten [FiR74] dann ziemlich unmittelbar auch Folgerungen für die Längen kürzester Beweise in allen leicht-erkennbaren (: d.h. in polynomialer Rechenzeit erkennbaren) Axiomatisierungen dieser Theorien ableiten (und damit wohl in den allermeisten konkreten, logisch sinnvollen Axiomatisierungen dieser Theorien). D.h. es wurde auch auf die Existenz unterer Schranken für die Längen kürzester Beweise in allen solchen Axiomatisierungen dieser Theorien geschlossen und zwar unteren Schranken von jeweils der selben Gestalt (die als Funktionen jedoch etwas langsamer wachsen) wie die für die Entscheidungskomplexität der entsprechenden Theorie zuvor erzielten. – Diese die Längen kürzester Beweise betreffenden Aussagen wurden dabei gerade

durch die Tatsache ermöglicht, daß die zuvor bewiesenen, die Schwer-Entscheidbarkeit der jeweiligen Theorie ausdrückenden Ergebnisse gerade bezüglich der Rechenzeit *nichtdeterministischer* Turingmaschinen Gültigkeit besitzen.

Zuletzt werden in [FiR74] als Verallgemeinerungen der geschilderten Aussagen mit Erweiterungen der vorgestellten Methoden ähnlich-gestaltige Komplexitätsaussagen über Theorien von bestimmten algebraischen Strukturen ausgesprochen und die dafür nötigen Beweisideen grob umrissen. Dabei wurde weiters auch eine doppelt-exponentiell-lineare untere Schranke für die Entscheidungskomplexität der entscheidbaren (jedoch nicht vollständigen) Theorie (1.Ordnung) FAG der endlichen abelschen Gruppen angekündigt sowie eine dreifach-exponentiell-lineare untere Schranke bezüglich nichtdeterministischer Turing-Rechenzeit für die Theorie $Th(\langle \mathbb{N}_0; . \rangle)$ bzw. für die Skolem-Arithmetik SkA (vgl. Abschnitt 2.5), die [FiR74] mit $MULT$ bezeichnen.

Die Aufarbeitung der Arbeit [FiR74] umfaßt hier hauptsächlich nur den die Ergebnisse der Entscheidungskomplexität der Theorien RA und $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ betreffenden (wesentlichen) Teil, nicht jedoch jenen (kleineren), der sich auf die Aussagen über die Komplexität kürzester Beweise in einfach-erkennbaren Axiomatisierungen dieser Theorien bezieht[1] (diese Aussagen und die dafür notwendigen Begriffe werden aber bei der Zusammenstellung der Hauptergebnisse in [FiR74] in Abschnitt 1 behandelt). Es wird dabei versucht, die Komplexitätsaussagen und -beweise in [FiR74] im Rahmen des in Kapitel 1 über Entscheidungskomplexität im allgemeinen und in Kapitel 2 über konkrete Axiomatisierungen der Presburger Arithmetik Dargestellten zu betrachten.

Zusätzlich zur Darstellung des Hauptteils der Komplexitätsaussagen und -beweise aus [FiR74] wird hier in Abschnitt 7 außerdem die doppelt-exponentiell-lineare untere Schranke für die Entscheidungskomplexität von $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ (bzw. von $PreAN_1$ und $PreAN$, sowie im weiteren auch von $PreAZ$ und $Th(\langle \mathbb{Z}; 0, 1, +, < \rangle)$) bzgl. nichtdeterministischer Turing-Rechenzeit auch auf die von M. Presburger ursprünglich betrachtete Theorie TAZ (bzw. auf deren semantisch definiertes Äquivalent $Th(\langle \mathbb{Z}; 0, 1, + \rangle)$) übertragen. Diese Theorie ist—wie in Abschnitt 2.1 bewiesen—logisch schwächer als $PreAZ$, da in ihr ein Ordnungssymbol $<$ nicht auf definitorische Weise so eingeführt werden kann, daß sich das Modell $\langle \mathbb{Z}; 0, 1, + \rangle$ von TAZ zu einem Modell $\langle \mathbb{Z}; 0, 1, +, < \rangle$, (wobei hierin $<$ für das in der gewöhnlichen Bedeutung verwendete Symbol „kleiner“ steht) für die entsprechende Erweiterungstheorie von TAZ erweitern ließe. – Der in [FiR74] für $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ geführte Komplexitätsbeweis (der ebenso für $PreAN$ geführt werden kann) läßt sich nun jedoch—eben wegen des (*wesentlichen*) Fehlens eines Ordnungssymbols in TAZ—nicht direkt auch auf TAZ übertragen (jedoch ziemlich unmittelbar schon auf $PreA\underline{Z}$). Weiters

[1] Für diese inhaltliche Beschränkung in der Aufarbeitung der Arbeit [FiR74] waren Umfangs- und auch zeitliche Gründe maßgebend. – :Im ganzen also in der Komplexitätstheorie auch behandelbare Fragen etwa von der Gestalt *Time versus Space* und *Time and Space*, wie R. Reischuk in der Einleitung zu [Rei90] eine beim Schreiben von Arbeiten, Büchern, Publikationen, etc. wohl allgemein bestehende Problematik durch die Zuhilfenahme komplexitätstheoretischer Begriffe und Problemstellungen recht treffend charakterisiert.

würde die in [FiR74] für Theorien bestimmter algebraischer Strukturen durchgeführte Verallgemeinerung ihrer Resultate nur eine einfach-exponentiell-lineare untere Schranke für die Entscheidungskomplexität von TAZ bzgl. nichtdeterministischer Turing-Rechenzeit implizieren.

Die hier vorgestellte Übertragung der in [FiR74] für $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ (bzw. in der Terminologie von Kapitel 2 etwa auch: für $PreAN_1$) erzielten doppelt-exponentiell-linearen unteren Schranke bzgl. nichtdeterministischer Turing-Rechenzeit auch auf TAZ verdankt sich aber im wesentlichen einer am Ende von [FiR74] als Skizze für einen Beweis von $SkA, MULT \notin NTime(2^{2^{2^{cn}}})$ (für ein reelles $c > 0$) dargestellten Idee.

3.1 Zusammenstellung der Hauptresultate aus [FiR74]

Die zentralen Ergebnisse in [FiR74] beziehen sich auf die entscheidbaren und vollständigen Theorien der Presburger Arithmetik (natürlicher Zahlen) und der Additionsarithmetik RA auf den reellen Zahlen (wobei $RA := Th(\langle \mathbb{R}; 0, 1, + \rangle)$) und behaupten die Existenz von mindestens exponentiellen unteren Schranken für die Entscheidungskomplexität dieser Theorien bezüglich der Rechenzeit nichtdeterministischer Turingmaschinen. Dabei haben diese unteren Schranken im Fall von RA einfach-exponentiell-lineare Gestalt 2^{dn} (für ein $d \in \mathbb{R}$, $d > 0$) und im Fall der Theorien der Presburger Arithmetik natürlicher Zahlen (etwa $PreAN$ oder $Th(\langle \mathbb{R}; 0, 1, + \rangle)$ bzw. (der dazu äquivalenten Theorie) $PreAN_1$) doppelt-exponentiell-lineare Gestalt $2^{2^{cn}}$ (für ein $c \in \mathbb{R}$, $c > 0$). Im letzteren Fall ist die erzielte Schranke also von „super-exponentieller" Gestalt, was zur Namensgebung für die Arbeit [FiR74] geführt hat.

Als wichtige Anwendung dieser Resultate konnten M. Fischer und M. Rabin unter wesentlicher Verwendung von Eigenschaften nichtdeterministischer Algorithmen (hier: nichtdeterministischer Turingmaschinen) auch zu unteren Schranken für die Längen der kürzesten Beweise in diesen Theorien gelangen; die dafür erzielten unteren Schranken sind von jeweils derselben Gestalt (jedoch mit kleineren, darin vorkommenden positiv-reellen Konstanten) wie die unteren Schranken für die Entscheidungskomplexität (bzgl. der Rechenzeit nichtdeterministischer Turingmaschinen) der betrachteten Theorie und gelten weiters nur für alle solchen Axiomatisierungen dieser Theorien, die „praktisch" und d.h. in polynomialer Rechenzeit erkennbar sind. Diese die Längen kürzester Beweise betreffenden Aussagen wurden dabei gerade durch die Tatsache ermöglicht, daß die zuvor bewiesenen, die Schwer-Entscheidbarkeit der jeweiligen Theorie ausdrückenden Ergebnisse gerade bezüglich der Rechenzeit *nichtdeterministischer* Turingmaschinen Gültigkeit besitzen.

Zuletzt werden in [FiR74] noch Resultate über die Entscheidungskomplexität anderer Theorien angekündigt und die Beweisideen dafür grob skizziert, wobei die wichtigsten Aussagen dabei sind: Eine doppelt-exponentiell-lineare unter Schranke (bzgl. nichtdeterministischer Turing-Rechenzeit) für die entscheidbare (und per def. vollständige) Theorie der Skolem-Arithmetik $SkA = Th(\langle \mathbb{N}_0, . \rangle)$, die [FiR74] mit $MULT$ bezeichnen.

Die die Entscheidungskomplexität der Theorien der Presburger Arithmetik natürlicher Zahlen betreffende Aussage der Super-Exponentialität (Theorem 1 in [FiR74]) läßt sich mit Hilfe der Begriffsbildungen und Bezeichnungen aus Kapitel 1 und Kapitel 2 z.B. so formulieren:

Satz 3.1.1. *T sei eine der Theorien $PreAN$, $PreAN_1$ oder $PreAN_0$ bzw. der dazu jeweils äquivalenten, semantisch definierten Theorien $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$, $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ oder $Th(\langle \mathbb{N}_0; + \rangle)$; $T^{((M))} = (\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ sei die als System von formalen Sprachen aufgefaßte Theorie T mit informatisch-sinnvoller Formelsyntax.*

Dann gilt: Es existiert ein $c \in \mathbb{R}$, $c > 0$ so, daß $2^{2^{cn}}$ eine untere Schranke für die Entscheidungskomplexität von T ist. Darüber hinaus kann ein $c \in \mathbb{R}$, $c > 0$ sogar so gewählt werden, daß

$$Thm_{T^{((M))}},\ \mathrm{co}{-}Thm_{T^{((M))}} \notin NTime\left(2^{2^{cn}}\right)$$

gilt[2]*.*

Es handelt sich bei Satz 1.1 um eine hier vorgestellte, im weiteren Verlauf dieser Aufarbeitung bewiesene Präzisierung der in [FiR74] für die Entscheidungskomplexität von Theorien der Presburger Arithmetik natürlicher Zahlen vorgestellten Aussage, nämlich von Theorem 1 in [FiR74]. Die inhaltliche Aussage von Satz 3.1.1 unterscheidet sich jedoch in einigen Punkten von der in Theorem 1 in [FiR74] ausgedrückten, die in Abschnitt 2 zusammengestellt und untersucht werden sollen. Dort wird versucht, zu begründen, daß die wesentliche Behauptung über die Existenz einer doppelt-exponentiell-linearen unteren Schranke für die Entscheidungskomplexität von Theorien der Presburger Arithmetik bezüglich der Rechenzeit nichtdeterministischer Turingmaschinen aus Theorem 1 in [FiR74] in Satz 3.1.1 formuliert und präzisiert worden ist.

Obwohl die sich auf die Längen kürzester Beweise in „einfach-angebbaren“ Axiomatisierungen für die hier behandelten arithmetischen Theorien beziehenden Komplexitätsaussagen in [FiR74] nicht Bestandteil dieser Aufarbeitung sind[3], sollen an dieser Stelle dennoch einige der dafür nötigen Begriffe kurz angesprochen und skizziert werden und weiters sollen noch einige Beobachtungen über die Anwendbarkeit des die Theorien der Presburger Arithmetik betreffenden Resultates für konkrete Axiomatisierungen einer solchen Theorie aus Kapitel 2 wiedergegeben werden.

Eine Präzisierung dieser die Beweislängen betreffenden Komplexitätsaussagen in [FiR74] erfordert eine genaue Festlegung davon, was unter einer einfach oder „praktisch“ zu erkennenden Axiomatisierung einer Theorie T zu verstehen ist. Eine solche Definition kann nun etwa dadurch geschehen, daß eine Axiomatisierung $T^{(ax)}$ einer formalisierten Theorie $T = (\Sigma_T, Fo_T, Thm_T)$ als 5-Tupel $T^{(ax)} = (\Sigma_T, Fo_T, Thm_T, Ax, Ru)$ mit bestimmten

[2] Mit „sogar so“ ist hier gemeint: Es existiert ein $c \in \mathbb{R}$, $c > 0$ so, daß *sowohl* $Thm_{T^{((M))}}$ *als auch* $\mathrm{co}{-}Thm_{T^{((M))}}$ nicht in $NTime(2^{2^{cn}})$ liegen, im Gegensatz dazu, daß nach Definition 1.5.1 die Folgerung „$2^{2^{cn}}$ ist untere Schranke für die Entscheidungskomplexität von T“ diese Aussage nur für eine dieser zwei Sprachen impliziert. (Wie man sich rasch klar macht, folgt das hier aus der Vollständigkeit der in Rede stehenden Theorien.)

[3] (genauer: weil ein diesbezüglicher Abschnitt letztlich aus Umfangsgründen ausgeklammert werden mußte)

Eigenschaften gesetzt bzw. als solches aufgefaßt wird; hierbei bezeichnet $Ax \subseteq Fo_T$ (mit im weiteren dann $Ax \subseteq Thm_T$) eine Menge von *Axiomen* und Ru eine endliche Menge von Schlußregeln $R \in Ru$ mit $R \subseteq (Fo_T)^{a(R)} \times Fo_T$, wobei Ax und alle $R \in Ru$ (total-) rekursive Mengen sind und $a\colon Ru \to \mathbb{N}$ eine Stelligkeitsfunktion für die Anzahl der Prämissen einer Schlußregel ist (die als Menge oder als Prädikat aufgefaßte Schlußregel $R \subseteq (Fo_T)^{a(R)} \times Fo_T$ drückt dabei die Ableitbarkeitseigenschaft für einzelne Formeln aus $a(R)$ Prämissen oder Voraussetzungen aus $(R \in Ru)$). – In dieser Formalisierung des Begriffes „Axiomatisierung" läßt sich nun für eine Zeichenkette $P \in (Fo_T \cup \{\$\})^+$ ($\$ ein Trennzeichen, $\$ \notin \Sigma_T$) exakt definieren, wann P einen *Beweis* einer Formel $\mathbf{A} \in Fo_T$ in $T^{(ax)}$ darstellt (dann nämlich, wenn P eine durch Trennzeichen getrennte Kette oder Liste von Formeln ist, deren jede entweder ein Axiom von $T^{(ax)}$ ist oder vermittels einer Schlußregel $R \in Ru$ aus $a(R)$ in P weiter links stehenden Formeln herleitbar ist, und wobei die letzte Formel in P gleich $\mathbf{A}$ ist).

Nun wird aber weiters von einer *Axiomatisierung* $T^{(ax)} = (\Sigma_T, Fo_T, Thm_T, Ax, Ru)$ einer Theorie $T = (\Sigma_T, Fo_T, Thm_T)$ noch gefordert, daß alle in $T^{(ax)}$ beweisbaren Formeln in Thm_T liegen; von einer *vollständigen* Axiomatisierung von T, daß auch die Umkehrung gilt. Unter einer *$\mathcal{P}$-erkennbaren Axiomatisierung* $T^{(ax)}$ wird eine solche Axiomatisierung verstanden, für die die Formelmenge Fo_T, die Axiomenmenge Ax und alle Schlußregeln $R \in Ru$ in deterministischer, polynomialer Turing-Rechenzeit erkannt, d.h. akzeptiert werden können, jeweils also in $\mathcal{P} = DTime(POL)$ liegen.

Die Länge eines Beweises P in einer Axiomatisierung $T^{(ax)}$ wird als die Symbollänge von P, also als die Anzahl der in P vorkommenden Symbole festgesetzt. Davon ausgehend kann unter einer unteren Schranke für die Längen der kürzesten Beweise in einer Axiomatisierung $T^{(ax)}$ einer Theorie T eine Funktion $f\colon \mathbb{N}_0 \to \mathbb{R}_0^+$ verstanden werden, für die gilt, daß es unendlich viele in $T^{(ax)}$ beweisbare Formeln $\mathbf{A}$ gibt, für die in $T^{(ax)}$ kein Beweis mit der Länge $\leq f(|\mathbf{A}|)$ existiert.

Mit Hilfe solcher Begriffsbildungen und Bezeichnungen lassen sich die in [FiR74] vorgestellten Beweislängen-Aussagen exakt darstellen. Im Fall der Theorien der Presburger Arithmetik natürlicher Zahlen ist auf einem solchen Weg eine Theorem 2, p. 3, in [FiR74] entsprechende Aussage in folgender Darstellung zu gewinnen:

Satz 3.1.2. *T sei eine der hier als formales Sprachsystem aufgefaßten Theorien $PreAN$, $PreAN_1$, $PreAN_0$ bzw. $Th(\langle \mathbb{N}_0; 0, 1, +, < \rangle)$, $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$, $Th(\langle \mathbb{N}_0; + \rangle)$;*
$T^{((M))} = (\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ sei diese nun als Sprachsystem aufgefaßte Theorie mit informatisch-sinnvoller Formelsyntax;
$(T^{((M))})^{(ax)}$ sei eine $\mathcal{P}$-erkennbare, vollständige Axiomatisierung von $T^{((M))}$.

Dann gilt: Es gibt ein $c_1 \in \mathbb{R}$, $c_1 > 0$ so, daß $2^{2^{c_1 n}}$ untere Schranke für die Längen der kürzesten Beweise in $(T^{((M))})^{(ax)}$ ist.

Wenn man z.B. die bei der Definition der Theorie $PreAN$ in Kapitel 2 in Definition 2.2.1 festgelegte Axiomatisierung (: im rein logischen Sinn dieses Begriffes inner-

halb des Konzeptes von Theorien 1. Ordnung von [Shoe67] verstanden) zur Konstruktion einer Axiomatisierung $(PreAN^{((M))})^{(ax)}$=$(\Sigma_{PreAN^{((M))}}, Fo_{PreAN^{((M))}}, Thm_{PreAN^{((M))}}, Ax, Ru)$ von $PreAN^{((M))}$ (: einer im hier skizzierten Sinn verstandenen Axiomatisierung) bzgl. der in $PreAN^{((M))}$ mit informatisch-sinnvoller Formelsyntax erfaßten Theorie $PreAN$ verwendet, so kann man dabei eine $\mathcal{P}$-erkennbare, (per def. von PreAN :) vollständige Axiomatisierung von $PreAN^{((M))}$ erhalten. Dafür müssen in Ax neben allen nichtlogischen Axiomen von $PreAN$ (bzw. deren Übertragung nach $PreAN^{((M))}$), die in Definition 2.2.1 angegeben wurden, auch alle logischen Axiome von $PreAN$ (bzw. deren Übertragung), die im System von [Shoe67] diesbezüglich auftreten, erfaßt werden; in Ru müssen Übertragungen aller sich auf Formeln aus $Fo_{PreAN^{((M))}}$ beziehenden Regelanwendungen einer der 5 in [Shoe67] als Deduktionsregeln verwendeten Schlußweisen *Expansion Rule*, *Contraction Rule*, *Associative Rule*, *Cut Rule* und $\exists$-*Introduction-Rule* erfaßt sein. Obzwar dafür natürlich ein ausführlicher Beweis wünschenswert wäre, ist dennoch aus der Gestalt der Axiome und Regeln leicht erkennbar, daß eine solche Axiomatisierung $(PreAN^{((M))})^{(ax)}$ für $PreAN^{((M))}$ $\mathcal{P}$-erkennbar sein wird. Völlig Analoges gilt für $PreAN_0$ und $PreAN_1$.

Hiermit impliziert nun aber der Satz 3.1.2 jeweils doppelt-exponentiell-lineare untere Schranken für die Längen der kürzesten Beweise in den Axiomatisierungen $(PreAN^{((M))})^{(ax)}$, $(PreAN_1^{((M))})^{(ax)}$ und $(PreAN_0^{((M))})^{(ax)}$; diese Aussagen lassen sich nun aber durchaus auch als Ergebnisse über die Längen der kürzesten Beweise in den Theorien $PreAN$, $PreAN_1$ und $PreAN_0$ selber verstehen, wenn man dabei berücksichtigt, daß sie sich nicht direkt auf Theoreme $\mathbf{A}$ und deren Beweise P in diesen Theorien beziehen, sondern auf die jeweiligen Übertragungen $\mathbf{A}^{((M))}$ von $\mathbf{A}$ und $P^{((M))}$ von P bezüglich jeweils einer fixierten, diesen Theorien zugrundegelegten informatisch-sinnvollen Formelsyntax (und eine solche, geringfügig relativierte Aussage besitzt natürlich dennoch (so gut wie :) ungebrochenene Bedeutung[4]).

Dem hier zuletzt gesagten ist allerdings sogar noch der unrelativierte Zusatz anzufügen, daß sich mit den hier ausgearbeiteten und in [FiR74] vorgestellten Methoden leicht auch einsehen läßt, daß sich das Ergebnis der Existenz einer doppelt-exponentiell-linearen unteren Schranke für die Längen der kürzesten Beweise auch direkt für $PreAN$ (und $PreAN_0$ und $PreAN_1$) zeigen läßt (und dem bezüglich des ganz gewöhnlichen Begriffs von Formel- und Beweislängen als Längen von im System von [Shoe67] genau festgelegten Zeichenketen innerhalb dieser Theorie(n)) und zwar so: Durch eine einfache Analyse der hier nachvollzogenen Komplexitätsbeweise kann erkannt werden, daß sich das Komplexitätsresultat

[4]Zumal ja außerdem kein Hindernis bestünde, Logikkalkülen (weitgehend allgemein oder wenigstens in der Beziehung auf entscheidbare Theorien, deren Entscheidungs- oder Beweislängen-Komplexität untersucht werden soll) von vorne herein eine informatisch-sinnvolle Formelsyntax zugrundezulegen (oder bei der Festlegung einer allgemeinen Syntax für die Formeln eines Kalküls wenigstens darauf zu achten, daß ein informatisch-sinnvoller syntaktischer Aufbau von Formeln einer mit diesem Kalkül überbauten Theorie immerhin als Spezialfall noch möglich bleibt).

einer doppelt-exponentiell-linearen unteren Schranke auch direkt für die Entscheidungskomplexität von $PreAN{=}(\Sigma_{PreAN}, Fo_{PreAN}, Thm_{PreAN})$, der unmittelbaren Erfassung von $PreAN$ in einem Sprachsystem, zeigen läßt. Daraus läßt sich (mit Hilfe eines—hier nicht dargestellten—exakten Beweises von Satz 3.1.2) auch eine ebenso-gestaltige untere Schranke für eine Axiomatisierung $(PreAN^{((M))})^{(ax)}{=}(\Sigma_{PreAN^{((M))}}, Fo_{PreAN^{((M))}}, Thm_{PreAN^{((M))}}, Ax, Ru)$ von $PreAN$ folgern bzw. nachweisen, wenn nur Ax und Ru in Bezug auf $PreAN$ und das System von [Shoe67] entsprechend gewählt werden (denn $PreAN^{(ax)}$ kann wohl ebenso direkt wie $(PreAN^{((M))})^{(ax)}$als $\mathcal{P}$-erkennbar eingesehen werden).

Der bezüglich Aussagen über die Entscheidungskomplexität qualitative Unterschied zwischen (z.B.) $PreAN$ und $PreAN^{((M))}$ (wobei hier angenommen sei, daß $PreAN^{((M))}$ entlang von Grammatik 2.6.1 präzisiert ist) zwischen (z.B.) $PreAN$ und $PreAN^{((M))}$ besteht in der in $PreAN$ ausschließlich unär, in $PreAN^{((M))}$ hingegen dezimal erfolgenden Variablenindizierung. Dabei ist klar, daß die $PreAN^{((M))}$ (und allgemein Theorien mit informatisch-sinnvoller Formelsyntax) betreffenden Komplexitätsresultate die „realistischeren", wichtigeren und grundlegenderen sind; allerdings ist es natürlich interessant, daß diese sich hier auch auf die bezüglich einer solchen Formelsyntax, der ausschließlich die unäre Indizierung von Variablen zugrundeliegt, formalisierten, entsprechenden Theorien übertragen lassen[5].

Im Fall von $Th(\langle \mathbb{R}; + \rangle)$ führen analoge Darstellungsweisen der Ergebnisse aus [FiR74] für die Entscheidungskomplexität von RA und die Längen der kürzesten Beweise in dieser Theorie (analoge Darstellungen wie in Satz 3.1.1 und Satz 3.1.2 gegenüber Theorem 1 und Theorem 2 in [FiR74]) auf folgende, Theorem 3 und Theorem 4, p. 4., in [FiR74] entsprechende Aussagen:

Satz 3.1.3. *T sei eine der semantisch-definierten Theorien 1. Ordnung der Additionsarithmetik auf den reellen Zahlen $Th(\langle \mathbb{R}; 0, 1, +, < \rangle)$, $Th(\langle \mathbb{R}; 0, 1, + \rangle)$ oder $Th(\langle \mathbb{R}; + \rangle)$; $T^{((M))} = (\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ sei die als System von formalen Sprachen aufgefaßte Theorie T mit informatisch-sinnvoller Formelsyntax.*

Dann gilt: Es existiert ein $d \in \mathbb{R}$, $d > 0$ so, daß 2^{dn} eine untere Schranke für die Entscheidungskomplexität von T ist. Darüber hinaus kann ein $d \in \mathbb{R}$, $d > 0$ so gewählt werden, daß

$$Thm_{T^{((M))}},\ \text{co}{-}Thm_{T^{((M))}} \notin NTime\,(2^{cn})$$

gilt.

[5] Ähnlich, wie es unter den $\mathcal{NP}$-vollständigen Problemen solche gibt, deren Instanzen aus Zahlen bestehen und die $\mathcal{NP}$-vollständig bleiben, wenn jene Variante des Problems, deren Instanzen ausschließlich aus Instanzen des ursprünglichen Problems mit unär dargestellten Zahlen bestehen, betrachtet wird. Solche Probleme heißen *$\mathcal{NP}$-vollständig in starkem Sinne* ("$\mathcal{NP}$-complete in the strong sense" , vgl. [Jo90]). Andererseits gibt es $\mathcal{NP}$-vollständige Probleme, für die ein *pseudopolynomial-Zeit* Algorithmus existiert, d.h. ein Algorithmus aus $\mathcal{P}$, der die unäre Variante des Problems löst.

Satz 3.1.4. *$T = (\Sigma_T, Fo_T, Thm_T)$ sei eine der hier als formales Sprachsystem aufgefaßten Theorien $Th(\langle\mathbb{R}; +\rangle)$ oder $Th(\langle\mathbb{R}; 0, 1, +\rangle)$; $T^{((M))}$ sei diese Theorie T mit informatisch-sinnvoller Formelsyntax; $(T^{((M))})^{(ax)}$ sei eine $\mathcal{P}$-erkennbare, vollständige Axiomatisierung von $T^{((M))}$.*

Dann gilt: Es gibt ein $d_1 \in \mathbb{R}$, $d_1 > 0$ so, daß $2^{d_1 n}$ untere Schranke für die Längen der kürzesten Beweise in $(T^{((M))})^{(ax)}$ ist.

Als ziemlich unmittelbare Anwendung dieser letzten beiden Aussagen formulieren [FiR74] noch ein Korollar, das sich auf die von A. Tarski als entscheidbar erkannte Theorie $TA := Th(\langle\mathbb{R}; 0, 1, +, .\rangle)$ (die „*Tarski Algebra*“) bezieht, nämlich Corollary 5, p. 4, in [FiR74].

Korollar 3.1.5. *Für die Tarski-Algebra $TA := Th(\langle\mathbb{R}; 0, 1, +, .\rangle)$ bzw. für die Theorie $Th(\langle\mathbb{R}; +, .\rangle)$ gelten analoge Aussagen über einfach-exponentiell-lineare untere Schranken für die Entscheidungskomplexität bzgl. der Rechenzeit nichtdeterministischer Turingmaschinen und für die Längen der kürzesten Beweise in allen $\mathcal{P}$-erkennbaren, vollständigen Axiomatisierungen dieser Theorie(n) wie in Satz 3.1.3 und in Satz 3.1.4 für RA formuliert.*

Als Verallgemeinerung ihrer für RA und für $Th(\langle\mathbb{N}_0; 0, 1, +\rangle)$ erzielten Komplexitätsaussagen gelang es [FiR74] (und gelingt es in der Tat durch eine kleinere Variation[6] der von Fischer und Rabin vorgestellten Methoden und Techniken) außerdem eine auf einige andere, v.a. auch algebraische Theorien anwendbare Aussage zu beweisen, die qualitativ mit den für RA erzielten Sätzen vergleichbar ist. (In [FiR74] handelt es sich dabei um Theorem 13, p. 22.)

Satz 3.1.6. *Sei L eine Sprache einer Theorie 1. Ordnung mit dem zweistelligen Funktionssymbol $+$ als einzigem nichtlogischen Symbol. Sei $\mathcal{A}$ eine Klasse von Strukturen für L, so, daß in allen Strukturen $\mathfrak{A} = \langle A; +\rangle \in \mathcal{A}$ die Funktion $+$ einer zweistelligen, assoziativen Verknüpfung auf A entspricht.*

Weiters sei angenommen, daß gilt:

$$(\forall k \in \mathbb{N})\,(\exists \mathfrak{A} = \langle A; +\rangle \in \mathcal{A})$$
$$(\exists u \in A)\,\big(u,\ \underline{2}\,u = u + u,\ \ldots,\ \underline{k}\,u = \underbrace{u + u + \ldots + u}_{k}$$
$$\text{sind (in } A\text{) paarweise verschieden }\big).$$

[6] (die in [FiR74] nicht näher beschrieben wird und die auch in dieser Aufarbeitung nicht enthalten ist)

Sei nun $Th(\mathcal{A}) := \bigcap_{\mathfrak{A} \in \mathcal{A}} Th(\mathfrak{A})$ [7] *(bzw.* $Th(\mathcal{A})$ *gleich jener Theorie mit Sprache* L*, die als nichtlogische Axiome genau die in allen Strukturen* $\mathfrak{A} \in \mathcal{A}$ *gleichzeitig gültigen Formeln von* L *besitzt).*

Dann gelten für $Th(\mathcal{A})$ *erneut (wie schon in Korollar 3.1.5 für die Tarski-Algebra formuliert) analoge Aussagen über einfach-exponentiell-lineare untere Schranken für die Entscheidungskomplexität von* $Th(\mathcal{A})$ *bzgl. der Rechenzeit nichtdeterministischer Turingmaschinen und für die Längen der kürzesten Beweise in allen* $\mathcal{P}$*-erkennbaren, vollständigen Axiomatisierungen dieser Theorie wie in Satz 3.1.3 und in Satz 3.1.4 für RA formuliert.*

Mit Hilfe von Satz 3.1.6 läßt sich (worauf [FiR74] hinweisen) die Existenz einer einfach-exponentiell-linearen unteren Schranke für die Entscheidungskomplexität folgender Theorien einsehen: Der Theorie $Th(\langle \mathbb{C}; + \rangle)$, der Theorie der endlichen zyklischen Gruppen, der Theorie der Ringe mit Charakteristik p, der Theorie der endlichen abelschen Gruppen (die [FiR74] mit FAG bezeichnen) und von $SkA = Th(\langle \mathbb{N}_0; . \rangle)$ (die [FiR74] mit $MULT$ bezeichnen).

Im Fall von FAG und SkA berichten Fischer und Rabin in [FiR74] jeweils noch von substantiell höheren, für die Entscheidungskomplexität dieser Theorien existierenden unteren Schranken bezüglich nichtdeterministischer Turing-Rechenzeit und zwar von einer solchen von doppelt-exponentiell-linearerer Gestalt für FAG (analog wie für $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ oder $PreAN$) sowie von einer von dreifach-exponentiell-linearer Gestalt für SkA. Für diese Komplexitätsaussagen werden in [FiR74] die prinzipiellen Beweisideen jeweils nur ganz kurz umrissen.

[7] (etwas leichtfertige modelltheoretische Schreibweise, die im formalen System von [Shoe67] nicht erlaubt ist; vgl. jedoch die Präzisierung dieser Festsetzung in der anschließenden Klammerung)

3.2 Diskussion der genauen Gestalt der in [FiR74] erzielten Komplexitätsresultate

Zwischen den Formulierungen der die Entscheidungskomplexität der behandelten Theorien betreffenden Komplexitätsresulate in [FiR74] und den hier in Abschnitt 1 vorgestellten Sätzen Satz 3.1.1 und Satz 3.1.3 bestehen neben formalen auch kleinere inhaltliche Unterschiede, die in diesem Abschnitt zusammengestellt und untersucht werden sollen. Es wird dabei versucht, zu begründen, daß die wesentliche Qualität der in [FiR74] erzielten Ergebnisse, die formal etwas stärker sind, schon in den hier angegebenen Sätzen enthalten und präzisiert worden ist. Und zwar soll dies exemplarisch anhand der die Theorien der Presburger Arithmetik natürlicher Zahlen betreffenden Aussagen, Theorem 1, p. 2, in [FiR74] und Satz 3.1.1 aus Abschnitt 1 geschehen. Die dabei angestellten Überlegungen beziehen sich allerdings im selben Umfang auch auf die analogen formalen und inhaltlichen Unterschiede zwischen den sich auf die Theorie RA der Additionsarithmetik auf den rellen Zahlen beziehenden Komplexitätssätze Theorem 3, p. 4, in [FiR74] und Satz 3.1.3 aus Abschnitt 1.

Es handelt sich bei Satz 3.1.1 um eine hier vorgestellte, im weiteren Verlauf dieser Aufarbeitung bewiesene Präzisierung von Theorem 1, p. 2, in [FiR74], deren wesentliche, sich auf Begriffe und Definitionen aus Kapitel 1 stützenden Behauptung in der Existenz einer doppelt-exponentiell-linearen unteren Schranke für die Entscheidungskomplexität von Theorien 1. Ordnung der Presburger Arithmetik natürlicher Zahlen bezüglich der Rechenzeit nichtdeterministischer Turingmaschinen besteht.

Demgegenüber läßt sich Theorem 1 in [FiR74] etwa so darstellen:

$$\begin{aligned}
&(\exists c \in \mathbb{R},\, c > 0)\,\big(\forall M \in \mathcal{C} \text{ Methode, die } Th(\langle \mathbb{N}_0; 0, 1, + \rangle) \text{ entscheidet}\big) \\
&\quad (\exists n_0 \in \mathbb{N})\,(\forall n \geq n_0,\, n \in \mathbb{N}\,) \\
&\qquad \big(\exists \mathbf{F} \text{ Theorem von } Th(\langle \mathbb{N}_0; 0, 1, + \rangle)\big) \\
&\qquad\quad \big[\, |\mathbf{F}| = n \;\&\; RS_M(\mathbf{F}) > 2^{2^{cn}}\,\big]
\end{aligned} \tag{3.1}$$

(wobei $\mathcal{C}$ eine Methodenklasse ist und RS eine die Rechenzeit oder die Berechnungsschritte von Methoden $M \in \mathcal{C}$ bezeichnende Ressource meint).

Hierin ist weitgehend unpräzisiert gelassen, was unter einer Entscheidungsmethode für $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ genau zu verstehen ist. Allerdings ist eine solche Formulierung sicher in der Absicht entstanden, nahezulegen und darauf zu verweisen, daß sich das in [FiR74] nur bezüglich einer konkreten und speziellen Klasse von als Entscheidungsverfahren in Frage kommenden Turingmaschinen erzielte Schwerentscheidbarkeits-Ergebnis auch auf viele andere universelle Methodenklassen (Klassen von Methoden aus Maschinen- oder Berechenbarkeitsmodellen) ausdehnen bzw. jeweils übertragen läßt. Dabei ist es jedoch für solche Ergebnisübertragungen wichtig und wesentlich, daß auch in solchen anderen betrachteten Methodenklassen sinnvoll definierte Begriffe von „Rechenzeit“ oder „Berechnungsschritt“

existieren oder eingeführt werden können und daß diese mit den für Turingmaschinen dafür bestehenden Festlegungen (durch dann mögliche, einfache gegenseitige Simulationen) in eine genau-beschreibbare Beziehung von geringer Aufwandskomplexität gebracht werden können (vgl. hierzu die in Abschnitt 1.4 erwähnte INVARIANZ THESE).

Naheliegende Präzisierungen von (3.1) beziehen sich ebenso wie die in [FiR74] eigentlich konkret erzielten Ergebnisse auf Turingmaschinen, die zur Entscheidung einer Theorie (hier von $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$) verwendet werden.

Am unmittelbarsten könnte eine Präzisierung von (3.1) für deterministische Turingmaschinen geschehen. Faßt man nämlich $T := Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ als Sprachsystem $T^{((M))}$ mit informatisch-sinnvoller Formelsyntax (vgl. Kapitel 1) auf, so können deterministische IOTM's zur Entscheidung von Formeln von $T^{((M))}$ dadurch herangezogen werden, indem sie für Zeichenketten $w \in \Sigma^*_{T^{((M))}}$

$$THM_{T^{((M))}}(w) \in \{ \text{“}\texttt{ist\_Theorem\_von\_T}\text{”}, \text{“}\texttt{ist\_Formel,\_kein\_Theorem\_T}\text{”}, \text{“}\texttt{ist\_keine\_Formel\_von\_T}\text{”} \}$$

berechnen (die Funktion $THM_{T^{((M))}}$ dabei wie in Abschnitt 1.5, (1.5)). Auf eine solche Weise gelangt man für $T^{((M))}$ wie hier angenommen, $THM_{T^{((M))}}$ zu $T^{((M))}$ wie in (1.5) festgesetzt, zu folgender Präzisierung von (3.1) für als Entscheidungsmethoden verwendete deterministische IOTM's:

$$\begin{aligned} &(\exists c \in \mathbb{R},\, c > 0)\, \big(\forall M \text{ det. IOTM, die } THM_{T^{((M))}} \text{ berechnet} \big) \\ &\quad (\exists n_0 \in \mathbb{N})\, (\forall n \geq n_0,\, n \in \mathbb{N}\,) \\ &\qquad \big(\exists \mathbf{F} \in Thm_{T^{((M))}} \big) \\ &\qquad\quad \big[\, |\mathbf{F}| = n \;\&\; RZ_M(\mathbf{F}) > 2^{2^{cn}} \,\big]\,. \end{aligned} \tag{3.2}$$

(3.2) ist eine etwas stärkere Aussage als

$$(\exists c \in \mathbb{R}, c > 0)\, \big(THM_{T^{((M))}} \notin DFTime(2^{2^{cn}}) \big)\,, \tag{3.3}$$

die auf einfachem Weg aus Satz 3.1.1 folgt. Dies deshalb, da für $c \in \mathbb{R}$, $c > 0$ mit $THM_{T^{((M))}} \in DFTime(2^{2^{cn}})$ sofort auch $Thm_{T^{((M))}}$, co$-Thm_{T^{((M))}} \in DFTime(2^{2^{cn}})$ folgt[8], was aber wegen Satz 3.1.1 wenigstens für hinreichend kleine $c \in \mathbb{R}$, $c > 0$ ausgeschlossen ist (v.a., da natürlich $DTime(2^{2^{cn}}) \subseteq NTime(2^{2^{cn}})$).

[8] Aus einer IOTM M, die $THM_{T^{((M))}}$ berechnet, können auf einfachem Weg zwei IOTM's M_1 und M_2, die $Thm_{T^{((M))}}$ bzw. co$-Thm_{T^{((M))}}$ akzeptieren, mit im wesentlichen gleicher Rechenzeitschranke wie M konstruiert werden. – Vgl. hierzu außerdem die Aussage 1.7, die analog auch für deterministische Komplexitätsklassen gilt.

(3.2) ist nun deshalb stärker als (3.3), weil (3.3) folgender Aussage entspricht:

$$\begin{array}{l}(\exists c \in \mathbb{R},\, c > 0)\,\big(\,\forall M \text{ det. IOTM, die } THM_{T^{((M))}} \text{ berechnet}\,\big)\\ \quad (\forall n_0 \in \mathbb{N})\,(\,\exists n \in \mathbb{N},\, n \geq n_0\,)\\ \qquad \big(\,\exists w \in \Sigma^*_{T^{((M))}}\,\big)\\ \qquad\quad \big[\,|w| = n \;\&\; RZ_M(w) > 2^{2^{cn}}\,\big]\end{array} \tag{3.4}$$

Der hier zu betrachtende qualitative Unterschied in der Aussage zwischen (3.2) und (3.4) besteht nicht darin, daß für Entscheidungs-IOTM's M in (3.2) die Existenz von *Theoremen* $\mathbf{F} \in Thm_{T^{((M))}} \subseteq Fo_T \subseteq \Sigma^*_T$, in (3.4) nur die von *Wörtern* $w \in \Sigma^*_T$ mit der Eigenschaft, von M nicht mit Rechenzeitschranke $2^{2^{cn}}$ entscheidbar zu sein, gefordert wird (ein solcher Unterschied besteht hier hauptsächlich formal wegen der besonders einfachen Art der Formulierung von mit Hilfe von Komplexitätsklassen; durch die Anwendung von Satz 3.4.1 (aus dem folgenden) sieht man jedoch, daß eine $w = |\mathbf{F}| \in Thm_{T^{((M))}}$ (für ein $\mathbf{F} \in Fo_{T^{((M))}}$) verlangende Forderung in (3.4) ebenfalls mit den hier präzisierten und verwendeten Methoden leicht beweisbar ist). Der zu beachtende Unterschied besteht vielmehr darin, daß in (3.2) die Existenz von Formeln $\mathbf{F}$ mit $|\mathbf{F}| = n$ *für fast alle* $n \in \mathbb{N}$ und mit der entsprechenden, den Entscheidungsaufwand betreffenden Eigenschaft gefordert ist, in (3.4) jedoch nur die Existenz von (unendlich vielen) *derartigen* $w \in \Sigma^*_{T^{((M))}}$ mit $|w| = n$ *für unendlich viele* $n \in \mathbb{N}$.

Dieser inhaltliche Unterschied zwischen (3.2) und (3.4) steht im Zusammenhang damit, was in Kapitel 1 anschließend an Definition 1.3.7 über mögliche Variationen bei der Definition oder Begriffsfestsetzung von unteren Schranken für den Lösungsaufwand eines Problems dargelegt wurde. So drückt (3.4) jedenfalls aus, daß die Suche nach möglichst effizienten Entscheidungsalgorithmen für $T = Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ bzw. für das zugehörige System $T^{((M))}$ jedenfalls der (sehr drastischen) Einschränkung unterliegt, daß es ein $c \in \mathbb{R}$, $c > 0$ gibt, so, daß für alle $THM_{T^{((M))}}$ berechnenden IOTM's M die Funktion $2^{2^{cn}}$ *nicht* Rechenzeitschranke für M ist (und wohl keine Hoffnung oder Aussicht besteht, daß sich eine andere Methodenklasse bezüglich eines anderen universellen Maschinen- oder Berechnungsmodells finden ließe, in Beziehung auf die eine vergleichbare Aussage nicht ebenso bewiesen werden könnte (bzw. auf die hin eine vergleichbare Aussage nicht übertragen werden könnte); das gilt wohl auch für reale Computer, allerdings in einer Weise, die vorsichtig präzisiert werden müßte (vgl. Abschnitt 1.6). – Wiederum könnte argumentiert werden, daß diese Aussage aber die wesentliche Charakterisierung der Entscheidungskomplexität von T „nach unten“ bezüglich einer Funktion $2^{2^{cn}}$ mit $c \in \mathbb{R}$, $c > 0$ fix (wie von (3.4) behauptet) ist.

Allerdings beinhält (3.4) im Gegensatz zu (3.2) für ein in Frage kommendes $c \in \mathbb{R}$, $c > 0$ und eine beliebige deterministische IOTM M nicht, *wie dicht* die Längen $n = |\mathbf{F}|$ von Formeln $\mathbf{F}$ (bzw. von Zeichenketten $w \in \Sigma^*_{T^{((M))}}$, vgl. jedoch oben) mit $RZ_M(\mathbf{F}) > 2^{2^{cn}}$

in $\mathbb{N}$ liegen; (3.2) behauptet, daß diese Formellängen n *fast ganz* $\mathbb{N}$ (mit einer endlichen Ausnahmemenge) ausmachen.

Eine genaue Analyse der Beweise in dieser Aufarbeitung kann jedoch zeigen, daß die Längen der entsprechenden, in den Beweisen hier konstruierten Formeln relativ dicht liegen und konstant wachsen, sodaß damit auf jeden Fall ausgeschlossen ist, daß sie für wachsendes $n \in \mathbb{N}$ in immer dünnerer Verteilung auftreten und es kann damit ziemlich unmittelbar auch gezeigt werden:

$$\begin{aligned}
&(\exists c \in \mathbb{R},\, c > 0)\, \big(\forall M \text{ det. IOTM, die } THM_{T^{((M))}} \text{ berechnet}\big) \\
&\quad (\forall n_0 \in \mathbb{N})\, (\,\exists n \in \mathbb{N},\, n \geq n_0\,) \\
&\qquad \big(\,\exists \mathbf{F} \in Thm_{T^{((M))}}\,\big) \\
&\qquad\quad \big[\,|\mathbf{F}| \leq n \;\&\; RZ_M(\mathbf{F}) > 2^{2^{cn}}\,\big]
\end{aligned} \tag{3.5}$$

(3.5) kommt (3.2) inhaltlich schon sehr nahe. Durch die Anwendung zusätzlicher formaler Konstruktionen im Beweis von Satz 3.1.1 (und nämlich im dafür verwendeten Beweis von Satz 3.4.1) kann weiters dann sicherlich auch (3.2) bewiesen werden. Ein solcher weiterer Beweisaufwand scheint aber ungerechtfertigt (und unterbleibt in dieser Aufarbeitung), zumal dadurch die Menge der zu einer IOTM M, die $THM_{T^{((M))}}$ berechnet, durch die Beweise konstruierten Formeln $\mathbf{F}$ mit $RZ_M(\mathbf{F}) > 2^{2^{c\cdot|\mathbf{F}|}}$ (für ein in (3.4) in Frage kommendes $c \in \mathbb{R}$, $c > 0$) keineswegs *qualitativ* erweitert und nur auf weitgehend formalem Weg zu einer Menge von solchen Formeln beliebiger Länge n mit $n \geq n_0$ für ein $n_0 \in \mathbb{N}$ ausgedehnt wird. Dadurch können aber prinzipielle Vorbehalte, die man gegen die Existenz einer unteren Schranke der Form aus Satz 3.1.1 (oder der Formulierung (3.4), die—wie gezeigt—daraus folgt) für z.B. $PreAN$ haben könnte, etwa, daß sich diese untere Schranke vielleicht nur einer besonders „künstlichen“ und „konstruierten“ Menge von besonders unangenehm zu entscheidenden Formeln verdanke, an denen im Gegensatz zu anderen möglicherweise sinnvoll definierbaren Teilmengen von interessanten und einfacher zu entscheidenden Formeln von $PreAN$ kein praktisches Interesse bestehe, *nicht* zerstreut werden[9] (vgl. dazu auch Abschnitt 1.6).

[9]Ein solcher Einwand scheint aber hier dennoch ziemlich unbegründet zu sein. Und zwar vermutlich ebenso wie eine gegen die Unvollständigkeit arithmetischer Theorien, etwa der Peano-Arithmetik (Theorie 1. Ordnung) PeA aus Abschnitt 2.5, zeitweilig geäußerte Meinung, sie beruhe vielleicht ausschließlich auf der Formulierung meta-mathematischer Überlegungen mit den Mitteln dieser Theorie selber zu beim Beweis der Gödelschen Sätze konstruierten formal-unentscheidbaren Sätzen bzw. Formeln bzw. Aussagen dieser Theorie (und zu strukturell und logisch mit diesen eng verwandten Aussagen) und gelte möglicherweise nicht für Formeln dieser Theorie, an denen ein unmittelbares mathematisches Interesse bestehen könne [: meine Worte in der Wiedergabe aus [Th95], S. 236, C.G.], ... ebenso wie eine solche Meinung inzwischen als unhaltbar erkannt worden ist (in diesem Zusammenhang wird häufig (auch in [Th95]) auf [PaHa77] und darin vorgestellte, in PeA unentscheidbare, kombinatorische Sätze verwiesen). – Wie in Abschnitt 1.6 erwähnt, dürfte man aber v.a. beim Versuch, eine Menge von „praktisch-interessanten“ Formeln mit niedrigerer Entscheidungskomplexität—von einfachen und bekannten Fällen und Einschränkungen abgesehen—zu präzisieren, auf erhebliche Schwierigkeiten stoßen. Denn man müßte dabei verhindern,

Der hier (weil daran mit standardisierten Begriffen besser darzustellende) am Fall der Betrachtung des deterministischen Falles geschilderte, zwischen den Aussagen (3.4) und (3.2) auftretende (leichte) inhaltliche Unterschied in der Gestalt zwischen den hier in dieser Aufarbeitung bewiesenen und den in [FiR74] formulierten Komplexitätsaussagen besteht ganz genauso, falls man diese Aussagen bezüglich der Verwendung von nichtdeterministischen Turingmaschinen untersucht. Insbesondere lassen sich die angeführten Überlegungen im nichtdeterministischen Fall völlig analog nachvollziehen, wenn man (3.2) bezüglich nichtdeterministischen IOTM's, die $THM_{T^{((M))}}$ berechnen, erweitert und demgegenüber in (3.3) die Komplexitätsklasse $NFTime(2^{2^{cn}})$ verwendet, die in Abschnitt 1.4 zu Motivationszwecken eingeführt wurde.

Weiters kann die vorstellbare Möglichkeit, daß Funktionen auch von nichtdeterministischen IOTM's berechnet werden könnten (etwa unter der Zugrundelegung von Setzung (1.4)) und daß damit nichtdeterministische IOTM's auch tatsächlich (unter solchen oder ähnlichen geeigneten einschränkenden Bedingungen) Entscheidungsprobleme lösen könnten, die der Definition von oberen und unteren Schranken für die Entscheidungskomplexität einer entscheidbaren Theorie im nichtdeterministischen Fall in Defintion 1.5.1 (v.a. als Motivation) zugrundeliegt, hier auch weiters als Argument dafür betrachtet werden, warum die wesentliche Aussage von Satz 3.1.1

$$(\exists c \in \mathbb{R}, c > 0)\left(Thm_{T^{((M))}}, \text{co}-Thm_{T^{((M))}} \notin NTime(2^{2^{cn}})\right) ,$$

(bzw. die im Lichte von (1.7) dazu äquivalente Aussage

$$(\exists c \in \mathbb{R}, c > 0)\left(THM_{T^{((M))}} \notin NFTime(2^{2^{cn}})\right))$$

als Präzisierung von (3.1) bezüglich der Verwendung von nichtdeterministischen Methoden aufgefaßt werden kann.

daß sich die in [FiR74] beim Beweis der Komplexitätsresultate verwendeten Hilfsformeln in der einen oder anderen abgeänderten Gestalt auch dann noch in dieser neuen Menge von „praktisch-interessanten" Formeln ausdrücken lassen. Da diese Hilfsformeln aber einfache Aussagen der Arithmetik betreffen und formulieren (der auf endliche Teilstücke von $\mathbb{N}_0$ beschränkten Arithmetik mit $+, \cdot$ und exp) scheint es eher unmöglich zu sein, daß sich das für eine—um „praktisch interessant" zu sein—hinreichend umfangreiche Klasse ausschließen läßt.

3.3 Für die Beweise verwendete Klasse von Turingmaschinen, benötigte Bezeichnungen

Die Beweise in [FiR74] zur Erzielung interessanter unterer Schranken für die Entscheidungskomplexität einiger entscheidbarer Theorien erfordern die Möglichkeit, zu einer vorgegebenen Rechenzeitschranke $f(n)$ die Eigenschaft einer Turingmaschine M, ein Eingabewort w mit Rechenzeitschranke $f(n)$ zu akzeptieren, mit den Ausdrucksmitteln der jeweils betrachteten Theorie T erfassen und also als Formel $\mathbf{F}_{M,w}$ in T formulieren zu können; dabei soll die Beweisbarkeit von $\mathbf{F}_{M,w}$ in T genau diese Eigenschaft von M in Beziehung zu w widerspiegeln. Dabei müssen im Fall des Beweises in [FiR74], damit die Beweismethode der Diagonalisierung angewendet werden kann, diese Formeln $\mathbf{F}_{M,w}$ immer effektiv aus einer Kodierung des Maschinencodes von M und dem Eingabewort w hergestellt werden können (diese Erzeugung von $\mathbf{F}_{M,w}$ muß sogar in polynomialer Rechenzeit erfolgen können).

Dieses Vorgehen erfordert also jedenfalls eine genaue Festlegung von Kodierungen für Turingmaschinen. Schon für die Definition von solchen Kodierungen ist es sinnvoll, die Klasse der im Beweis betrachteten Turingmaschinen irgendwie einzuschränken, beispielsweise auf eine Klasse mit beschränktem und fixiertem Bandalphabet.

Außerdem besteht auch noch im Hinblick auf die Darstellung der Komplexitätsbeweise (und dabei v.a. für die der Transformation von Maschinencode $\langle M \rangle$ für M und Eingabewort w zur Formel $\mathbf{F}_{M,w}$), die ohnehin recht aufwendig ist, ein Interesse an einer einfach zu beschreibenden, eingeschränkten Klasse von Turingmaschinen.

Bei der Wahl einer solchen eingeschränkten Klasse darf aber andererseits gegenüber der allgemeinen und umfassenden Klasse aller Turingmaschinen möglichst kein großer Komplexitätsspielraum verloren gehen. Dies deswegen, damit Komplexitätsaussagen, die zuerst nur in Beziehung zur eingeschränkten Klasse bewiesen werden, dann auf die Klasse aller Turingmaschinen übertragen werden können, ohne daß dabei die Qualität der betrachteten und zu übertragenden Komplexitätsaussagen weitgehend abhanden gerät.

Eine in Frage kommende, sinnvolle Klasse von Turingmaschinen mit diesen Eigenschaften ist nun sicherlich die Klasse der Turingmaschinen mit nur einem Turingband, das außerdem nur einseitig (rechtsseitig) unendlich ist. Denn für allgemeine Turingmaschinen existieren immer Simulationen auf einer 1-Band-Maschine mit (von der Wachstumsordnung her) quadratisch höherer Rechenzeitschranke. In diesem Fall kann dann z.B. aus einer für ein Problem P bezüglich deterministischen 1-Band-Maschinen bewiesenen unteren Schranke bezüglich Rechenzeit von der Gestalt 2^{cn} für ein fixes $c \in \mathbb{R}$, $c > 0$ die untere Schranke $2^{\frac{1}{2}cn}$ für P bezüglich Rechenzeit beliebiger deterministischer Turingmaschinen hergeleitet werden.

[FiR74] verwenden als eingeschränkte Maschinenklasse 1-Band-Turingmaschinen mit einseitig unendlichem Band und mit Bandalphabet $\{0, 1\}$. Die Wahl eines solchen, für

Turingmaschinen kleinstmöglichen Alphabets erfolgte in [FiR74] im Hinblick darauf, daß ein wesentlicher Beweisschritt bei der Konstruktion der Formeln $\mathbf{F}_{M,w}$ in der Beschreibung von Binärwörtern vorgegebener Länge durch Formeln der jeweils betrachteten Theorie T besteht und sich Berechnungen von Maschinen aus dieser Klasse ziemlich unmittelbar durch Binärwörter beschreiben lassen.

Die Verwendung von Turingmaschinen aus dieser Klasse hat aber jedenfalls den (zuerst nur formalen) Nachteil, daß sie, um zur Erzielung von Komplexitätsaussagen überhaupt tauglich benutzt werden können, in einer Nicht-Standard-Weise eingesetzt werden müssen. Eine wie üblich definierte Turingmaschine mit Bandalphabet $\{0,1\}$ wäre nämlich eine *unäre* Maschine, d.h. es müßte jedenfalls ein Zeichen als Leersymbol (z.B. das Symbol 0) definiert und verwendet werden und eine solche Maschine könnte dementsprechend (jedenfalls als Ein- und Ausgaben) ausschließlich unäre Strichcodes (z.B. Eingabe 01111111111111110 für die Zahl 17) verarbeiten. Dadurch würden Komplexitätsaussagen aber in dramatischer Weise verzerrt werden, da demgegenüber realistische Längen von Eingaben und Ausgaben logarithmisch kürzer wären und die Eingabelänge ja für alle hier betrachteten Komplexitätsaussagen den Vergleichsmaßstab für Aufwandsabschätzungen bildet.

Um solche Turingmaschinen dennoch in brauchbarer Weise verwenden zu können, ist es notwendig, auch als Eingabe(symbol-)menge die ganze Menge $\{0,1\}$ zu setzen und also den Einsatz von Binärwörtern als Eingabestrings zu gestatten. In diesem Fall kann dann allerdings das Ende einer Eingabe-Zeichenkette nicht mehr durch folgende Leersymbole erkennbar sein (da es ein festgesetztes Leersymbol auf solchen Maschinen dann nicht mehr gibt) und damit müssen die Ein- und Ausgabemengen solcher Maschinen zusätzlichen Spezifikationen unterworfen werden. Das kann etwa dadurch geschehen, daß bei der Erstellung des Programmcodes einer jeden solchen Maschine davon ausgegangen wird, daß die Eingabe in der Form von Binärblöcken einer fixen Länge $l \in \mathbb{N}$, $l \geq 2$ vorliegt und aufeinanderfolgende l-Blöcke in festgesetzter Weise als Symbole aus einem Alphabet mit Mächtigkeit $\leq 2^l$ zu interpretieren sind.

Die genaue Formalisierung eines solchen Vorgehens würde eine neue Spezifikation solcher Turingmaschinen z.B. mit Rücksicht auf die Länge der verwendeten bit-Blöcke, die Interpretation dieser bit-Blöcke als Symbole festgelegter Alphabete und die Ein- und Ausgabemengen solcher Maschinen erfordern. [FiR74] vermeiden jedoch eine solche exakte Formalisierung der verwendeten Turingmaschinen und gehen zum Zweck der Darstellung der wesentlichen Schritte ihres Beweises nur vom Vorliegen fixierter und *erkennbarer* Kodierungen von Maschinen aus dieser Klasse, von Binärwörtern[10] und von Formeln der betrachteten Theorien als (erkennbare) Binärwörter aus, ohne diese Kodierungen aller-

[10] Eine Turingmaschine mit Bandalphabet $\{0,1\}$ kann ja das Ende eines als Eingabe vorliegenden Binärwortes $w \in \{0,1\}^*$ (auch wenn es nach rechts durch unendlich viele Symbole 0 begrenzt ist) nicht erkennen, ohne von zusätzlichen Annahmen über die Gestalt von w auszugehen.

dings explizit festzulegen.

In der Aufarbeitung hier wird aber die Verwendung von Turingmaschinen mit Bandalphabet $\{0,1\}$, eine dafür notwendige genaue Formalisierung solcher Maschinen und die Verwendung von erkennbaren Binärkodierungen für Maschinen, Binärwörter und Formeln dadurch umgangen, daß als eingeschränkte Maschinenklasse im wesentlichen die gesamte Klasse der 1-Band-Turingmaschinen mit einseitig unendlichem Band benutzt wird. (Für die Beweise wird diese Klasse dann noch zeitweilig auf die Menge aller solchen Maschinen, die über einem gegebenen, endlichen Bandalphabet Γ operieren, eingeschränkt.)

Dieses Vorgehen hat gegenüber dem von [FiR74] aufgezeigten Weg den Vorteil, sich auf ein ausgearbeitetes und bekanntes, formales Konzept von Turingmaschinen stützen zu können und dadurch später auch den Nachweis der Übertragbarkeit von für diese eingeschränkte Maschinenklasse nachgewiesenen Komplexitätsaussagen zu allgemein gültigen weitgehend informell (mit dem Hinweis auf bekannte Simulationsergebnisse) gestalten zu können. Weiters wird dadurch auch die Verwendung von expliziten, erkennbaren Binärkodierungen für Eingabewörter und Formeln unnötig (eine Kodierung für Maschinen (nicht unbedingt eine Binärkodierung) muß dennoch verwendet werden). – Allerdings verschiebt sich dadurch das Problem der Übertragung von Wörtern über beliebigen Alphabeten zu diesen entsprechenden Binärwörtern in die Komplexitätsbeweise hinein und muß darin behandelt werden; das verursacht aber keinen bedeutenden Mehraufwand.

Es tritt hier jedoch noch ein zusätzliches Problem auf, das bei dem in [FiR74] gewählten Vorgehen durch die Verwendung von Binärkodierungen und der ausschließlichen Benutzung von Turingmaschinen mit Bandalphabet $\{0,1\}$ vermieden wird: Die in [FiR74] gewählte, direkte Beweismethode der Diagonalisierung macht es notwendig, daß die gewählte Maschinenklasse und die für diese definierte Kodierung so aufgebaut sind, daß Kodierungen von Maschinen dieser Klasse auch von einer Maschine aus der Klasse selbst erkannt werden können. – Diese Einschränkung an die betrachtete Maschinenklasse und die dafür verwendete Kodierung ist aber nicht wirklich gravierend und ihr wird hier durch die Festsetzung eines fixen (für die Beweise aber weitgehend unspezifiziert gelassenen), endlichen Bandalphabets Γ für die verwendeten 1-Band-Turingmaschinen und eine explizit gewählte Kodierung dieser Maschinen in die Menge Γ^* entsprochen.

Als Formalisierung des Konzeptes der 1-Band-Turingmaschine mit einseitig (rechtsseitig) unendlichem Band wird hier die Formalisierung aus [HoUl79] verwendet. Nach dieser kann jede solche Maschine als 7-Tupel $M = (Q, \Sigma, \Gamma, \delta, q_0, \#, F)$[11] aufgefaßt werden, wobei die Bezeichnungen

Q ... eine endliche Menge von *Zuständen*;
Γ ... eine endliche Menge von zulässigen *Bandsymbolen*;

[11] Das in [HoUl79] verwendete Leersymbol B ist hier—um Mißverständnisse zu vermeiden—durch # ersetzt worden, das auch schon bei der Definition von IOTM's in Kapitel 1 als Leersymbol verwendet worden ist.

$\#$ ... $\# \in \Gamma$, ein spezielles Symbol aus Γ, das *Leersymbol*;
Σ ... $\Sigma \subseteq \Gamma \backslash \{\#\}$, eine $\#$ nicht enthaltende Teilmenge von Γ, die Menge der *Eingabesymbole*;
δ ... die *Übergangsfunktion*, die im deterministischen Fall eine partielle Funktion $\delta\colon (Q \backslash F) \times \Gamma \to Q \times \Gamma \times \{L, R\}$ und im nichtdeterministischen Fall eine partielle Funktion der Gestalt $\delta\colon (Q \backslash F) \times \Gamma \to 2^{Q \times \Gamma \times \{L,R\}}$ ist;
q_0 ... $q_0 \in Q$, der *Startzustand*;
F ... $F \subseteq Q$, die Menge der *Endzustände*;

gelten.

Die für die Beschreibung von Berechnungen von Turingmaschinen dieses Konzeptes verwendeten Bezeichnungen werden der Form nach hier aus [HoUl79] entnommen, jedoch mit den für IOTM's in Kapitel 1 erfolgten Bezeichnungen und Definitionen in Verbindung gebracht. Da sich die Beschreibung der Begriffe hier wesentlich auf die Definitionen in Kapitel 1 stützt, nimmt diese hier nicht die Form eigenständiger Definitionen an.

Eine *Konfiguration* (oder *Augenblicksbeschreibung* einer 1-Band-Turingmaschine M ist von der Gestalt $\alpha_1 q \alpha_2$ mit $\alpha_1 \in \Gamma^*$, $q \in Q$, $\alpha_2 \in \Gamma^*(\Gamma \backslash \{\#\}) \cup \{\epsilon\}$; dabei ist $\alpha_1\alpha_2$ jene Zeichenkette, die dem Inhalt des Bandes zum betrachteten Zeitpunkt vom ersten (linksäußersten) Bandkästchen bis zum am weitesten rechts befindlichen Zeichen ungleich $\#$ (und einschließlich jenes Zeichens) entspricht, q der gegenwärtige Zustand der Maschine M (um Mißverständnisse zu vermeiden, seien die Mengen Q und Γ als disjunkt vorausgesetzt); die Position des Schreib-Lese-Kopfes (SLK) von M zum betrachteten Zeitpunkt wird von $\alpha_1 q \alpha_2$ dadurch beschrieben, daß hierdurch gefordert ist, der SLK befinde sich auf dem $(|\alpha_1| + 1))$-ten Bandkästchen, jenem Kästchen, auf dem sich das erste Symbol von α_2 befindet (falls $\alpha_2 = \epsilon$, befindet sich der SLK auf einem Kästchen, das $\#$ trägt).

Ein *Zug* $\alpha \vdash_M \beta$ einer 1-Band-Turingmaschine M ist der Übergang zwischen Konfigurationen α, β von M durch die Ausführung eines elementaren Berechnungsschrittes von M, der im Lesen eines Zeichens vom Band, dem Drucken eines (eventuell neuen) Zeichens an der gleichen Stelle auf das Band und der anschließenden Bewegung des SLKes von M auf ein benachbartes Bandkästchen besteht.

Für eine *deterministische* Turingmaschine M ist dabei für zwei Konfigurationen α, β ein Zug $\alpha \vdash_M \beta$ genau dann möglich, falls $\alpha_1 \in \Gamma^*$, $X, Y, Z \in \Gamma$, $q, p \in Q$ und $\alpha_2 \in \Gamma^*(\Gamma \backslash \{\#\}) \cup \{\epsilon\}$ existieren, sodaß

$$
\begin{aligned}
\text{(i):} \quad & \big[\alpha = \alpha_1 Z q X \alpha_2 \;\&\; \delta(q, X) = (p, Y, L) \;\& \\
& \quad \&\; (\alpha_2 \neq \epsilon \;\Rightarrow\; \beta = \alpha_1 p Z Y \alpha_2) \;\& \\
& \quad \&\; (\alpha_2 = \epsilon \;\&\; Y \neq \# \;\Rightarrow\; \beta = \alpha_1 p Z Y) \;\& \\
& \quad \&\; (\alpha_2 = \epsilon \;\&\; Y = \# \;\&\; Z \neq \# \;\Rightarrow\; \beta = \alpha_1 p Z) \;\& \\
& \quad \&\; (\alpha_2 = \epsilon \;\&\; Y = \# \;\&\; Z = \#\& \;\Rightarrow\; \beta = \alpha_1 p)\big] \;\vee
\end{aligned}
$$

$$\vee \big[\alpha = \alpha_1 Z q \;\&\; \delta(q,\#) = (p,Y,L) \;\&\; \\ \&\; (Y \neq \# \;\Rightarrow\; \beta = \alpha_1 p Z Y) \;\&\; \\ \&\; (Y = \# \;\&\; Z \neq \# \;\Rightarrow\; \beta = \alpha_1 p Z) \;\&\; \\ \&\; (Y = \# \;\&\; Z = \# \;\Rightarrow\; \beta = \alpha_1 p)\big]$$

oder

$$\text{(ii):} \qquad \alpha = \alpha_1 q X \alpha_2 \;\&\; \delta(q,X) = (p,Y,R) \;\&\; \beta = \alpha_1 Y p \alpha_2 \quad \vee \\ \vee\, \alpha = \alpha_1 q \;\&\; \delta(q,\#) = (p,Y,R) \;\&\; \beta = \alpha_1 Y p$$

gilt.

Für eine *nichtdeterministische* 1-Band-Turingmaschine M und zwei Konfigurationen α, β von M ist ein Zug $\alpha \vdash_M \beta$ genau dann möglich, falls $\alpha_1 \in \Gamma^*$, $\alpha_2 \in \Gamma^*(\Gamma \setminus \{\#\}) \cup \{\epsilon\}$, $X, Z \in \Gamma$, $p \in Q$ ein $Y \in \Gamma$ und ein $p \in Q$ existieren, sodaß (i)' und (ii)' gelten, wobei (i)' und (ii)' aus den oben dargestellten Bedingungen (i) und (ii) durch die Ersetzung aller Ausdrücke $\delta(q,X) = (p,Y,M)$ und $\delta(q,\#) = (p,Y,M)$ durch Ausdrücke $(p,Y,M) \in \delta(q,X)$ und $(p,Y,M) \in \delta(q,\#)$ hervorgehen (für beliebiges $M \in \{L,R\}$).

Sei $M = (Q,\Sigma,\Gamma,\delta,q_0,\#,F)$ eine deterministische oder nichtdeterministische 1-Band-Turingmaschine.

Falls für zwei Konfigurationen α, β von M $\alpha \vdash_M^* \beta$ gilt, so heißt β der *Nachfolger* von α bzw. die *Nachfolgekonfiguration* von α. Die *Anfangskonfiguration* $\sigma_M(x)$ von M für Eingabewort $x \in \Sigma^*$ sei durch $\sigma_M(x) := q_0 x$ gegeben; eine Konfiguration von M ist eine *Endkonfiguration*, falls darin ein Endzustand vorkommt.

Die Definitionen für $\alpha \vdash_M^{(l)} \beta$ ($l \in \mathbb{N}_0$), $\alpha \vdash_M^* \beta$, $\alpha \vdash_M^+ \beta$ (für zwei Konfigurationen α und β von M) sowie von „C ist *Berechnungspfad* von M *für Eingabewort* x“, „C ist *akzeptierender Berechnungspfad* von M *für Eingabewort* x“, „n ist *Länge* eines Berechnungspfades“, „C_1 ist *Teilpfad* eines Berechnungspfades C_2“ können nun aus Definition 1.4.3 (die dort für IOTM's Festsetzungen trifft) für (eine 1-Band-Maschine) M (hierher) übernommen werden.

Für die Definition der von einem akzeptierenden Berechnungspfad erhaltenen Ausgabe ist es jedoch sinnvoll, hier einschränkender als in Definition 1.4.3 folgende Setzung zu verwenden: Ein akzeptierender Berechnungspfad $C = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ von M für Eingabewort $x \in \Sigma^*$ *erhält Ausgabe* $y \in \Gamma^*(\Gamma \setminus \{\#\}) \cup \{\epsilon\}$ genau dann, wenn für ein $q \in F$ $\alpha_n = qy$ gilt (dabei wird also gefordert, daß der SLK am Ende der Berechnung wieder ganz links positioniert ist).

M *akzeptiert* ein Wort $x \in \Sigma^*$, falls es einen akzeptierenden Berechnungspfad von M für ein Eingabewort x gibt. Die von M *akzeptierte Sprache* $L(M)$ sei als $L(M) := \{x \in \Sigma^* / M \text{ akzeptiert } x\} \subseteq \Sigma^*$ definiert.

Sei $f\colon \Sigma^* \to \Delta^*$ eine Funktion für $\Delta \subseteq \Gamma$, Δ ein Alphabet. Falls M eine deterministische Maschine ist, sei gesetzt:

$$\begin{aligned} &M \text{ berechnet die Funktion } f \iff \\ \iff\ &(\forall x \in \Sigma^*)(\exists C \text{ Berechnungspfad}) \\ &\quad \big(C \text{ ist akzeptierender Berechnungspfad von } M \\ &\quad \text{für Eingabewort } x, \text{ der Ausgabe } f(n) \text{ erhält}\big). \end{aligned}$$

Die *Länge* $|C|$ eines Berechnungspfades $C = (\alpha_0, \alpha_1, \ldots, \alpha_n)$ von M auf Eingabe x sei als $|C| := n$ definiert, der *Speicherplatzbedarf* $SP(C)$ des Berechnungspfades C als $SP(C) := max\{|\alpha_i| \,/ i \in \mathbb{N}, 0 \leq i < n\}$ definiert (also als das Maximum von Eingabelänge $|x|$ und der Nummer des während des Ablaufes von C am weitesten rechts auf dem Band aufgesuchten Bandkästchens). Die Definition der *Rechenzeitfunktionen* $Min\text{–}RZ_M(x)$ und der *Speicherplatzfunktion* $Min\text{–}SP_M(x)$ von M für Eingabe x (bzw. von $RZ_M(x)$ und $SP_M(x)$ im Fall, daß M deterministisch ist) können nun aus Definition 1.4.6 übernommen werden.

Für eine Sprache $L \subseteq \Sigma^*$, Funktionen $f : \Sigma^* \to \Delta^*$ mit $\Delta \subseteq \Gamma$, Δ ein Alphabet, Schrankenfunktionen $s, t : \mathbb{N}_0 \to \mathbb{N}_0$ können nun die Definitionen von „*M akzeptiert L mit Rechenzeitschranke $t(n)$*“, „ *... mit Speicherplatzschranke $s(n)$*“, „ *... mit Rechenzeitschranke $t(n)$ und mit Speicherplatzschranke $s(n)$*“ sowie von „*M berechnet f mit Rechenzeitschranke $t(n)$*“ etc. aus Definition 1.4.7 übernommen werden.

Dasselbe gilt für analoge Aussagen *strikte* Schrankenfunktionen betreffend.

Davon ausgehend lassen sich nun analog zu Definition 1.4.8 für Schrankenfunktionen $t, s\colon \mathbb{N}_0 \to \mathbb{R}_0^+$ Komplexitätsklassen für von 1-Band-Turingmaschinen akzeptierten Sprachen bzw. berechneten Funktionen definieren, wofür stellvertretend

$$\begin{aligned} \boldsymbol{DTime_{1\text{-}Band}(t(n))} := \big\{L/&(\exists \Sigma \text{ endl. Alph.}) \\ &(\exists \text{det. 1-Band-Tm. } M \text{ mit Eing.alph. } \Sigma) \\ &(L \subseteq \Sigma^* \ \&\ M \text{ akzeptiert } L \\ &\text{mit Rechenzeitschranke } t(n))\big\}; \end{aligned}$$

$$\begin{aligned} \boldsymbol{NTimeSpace_{1\text{-}Band,\Sigma}(t(n), s(n))} := \\ \big\{L \subseteq \Sigma^*/&(\exists \text{1-Band-Tm. } M \text{ mit Eing.alph. } \Sigma) \\ &(L \subseteq \Sigma^* \ \&\ M \text{ akzeptiert } L \text{ mit Rechenzeit-} \\ &\text{schranke } t(n) \text{ und Speicherplatzschranke } s(n))\big\}; \end{aligned}$$

$$\begin{aligned} \boldsymbol{DFTime^*_{1\text{-}Band,\Sigma,\Delta}(t(n))} := \big\{f\colon \Sigma^* \to \Delta^*/ \\ (\exists \text{1-Band-Tm. } M \text{ mit Eing.alph. } \Sigma, \text{ Bandalph. } \Gamma) \\ \big(\Delta \subseteq \Gamma \ \&\ M \text{ berechnet } f \text{ mit} \\ \textit{strikter} \text{ Rechenzeitschranke } t(n)\big)\big\}; \end{aligned}$$

(für endliche Alphabete Σ, Δ) definiert seien. Analog zu Definition 1.4.8 seien damit hier dann auch bezüglich Funktionenmengen (als Schrankenfunktionen) definierte Komplexitätsklassen erklärt.

Da für die zu definierende Klasse von 1-Band-Turingmaschinen mit Bandalphabet Γ eine handhabbare Kodierungsfunktion festgelegt werden soll, ist es nützlich, die Klasse aller 1-Band-Turingmaschinen mit Bandalphabet Γ noch unwesentlich, aber auf eine *Menge*[12] $\mathcal{EM}_\Gamma$ einzuschränken, für die eine Kodierungsfunktion direkt angegeben werden kann.

Definition 3.3.1. Die Menge $\mathcal{EM}_\Gamma$ von 1-Band-Turingmaschinen mit fixiertem Bandalphabet Γ, die Klasse $\mathcal{EM}$.

Γ sei ein beliebiges endliches Alphabet, $\# \in \Gamma$ ein als dieses Symbol hier fixiertes Leersymbol.

Dann sei die (spezielle) Menge $\mathcal{EM}_\Gamma$ von 1-Band-Turingmaschinen mit einseitig unendlichem Band und Bandalphabet Γ wie folgt erklärt:

$$\boldsymbol{\mathcal{EM}_\Gamma} := \{M = (Q, \Gamma, \Sigma, \delta, q_1, \#, F)/$$
$$M \text{ ist eine det. od. nichtdet. 1-Band-Tm.}$$
$$\text{mit rechtss. unendl. Band;}$$
$$\text{es existiert } k \in \mathbb{N}, \text{ sodaß } Q = \{q_1, \ldots, q_k\} \text{ und } F = \{q_k\}\}$$

Für Schrankenfunktionen $s, t : \mathbb{N}_0 \to \mathbb{N}_0$ seien mit $\boldsymbol{DTime_{\mathcal{EM}_\Gamma}(t(n))}$, $\boldsymbol{NSpace_{\mathcal{EM}_\Gamma}(s(n))}$, $\boldsymbol{DFTime_{\mathcal{EM}_\Gamma}(t(n))}$, $\boldsymbol{DFTimeSpace_{\mathcal{EM}_\Gamma}(t(n), s(n))}$, etc. die Einschränkungen der Komplexitätsklassen $DTime(t(n))$, $NSpace(s(n))$, $DFTime(t(n))$, $DFTimeSpace(t(n), s(n))$, etc. (bzw. $DTime_{\text{1-Band}}(t(n))$, ...) auf die von $\mathcal{EM}_\Gamma$-Maschinen mit den jeweiligen Rechenzeit- oder bzw. und Speicherplatzschranken akzeptierten Sprachen L mit $L \subseteq (\Gamma \backslash \{\#\})^*$ bzw. berechenbaren Funktionen f (mit $f : \Sigma^* \to \Delta^*$ bezügliche Alphabeten Σ, Δ mit $\Sigma \subseteq \Gamma \backslash \{\#\}$ und $\Delta \subseteq \Gamma$) gemeint und bezeichnet; dasselbe gelte für die bezüglich strikter Schrankenfunktionen definierten Klassen $\boldsymbol{DTime^*_{\mathcal{EM}_\Gamma}(t(n))}$, ...

Weiters sei noch die Klasse $\mathcal{EM}$ durch

$$\boldsymbol{\mathcal{EM}} := \{M/(\exists \Gamma \text{ endl. Alph.})\ (\# \in \Gamma \text{ Leersymbol}, M \in \mathcal{EM}_\Gamma)\}$$

festgesetzt.

Das Eingabealphabet Σ von $M = (Q, \Gamma, \Sigma, \delta, q_1, \#, F) \in \mathcal{EM}_\Gamma$ wird weiters öfter in der Bezeichung $\Sigma(M) := \Sigma\ (\subseteq \Gamma \backslash \{\#\})$ verwendet.

[12] Hiermit ist in diesem Fall im besonderen nur gemeint, daß die Zustandsmenge als Teilmenge einer fixierten abzählbaren Grundgesamtheit von möglichen Zuständen $\{q_1, q_2, \ldots\}$ angenommen wird und man dann—einem in der Mathematik verbreiteten Wortgebrauch von „Mengen“ versus „Klassen“ folgend—auch von einer Menge von Turingmaschinen sprechen kann.

Es ist leicht einzusehen, daß sich jede beliebige 1-Band-Turingmaschine M mit Bandalphabet Γ nur durch die Umbenennung von Zuständen (und die dementsprechende Abänderung der Übergangsfunktion δ) und weiters noch einer geringfügigen Änderung von δ in Bezug auf die Endzustände zu einer Maschine $M' \in \mathcal{EM}_\Gamma$ mit dem gleichen Verhalten (für alle möglichen) Eingaben umbilden läßt (und mit insbesondere auch derselben Rechenzeit- und Speicherplatzfunktion).

Es ergibt sich daraus natürlich, daß die Definition gesonderter $\mathcal{EM}$- und $\mathcal{EM}_\Gamma$-Komplexitätsklassen oben inhaltlich eigentlich nicht gerechtfertigt oder nötig ist, da diese deshalb immer mit den entsprechenden Komplexitätsklassen bezüglich 1-Band-Turingmaschinen zusammenfallen. So gelten also beispielsweise die Aussagen

$$DTime_{\mathcal{EM}_\Gamma}(t(n)) = DTime_{\text{1-Band},\Gamma}(t(n)),$$
$$NTimeSpace^*_{\mathcal{EM}}(t(n), s(n)) = NTimeSpace^*_{\text{1-Band}}(t(n), s(n))$$

für alle Schrankenfunktionen $s, t : \mathbb{N}_0 \to \mathbb{R}_0^+$. – Diese speziellen Bezeichnungen wurden hier aber dennoch eingeführt, damit in den später dargestellten Komplexitätsbeweisen direkt erzielte Komplexitätsaussagen von durch Übertragung mittels Simulationen erzielten Aussagen auch durch eine Bezeichnung klar unterschieden werden können.

Wird nun für ein endliches Alphabet Γ, das ein als solches vorgesehenes Leersymbol $\#$ enthält, noch eine Symbolfunktion $Symb : \{0, 1, \ldots, |\Gamma| - 1\} \to \Gamma$, die bijektiv ist und also die Symbole von Γ zu nummerieren gestattet, gewählt, so ist damit eine explizite Kodierungsfunktion $\langle\cdot\rangle_{\Gamma,Symb} : \mathcal{EM}_\Gamma \to (\Gamma \setminus \{\#\}) \cup \Sigma_{\text{code}}$ definierbar, wobei Σ_{code} ein noch anzugebendes Alphabet von Symbolen ist, die zum Zweck der Kodierung zusätzlich verwendet werden.

Definition 3.3.2. Eine Kodierung für $\mathcal{EM}_\Gamma$-Maschinen.

Γ sei ein endliches Alphabet, $\# \in \Gamma$ ein hiermit fixiertes Leersymbol, $Symb : \{0, 1, \ldots, |\Gamma| - 1\} \to \Gamma$ eine bijektive Funktion mit $Symb(0) = \#$.

Dann sei $\langle\cdot\rangle_{\Gamma,Symb} : \mathcal{EM}_\Gamma \to \big((\Gamma \setminus \{\#\}) \cup \Sigma_{\text{code}}\big)^+$ mit

$$\Sigma_{\text{code}} = \{\mathbf{A}, \mathbf{B}, \ldots, \mathbf{Z}, \mathbf{0}, \mathbf{1}, \ldots, \mathbf{9}, \mathbf{:}, \mathbf{\text{-}}, \mathbf{\_}, \mathbf{\{}, \mathbf{\}}, \mathbf{(}, \mathbf{)}, \mathbf{;}, \mathbf{,}, \mathbf{.}\} \qquad (\# \notin \Sigma_{\text{code}})$$

die wie folgt definierte (injektive) Kodierungsfunktion:

Für $M \in \mathcal{EM}_\Gamma$, $M = (Q, \Gamma, \Sigma, \delta, q_1, \#, F)$ mit $Q = \{q_1, \ldots, q_k\}$ $(k \in \mathbb{N})$ und $\Sigma = \{Symb(i_1), Symb(i_2), \ldots, Symb(i_m)\}$ mit $m \in \mathbb{N}$, $m \geq 2$, und $i_1, \ldots, i_m \in \mathbb{N}$,

$1 \leq i_1 < i_2 < \ldots < i_m < |\Gamma|$ *sei* $\langle M \rangle_{\Gamma,Symb}$ *wie folgt erklärt:*

$$\begin{aligned}\langle M \rangle_{\Gamma,Symb} := \ & \textbf{MACHINE:\_INPUT-ALPHABET} \circ \\ & \quad \circ \ \textbf{\{SY } Symb(i_1)\textbf{ , } \ldots \textbf{ , SY } Symb(i_m)\textbf{\}; } \circ \\ & \circ \ \textbf{BEGIN} \circ \\ & \quad \circ \ I_1 \textbf{ ; } I_2 \textbf{ ; } \ldots \textbf{ ; } I_k \circ \\ & \circ \ \textbf{END.}\end{aligned}$$

(hierin bezeichnet $\circ$ *das Verkettungssymbol, das nicht Teil des Kode-Strings ist, sondern nur andeuten soll, daß dieser an der betreffenden Stelle noch nicht zuende ist, sondern nur strukturiert geschrieben wurde), wobei die noch zu definierenden Zeichenketten* I_i *(*$1 \leq i \leq k$*) Kodierungen der Übergangsfunktion* δ *im Zustand* q_i *entsprechen und so festgelegt sind:*

Für $i \in \mathbb{N}$, $i = k$ *als*

$$I_k := \mathbf{Q}(k)_{10}\textbf{:\_ STOP}$$

(wobei hier und im weiteren $(n)_{10}$ *die im Dezimalsystem geschriebene Zahl* $n \in \mathbb{N}$ *bedeutet (vgl. Definition 3.3.4) und also eine Zeichenkette aus* $\{\mathbf{1}, \ldots, \mathbf{9}\}\{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{9}\}^*$ *ist),*
für $i \in \mathbb{N}$, $i < k$ *als*

$$\mathbf{Q}\ (i)_{10}\textbf{:\_ BLANK,\{}L_{i,0}\textbf{\}; } Symb(1)\textbf{ ,\{}L_{i,1}\textbf{\}; } \ldots \textbf{; } Symb\ (|\Gamma| - 1)\textbf{ ,\{}L_{i,|\Gamma|-1}\textbf{\}}$$

wobei die noch zu präzisierenden Zeichenketten $L_{i,j}$ *(*$i, j \in \mathbb{N}_0$, $1 \leq i \leq k-1$, $j < |\Gamma|$*) Kodierungen der im Zustand* q_i *auf Bandsymbol* $Symb(j)$ *möglichen Aktionen von* M *sind. Diese Strings* $L_{i,j}$ *sind wie folgt definiert:*

$$L_{i,j} := \epsilon$$

falls $\delta(q_i, Symb(j)) = \emptyset$ *(im Fall, daß* M *nichtdeterministisch ist) bzw. falls* $\delta(q_i, Symb(j))$ *undefiniert ist (im Fall, daß* M *deterministisch ist), und*

$$L_{i,j} := \textbf{(}\mathbf{Q}\ (\tilde{I}_1)_{10}\textbf{ , }S_1\textbf{ , }M_1\textbf{),(}\mathbf{Q}\ (\tilde{I}_2)_{10}\textbf{ , }S_2\textbf{ , }M_2\textbf{), } \ldots \textbf{ ,}\mathbf{Q}\ (\tilde{I}_N)_{10}\textbf{ , }S_N\textbf{ , }M_N\textbf{)}$$

falls $N \in \mathbb{N}$, $\tilde{I}_1, \ldots, \tilde{I}_N \in \{1, \ldots, k\}$, $J_1, \ldots, J_N \in \{0, 1, \ldots, |\Gamma| - 1\}$, $M_1, \ldots, M_N \in \{\mathbf{L}, \mathbf{R}\}$ *existieren, sodaß mit* $S_1, \ldots, S_N \in (\Gamma \setminus \{\#\}) \cup \{\mathbf{BLANK}\} \subseteq$ $\subseteq \big((\Gamma \cup \{\mathbf{B}, \mathbf{L}, \mathbf{A}, \mathbf{N}, \mathbf{K}\}) \setminus \{\#\}\big)^*$ *gilt:*

(1) $\delta(q_i, Symb(j)) = \{(q_{\tilde{I}_1}, Symb(J_1), M_1), \ldots, (q_{\tilde{I}_N}, Symb(J_N), M_N)\}$
(im Fall, daß M *nichtdeterministisch ist), bzw.*
$\delta(q_i, Symb(j)) = (q_{\tilde{I}_N}, Symb(J_1), M_1)$ *und* $N = 1$
(im Fall, daß M *nichtdeterministisch ist);*

(2) die 3*-Tupel* $(\tilde{I}_1, J_1, M_1), \ldots, (\tilde{I}_N, J_N, M_N)$ *lexikographisch aufsteigend geordnet sind;*

(3) für $l \in \{1, \ldots, N\}$ *gilt:*

$$S_l := \begin{cases} \textbf{BLANK} & \ldots\ J_l = 0 \\ Symb(J_l) & \ldots\ J_l > 0 \end{cases}$$

Für den wichtigen äußeren Teil der Komplexitätsbeweise in [FiR74], jenen Teil, in dem die Methode der Diagonalisierung wirklich zum Tragen kommt, ist es wesentlich, daß die verwendeten Kodierungen von Turingmaschinen nicht nur erkennbar, sondern auch in deterministischer[13] polynomialer Rechenzeit von einer 1-Band-Turingmaschine der eingeschränkten Klasse erkannt werden können. Obwohl im vorliegenden Fall der Kodierungen $\langle\cdot\rangle_{\Gamma,Symb}$ leicht einzusehen ist, daß das der Fall ist (es stecken in diesen Kodierungen keine schwer-erkennbaren Komplexitäten), sollte man sich davon dennoch auch ausführlich überzeugen. Das geschieht jedoch nur skizzenhaft beim Beweis des folgenden Lemmas:

Lemma 3.3.3. Γ *ein endliches Alphabet,* $\# \in \Gamma$ *ein hiermit fixiertes Leersymbol,* $Symb : \{0, 1, \ldots, |\Gamma| - 1\} \to \Gamma$ *bijektiv mit* $Symb(0) = \#$, Σ_{code} *wie in Definition 3.3.2,* $\langle\cdot\rangle_{\Gamma,Symb} : \mathcal{EM}_\Gamma \to \big((\Gamma \setminus \{\#\}) \cup \Sigma_{\text{code}}\big)^+$ *die wie in Definition 3.3.2 beschriebene Kodierungsfunktion für* $\mathcal{EM}_\Gamma$*-Turingmaschinen.*

Dann gilt: Die Menge der Kodes von $\mathcal{EM}_\Gamma$*-Turingmaschinen bzgl.* $\langle\cdot\rangle_{\Gamma,Symb}$ *ist mit Hilfe einer* $\mathcal{EM}_{\Gamma\cup\Sigma_{\text{code}}}$*-Turingmaschine in deterministischer polynomialer Rechenzeit erkennbar. Insbesondere gilt für* $L := \{\langle M\rangle_{\Gamma,Symb} / M \in \mathcal{EM}_\Gamma\} \subseteq ((\Gamma \setminus \{\#\}) \cup \Sigma_{\text{code}})^+$

$$L,\ \text{co}-L \in DTime_{\mathcal{EM}_{\Gamma\cup\Sigma_{\text{code}}}}(POL).$$

Beweisskizze. Hier seien nur die für die Überprüfung einer Zeichenkette $w \in \big((\Gamma \setminus \{\#\}) \cup \Sigma_{\text{code}}\big)^*$, ob diese einen Maschinencode $\langle M\rangle_{\Gamma,Symb}$ für $M \in \mathcal{EM}_\Gamma$ darstellt, nötigen äußeren Schritte beschrieben. Es ist aber trotzdem aus der Form dieser Schritte ersichtlich, daß sie von einer deterministischen $\mathcal{EM}_{\Gamma\setminus\{\#\}\cup\Sigma_{\text{code}}}$-Maschine nacheinander, jeweils in polynomialer Rechenzeit und so insgesamt in polynomialer Rechenzeit ausgeführt werden können. Diese Schritte sind:

(1) Überprüfen, ob w die äußere Form eines Maschinencodes hat, insbesondere

[13] Für den wesentlichen in Satz 3.4.1 formalisierten Teil der Komplexitätsbeweise würde eigentlich auch nichtdeterministische polynomiale Rechenzeit genügen, wenn zusätzlich die Erkennung vom Anfang und Ende eines Kodestrings auch diese Eigenschaft hat. – Da in den Beweisen später mit diesen Kodierungen aber auch operiert werden muß, d.h. insbesondere Formeln $\mathbf{F}_{M,w}$ aus $\langle M\rangle_{\Gamma,Symb}$ und w immer in deterministischer polynomialer Rechenzeit hergestellt werden müssen, ist diese Beobachtung praktisch (sehr wahrscheinlich) unbedeutend.

(i) ob w die Gestalt

$$\textbf{MACHINE:\_INPUT-ALPHABET\{}\,IL\,\textbf{\};}$$
$$\textbf{BEGIN}\,I_1\,\textbf{;}\,I_2\,\textbf{;}\,\ldots\,\textbf{;}\,I_k\,\textbf{END.}$$

für Strings $IL, I_1, \ldots, I_k \in (\Sigma_{\text{code}} \cup \Gamma)^*$ $(k \in \mathbb{N})$, die noch weiter untersucht werden, hat;

(ii) ob IL der Gestalt $\textbf{SY}a_1\textbf{,SY}a_2\textbf{,SY}a_3\textbf{,}\ldots\textbf{,SY}a_m$ mit $m \in \mathbb{N}$, $m \geq 2$ und $a_j \in \Gamma$ $(1 \leq j \leq m)$ ist;

(iii) ob I_i (falls $i < k$) von der Form

$$\textbf{Q}w\textbf{:\_BLANK,\{}L_{i,0}\textbf{\};}\,Symb(1)\,\textbf{,\{}L_{i,1}\textbf{\};}\ldots\textbf{;}\,Symb(|\Gamma|-1)\,\textbf{,\{}L_{i,|\Gamma|-1}\textbf{\};}$$

mit $w \in \{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{9}\}^+$ und noch weiter zu untersuchenden $L_{i,j}$ ist, bzw. ob I_i (falls $i = k$) (und also danach nur **END.** folgt) von der Form

$$\textbf{Q}\ w\textbf{:\_STOP}$$

mit $w \in \{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{9}\}^+$ ist;

(iv) ob die Listen $L_{i,j}$ in I_i entweder leere Listen oder durch Beistriche getrennte Listen von 3-Tupel der Gestalt

$$\textbf{(Q}\ w\textbf{,}\ a\textbf{,}\ M\textbf{)}$$

mit $w \in \{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{9}\}^+$, $a \in (\Gamma \setminus \{\#\}) \cup \{\textbf{BLANK}\}$, $M \in \{\mathbf{L}, \mathbf{R}\}$ sind.

(2) Überprüfen, ob die dem Eingabealphabet zugeordnete Liste $a_1, \ldots, a_m$ in IL nur Symbole von $\Gamma \setminus \{\#\}$ enthält, ob die Symbole a_j $(1 \leq j \leq m)$ von einer aufsteigenden Folge $1 \leq i_1 < i_2 \ldots < i_m \leq |\Gamma| - 1$ vermittels $a_j := Symb(i_j)$ $(1 \leq j \leq m)$ stammen.

(3) Überprüfen, ob die Nummerierung der Zustände in den I_i, von 1 beginnend, fortlaufend ist, ob also I_i wirklich mit

$$\textbf{Q}\ (i)_{10}\ \textbf{:\_}\ldots$$

beginnt.

(4) Überprüfen, ob die 3-Tupel in den Listen $L_{i,j}$ $(1 \leq i \leq k,\ 0 \leq j < |\Gamma|,\ i, j \in \mathbb{N}_0)$ in ihrer ersten Komponente zulässige, den Zahlen $1 \ldots k$ in dezimaler Darstellung entsprechende Strings aus $\{\mathbf{1}, \ldots, \mathbf{9}\}\{\mathbf{0}, \mathbf{1}, \ldots, \mathbf{9}\}^*$ enthalten.

(5) Überprüfen, ob die den 3-Tupel in den Listen $L_{i,j}$ zugeordneten Tupel $\tilde{I}_1, J_1, M_1, \ldots, \tilde{I_N}, J_N, M_N$ (vgl. Definition 3.3.2) ($N \in \mathbb{N}$), $\tilde{I}_1, \ldots, \tilde{I_N} \in \{0, 1, \ldots, |\Gamma| - 1\}$, $J_1, \ldots, J_N \in \{0, 1, \ldots, |\Gamma| - 1\}$, $M_1, \ldots, M_N \in \{\mathbf{L}, \mathbf{R}\}$) lexikographisch aufsteigend geordnet sind.

$\diamondsuit$

Definition 3.3.4. Bezeichnungen für Zahlen im a-adische System und Binärwörter.

(i) *Sei* $a \in \mathbb{N}$, $2 \leq a \leq 10$.

Die Darstellung einer natürlichen Zahl n im a-adischen Zahlensystem wird durch folgende Funktion beschrieben:

$$(\cdot)_a : \mathbb{N}_0 \longrightarrow \{1, \ldots, a-1\}\{0, 1, \ldots, a-1\}^* \cup \{0\}$$
$$n \longmapsto (n)_a := \textit{Zahl } n\textit{, in der Darstellung als Zahlwort im a-adischen System.}$$

(ii) $BW := \{0,1\}^*$ *sei die Menge der Binärwörter;*
$BW0 := \{0,1\}^+$ *sei die Menge aller Binärwörter positiver Länge;*
$BZW := 1\{0,1\}^* \cup \{0\}$ *sei die Menge der Dualzahlen darstellenden Binärwörter (es gilt* $BZW = \{(n)_2 / n \in \mathbb{N}_0\}$*);*
$BW1 := \{0,1\}^*1 \cup \{0\}$ $(\subseteq BW)$ *sei jene Menge von Binärwörtern, die umgedrehten Dualzahlen entsprechen (es gilt* $BW1 = \{((n)_2)^R / n \in \mathbb{N}_0\}$*);*
$DZW := \{1, \ldots, 9\}\{0, 1, \ldots, 9\}^* \cup \{0\}$ *sei die Menge der dezimalen Zahlwörter (es gilt* $DZW = \{(n)_{10} / n \in \mathbb{N}_0\}$*).*

(iii) *Für Binärwörter* $w \in BW$ *sei hier (zum Zweck einfacherer Schreibweise in den folgenden Beweisen) in Erweiterung der Setzung von Definition 1.3.2 das* $(i+1)$*-te Sumbol* ($i \in \mathbb{N}_0$) *von w auch dann definiert, wenn w weniger als* $i+1$ *Symbole hat; in diesem Fall erfolgt als Setzung für dieses Symbol das Symbol* 0*:*

Für $w \in BW$ *mit* $|w| = n$ ($n \in \mathbb{N}$) *und* $w = x_1 \circ \ldots \circ x_n$ *mit* $x_i \in \{0,1\}$ ($1 \leq i \leq n$, $i \in \mathbb{N}$) *sei für alle* $i \in \mathbb{N}_0$ *gesetzt:*

$$w(i) := \begin{cases} x_{i+1} & \ldots \ 0 \leq i < n \\ 0 & \ldots \ i \geq n \end{cases}$$

Für $w \in BW$ *mit* $w = \epsilon$ *sei*

$$w(i) := 0 \qquad (i \in \mathbb{N}_0).$$

In den Komplexitätsbeweisen in den folgenden Abschnitten spielen an vielen Stellen Eigenschaften wie die von Formeln $\mathbf{A}_n$ aus Familien $\{\mathbf{A}_n\}_{n\in\mathbb{N}_0}$ von Formeln einer Theorie T, $O(n)$-längenbeschränkt zu sein und in von $|(n)_{10}|$ abhängigem $POLYLIN$-Aufwand mechanisch bzw. algorithmisch hergestellt werden zu können, eine wichtige Rolle. Diese Eigenschaften sowie recht ähnliche, sich auf Formeln $\mathbf{B}_w$ aus Familien $\{\mathbf{B}_w\}_{w\in BW0}$ beziehende sollen durch die folgende Definition fixiert werden.

Definition 3.3.5. Die Längen- und Konstruierbarkeitsbedingungen (A) und (B) für Formelfamilien.

$T = (\Sigma_T, Fo_T, Thm_T)$ sei eine als System formaler Sprachen aufgefaßte mathematisch-logische Theorie. $\{\mathbf{A}_n\}_{n\in\mathbb{N}_0}$ und $\{\mathbf{B}_w\}_{w\in BW0}$ seien Familien von Formeln von T. Dann sei festgesetzt:

(i): Die Familie $\{\mathbf{A}_n\}_{n\in\mathbb{N}_0}$ genügt der **(Längen- und Konstruierbarkeits-) Bedingung (A)**, *falls (α) und (β) gelten, wobei:*

(α): *Für* $g_1 : \begin{array}{ccc} \mathbb{N}_0 & \longrightarrow & \mathbb{N}_0 \\ n & \longmapsto & |\mathbf{A}_n| \end{array}$ *gilt:* $g_1 \in O(n)$;

(β): *Für* $g_2 : \begin{array}{ccc} DZW & \longrightarrow & Fo_T \\ (i)_{10}\ [\text{für } i \in \mathbb{N}_0] & \longmapsto & \mathbf{A}_i \end{array}$ *gilt:* $g_2 \in POLYLIN$.

(ii): Die Familie $\{\mathbf{B}_w\}_{w\in BW0}$ genügt der **(Längen- und Konstruierbarkeits-) Bedingung (B)**, *falls (α) und (β) gelten, wobei:*

(α): *Für* $g_1 : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ *gilt:* $g_1 \in O(n)$;

$$n \longmapsto \begin{cases} 0 & \dots\ n = 0 \\ \max\limits_{\substack{w\in BW0,\\ |w|=n}} |\mathbf{B}_w| & \dots\ n \geq 1 \end{cases}$$

(β): *Für* $g_2 : \begin{array}{ccc} BW0 & \longrightarrow & Fo_T \\ w & \longmapsto & \mathbf{B}_w \end{array}$ *gilt:* $g_2 \in POLYLIN$.

In leichter Erweiterung des in [Shoe67] für Theorien 1. Ordnung verwendeten Formalismus wird hier auch die dezimale Indizierung von Variablen in Formeln einer Theorie 1. Ordnung im Sinn von [Shoe67] gestattet; dies deswegen, weil bei der Darstellung der Komplexitätsbeweise, die sich ja v.a. auf Formelsprachen mit informatisch-sinnvoller Syntax beziehen sollen, ein allzugroßer Beschreibungsaufwand entstehen würde, wenn Formeln zuerst mit unärer Strichindizierung wie in [Shoe67] und dann noch einmal mit dezimaler Subscript-Indizierung angeschrieben werden müßten. Es ist aber klar, daß sich hieraus keine weiterreichenden, den logischen Kalkül einer Theorie 1. Ordnung nach [Shoe67] betreffenden Konsequenzen ergeben.

Weiters werden—einer verbreiteten Bezeichungsweise folgend, die auch in [FiR74] benutzt wird—Formeln $\mathbf{A}$, in denen *genau* die n paarweise verschiedenen Variablen $\mathbf{x}_1, \ldots, \mathbf{x}_n$ frei vorkommen, auch durch $\mathbf{A}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ bezeichnet. (Im Gegensatz dazu verwenden aber z.B. [HiBe68] diese Bezeichungsweise für Formeln $\mathbf{A}$, in denen *jedenfalls* $\mathbf{x}_1, \ldots, \mathbf{x}_n$ frei vorkommen).

Aus dieser Bezeichnungsweise ergeben sich jedoch folgende erwähnenswerte, Substitutionen in diesen Formeln betreffende Folgerungen bzw. Unterschiede mit der Handhabung von Substitutionen in Formeln in [Shoe67]: Sollen in einer Formel $\mathbf{A}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ für die Variablen $\mathbf{x}_1, \ldots, \mathbf{x}_n$ die Terme $\mathbf{a}_1, \ldots, \mathbf{a}_n$ gesetzt bzw. substituiert werden, so wird *eine* dafür entstehende Substitutionsformel (bzw. *Instanz* von $\mathbf{A}$) mit $\mathbf{A}(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ bezeichnet. Hierbei entsteht $\mathbf{A}(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ aus $\mathbf{A}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ durch die *gleichzeitige* Ersetzung aller Variablen $\mathbf{x}_i$ in $\mathbf{A}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$, die an solchen Stellen darin vorkommen, an denen $\mathbf{x}_i$ frei in $\mathbf{A}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ auftritt, durch $\mathbf{a}_i$ $(1 \leq i \leq n)$; und zwar selbst dann, wenn solche Substitutionen die vorherige Umbenennung von gebundenen Variablen in $\mathbf{A}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ nötig machen, um zu verhindern, daß durch die beschriebenen Einsetzungen der Terme $\mathbf{a}_1, \ldots, \mathbf{a}_n$ für $\mathbf{x}_1, \ldots, \mathbf{x}_n$ eine der in $\mathbf{a}_1, \ldots, \mathbf{a}_n$ vorkommenden Variablen durch eine Quantifikation in $\mathbf{A}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ gebunden wird. – Demgegenüber setzt [Shoe67] beim Gebrauch von $\mathbf{A}_{\mathbf{x_1},\ldots,\mathbf{x_n}}[\mathbf{a}_1, \ldots, \mathbf{a}_n]$ immer voraus, daß dabei durch die Einsetzungen der $\mathbf{a}_1, \ldots, \mathbf{a}_n$ *kein* solcher Konflikt mit den in $\mathbf{A}$ gebunden erscheinenden Variablen entsteht; in diesem Fall würden, ausgehend von einer Formel $\mathbf{A}$, in der genau $\mathbf{x}_1, \ldots, \mathbf{x}_n$, die paarweise verschieden sind, auftreten und die hier als $\mathbf{A}(\mathbf{x}_1, \ldots, \mathbf{x}_n)$ angeschrieben werden könnte, die Formel $\mathbf{A}_{\mathbf{x_1},\ldots,\mathbf{x_n}}[\mathbf{a}_1, \ldots, \mathbf{a}_n]$ und *die* Formel $\mathbf{A}(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ aber übereinstimmen.

Solche sich aus dieser Formelbezeichnungsweise ergebende, Substitutionen betreffende Probleme werden allerdings bei der genauen Festlegung von in den Komplexitätsbeweisen verwendeten Formeln immer vermieden werden, und zwar dadurch, daß Substitutionen (v.a. auch aus anderen Gründen) darin immer umgangen werden. Diese exakten Festlegungen werden aus Umfangsgründen jedoch nicht immer ausführlich angeschrieben (weil deren Gestalt sich aus kürzer angeschriebenen Formeln dann oft leicht finden läßt) und daher sollte an dieser Stelle auf (möglicherweise unerwünschte und hier immer zu vermeidende) Konsequenzen dieser Schreibweise aufmerksam gemacht werden.

In den folgenden Abschnitten tritt in einigen Beweisen ein einfaches Abschätzungsproblem auf, das hier allgemein behandelt werden soll. So steht hinter den Fragen, wieviele Variablen in einer Formel gegebener Länge (bei festgesetzter Formelsyntax und also auch fixierter Art der Variablenindizierung) höchstens vorkommen können, oder, wieviele Anweisungen ein Programmcode gegebener Länge (ebenfalls bei fixierter Syntax) höchstens enthalten kann, jedenfalls auch die Frage, wieviele verschiedene Zahlen im a-adischen System ($a \in \mathbb{N}$, $a \geq 2$) bei vorgegebener Gesamtstellenlänge n höchstens angeschrieben werden können. Das einfachere und bekanntere umgekehrte Problem, welche Gesamtstellenlänge das Anschreiben der Zahlen $0, 1, 2, \ldots, n$ $(n \in \mathbb{N}_0)$ im a-adischen Zahlsystem

($a \in \mathbb{N}$, $a \geq 2$) erfordert, besitzt als Lösung eine Funktion von der assymptotischen Größenordung $n \log_a n$.

Definition 3.3.6. *Sei ($a \in \mathbb{N}$, $a \geq 2$). Die Funktionen $h_a : \mathbb{N}_0 \to \mathbb{N}$ und $g_a : \mathbb{N} \to \mathbb{N}_0$ seien wie folgt definiert:*

$$\begin{aligned} h_a(n) := \;& \textit{Gesamtsymbolanzahl, die im } a\textit{-adischen Zahlensystem nötig ist,} \\ & \textit{um die Zahlen } 0, 1, 2, \ldots, n \textit{ anzuschreiben ;} \\ g_a(n) := \;& (\nu z)^{14}\,[h_a(m) \leq z] = (\mu z)^{15}\,[h_a(m+1) > z] = \\ = \;& \textit{maximales } n \in \mathbb{N}_0 \textit{ so, daß das Anschreiben der Zahlen} \\ & \textit{aus } \mathbb{N}_0\textit{, die kleiner als } n \textit{ sind, eine Gesamtsymbolanzahl} \\ & \leq m \textit{ besitzt .} \end{aligned}$$

Lemma 3.3.7. *$a \in \mathbb{N}$, $a \geq 2$, g_a, h_a wie in Definition 3.3.6. Dann gilt*[16]*:*

(i) $h_a(0) = 1$, $h_a(n) = 1 + p \cdot (n+1) - \dfrac{a^p - 1}{a - 1}$ *mit* $p = \lfloor \log_a n \rfloor + 1$ *für* $n \in \mathbb{N}$ *;*

(ii) $h_a(n) \sim n \cdot \log_a n$ *;*

(iii) $g_a(m) \cdot \log_a g_a(m) \sim m$ *(daraus folgt sofort auch* $g_a(m) \in o(m)$*).*

Beweis. (i): (a) Für

$$s_n^{(a)} := \sum_{i=0}^{n} a^i\,, \qquad s_n^{(a,1)} := \sum_{i=0}^{n} i \cdot a^i \qquad (n \in \mathbb{N}_0)$$

gilt:

$$s_n^{(a)} = \frac{a^{p-1} - 1}{a - 1}\,, \qquad s_n^{(a,1)} = \frac{1}{a-1}\left[\, n\, a^{n+1} - s_n^{(a)} + 1 \right] \qquad (n \in \mathbb{N}_0)$$

Hierbei ist der Ausdruck für $s_n^{(a)}$ die bekannte Summenformel für die (endliche) arithmetische Reihe, der Ausdruck für $s_n^{(a,1)}$ läßt sich durch Induktion bestätigen:

[15] „$(\nu z)[\ldots]$“ steht für das größte $z \in \mathbb{N}_0$ mit der Eigenschaft $[\ldots]$, falls ein solches existiert, und ist sonst undefiniert.

[15] „$(\mu z)[\ldots]$“ steht für das kleinste $z \in \mathbb{N}_0$ mit der Eigenschaft $[\ldots]$, falls überhaupt ein solches $z \in \mathbb{N}_0$ existiert, sodaß $[\ldots]$ gilt, und ist andernfalls undefiniert.

[16] Für die Definition von $f(n) \sim g(n)$ (assymptotisch gleiches Wachstum) für zahlentheoretische Funktionen $f, g : \mathbb{N}_0 \to \mathbb{R}_0^+$ vgl. Definition 1.3.6

Induktionsanfang, $n = 0$: Durch Einsetzen und Nachrechnen direkt einzusehen.
Induktionsschritt $n \to n+1$:

$$\begin{aligned} s_{n+1}^{(a,1)} &= s_n^{(a,1)} + (n+1)\,a^{n+1} = \frac{1}{a-1}\Big[\,n\,a^{n+1} - s_n^{(a)} + 1\Big] + (n+1)\,a^{n+1} \\ &= \frac{1}{a-1}\Big[\,a^{n+1}((n-1)\,(a-1)+n) - s_n^{(a)} + 1\Big] \\ &= \frac{1}{a-1}\big[\,a^{n+1}(n+1) - \underbrace{a^{n+1} - s_n^{(a)}}_{=-s_{n+1}^{(a)}} + 1\,\big] \end{aligned}$$

Hier ist der Ausdruck für $s_n^{(a)}$ die bekannte Summenformel für die (endliche) arithmetische Reihe, der Ausdruck für $s_n^{(a,1)}$ läßt sich durch Induktion bestätigen:

(b) $h_a(a^p - 1) = 1 + p\,a^p - s_{p-1}^{(a)}$ für $p \in \mathbb{N}$:

$$\begin{aligned} h_a(a^p-1) &= a\cdot 1 + (a-1)\,a\cdot 2 + (a-1)\,a^2\cdot 3 + \ldots + (a-1)\,a^{p-1}\cdot p \\ &= \underbrace{a\cdot 1 - (a-1)\,a^0\cdot 1}_{=1} + (a-1)\sum_{i=0}^{p-1} a^i\cdot(i+1) \\ &= 1 + (a-1)\,\big[\,\underbrace{s_{p-1}^{(a)} + s_{p-1}^{(a,1)}}_{=\frac{1}{a-1}\left[(p-1)a^p - \frac{a^{p-1}-1}{a-1} + 1 + a^p - 1\right]}\,\big] \\ &= 1 + p\,a^p - \frac{a^{p-1}-1}{a-1} \end{aligned}$$

(c) Es gilt die Aussage von (i):
Für $n = 0$ gilt:

$$\begin{aligned} h_a(0) = {} & \text{Symbolanzahl, um im } a\text{-adischen System die Zahl 0} \\ & \text{anzuschreiben } = 0\,; \end{aligned}$$

Für $n \in \mathbb{N}$ gilt mit $p := \lfloor \log_a n \rfloor + 1$ (d.h. p so, daß $a^{p-1} \le n < a^p$)

$$\begin{aligned} h_a(n) &= h_a(a^{p-1}-1) + p\,(n - a^{p-1} + 1) \\ &\underset{\text{(b)}}{=} 1 + (p-1)\,a^{p-1} - \frac{a^{p-1}-1}{a-1} + p\,(n - a^{p-1} + 1) \\ &= 1 - a^{p-1} - \frac{a^{p-1}-1}{a-1} + p\,(n+1) \\ &= 1 + p\,(n+1) - \frac{a^{p-1}-1}{a-1}\,. \end{aligned}$$

(ii): folgt aus (i), denn es gilt:

$$h_a(n) = 1 + \underbrace{(\lfloor \log_a n \rfloor + 1) \cdot (n+1)}_{\sim n \log_a n} - \underbrace{\frac{a^{\lfloor \log_a n \rfloor + 1}}{a-1}}_{= \frac{a^{2 \cdot n - 1}}{a-1} \in O(n)} \sim n \log_a n \,.$$

(iii): folgt aus (ii) und der Definition von g_a, h_a: Wegen der Definition von g_a gilt:

$$\begin{gathered} h_a(g_a(m)) \leq m, \qquad m < h_a(g_a(m)+1) \\ (m \in \mathbb{N}) \,. \end{gathered} \tag{3.6}$$

Wegen (ii) gilt aber (wegen $\lim_{m \to \infty} g_a(m) = +\infty$)

$$\begin{aligned} h_a(g_a(m)) &\sim g_a(m) \cdot \log_a g_a(m) \,, \\ h_a(g_a(m)+1) &\sim (g_a(m)+1) \cdot \log_a(g_a(m)+1) \\ &\sim g_a(m) \cdot \log_a g_a(m) \\ &(m \in \mathbb{N}_0) \,. \end{aligned} \tag{3.7}$$

Aus (3.6), (3.7) folgen jedenfalls

$$\begin{aligned} \limsup_m \frac{g_a(m) \cdot \log_a g_a(m)}{m} &\leq 1 \,, \\ \liminf_m \frac{g_a(m) \cdot \log_a g_a(m)}{m} &\geq 1 \,, \end{aligned}$$

also $\lim_{m \to \infty} \frac{g_a(m) \cdot \log_a g_a(m)}{m} = 1$, d.h. $g_a(m) \cdot \log_a g_a(m) \sim m$. Weiters gilt natürlich $\frac{g_a(m)}{m} \sim \frac{g_a(m)}{g_a(m) \cdot \log_a g_a(m)} \sim \frac{1}{\log_a g_a(m)} \underset{m \to \infty}{\to} 0$, daraus folgt $g_a(m) = o(m)$.

□

3.4 Allgemeiner Teil der Komplexitätsbeweise

Wie im Abschnitt 2 angedeutet, beruht die in [FiR74] entwickelte und verwendete Methode zur Erzielung unterer Schranken für die Entscheidungskomplexität von bekannten entscheidbaren Theorien der Additionsarithmetik v.a. auf: Der Entwicklung von Formeln $\mathbf{F}_{M,w}$ in den behandelten Theorien, die zu einer vorgegebenen Schrankenfunktion $f(n)$ die Eigenschaft einer Turingmaschine M (aus einer eingeschränkten, aber universellen Klasse), ein Eingabewort w (über einem in Frage kommenden Alphabet) mit (im wesentlichen) Rechenzeitschranke) $f(n)$ zu akzeptieren, genau ausdrücken; damit ist gemeint, daß diese Formeln $\mathbf{F}_{M,w}$ in der jeweils behandelten Theorie Theoreme sind, genau dann, wenn die zugehörige, hier beschriebene Eigenschaft von M und w bezüglich $f(n)$ gilt. Es muß bei diesem Vorgehen also die Eigenschaft von M, ein Wort w (für genau spezifizierte Turingmaschinen M und Wörter w) mit $Min\text{-}RZ_M(w) \leq f(|w|)$ zu akzeptieren, in T *ausdrückbar* sein.

Der in diesem Abschnitt behandelte allgemeine Teil der Komplexitätsbeweise in [FiR74] gliedert sich in zwei Schritte: Erstens in eine Aussage, wie unter der Voraussetzung dieser erwähnten Ausdrückbarkeitseigenschaft eine untere Schranke für die jeweils behandelte Theorie bewiesen werden kann. Und zweitens in eine allgemeine Methode, wie unter der Annahme der Existenz von bestimmten Grundformeln mit präzisierten Längen- und Konstruierbarkeitseigenschaften, die Binärwörter der Länge $(f(n))^2$ beschreiben helfen, Formeln $\mathbf{F}_{M,w}$ aufgebaut werden können, die den Vorausetzungen des ersten Teiles genügen. Dabei müssen die erwähnten Grundformeln, um die Komplexitätsbeweise abzuschließen, später in den einzelnen behandelten Theorien der Additionsarithmetik gesondert konstruiert werden (vgl. Abschnitt 5, Abschnitt 6 und Abschnitt 7).

Der erste Schritt besteht in der Hauptsache aus dem folgenden Satz 3.4.1, der allgemeine Bedingungen enthält und angibt, unter denen exponentiell-lineare oder doppeltexponentiell-lineare untere Schranken für die Entscheidungskomplexität einer entscheidbaren Theorie T bewiesen werden können. Diese Schranken beziehen sich dabei zuerst nur auf die Rechenzeit von nichtdeterministischen $\mathcal{EM}_\Gamma$-Turingmaschinen für ein endliches Bandalphabet Γ. Satz 3.4.1 entspricht dabei einer Übertragung von Theorem 6 in [FiR74] auf die Situation beim hier eingeschlagenen Weg, die direkten Komplexitätsresultate nicht für (Nicht-Standard-)Turingmaschinen mit Bandalphabet $\{0,1\}$ (wie in [FiR74]), sondern für 1-Band-Turingmaschinen aus der Menge $\mathcal{EM}_\Gamma$ zu erzielen (und diese dann nachher zu für allgemeine IOTM's geltenden zu erweitern).

Die Erweiterung der Komplexitätsresultate von bezüglich $\mathcal{EM}_\Gamma$-Maschinen erzielten zu bezüglich allgemeinen IOTM's gültigen wird anschließend in Korollar 3.4.2 erfolgen, wobei diese Ausdehnung der hier nun vorgestellten Aussage Satz 3.4.1—wie früher erwähnt—weitgehend durch die Anwendung von bekannten Simulationsergebnissen für Turingmaschinen erfolgen kann.

Satz 3.4.1. *Sei* $f: \mathbb{N}_0 \to \mathbb{N}_0$ *eine der beiden durch* $n \mapsto 2^n$ *bzw. durch* $n \mapsto 2^{2^n}$ *definierten Funktionen;* $T = (\Sigma_T, Fo_T, Thm_T)$ *sei eine formalisierte Theorie 1. Ordnung*[17]*, die vollständig*[18] *ist;* Γ *sei ein endliches Alphabet und* $\Gamma \supseteq \Sigma_T \cup \Sigma_{code} \cup \{\#\}$*, wobei* Σ_{code} *wie in Definition 3.3.2,* $\#$ *das Leersymbol,* $\# \notin \Sigma_T$*; Symb eine Funktion Symb* $: \{0, 1, \ldots, |\Gamma| - 1\} \to \Gamma$*, die bijektiv ist und für die* $Symb(0) = \#$ *gilt;* $\langle\cdot\rangle_{\Gamma,Symb} : \mathcal{EM}_\Gamma \to (\Gamma\backslash\{\#\})^+$ *die wie in Definition 3.3.2 festgelegte Kodierung für* $\mathcal{EM}_\Gamma$*-Turingmaschinen.*

Angenommen, *es gilt nun:*

$$
\begin{array}{l}
(\exists d \in \mathbb{R},\ d > 0)(\exists e : \mathbb{N}_0 \to \mathbb{N}_0,\quad \textit{Funktion}) \\
\quad (\exists g : (\Gamma\backslash\{\#\})^* \to \Sigma_T^*,\ g \in DFTime_{\mathcal{EM}_\Gamma}(POL)) \\
\quad\quad (\forall M \in \mathcal{EM}_\Gamma)(\forall w \in (\Gamma\backslash\{\#\})^*) \\
\quad\quad\quad (\exists \mathbf{F}_{M,w} \in Fo_T \textit{ geschlossene Formel}) \\
\quad\quad\quad\quad [\ \textit{es gelten die Forderungen (i), (ii) und (iii)}\ ]
\end{array}
$$

wobei:

(i): $\mathbf{F}_{M,w} \in Thm_T \iff w \in (\Sigma(M))^*$ & M *akzeptiert* w & $Min\text{-}RZ_M(w) \leq f(|w|)$;

(ii): $|\mathbf{F}_{M,w}| \leq e(|\langle M\rangle_{\Gamma,Symb}|) + d \cdot |w|$;

(iii): $g(\langle M\rangle_{\Gamma,Symb} \circ w) = \mathbf{F}_{M,w}$.

Dann gilt *folgende Aussage über die Entscheidungskomplexität der Theorie T: Es existiert ein* $c \in \mathbb{R}$*,* $c > 0$ *so, daß* $f(cn)$ *untere Schranke für die Entscheidungskomplexität von T bezüglich der Rechenzeit nichtdeterministischer* $\mathcal{EM}_\Gamma$*-Turingmaschinen ist. Genauer:*

$$\textit{Es existiert ein } c \in \mathbb{R},\ c > 0 \textit{ so, daß } Thm_T,\ \text{co}\text{-}Thm_T \notin NTime_{\mathcal{EM}_\Gamma}(f(cn)).$$

Bzw. in ausführlicher und weiter präzisierter[19] *Schreibweise dieser Aussagen:*

[17] Für eine solche Formalisierung einer Theorie 1. Ordnung T als ein System formaler Sprachen $T = (\Sigma_T, Fo_T, Thm_T)$ könnte natürlich auch ein System $T^{((M))} = (\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ mit informatisch-sinnvoller Formelsyntax (vgl. Kap. 1) für T stehen bzw. gewählt werden; eine solche, an die Formalisierung von T gerichtete, äußere Einschränkung ist hier einerseits formal nicht notwendig und wurde auch weiters in der Absicht vermieden, überlange Bezeichnungen zu umgehen.

[18] Vgl. jedoch den Zusatz in der Folgerung des Theorems, daß diese Forderung für die co$-Thm_T$ betreffende Komplexitätsaussage nicht notwendig ist.

[19] Die „weitere Präzisierung" betrifft hier den sich auf co$-Thm_T$ beziehenden Teil dieser Komplexitätsaussage.

$$
\begin{aligned}
&(\exists c \in \mathbb{R},\ c > 0)(\forall M_E \in \mathcal{EM}_\Gamma) \\
&\quad \big[L(M_E) = Thm_T \ \vee\ L(M_E) = \mathrm{co}{-}Thm_T \implies \\
&\qquad \implies (\forall n_0 \in \mathbb{N})(\exists n > n_0,\ n \in \mathbb{N}) \\
&\qquad\quad (\exists \mathbf{A} \in Fo_T) \\
&\qquad\qquad \big(|\mathbf{A}| = n \ \&\ \mathbf{A} \in L(M_E) \ \&\ Min{-}RZ_{M_E}(\mathbf{A}) > f(c \cdot |\mathbf{A}|)\big)\big] \qquad (3.8)
\end{aligned}
$$

Hierbei kann $c \in \mathbb{R}$ beliebig mit $0 < c < \frac{1}{d}$ bezüglich eines in der Annahme zulässigen $d \in \mathbb{R}$, $d > 0$ gewählt werden.

Die Voraussetzung über die Theorie T, vollständig zu sein, ist für die $\mathrm{co}{-}Thm_T$ betreffende, hier gefolgerte Komplexitätsaussage nicht erforderlich.

[Die Rolle dieses Satzes entspricht im Kontext dieser Aufarbeitung der Rolle, die in [FiR74] Theorem 6, p. 7, innehat.]

Beweis. Seien $f, T, \Gamma, \#, Symb, \langle\cdot\rangle_{\Gamma,Symb}$ wie in der Voraussetzung des Theorems.

Seien $d \in \mathbb{R}$, $d > 0$, $e : \mathbb{N}_0 \to \mathbb{N}_0$, $g : (\Gamma\backslash\{\#\})^* \to \Sigma_T^*$, $g \in DFTime_{\mathcal{EM}_\Gamma}(POL)$ so, daß

$$
\begin{aligned}
&(\forall M \in \mathcal{EM}_\Gamma)(\forall w \in (\Gamma\backslash\{\#\})^*)(\exists \mathbf{F}_{M,w} \in Fo_T \text{ geschlossene Formel}) \\
&\quad \big(\text{es gelten die Forderungen (i), (ii), (iii) in der Annahme des Satzes.}\big)
\end{aligned}
$$

gilt.

Im Beweis hier wird von einer mit $\mathbf{F}_{M,w}$ für $M \in \mathcal{EM}_\Gamma$ und $w \in \Sigma(M)$ bezeichneten und in dieser Gestalt auftretenden Formel immer vorausgesetzt, daß es sich dabei um die für e,d,f wie angenommen bezüglich M und w nach Annahme hier existierenden, immer eindeutige Formel mit den Eigenschaften (i), (ii), (iii) handelt.

Sei weiters $M_h \in \mathcal{EM}_\Gamma$ eine $\mathcal{EM}_\Gamma$-Maschine, die g in polynomialer Rechenzeit berechnet.

(1) Zeige nun—davon ausgehend—die Folgerung des Theorems und dabei zuerst nur die sich auf die Komplexität von Thm_T beziehende Aussage von (3.8):

$$
\begin{aligned}
&(\exists c \in \mathbb{R},\ c > 0)(\forall M_E \in \mathcal{EM}_\Gamma) \\
&\quad \big[L(M_E) = Thm_T \implies \\
&\qquad \implies (\forall n_0 \in \mathbb{N})(\exists n \geq n_0,\ n \in \mathbb{N}) \\
&\qquad\quad (\exists \mathbf{A} \in Thm_T) \\
&\qquad\qquad \big(|\mathbf{A}| = n \ \&\ Min{-}RZ_{M_E}(\mathbf{A}) > f(c \cdot |\mathbf{A}|)\big)\big] \qquad (3.9)
\end{aligned}
$$

Sei dazu $c \in \mathbb{R}$, $c > 0$ mit $0 < c < \frac{1}{d}$ und $M_E \in \mathcal{EM}_\Gamma$ mit $L(M_E) = Thm_T$ beliebig, aber fix gewählt. Für c und M_E wird im weiteren die Erfülltheit der in den eckigen Klammern stehenden, inneren Bedingung in (3.9) nachgewiesen.

Programm 3.4.1 Die Turingmaschine $M_0^{(M_E)}$:

program $M_0^{(M_E)}(x)$**;**

`Eingabe:` $x \in (\Gamma \setminus \{\#\})^*$.
`Akzeptieren`
`der Eingabe:` `ja, falls` $x = \langle M \rangle_{\Gamma,Symb} \circ 1^i$ `und` $\neg\, \mathbf{F}_{M,x} \in Thm_T$
`für ein` $M \in \mathcal{EM}_\Gamma$ `und ein` $i \in \mathbb{N}_0$`;`
`nein, andernfalls.`

begin
if not$(x = \langle M \rangle_{\Gamma,Symb} \circ 1^s$ `für ein` $M \in \mathcal{EM}_\Gamma$`,` $s \in \mathbb{N}_0)$ **then**
`halte, ohne zu akzeptieren;`
`Y:=`$\langle M \rangle_{\Gamma,Symb}$`;` {`Extrahiere` $\langle M \rangle_{\Gamma,Symb}$ `aus` x`, d.h. stelle auf dem Turingband` $Y \circ x$ `her`}
`F:=`M_h`(Y`$\circ x$`);` {`Berechne` $\mathbf{F}_{M,x}$}
`F:=`$\neg$`F;` {`Stelle` $\neg \mathbf{F}_{M,x}$ `her`}
M_E`(F);` { ``Erkenne'' mittels M_E die Formel $\neg\, \mathbf{F}_{M,x}$ }
end $M_0^{(M_E)}$.

Ausgehend von M_E wird nun eine $\mathcal{EM}_\Gamma$-Maschine $M_0^{(M_E)}$ aufgebaut, aus deren Terminationseigenschaft durch Diagonalisierung dann die gewünschte Eigenschaft von $f(cn)$, nicht Rechenzeitschranke für M_E sein zu können, hergeleitet wird.

Die Maschine $M_0^{(M_E)}$ sei dabei in Pseudocode wie in Programm 3.4.1 definiert.

Der Programmcode von $M_0^{(M_E)}$ in Programm 3.4.1 ist insgesamt so zu verstehen, daß $M_0^{(M_E)}$ für eine Eingabe $x \in (\Gamma \setminus \{\#\})^*$ zuerst prüft, ob x von der Gestalt $\langle M \rangle_{\Gamma,Symb} \circ 1^i$ für $M \in \mathcal{EM}_\Gamma$, $i \in \mathbb{N}_0$ ist, falls nein, hält, ohne zu akzeptieren, falls ja, daraus auf dem Turingband zuerst $\langle M \rangle_{\Gamma,Symb} \circ \langle M \rangle_{\Gamma,Symb} \circ 1^i$ (mit dem SLK der Maschine auf dem 1. Zeichen) herstellt (also *berechnet*), daraus mit Hilfe von M_h dann weiter $\mathbf{F}_{M,\langle M \rangle_{\Gamma,Symb} \circ 1^i}$ aufbaut (wieder zuletzt mit dem SLK auf dem linksäußersten Zeichen), diese Formel negiert und erneut den SLK ganz nach rechts bringt (Hierfür ist möglicherweise der Zwischenschritt der Einführung eines Begrenzungszeichens[20] am Bandende, das zum Schluß wieder entfernt wird, nötig) und schließlich die „Entscheidungsmaschine“ M_E (die ja nur für Theoreme von T akzeptierend hält, für Zeichenketten, die keine Theoreme sind, aber entweder nicht terminiert oder ohne zu akzeptieren hält—und so eigentlich nur die Theoreme von

[20](als solches kann das Leerzeichen # verwendet werden)

T erkennt) auf $\neg\,\mathbf{F}_{M,\langle M\rangle_{\Gamma,Symb}\circ 1^i}$ anwendet.

Hierbei sind diese einzelnen Schritte im Programmcode Abkürzungen von $\mathcal{EM}_\Gamma$-Maschinen, die Teile von $M_0^{(M_E)}$ bilden bzw. $M_0^{(M_E)}$ aufbauen. Die Erkennung der Eingabe x, also die Frage, ob x von der Gestalt $x = \langle M\rangle_{\Gamma,Symb}\circ 1^i$ für ein $M \in \mathcal{EM}_\Gamma$ und ein $s \in \mathbb{N}_0$ ist, kann von einer $\mathcal{EM}_\Gamma$-Maschine in deterministischer, durch $p_1(|x|)$ (für ein Polynom $p_1 \in \mathbb{N}_0[x]$)[21] beschränkter Rechenzeit entschieden werden: hierfür ist im wesentlichen die Aussage von Lemma 3.3.3 maßgeblich. (Es ist dafür auch entscheidend, daß Γ so gewählt wurde, daß $\Gamma \supseteq \Sigma_{code}$ und $\# \notin \Sigma_{code}$ gilt und deshalb $\langle\cdot\rangle_{\Gamma,Symb}$ die Menge $\mathcal{EM}_\Gamma$ in $(\Gamma\setminus\{\#\})^+$ abbildet. Nur dadurch ist es möglich, daß eine $\mathcal{EM}_\Gamma$-Maschine mit den Kodes anderer $\mathcal{EM}_\Gamma$-Maschinen (oder eben auch—wie später wichtig—mit dem eigenen Code) operieren kann.)

Die Konstruktion von $\langle M\rangle_{\Gamma,Symb}\circ x$ aus $x = \langle M\rangle_{\Gamma,Symb}\circ 1^i$, wobei am Beginn und am Ende dieser Berechnung der SLK ganz links außen positioniert ist, kann dann in polynomialer Rechenzeit $p_2(|x|)$ (für ein Polynom $p_2 \in \mathbb{N}_0[x]$) erfolgen (hierbei ist hauptsächlich ausschlaggebend, daß der Anfang und das Ende von $\langle\cdot\rangle_{\Gamma,Symb}$-Kodierungen jeweils direkt zu erkennen sind; p_2 kann quadratisch, d.h. mit Grad 2 gewählte werden). Aus $\langle M\rangle_{\Gamma,Symb}\circ x = \langle M\rangle_{\Gamma,Symb}\circ\langle M\rangle_{\Gamma,Symb}\circ 1^i$ kann nun durch den Einsatz von $M_h \in \mathcal{EM}_\Gamma$ (M_h wie in der Annahme des Beweises) in durch $p_3(|\langle M\rangle_{\Gamma,Symb}\circ x|) \leq p_3(2\,|x|)$ beschränkter Rechenzeit (für ein Polynom $p_3 \in \mathbb{N}_0[x]$, das Rechenzeitschranke für M_h ist) $\mathbf{F}_{M,x}$ berechnet werden; daraus kann in linearer Rechenzeit (sicher in Rechenzeit $\leq 2\,|\mathbf{F}_{M,x}| + 4$) die Formel $\neg\,\mathbf{F}_{M,x}$ hergestellt und dabei auch der SLK wieder ganz nach links gebracht werden. Insgesamt sind zu $x = \langle M\rangle_{\Gamma,Symb}\circ 1^i$ ($x = \langle M\rangle_{\Gamma,Symb}$, $i \in \mathbb{N}_0$) nicht mehr als

$$p_1(|x|) + p_2(|x|) + p_3(2\,|x|) + 2p_3(2\,|x|) + 4 =: p(|x|)$$

Rechenzeitschritte (mit $p \in \mathbb{N}_0[x]$, $p(x) := p_1(x) + p_2(x) + 3p_3(2x) + 4$) zur Konstruktion von $\neg\,\mathbf{F}_{M,x}$ nötig.

Das Terminationsverhalten von $M_0^{(M_E)}$ kann nun wegen der Voraussetzungen und Beweisannahmen für Eingaben der Gestalt $x = \langle M\rangle_{\Gamma,Symb}\circ 1^i$ ($M \in \mathcal{EM}_\Gamma$, $i \in \mathbb{N}_0$)

[21] Ist R ein Integritätsbereich, so bezeichnet $R[x]$ die Menge der Polynome mit Koeffizienten in R. $\mathbb{N}[x]$ ist also die Menge der Polynome mit Koeffizienten in N_0.

auf folgende Weise charakterisiert werden:

$$\begin{aligned} & M_0^{(M_E)} \text{ akzeptiert x} \iff \\ & \iff \quad \neg\, \mathbf{F}_{M,x} \in Thm_T \\ & \iff \quad \mathbf{F}_{M,x} \notin Thm_T \\ & \iff \quad \neg\, [x \in (\Sigma(M))^* \;\&\; M \text{ akzeptiert } x \;\&\; Min{-}RZ_M(x) < f(|x|)] \\ & \iff \quad x \notin (\Sigma(M))^* \;\vee\; \big(x \in (\Sigma(M))^* \;\&\; M \text{ akzeptiert } x \text{ nicht}\big) \;\vee \\ & \qquad \vee \;\; \big(x \in (\Sigma(M))^* \;\&\; M \text{ akzeptiert } x \;\&\; Min{-}RZ_M(x) \geq f(|x|)\big) \end{aligned} \tag{3.10}$$

(Hierbei folgt die erste Äquivalenz aus der Konstruktion von $M_0^{(M_E)}$, die zweite aus der Vollständigkeit von T zusammen mit der Beweisannahme, daß die Formeln $\mathbf{F}_{M,x}$ geschlossen sind und die dritte Äquivalenz aus der Bedingung (i) in der Annahme des Theorems.)

Weiters läßt sich wegen der oben angeführten Überlegung über den Rechenzeitaufwand von $M_0^{(M_E)}$ bis zur Ausführung von M_E innerhalb von $M_0^{(M_E)}$ mit $p(x)$ wie oben noch für alle $x = \langle M \rangle_{\Gamma,Symb} \circ 1^i$ ($M \in \mathcal{EM}_\Gamma$, $i \in \mathbb{N}_0$) das folgende aussagen:

$$\begin{aligned} & M_0^{(M_E)} \text{ akzeptiert } x \Longrightarrow \\ & \Longrightarrow \quad Min{-}RZ_{M_0^{(M_E)}}(x) \leq p(|x|) + Min{-}RZ_{M_E}(\neg\, \mathbf{F}_{M,x}) \end{aligned} \tag{3.11}$$

Da jedoch nach Konstruktion $M_0^{(M_E)} \in \mathcal{EM}_\Gamma$ gilt, kann nun (3.10) auch auf alle $x = \langle M \rangle_{\Gamma,Symb} \circ 1^i$ ($i \in \mathbb{N}_0$) selbst angewendet werden und durch ein solches Vorgehen (hinter dem die bekannte Methode der Diagonalisierung steckt) kann nun eingesehen werden, daß $f(n)$ nicht Rechenzeitschranke für $M_0^{(M_E)}$ sein kann.

Wegen (3.10) und $\Sigma(M_0^{(M_E)}) = \Gamma \setminus \{\#\}$ (vgl. die Festlegung von $M_0^{(M_E)}$ in Programm 3.4.1) gilt nämlich für alle $x_i := \langle M_0^{(M_E)} \rangle_{\Gamma,Symb} \circ 1^i \in (\Gamma \setminus \{\#\})^*$ ($i \in \mathbb{N}_0$):

$$\begin{aligned} & M_0^{(M_E)} \text{ akzeptiert } x_i \iff \\ & \iff \quad \neg\, \mathbf{F}_{M_0^{(M_E)},x_i} \in Thm_T \\ & \iff \quad \big(M_0^{(M_E)} \text{ akzeptiert } x_i \text{ nicht}\big) \;\vee \\ & \qquad \vee \;\; \big(M_0^{(M_E)} \text{ akzeptiert } x_i \;\&\; Min{-}RZ_{M_0^{(M_E)}}(\neg\, \mathbf{F}_{M_0^{(M_E)},x_i}) > f(|x_i|)\big) \end{aligned} \tag{3.12}$$

Da die Annahme „$M_0^{(M_E)}$ akzeptiert x_i nicht“ innerhalb von (3.12) aber auf einen Widerspruch führt (es würde folgen, daß $M_0^{(M_E)}$ das Wort x_i dann doch akzeptieren

müßte), folgt aus (3.12) unmittelbar, daß für alle x_i ($i \in \mathbb{N}_0$) gilt:

$$\begin{aligned} M_0^{(M_E)} \text{ akzeptiert } x_i \;\&\; \neg\, \mathbf{F}_{M_0^{(M_E)},x_i} \in Thm_T \;\& \\ \&\; Min\text{-}RZ_{M_0^{(M_E)}}(x_i) > f(|x_i|) \end{aligned} \tag{3.13}$$

Insbesondere kann also $f(n)$ nicht Rechenzeitschranke für $M_0^{(M_E)}$ sein. Aus dieser Tatsache läßt sich nun im weiteren mit Hilfe von (3.11) auch zeigen, daß dann (für das am Anfang des Beweises gewählte c) $f(cn)$ auch keine Rechenzeitschranke für M_E sein kann.

Sei hierfür nun $\varepsilon > 0$ hinreichend klein so gewählt, daß gilt:

$$(1-\varepsilon)^2 \cdot \frac{1}{d} > c, \tag{3.14}$$

was wegen der Wahl von c als $c \in \mathbb{R}$, $0 < c < \frac{1}{d}$ (und eben $d \in \mathbb{R}$, $d > 0$ nach Beweisannahme) immer möglich ist. Weiters werden im weiteren die folgenden Setzungen verwendet:

$$\begin{aligned} \mathbf{A}_i &:= \neg\, \mathbf{F}_{M_0^{(M_E)},x_i}, \\ m_i &:= \left|\langle M_0^{(M_E)}\rangle \circ 1^i\right| = |x_i| \\ n_i &:= |\mathbf{A}_i| \qquad\qquad \text{(für alle } i \in \mathbb{N}_0) \end{aligned} \tag{3.15}$$

Wegen (3.11) und (3.13) folgt nun jedenfalls:

$$\begin{aligned} Min\text{-}RZ_{M_E}(\mathbf{A}_i) &\geq Min\text{-}RZ_{M_0^{(M_E)}}(x_i) - p(|x_i|) \geq \\ &\geq f(|x_i|) - p(|x_i|) \\ &\qquad\qquad \text{(für alle } i \in \mathbb{N}_0) \end{aligned} \tag{3.16}$$

Da $f(n) - p(n) >_{ae} f((1-\varepsilon)n)$ (das folgt aus $f((1-\tilde{\varepsilon})n) \in o(f(n) - \tilde{p}(n))$ für beliebige Polynome $\tilde{p} \in \mathbb{N}_0[x]$ und $\tilde{\varepsilon} \in \mathbb{R}$, $\tilde{\varepsilon} > 0$; dies wiederum ist eine einfache analytische Eigenschaft der Exponentialfunktionen 2^n bzw. 2^{2^n}) und $|x_i| = |x_0| + i \to \infty$ (für $i(\in \mathbb{N}) \to +\infty$), folgt aus (3.16) die Existenz eines $i_0 \in \mathbb{N}$ so, daß

$$\begin{aligned} Min\text{-}RZ_{M_E}(\mathbf{A}_i) \geq & f(|x_i|) - p(|x_i|) > f((1-\varepsilon)\cdot|x_i|) \\ & \text{(für alle } i \in \mathbb{N}_0,\ i \geq i_0) \end{aligned} \tag{3.17}$$

Sei $i_0 \in \mathbb{N}$ entsprechend gewählt. Aus (3.17) folgt nun, daß es unter den Formeln der Folge $\{\mathbf{A}_i\}_{i\in\mathbb{N}_0}$ unendlich viele verschiedene und solche von beliebiger Länge geben muß: Da $\mathbf{A}_i \in Thm_T$ ((3.15) und (3.13)) und $L(M_E) = Thm_T$ sind

$Min\text{-}RZ_{M_E}(\mathbf{A}_i)$ immer definierte Zahlen in $\mathbb{N}_0$. Da aus $|x_i| \to +\infty$ mit $i \to \infty$ (das gilt, siehe oben) $f((1-\varepsilon).|x_i|) \to +\infty$ mit $i \to +\infty$ folgt, muß es wegen (3.17) unendlich viele verschiedene minimale Rechenzeiten von M_E auf Formeln $\mathbf{A}_i$ ($i \in \mathbb{N}$) geben und also daher auch unendlich viele verschiedene Formeln unter den $\mathbf{A}_i$ ($i \in \mathbb{N}$). Da jedoch Formeln Zeichenketten über dem endlichen Alphabet Σ_T sind und es also zu jeder Zahl $n \in \mathbb{N}$ nur endlich viele Formeln mit Länge n geben kann, muß es Formeln $\mathbf{A}_i$ von beliebiger Länge geben. Insbesondere ist daher eine Teilfolge $\{\mathbf{A}_{i_j}\}_{j\in\mathbb{N}}$ von $\{\mathbf{A}_i\}_{i\in\mathbb{N}_0}$ wählbar, für die gilt:

$$\begin{aligned} &|\mathbf{A}_{i_1}| < |\mathbf{A}_{i_2}| < |\mathbf{A}_{i_3}| < \ldots < \left|\mathbf{A}_{i_j}\right| < \left|\mathbf{A}_{i_{j+1}}\right| < \ldots , \\ &i_1 \geq i_0. \end{aligned} \tag{3.18}$$

Mit den neuen Setzungen

$$\begin{aligned} \mathbf{A}'_j &:= \mathbf{A}_{i_j}, & x'_j &:= x_{i_j}, \\ n'_j &:= n_{i_j}, & m'_j &:= m_{i_j}, \qquad (j \in \mathbb{N}) \end{aligned} \tag{3.19}$$

folgt nun wegen (3.17) und (3.18) auch:

$$Min\text{-}RZ_{M_E}(\mathbf{A}'_j) > f((1-\varepsilon)\cdot\left|x'_j\right|) \qquad (\text{für alle } j \in \mathbb{N}) \tag{3.20}$$

Diese Abschätzung für die Rechenzeit von M_E auf Eingabe $\mathbf{A}'_j$ verwendet allerdings noch nicht die Länge der Formel $\mathbf{A}'_j$, nämlich n'_i, sondern $\left|x'_j\right| = m'_j$. Es gilt aber:

$$\begin{aligned} n'_j = \left|\mathbf{A}'_j\right| = \left|\neg\,\mathbf{F}_{M_0^{(M_E)},x'_j}\right| &\underset{\text{[Ann. (ii)]}}{\leq} e\left(\left|\langle M_0^{(M_E)}\rangle_{\Gamma,Symb}\right|\right) + d\cdot\left|x'_j\right| + 1 \\ &= e(m_0) + d\cdot m'_j + 1 \\ &\qquad\qquad (\text{für alle } i \in \mathbb{N}_0). \end{aligned}$$

Hieraus folgt aber $m'_j \geq \frac{1}{d}(n'_j - e(m_0) - 1)$ und damit aus (3.20)

$$Min\text{-}RZ_{M_E}(\mathbf{A}'_j) > f\left((1-\varepsilon)\frac{1}{d}(n'_j - e(m_0) - 1)\right) \qquad (\text{für alle } j \in \mathbb{N}) \tag{3.21}$$

Wegen $n'_j = \left|\mathbf{A}'_j\right| = n_{i_j} = \left|\mathbf{A}_{i_j}\right| \to +\infty$ mit $j \to \infty$ (wegen (3.18)) folgt nun auch $f\left((1-\varepsilon)\frac{1}{d}(n'_j - e(m_0) - 1)\right) \to +\infty$ mit $j \to \infty$; da weiters allgemein $f(\tilde{c}(n-\tilde{d})) >_{ae} f((1-\varepsilon)\tilde{c}n)$ für alle $\tilde{c}, \tilde{d}, \varepsilon \in \mathbb{R}$, $\tilde{c}, \varepsilon > 0$ gilt (wiederum eine leicht einzusehende analytische Eigenschaft der Exponentialfunktionen 2^n, 2^{2^n}; insbesondere gilt: $f((1-\varepsilon)\tilde{c}n) \in o\left(f(\tilde{c}(n-\tilde{d}))\right)$ für alle $\tilde{c}, \tilde{d}, \varepsilon \in \mathbb{R}$, $\tilde{c}, \varepsilon > 0$), folgt damit aus (3.21) die Existenz eines $j_0 \in \mathbb{N}$ so, daß gilt:

$$Min\text{-}RZ_{M_E}(\mathbf{A}'_j) > f\left((1-\varepsilon)^2\frac{1}{d}n'_j\right) \qquad (j \in \mathbb{N},\ j \geq j_0) \tag{3.22}$$

Sei j_0 entsprechend gewählt.
Aus (3.22) folgt nun wegen (3.14)

$$Min{-}RZ_{M_E}(\mathbf{A}'_j) > f(cn_j) \;\&\; \left|\mathbf{A}'_j\right| = n'_j \qquad (\text{für alle } j \in \mathbb{N},\ j \geq j_0) \tag{3.23}$$

Hiermit ist nun aber die Existenz unendlich vieler Formeln $\mathbf{A}'_j$ (für $j \in \mathbb{N}$, $j \geq j_0$) gezeigt worden, für deren Erkennung M_E jeweils mehr Rechenzeit als $f(c \cdot \left|\mathbf{A}'_j\right|)$ Schritte (selbst im Fall kürzester nichtdeterministischer Berechnungen) benötigt. Für c, M_E ist damit

$$\begin{aligned}&(\forall n_0 \in \mathbb{N})(\exists n \geq n_0,\ n \in \mathbb{N})\\ &\quad(\exists \mathbf{A} \in Thm_T)\\ &\qquad\big(|\mathbf{A}| = n \;\&\; Min{-}RZ_{M_E}(\mathbf{A}) > f(c \cdot |\mathbf{A}|)\big)\end{aligned}$$

nachgeweisen worden. Da $M_E \in \mathcal{EM}_\Gamma$ beliebig, jedoch im Beweis fest war, folgt hiermit (3.9).

(2) Eine (3.9) entsprechende, die Menge co$-Thm_T$ betreffende Komplexitätsaussage ist auf zum Beweis in (i) analoge Weise zu gewinnen:

Es muß dabei im Aufbau der Maschine $M_0^{(M_E)}$ für ein $M_E \in \mathcal{EM}_\Gamma$ mit $L(M_E)=$ $=$co$-Thm_T$ nur die Anweisung

$$\texttt{F := } \neg \texttt{F;}$$

also die Negierung von $\mathbf{F}_{M,x}$ weggelassen werden. Die zu einem $M_E \in \mathcal{EM}_\Gamma$ mit $L(M_E)$ =co$-Thm_T$ analog zu $M_0^{(M_E)}$ aufgebaute, hier wie beschrieben leicht abgeänderte Maschine sei mit $M_1^{(M_E)}$ bezeichnet und erfüllt ebenso wie $M_0^{(M_E)}$ die Eigenschaften $M_1^{(M_E)} \in \mathcal{EM}_\Gamma$, $\Sigma(M_1^{(M_E)}) = \Gamma \setminus \{\#\}$. Für das Terminationsverhalten dieser Maschine $M_1^{(M_E)}$ folgt nun die (3.10) vergleichbare Aussage, nämlich, daß für alle $x = \langle M \rangle_{\Gamma,Symb} \circ 1^s$ ($M_E \in \mathcal{EM}_\Gamma$, $s \in \mathbb{N}$) gilt:

$$\begin{aligned}&M_1^{(M_E)} \text{ akzeptiert } x \iff \\ &\iff \quad \mathbf{F}_{M,x} \in \text{co}{-}Thm_T \\ &\iff \quad \mathbf{F}_{M,x} \notin Thm_T \\ &\iff \quad \neg\,[x \in (\Sigma(M))^* \;\&\; M \text{ akzeptiert } x \;\&\; Min{-}RZ_M(x) < f(|x|)] \\ &\iff \quad x \notin (\Sigma(M))^* \;\vee\; \big(x \in (\Sigma(M))^* \;\&\; M \text{ akzeptiert } x \text{ nicht}\big) \;\vee \\ &\qquad\vee\; \big(x \in \Sigma(M) \;\&\; M \text{ akzeptiert } x \;\&\; Min{-}RZ_M(x) \geq f(|x|)\big)\end{aligned} \tag{3.24}$$

Durch Einsetzen von $x_i = \langle M_1^{(M_E)} \rangle_{\Gamma,Symb} \circ 1^s$ $(i \in \mathbb{N}_0)$ in (3.24) und Betrachtung der analog zu (3.12) entstehenden Kette von Äquivalenzen ergibt sich hier analog zu (3.13):

$$\begin{aligned} M_1^{(M_E)} \text{ akzeptiert } x_i \;\&\; \mathbf{F}_{M_1^{(M_E)},x_i} \in \text{co}-Thm_T \;\& \\ \& \; Min-RZ_{M_1^{(M_E)}}(x_i) > f(|x_i|) \end{aligned} \tag{3.25}$$

Aus (3.25) ergibt sich nun die Existenz (und die Art der Wahl von unendlich vielen Formeln $\mathbf{A}''_j \in Fo_T$ $(j \in \mathbb{N})$ mit

$$\begin{aligned} \mathbf{A}''_j \text{ ist geschlossene Formel } \;\&\; \left|\mathbf{A}''_1\right| < \left|\mathbf{A}''_2\right| < \left|\mathbf{A}''_3\right| < \ldots \;\& \\ \&\; \mathbf{A}''_j \in \text{co}-Thm_T \;\&\; Min-RZ_{M_E}(\mathbf{A}''_j) > f(c \cdot \left|\mathbf{A}''_j\right|) \\ (j \in \mathbb{N}) \end{aligned} \tag{3.26}$$

völlig analog zum Beweis in (1). Damit folgt dann für jedes $M_E \in \mathcal{EM}_\Gamma$ mit $L(M_E) = \text{co}-Thm_T$ auch

$$\begin{aligned} &(\forall n_0 \in \mathbb{N})(\exists n \geq n_0,\ n \in \mathbb{N}) \\ &\quad (\exists \mathbf{A} \in \text{co}-Thm_T \cap Fo_T)^{22} \\ &\qquad \big(|\mathbf{A}| = n \;\&\; Min-RZ_{M_E}(\mathbf{A}) > f(c \cdot |\mathbf{A}|)\big) \end{aligned}$$

also die gewünschte $\text{co}-Thm_T$ betreffende Komplexitätsaussage.

Es muß weiters noch auf die Beobachtung hingewiesen werden, daß in diesem Beweisteil die Vollständigkeit von T an keiner Stelle eingeht. Insbesondere wird sie für (3.24) nicht benötigt, während sie für (3.10) an wesentlicher Stelle (beim Schluß $\neg\mathbf{F}_{M,x} \in Thm_T \iff \mathbf{F}_{M,x} \notin Thm_T$ für die geschlossene Formel $\mathbf{F}_{M,x}$) verwendet wurde.

Eine andere Möglichkeit zur Erzielung eines Ergebnisses der Gestalt

$$\text{co}-Thm_T \notin NTime_{\mathcal{EM}_\Gamma}(f(\tilde{c}n)) \qquad (\text{für ein } \tilde{c} \in \mathbb{R},\ \tilde{c} > 0)$$

unter der Voraussetzung der Vollständigkeit von T hätte in der Übertragung des in (1) für Thm_T erzielten Ergebnisses zu einem $\text{co}-Thm_T$ betreffenden bestanden. Dabei kann die in allen vollständigen Theorien $\tilde{T}$ gültige Aussage

$$\vdash_{\tilde{T}} \mathbf{A} \iff \nvdash_{\tilde{T}} \neg\, \mathbf{A}^c$$

[22] (d.h. natürlich auch: $(\exists \mathbf{A} \in Fo_T \setminus Thm_T)$)

Programm 3.4.2 Die Turingmaschine $M_{E:T}^{(M_{E:CT})}$:

program $M_{E:T}^{(M_{E:CT})}(x)$;

Eingabe: $x \in \Sigma_T^*$.
Akzeptieren
der Eingabe: ja, falls $x = \mathbf{A}$ für ein $\mathbf{A} \in Thm_T$;
nein, andernfalls.

begin
if not $(x = \mathbf{A}$ fuer ein $\mathbf{A} \in Fo_T)$ **then**
halte, ohne zu akzeptieren;
A:=x;
A:=A^c; {Bilde den Abschluss von A}
A:=$\neg$ A; {Bilde die Negation von A}
$M_{E:CT}$(A); {Lasse Maschine $M_{E:CT}$ auf Eingabe A arbeiten}
end $M_{E:T}^{(M_{E:CT})}$.

(wobei $\tilde{T}$ hier eine logische Theorie 1. Ordnung meint, sowie $\mathbf{A}^c$ den Abschluß der Formel $\mathbf{A}$) bzw.

$$\mathbf{A} \in Thm_{\tilde{T}} \iff \neg\, \mathbf{A}^c \in \mathrm{co}{-}Thm_{\tilde{T}}$$

(falls die logische Theorie 1. Ordnung $\tilde{T}$ als formales System $\tilde{T} = (\Sigma_{\tilde{T}}, Fo_{\tilde{T}}, Thm_{\tilde{T}})$ aufgefaßt wird) zur Konstruktion einer $\mathcal{EM}_\Gamma$-Maschine $M_{E:T}$ mit $L(M_{E:T}) = Thm_T$ zu einer beliebig gewählten $\mathcal{EM}_\Gamma$-Maschine $M_{E:CT}$ mit $L(M_{E:CT}) = \mathrm{co}{-}Thm_T$ verwendet werden (vgl. Programm 3.4.2), deren (minimale) Rechenzeit für eine Eingabeformel $\mathbf{A} \in Fo_T$ durch die (minimale) Rechenzeit von $M_{E:CT}$ auf $\neg\, \mathbf{A}^c$ und einem von $|\mathbf{A}|$ polynomial abhängenden Summanden beschränkt ist. Ist nun c eine nach (i) existierende, positiv-reelle Konstante so, daß $f(cn)$ für keine Maschine $M_{E:T}$ mit $L(M_{E:T}) = Thm_T$ Rechenzeitschranke ist, so folgt daraus hier jedenfalls, daß dann für alle $M_{E:CT}$ mit $L(M_{E:CT}) = \mathrm{co}{-}Thm_T$ die Funktion $f((1-\varepsilon)\frac{1}{3}cn)$ nicht Rechenzeitschranke sein kann (hier geht eine (grobe) Längenabschätzung der Form $|\neg\, \mathbf{A}^c| \leq 3\,|\mathbf{A}| + 1$ ein). Aus $Thm_T \notin NTime_{\mathcal{EM}_\Gamma}(f(cn))$ (für ein $c \in \mathbb{R}$, $c > 0$) ist also jedenfalls

$$\mathrm{co}{-}Thm_T \notin NTime_{\mathcal{EM}_\Gamma}\big(f((1-\varepsilon)\frac{1}{3}cn)\big)$$

(für ein beliebiges $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ und mit einem in der vorigen Aussage zulässigen c sowie unter der Voraussetzung der Vollständigkeit von T) beweisbar; dieses Übertra-

gungsergebnis ist also außerdem—was die Größe der in der erzielten Schrankenfunktion auftretenden multiplikativen Konstanten betrifft—noch (geringfügig) schwächer als ein oben direkt, aber analog zu (1) und ohne Verwendung der Vollständigkeit gezeigtes Ergebnis.

□

An dieser Stelle sei als Anmerkung zu Satz 3.4.1 und dem obigen Beweis dafür angefügt: Die Einschränkung der die Gestalt der Schrankenfunktion bestimmenden Funktion $f(n)$ auf 2^n oder 2^{2^n} in der Voraussetzung von Satz 3.4.1 entspringt ausschließlich der Anwendung dieses Satzes bei der Erzielung der Komplexitätsresultate in [FiR74][23] und wird nicht durch eine formal-technische Beschränkung in der Beweisführung für Satz 3.4.1 verursacht: Es ist leicht zu überprüfen, daß von $f(n)$ dabei neben den in die Annahme des Satzes eingehenden Eigenschaften *wesentlich* nur

$$\begin{aligned} &f((1-\varepsilon)n) \in o(f(n) - p(n)) && \text{(f.a. } \varepsilon \in \mathbb{R},\ \varepsilon > 0 \text{ und Polynome } p \in \mathbb{N}_0[x]), \\ &f(c(1-\varepsilon)n) \in o(f(n-d)) && \text{(f.a. } \varepsilon, c, d \in \mathbb{R},\ \varepsilon, c > 0,\ d \geq 0) \end{aligned} \tag{3.27}$$

verwendet werden und daß der Beweis für $f : \mathbb{N}_0 \to \mathbb{R}_0^+$ mit (3.27) als Voraussetzung über f genauso erfolgen könnte. (3.27) gilt für viele exponentielle und super-exponentielle Funktionen wie z.B. $f(n) = a^{cn}$ $(a \in \mathbb{R},\ a > 1,\ c \in \mathbb{R},\ c > 0)$ oder $f(n) = a^{a^{cn}}$ $(a \in \mathbb{R},\ a > 1)$, aber auch für Funktionen wie $a^{cn \log n}$ $(a \in \mathbb{R},\ a > 1,\ c \in \mathbb{R},\ c > 0)$.

Die angekündigte Erweiterung des Schlusses von Satz 3.4.1 zur Erzielung allgemeingültiger unterer Schranken (von der hier behandelten exponentiell-linearen oder doppelt-exponentiell-linearen Gestalt), allgemeingültigen Schranken, d.h. Schranken im Sinne von Definition 1.5.1, erfolgt nun durch die Anwendung bekannter Simulationsresulate und ist in der Aussage des folgenden Korollars enthalten und formuliert.

[23] Implizit liegt der Darstellung hier auch zugrunde, daß mit den Methoden aus [FiR74] und naheliegenderen Verallgemeinerungen davon bei Verwendung von $f(n) = a^{a^n}$ bzw. $f(n) = a^n$ mit $a \in \mathbb{N}$, $a > 2$ leider keine höheren unteren Schranken erzielt werden können (diese Verallgemeinerungen des Beweises in [FiR74] würden sogar nur auf solche Schranken 2^{cn}, $2^{2^{cn}}$ mit niedrigeren multiplikativen Konstanten $c \in \mathbb{R}$, $c > 0$ führen). Insbesondere kann auf eine solche Weise dann auch $PreAN \notin \bigcup_{c \in \mathbb{N}} NTime(2^{2^n})$ leider nicht gezeigt werden.

Korollar 3.4.2. *Unter den Voraussetzungen und Annahmen von Satz 3.4.1 folgt für die Entscheidungskomplexität der Theorie T bezüglich der Rechenzeit nichtdeterministischer Turingmaschinen:*

$$Thm_T,\ \mathrm{co}{-}Thm_T \notin NTime\,(f(cn)) \quad \textit{(für ein } c \in \mathbb{R},\ c > 0\textit{)}^{24}.$$

Unter Weglassung der Voraussetzung der Vollständigkeit von T kann jedenfalls noch

$$\mathrm{co}{-}Thm_T \notin NTime\,(f(cn)) \quad \textit{(für ein } c \in \mathbb{R},\ c > 0\textit{)}^{24}$$

gefolgert werden. In beiden Fällen ist für ein in Frage kommendes $c \in \mathbb{R}$, $c > 0$ dann $f(cn)$ jedenfalls untere Schranke für die Entscheidungskomplexität bzgl. nichtdeterministischer Turingmaschinen (gemäß Definition 1.5.1).

Beweis. Diese Aussagen über die Entscheidungskomplexität einer Theorie T, für die die Voraussetzungen und Bedingungen von Satz 3.4.1 erfüllbar sind, können nun—wie angekündigt—aus der Folgerung von Satz 3.4.1 mittels einfacher und bekannter Simulationsresultate erzielt werden. Seien für $T = (\Sigma_T, Fo_T, Thm_T)$, die zuerst nur als entscheidbar vorausgesetzt wird, die weiteren Voraussetzungen von Satz 3.4.1 für fix gewählte $f, \Gamma, \#, Symb, \langle\cdot\rangle_{\Gamma,Symb}$ erfüllt. Weiters sei die Annahme von Satz 3.4.1 mit $d \in \mathbb{R}$, $d > 0$, $e\colon \mathbb{N}_0 \to \mathbb{N}_0$ und $g\colon (\Gamma\setminus\{\#\})^* \to \Sigma_T^*$ erfüllt.

(1) T sei weiters noch als vollständig vorausgesetzt.
Zeige nun die Thm_T betreffende Aussage

$$Thm_T \notin NTime\,(f(cn)) \quad (\text{für ein } c \in \mathbb{R},\ 0 < c < \tilde{d}) \tag{3.28}$$

wobei $\tilde{d} := \frac{1}{2d}$, falls $f(n) = 2^n$, und $\tilde{d} := \frac{1}{d}$, falls $f(n) = 2^{2^n}$: Führe dazu die Annahme, daß das nicht der Fall ist, auf einen Widerspruch zur Folgerung von Satz 3.4.1. Angenommen, es würde gelten:

$$Thm_T \in NTime\,(f(cn)) \quad (\text{für ein } c \in \mathbb{R},\ 0 < c < \tilde{d}) \tag{3.29}$$

Sei ein $c \in \mathbb{R}$, $0 < c < \tilde{d}$ beliebig, im folgenden fest so gewählt, daß damit (3.29) gilt. Dann existiert eine (nichtdeterministische) (Mehrband-)Turingmaschine (nämlich eine IOTM) M_0 mit Bandalphabet Γ_0 und Eingabealphabet $\Sigma_0 = \Sigma_T$, die Thm_T akzeptiert (für die also $L(M_0) = Thm_T$ gilt) und die dies auch noch mit (nichtdeterministischer) Rechenzeitschranke $f(cn)$ tut. – M_0 kann nun von einer nichtdeterministischen 1-Band-Turingmaschine M_1 (mit einseitig unendlichem Band) mit

[24] c kann im Fall $f(n) = 2^n$ beliebig mit $0 < c < \frac{1}{2d}$, und im Fall $f(n) = 2^{2^n}$ beliebig mit $0 < c < \frac{1}{d}$ für ein zusammen mit e, g die Annahme von Satz 3.4.1 bezüglich T, f, $\langle\cdot\rangle_{\Gamma,Symb}$ erfüllendes $d \in \mathbb{R}$, $d > 0$ gewählt werden.

quadratisch schneller wachsender (nichtdeterministischer) Rechenzeitschranke simuliert werden (Band-Reduktions-Satz[25]); M_1 hat Bandalphabet Σ_1, Eingabealphabet $\Sigma_1 = \Sigma_T \subseteq \Gamma_1$ und akzeptiert Thm_T mit Rechenzeitschranke $c_1 (f(cn))^2$ für ein $c_1 \in \mathbb{R}$, $c_1 > 0$. – M_1 kann nun von einer 1-Band-Turingmaschine M_2 (mit einseitig unendlichem Band) mit Bandalphabet $\Gamma_2 = \Gamma$ in linear erhöhter nichtdeterministischer Rechenzeit simuliert werden (Alphabet-Reduktions-Satz[26]); M_2 hat Eingabealphabet $\Sigma_2 = \Sigma_T$, akzeptiert Thm_T und tut dies mit Rechenzeitschranke $c_2 (f(cn))^2$ für ein $c_2 \in \mathbb{R}$, $c_2 > 0$. – M_2 kann nun (durch Umbenennung von Zuständen, Reduktion der Endzustandsmenge F auf einen Zustand und entsprechende Änderung der Übergangsfunktion δ) zu einer völlig äquivalenten 1-Band-Turingmaschine $M_3 \in \mathcal{EM}_\Gamma$ umgebaut werden; insbesondere gilt für M_3 auch $L(M_3) = Thm_T$ und: M_3 akzeptiert Thm_T mit Rechenzeitschranke $c_2 (f(cn))^2$.

Für diese Rechenzeitschranke $c_2 (f(cn))^2$ ergibt sich nun für beliebiges $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ im Fall $f(n) = 2^n$

$$c_2 (f(cn))^2 = c_2 (2^{cn})^2 = c_2 2^{2cn} \leq_{\text{ae}} 2^{2(1+\varepsilon)cn} = f(2(1+\varepsilon)cn) \tag{3.30}$$

und im Fall $f(n) = 2^{2^n}$

$$c_2 (f(cn))^2 = c_2 \left(2^{2^{cn}}\right)^2 + c_2 2^{2^{cn+1}} \leq_{\text{ae}} 2^{2^{(1+\varepsilon)cn}} = f((1+\varepsilon)cn). \tag{3.31}$$

Wird nun $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ hinreichend klein, beliebig, aber für das folgende fest so gewählt, daß

$$(1+\varepsilon)c < \tilde{d}$$

gilt (das ist wegen $0 < c < \tilde{d}$, der Annahme über c, immer möglich), so gilt im Fall $f(n) = 2^n$ mit $\bar{c} := 2(1+\varepsilon)c$

$$\bar{c} = 2(1+\varepsilon)c < 2\tilde{d} = 2\frac{1}{2d} = \frac{1}{d}$$

und im Fall $f(n) = 2^{2^n}$ mit $\bar{c} := (1+\varepsilon)c$

$$\bar{c} = (1+\varepsilon)c < \tilde{d} = \frac{1}{d}$$

Für das so jeweils gewählte $\bar{c}$ folgt insgesamt wegen (3.30), (3.31) in beiden Fällen

$$c \in \mathbb{R} \;\&\; 0 < \bar{c} < \frac{1}{d} \;\&\; \tilde{c}_2 (f(cn))^2 \leq_{\text{ae}} f(\bar{c}n) \tag{3.32}$$

[25] vgl. etwa [Rei90], S.44: Für alle Zeitschranken T gilt: $DTime(T) \subseteq DTime_{\text{1-Band}}(O(T^2))$.

[26] vgl. etwa [Rei90], S.40: Jede Sprache in $DTime_{k\text{-Band}}(T, S)$ kann von einer $O(T)$-zeitbeschränkten und $O(S)$-platzbeschränkten k-Band-DTM akzeptiert werden, die in ihrem Speicher nur ein zweielementiges Alphabet verwendet.

Hieraus ist aber nun unmittelbar ein Widerspruch der Annahme (3.29) zur Folgerung von Satz 3.4.1 ableitbar: Einerseits akzeptiert die unter der Annahme (3.29) konstruierte $\mathcal{EM}_\Gamma$-Maschine M_3 die Sprache Thm_T mit Rechenzeitschranke $c_2\,(f(cn))^2$. Andererseits erzwingt die Folgerung von Satz 3.4.1, daß keine $\mathcal{EM}_\Gamma$-Maschine die Sprache $Thm_T \subseteq \Sigma_T^*$ mit einer Rechenzeitschranke $f(\tilde{c}n)$ für ein $\tilde{c} \in \mathbb{R}$ mit $0 < \tilde{c} < \frac{1}{d}$ akzeptieren kann: wegen (3.32) schließt das aber insbesondere auch aus, daß $c_2\,(f(cn))^2$ Rechenzeitschranke von M_3 für die Erkennung von Thm_T sein kann. Die Annahme (3.29) muß daher verworfen werden, womit (3.28) gezeigt ist.

(2) Die co$-Thm_T$ betreffende Aussage

$$\text{co}-Thm_T \notin NTime\,(f(cn)) \quad \text{für ein } c \in \mathbb{R},\ 0 < c < \tilde{d},$$

wobei $\tilde{d}$ wie in (1), kann nun unter Weglassung der zusätzlichen Forderung, daß T vollständig sei, völlig analog wie in (1) gezeigt werden (denn die für co$-Thm_T$ im Beweis dafür maßgebliche Aussage

$$\text{co}-Thm_T \notin NTime\,(f(\bar{c}n)) \quad \text{für ein } \bar{c} \in \mathbb{R},\ 0 < \bar{c} < \tfrac{1}{d},$$

kann aus Satz 3.4.1 ja ohne die Voraussetzung an T, vollständig zu sein, gefolgert werden.

□

Es soll an dieser Stelle noch eine zweite Beweismethode vorgestellt werden, wie unter der Voraussetzung der schon in Satz 3.4.1 verwendeten Ausdrückbarkeitseigenschaft untere Schranken für die in [FiR74] behandelten Theorien (und natürlich allgemeiner für alle Theorien, die entsprechenden, analogen Bedingungen genügen) gewonnen und nachgewiesen werden können. Diese zweite Methode wird auch öfter bei der Darstellung der Resultate und Beweise von [FiR74] benützt (vgl. z.B. [FeRa79] und [HoUl79]) und erzielt die Existenz der unteren Schranken nicht auf dem im Beweis zu Satz 3.4.1 verwendeten Weg der Konstruktion und Ausnutzung eines Diagonalisierungsargumentes (der als ein direkter Weg angesehen werden kann), sondern stützt sich auf eine Aussage von S. Cook ([Co73])[27] über Hierarchien von $NTime\,(t(n))$-Komplexitätsklassen und verwendet dabei $\leq_{pl}$-Reduktionen.

Ein Grund, warum eine solche Vorgangsweise zum Beweis der Ergebnisse in [FiR74] hier zusätzlich zu der schon für den Beweis von Satz 3.4.1 vorgestellten Methode angegeben wird, besteht darin, daß hierbei die an die Formeln $\mathbf{F}_{M,w}$ zu richtenden Bedingungen schwächer als in Satz 3.4.1 sind und insbesondere die an $\mathbf{F}_{M,w}$ gestellte Längenbedingung

[27] [FeRa79] verweisen außerdem noch auf [SFM73] und [SFM78]; [Rei90] verweist zusätzlich noch auf [Z83].

von deutlich schwächerer Gestalt ist. Letzteres führt bei der Konstruktion der Formeln $\mathbf{F}_{M,w}$ durchaus zu bedeutenden Vereinfachungen und würde die betreffenden Beweise beträchtlich abkürzen. – Da hier jedoch versucht wird, möglichst nahe am von [FiR74] skizzierten Beweisweg zu bleiben, werden diese Vereinfachungen zwar erwähnt, dennoch aber der ganze zur Erfüllung der Annahmen von Satz 3.4.1 nötige Aufwand beschrieben. (Allerdings sind die dabei erzielten Aussagen auch etwas konkreter als die auf die nun folgend beschriebene Weise bewiesenen, jedoch nicht prinzipiell, nur müßten die verwendeten Hierarchie-Sätze genau analysiert werden, um zu ähnlich konkreten Ergebnissen über die Gestalt der unteren Schranken zu gelangen.)

Zusätzlich zu dem Erwähnten, daß mit der hier im folgenden aufgeführten Beweismöglichkeit schwächere Annahmen über die Längen der Formel $\mathbf{F}_{M,w}$ verbunden sind, sollte gesagt werden, daß die Möglichkeit durchaus denkbar ist, daß sich auch die für Satz 3.4.1 benutzte Beweismethode für die hier nun geforderte, schwächere Längenbedingung verallgemeinern läßt (beispielsweise, indem die Methoden, die zur Erzielung der hier verwendeten Hierarchie-Sätze verwendet wurden, übertragen werden könnten; bei diesen handelt es sich um aufwendigere Diagonalisierungsargumente).

Satz 3.4.3. *$f : \mathbb{N}_0 \to \mathbb{N}_0$ sei eine der durch $n \mapsto 2^n$ bzw. durch $n \mapsto 2^{2^n}$ definierten Funktionen, $T = (\Sigma_T, Fo_T, Thm_T)$ [28] sei eine formalisierte Theorie.*

Angenommen, *es gilt:*

$$(\forall M \in \mathcal{EM})\,(\exists c_M \in \mathbb{R}, c > 0)$$
$$(\exists g_M : (\Sigma(M))^* \to \Sigma_T^*,\ g_M \in POLYLIN)$$
$$(\forall w \in (\Sigma(M))^*)\,(\exists \mathbf{F}_{M,w} \in Fo_T)$$
$$[\ \textit{es gelten die Bedingungen (i), (ii), (iii)}\ ]$$

wobei:

(i): $\mathbf{F}_{M,w} \in Thm_T \iff w \in L(M)\ \&\ Min\text{-}RZ_M(w) \leq f(|w|)$

(ii): $|\mathbf{F}_{M,w}| \leq c_M \cdot |w|$

(iii): $g_M(w) = \mathbf{F}_{M,w}$

Dann gilt *zuerst $NTime^*_{\mathcal{EM}}(f(n)) \leq_{pl} Thm_T$, woraus $NTime\left(f\left(\frac{n}{2}\right)\right) \leq_{pl} Thm_T$ folgt und letztlich*

$$Thm_T \notin NTime\,(f(cn)) \qquad \textit{für ein } c \in \mathbb{R},\ c > 0,$$

d.h. also, daß für ein solches c dann $f(cn)$ untere Schranke für die Entscheidungskomplexität von T ist.

[28] Vgl. Fußnote 17 zu Satz 3.4.1.

Beweis. Seien f und T wie vorausgesetzt. Die Annahme des Satzes sei gültig.

(1) Ziemlich unmittelbar aus der Annahme des Satzes ist erkennbar:

$$NTime^*_{\mathcal{EM}}(f(n)) \leq_{pl} Thm_T \tag{3.33}$$

Denn: Sei $L \in NTime^*_{\mathcal{EM}}(f(n))$ beliebig, im folgenden fest. Dann existiert $M \in \mathcal{EM}$ so, daß

$$L(M) = L \;\&\; (\forall x \in \Sigma(M))\,(x \in L \;\Rightarrow\; Min{-}RZ_M(x) \leq f(|x|)) \tag{3.34}$$

Wegen der Annahme des Satzes existieren nun eine Konstante $c_M \in \mathbb{R}$, $c_M > 0$ und eine Funktion $g_M : (\Sigma(M))^* \to \Sigma_T^*$ mit $g_M \in POLYLIN$ und der Eigenschaft, daß für alle $x \in (\Sigma(M))^*$ Formeln $\mathbf{F}_{M,x} \in Fo_T$ mit

$$\begin{aligned} &\mathbf{F}_{M,x} \in Thm_T \iff x \in L(M) \;\&\; Min{-}RZ_M(x) \leq f(|x|) \\ &|\mathbf{F}_{M,x}| \;\leq\; c_M \cdot |x| \\ &g_M(x) \;=\; \mathbf{F}_{M,x} \end{aligned} \tag{3.35}$$

existieren. Mit den hierdurch für alle $x \in (\Sigma(M))^*$ eindeutig bestimmten Formeln $\mathbf{F}_{M,x} \in Fo_T$ gilt nun für alle $x \in (\Sigma(M))^*$ wegen (3.34), (3.35)

$$\begin{aligned} &g_M(x) \in Thm_T \iff \\ &\quad\iff\quad \mathbf{F}_{M,x} \in Thm_T \\ &\quad\iff\quad x \in L(M) \;\;\&\;\; Min{-}RZ_M(x) \leq f(|x|) \\ &\quad\iff\quad x \in L \end{aligned}$$

woraus zusammen mit der Eigenschaft von g_M, linear beschränkt zu sein ((3.35), 2. Aussage) und $g_M \in POLYLIN$ folgt, daß $L \leq_{pl} Thm_T$ gilt.

Da L beliebig aus $NTime^*_{\mathcal{EM}}(f(n))$ war, folgt (3.33).

(2) Für $f(n) = 2^n$ gilt:

$$NTime\left(f\left(\frac{n}{2}\right)\right) \subseteq NTime^*_{\text{1-Band}}(f(n)) = NTime^*_{\mathcal{EM}}(f(n)) \tag{3.36}$$

Sei zum Beweis von 3.36 eine Sprache $L \subseteq \Sigma^*$ (Σ ein endliches Alphabet) mit $L \in NTime\left(f\left(\frac{n}{2}\right)\right)$ gegeben und vorerst fest gewählt.

Dann existiert eine Mehrband-IOTM M_1 mit Eingabealphabet Σ so, daß

$$L(M_1) = L \;\&\; (\forall x \in \Sigma^*)\left(x \in L \Rightarrow Min\text{-}RZ_{M_1}(x) \leq_{\text{ae}} f\left(\frac{|x|}{2}\right)\right)$$

gilt. Wegen $f(n) \geq 1$ (für alle $n \in \mathbb{N}_0$) folgt daraus die Existenz eines $C_1 \in \mathbb{N}$ so, daß:

$$L(M_1) = L \;\&\; (\forall x \in \Sigma^*)\left(x \in L \Rightarrow Min\text{-}RZ_{M_1}(x) \leq C_1 \cdot f\left(\frac{|x|}{2}\right)\right)$$

gilt. Wegen einem Satz[29] von der Band-Reduktion für Turingmaschinen existiert zu M_1 eine 1-Band-Turingmaschine M_2 mit Eingabealphabet Σ, die M_1 mit einer (strikten) Rechenzeitschranke aus der Menge $O\left(\left(C_1 \cdot f\left(\frac{x}{2}\right)\right)^2\right) = O\left(\left(f\left(\frac{x}{2}\right)\right)^2\right) = O(f(n))$ simuliert; es existiert also ein $C_2 \in \mathbb{N}$ so, daß

$$L(M_2) = L \;\&\; (\forall x \in \Sigma^*)\left(x \in L \Rightarrow Min\text{-}RZ_{M_2}(x) \leq C_2 \cdot f\left(|x|\right)\right)$$

gilt. Wegen einem Satz[30] von der linearen Beschleunigung von 1-Band-Turingmaschinen (der wegen $n^2 \in o(f(n))$ und $f(n) \geq n+1$ (für alle $n \in \mathbb{N}_0$) anwendbar ist) folgt die Existenz einer 1-Band-Turingmaschine M_3, die M_2 mit Beschleunigungsfaktor $\geq \frac{1}{C_2}$ simuliert und für die gilt:

$$L(M_3) = L \;\&\; (\forall x \in \Sigma^*)\left(x \in L \Rightarrow Min\text{-}RZ_{M_3}(x) \leq f\left(|x|\right)\right),$$

die also L mit strikter Rechenzeitschranke $f(n)$ akzeptiert. Es gilt nun also auch $L \in NTime^*_{\text{-Band}}(f(n))$.

Da im Beweis $L \in NTime\left(f\left(\frac{n}{2}\right)\right)$ beliebig war, am Anfang jedoch fest gewählt wurde, sind diese Schritte für alle $L \in NTime\left(f\left(\frac{n}{2}\right)\right)$ durchführbar und ist

$$NTime\left(f\left(\frac{n}{2}\right)\right) \subseteq NTime^*_{\text{-Band}}(f(n))$$

gezeigt. Die für (3.36) nun zuletzt noch nötige Inklusion (die Umkehrung ist nämlich offensichtlich gültig)

$$NTime^*_{\text{-Band}}(f(n)) \subseteq NTime^*_{\mathcal{EM}}\left(f(n)\right)$$

[29] Vgl. [Rei90], S.44, Korollar 1.4.7: $NTime(T(n)) \subseteq NTime_{1\text{-Band}}\left(O\left(\left(T(n)\right)^2\right)\right)$ für alle Zeitschranken T.

[30] vgl. z.B. [HoUl69], p.143, Theorem 10.6: Wird die Sprache L von einer 1-Band-Turingmaschine M_1 mit strikter Rechenzeitschranke $T(n)$ akzeptiert, so wird L für jedes $c > 0$ auch von einer 1-Band-Turingmaschine M_2 mit strikter Rechenzeitschranke $c \cdot T(n) := max\left(n+1, \lceil c \cdot T(n) \rceil\right)$ akzeptiert, vorausgesetzt, daß $\liminf_{n\to\infty} \frac{T(n)}{n^2} = \infty$ gilt [sinngemäße Übertragung von mir, C.G.].

folgt daraus, daß—wie bei der Definition von $\mathcal{EM}$ bemerkt—sich jede 1-Band-Turingmaschine leicht zu einer Maschine aus $\mathcal{EM}$ mit identischem Aktionsverhalten (gleiche Berechnungslängen, gleiche akzeptierte Sprachen, gleiche Speicherplatz-Komplexität) umbauen läßt.

(3) Es ist leicht einzusehen, daß (3.36) auch für $f(n) = 2^{2^n}$ gilt. In diesem Fall würde sogar

$$NTime\,(f(n-1)) \subseteq NTime^*_{\text{-Band}}(f(n)) = NTime^*_{\mathcal{EM}}\,(f(n))$$

gelten und dem Vorgehen im Beweis zu (2) für dieses f sogar eher angemessen zu sein.

(4) Es läßt sich nun unter Verwendung eines Resultats über die Hierarchien der Komplexitätsklassen bezüglich der Rechenzeit nichtdeterministischer Turingmaschinen die Aussage

$$Thm_T \notin NTime\,(f(cn)) \qquad (\text{für ein } c \in \mathbb{R},\, c > 0) \tag{3.37}$$

des Satzes zeigen:

Wegen (2), (3) und (1) gilt jedenfalls

$$NTime\big(f\big(\tfrac{n}{2}\big)\big) \leq_{pl} Thm_T. \tag{3.38}$$

Da nach einem Ergebnis aus [SFM73][31]

$$NTime\,(T_2(n)) \setminus NTime\,(T_1(n)) \neq \emptyset$$

für alle Zeitschranken $T_1, T_2 : \mathbb{N}_0 \to \mathbb{N}$, für die T_2 vollständig Rechenzeit-konstruierbar[32] ist und $T_1\,(n+1) \in o\,(T_2(n))$ erfüllt ist, gilt, existiert eine Sprache L_0 [33] so, daß

$$L_0 \in NTime\big(f\big(\big\lfloor\tfrac{n}{2}\big\rfloor\big)\big) \setminus NTime\big(f\big(\tfrac{n}{4}\big)\big) \tag{3.39}$$

[31] (dort: Theorem 1)

[32] $T : \mathbb{N}_0 \to \mathbb{N}_0$ heißt *Rechenzeit-konstruierbar*, falls eine deterministische IOTM M existiert, deren Rechenzeit für alle Eingaben w durch $T\,(|w|)$ beschränkt ist, und für die es zu jedem $n \in \mathbb{N}_0$ ein Eingabewort w mit $|w| = n$ gibt, für das $RZ_M(w) = T\,(|w|)$ gilt. T heißt *vollständig Rechenzeit-konstruierbar*, wenn es eine IOTM M gibt, für die für alle Eingabewörter w gilt: $RZ_M(w) = T\,(|w|)$.

[33] Die Existenz einer solchen Sprache folgt auch aus einem Hierarchieresultat in [Co73]; außerdem verweist [Rei90] noch auf [SFM78] und [Z83].

gilt. (Die vollständige Rechenzeit-Konstruierbarkeit von $f\left(\lfloor\frac{n}{2}\rfloor\right)$ folgt einfach aus der vollständigen Rechenzeit-Konstruierbarkeit von 2^n und also von $f(n)$ und der Berechenbarkeit von $\lfloor\frac{n}{2}\rfloor$ [34].) Wegen (3.38) gilt nun jedenfalls auch

$$L_0 \leq Thm_T. \tag{3.40}$$

Durch die Anwendung von Lemma 2.6.5, (und einem Beweis, der völlig analog zum Beweis von Satz 2.6.4, (ii), verläuft) folgt hieraus wegen $L_0 \notin NTime\left(\frac{n}{4}\right)$ (vgl. (3.39)) die Existenz einer Konstanten $c_0 \in \mathbb{R}$, $c_0 > 0$ so, daß

$$Thm_T \notin NTime\big(c_0 \cdot \frac{n}{4}\big),$$

woraus (3.37) unmittelbar folgt. Es läßt sich also die $\leq_{pl}$-Reduzierbarkeit von L_0 auf Thm_T zur Übertragung einer unteren Schranke von L_0 auf Thm_T nutzen. Die dabei ins Spiel kommende Konstante c_0 kann (wie aus dem Beweis von Satz 6.4 (ii) hervorgeht) dabei beliebig, aber kleiner als der Kehrwert einer in der linear-Beschränkt-heit einer *POLYLIN*-Funktion g, die die Reduktion (3.40) durchzuführen erlaubt, auftretenden Konstanten gewählt werden (diese Konstante müßte aber erst als ein in der Annahme des Satzes auftretendes c_M für eine Turingmaschine M, die L_0 akzeptiert, konstruiert werden und müßte durch eine genaue Analyse des verwendeten Hierarchie-Resultats—für den vorliegenden Fall spezifiziert—gewonnen werden.

□

Der zweite Schritt im allgemeinen Teil der Komplexitätsbeweise in [FiR74] besteht aus einer Aussage, daß bzw. wie in allen behandelten Theorien der Additionsarithmetik unter der Voraussetzung der Existenz von Grundformeln mit geeigneten Eigenschaften, solchen Grundformeln, die Binärwörter der Länge $f(n)^2$ zu beschreiben helfen ($f(n) = 2^n$ oder 2^{2^n}), die Annahme von Satz 3.4.1 (über die Existenz von Formeln $\mathbf{F}_{M,w}$ ($M \in \mathcal{EM}_\Gamma$, $w \in (\Sigma(M))^*$) in der jeweils behandelten Theorie mit den dort aufgeführten Eigenschaften) erfüllt werden kann; daß und wie also Formeln $\mathbf{F}_{M,w}$ unter Zuhilfenahme von Grundformeln, die noch näher anzugebenden Bedingungen genügen, (effektiv) konstruiert werden können. – Diese Hilfsformeln müssen dann—um die Komplexitätsbeweise abzuschließen—in den einzelnen Theorien weitgehend gesondert entwickelt werden (vgl. Abschnitt 5, Abschnitt 6, Abschnitt 7).

In die Beweise dieser im folgenden in Satz 3.4.4 (für RA und die Theorien der Presburger Arithmetik natürlicher Zahlen) und in Satz 3.4.6 (für TAZ) formulierten Aussage geht eine wichtige Hilfsaussage ein, Lemma 3.4.5, mit deren Verwendung es möglich wird, allgemeine Berechnungen und akzeptierende Berechnungen der Länge $f(n)$ von $\mathcal{EM}_\Gamma$-Turingmaschinen (Γ ein endliches Bandalphabet, $|\Gamma| \geq 2$) durch 3 Wörter U, V, W der Länge

[34] wenigstens für hinreichend große n (das dürfte sicherlich für die Anwendbarkeit des Hierarchie-Resulats ausreichen)

$(f(n))^2$ genau zu beschreiben, insbesondere auch genaue formale Bedingungen anzugeben, unter denen 3 solche Wörter U, V, W eine akzeptierende Berechnung von einem $M \in \mathcal{EM}_\Gamma$ auf einem Eingabewort $w \in (\Sigma(M))^*$ der Länge $< f(n)$ darstellen. – Diese Hilfsaussage wird dann im weiteren zum Beweis von Satz 3.4.4 und Satz 3.4.6 bei der Konstruktion der gesuchten Formeln $\mathbf{F}_{M,w}$ herangezogen und zwar dadurch, daß die Wörter U und W in Binärwörter $U_1, \ldots, U_p$ und $W_1, \ldots, W_q$ $(p, q \in \mathbb{N})$ der Länge $(f(n))^2$ zerteilt werden, für deren Beschreibung dann die vorausgesetzten Grundformeln verwendet werden können.

Der Grund dafür, warum die für diesen Beweisschritt benötigte Aussage zweimal formuliert wird, einmal für RA (und verwandte Theorien) und für Theorien der Presburger Arithmetik natürlicher Zahlen und dann noch unabhängig davon für TAZ liegt darin, daß dabei jeweils unterschiedliche verwendete Arten der Kodierung von Binärwörtern durch (ganze bzw. natürliche) Zahlen ins Spiel kommen.

Während im ersten Fall

$$\begin{aligned} Bw_1 : \mathbb{N}_0 &\to BW1 \\ n &\mapsto Bw_1(n) := ((n)_2)^R \end{aligned} \tag{3.41}$$

verwendet wird, kommt im zweiten Fall

$$Bw_2 : \mathbb{Z} \to BW1 \tag{3.42}$$

$$a \mapsto \begin{cases} 0 & \ldots\ a = 0, 1, -1 \\ \operatorname{sgn}(i_1) \circ \operatorname{sgn}(i_2) \circ \ldots & \ldots\ a = (-1)^{i_0} \cdot p_1^{i_1} \cdot p_2^{i_2} \cdot \ldots \cdot p_{m-1}^{i_{m-1}} \cdot p_m^{i_m+1}, \\ \quad \ldots \circ \operatorname{sgn}(i_{m-1}) \circ 1 & \quad |a| \geq 2,\ (m \in \mathbb{N},\ i_0 \ldots i_m \in \mathbb{N}_0, \\ & \quad p_1, p_2, p_3, \ldots \text{ Reihe der Primzahlen}) \end{cases}$$

vor (worin sgn für die Signumfunktion steht); Bw_1 ist dabei bijektiv, Bw_2 nur surjektiv. Im ersten Fall wird also ein Binärwort $w \in BW1$ durch eine natürliche Zahl n mit

$$n = Bw_1^{-1}(w) = w(0) + w(1) \cdot 2^1 + \ldots + w(|w| - 1) \cdot 2^{|w|-1}$$

kodiert, im zweiten Fall, falls $w \neq 0$, durch alle $a \in \mathbb{Z}$ mit

$$a \neq 0 \ \ \& \ \ (\forall i \in \mathbb{N}_0) \left(p_{i+1} \mid a \iff w(i) = 1 \right),$$

bzw., falls $w = 0$, durch 0, 1 oder -1 (beidemale jeweils also durch alle $a \in \mathbb{Z}$ mit $Bw_2(a) = w$).

Es wird im folgenden bei der Beschreibung der Eigenschaften von in den betrachteten additiven Theorien zu entwickelnden Formeln eine abkürzende Schreibweise verwendet, die es erlaubt, gewünschte, durch die Formel ausgedrückte Beziehungen sehr knapp und inhaltlich-orientiert, jedoch ohne auf eine gegebene Semantik für diese Theorien dabei unmittelbar Bezug zu nehmen, darstellen zu können. So wird zum Beispiel eine in RA

und $PreAN$ zu entwickelnde Formel $\mathbf{M}_n(x,y,z)$, die in diesen Theorien die Multiplikation jedenfalls für einen begrenzten Abschnitt von $\mathbb{N}_0$ ausdrücken soll, durch

$$\vdash_{RA} \mathbf{M}_n(x,y,z) \leftrightarrow [\![\, x \in \mathbb{N}_0,\ x < 2^{2^n},\ x \cdot y = z \,]\!] \tag{3.43}$$

beschrieben werden. Dabei ist mit der Klammerungsschreibweise auf der rechten Seite eigentlich eine geeignete, durch den Inhalt der Klammer weitgehend bestimmte Formel von RA gemeint, die dadurch beschrieben und abgekürzt wird. Ausführlich bedeutet (3.43) also etwa

$$\vdash_{RA} \mathbf{M}_n(x,y,z) \leftrightarrow \bigvee_{\substack{i\in\mathbb{N}_0,\\ i<2^{2^n}}} \big(\, x = \underline{\underline{i}} \,\&\, z = \underline{i}\, y \,\big) \tag{3.44}$$

(wobei die Schreibweisen $\underline{\underline{i}}$ und $\underline{i}\, a$ für Zahlen $i \in \mathbb{N}_0$ und Terme $\mathbf{a}$ wie in den Definitionen der Theorien der Presburger Arithmetik in Kapitel 2, Definition 2.1.1; $\underline{\underline{3}}$ ist also $1+(1+1)$, $\underline{3}\,\underline{\underline{2}}$ ist gleich $(1+1)+((1+1)+(1+1))$).

(Hierbei spielt eine Charakterisierung von $\mathbf{M}_n(x,y,z)$ durch (3.43) bzw. (3.44) deshalb eine Rolle und die gesuchte Formel $\mathbf{M}_n(x,y,z)$ ist nicht einfach in

$$\bigvee_{\substack{i\in\mathbb{N}_0,\\ i<2^{2^n}}} \big(\, x = \underline{\underline{i}} \,\&\, z = \underline{i}\, y \,\big) \tag{3.45}$$

gefunden worden, weil $\mathbf{M}_n(x,y,z)$ im folgenden auch noch der Längenbedingung $(n \mapsto |\mathbf{M}_n(x,y,z)|) \in O(n)$ genügen soll und (3.45) ja doppelt-exponentiell von n abhängende Länge hat).

Wenn eine solche Klammerungsschreibweise zur inhaltlichen Erfassung der von einer Formel ausgedrückten Beziehungen im folgenden verwendet wird, so liegt einem solchen Gebrauch dann immer gleichzeitig die Behauptung zugrunde, daß eine so abgekürzte Formel in der jeweils betrachteten Theorie auch tatsächlich auf ganz unmittelbare und naheliegende Weise konstruiert und angegeben werden kann.

Die hier in (3.44) und (3.45) verwendeten abkürzenden Schreibweisen für Terme $\underline{\underline{i}}$ und $\underline{i}\mathbf{a}$ (für $i \in \mathbb{N}_0$) aus Definition 2.1.1 werden auch im folgenden an einigen Stellen verwendet werden.

Satz 3.4.4. *$f(n)$ sei eine der beiden Funktionen $n \mapsto 2^n$ oder $n \mapsto 2^{2^n}$ [35]; T eine Theorie 1.Ordnung der Gestalt $T = Th(\langle A; 0, 1, +, \dots\rangle)$ mit $\mathbb{N}_0 \subseteq A$; $T^{((M))}$ sei die als System formaler Sprachen aufgefaßte Theorie T mit informatisch-sinnvoller Formelsyntax; Bw_1 wie in* (3.41).

[35] Die Einschränkung von $f(n)$ auf diese zwei Funktionen ist durch den Beweis von Satz 3.4.4 nicht gerechtfertigt (hier könnte *jedes* $f\colon \mathbb{N}_0 \to \mathbb{N}_0$ mit $f(n) > \max\{n, 1\}$ (für alle $n \in \mathbb{N}_0$) verwendet werden). Die Aussage dieses Satzes hängt jedoch auch über $f(n)$ mit den anderen Sätzen zusammen und diese konnten in [FiR74] für $f(n)$ wie hier angenommen oft besonders konkret bewiesen werden (und in der Aufarbeitung hier wird versucht, dem Beweisweg in [FiR74] möglichst nahe zu bleiben).

Angenommen, *es existieren für alle* $n \in \mathbb{N}_0$ *Formeln* $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$, $\mathbf{L}_n(x)$ *und* $\mathbf{S}_n(x,y)$, *sowie für alle* $w \in BW0$ *Formeln* $\mathbf{H}_w(x)$ *in* T, *sodaß die beiden Bedingungen (i) und (ii) gelten, wobei:*

(i) Es gilt für alle $n \in \mathbb{N}_0$, $w \in BW0$, $|w| = n$*:*

$$\vdash_T \mathbf{I}_n(x) \leftrightarrow [\![\, x \in \mathbb{N}_0,\ x < (f(n))^2 \,]\!] \ ;$$
$$\vdash_T \mathbf{J}_n(x) \leftrightarrow x = \underline{\underline{f(n)}}\ ^{36};$$
$$\vdash_T \mathbf{L}_n(x) \leftrightarrow \left[\!\!\left[\, x \in \mathbb{N}_0,\ x < 2^{(f(n))^2} \,\right]\!\!\right] ;$$
$$\vdash_T \mathbf{S}_n(x,y) \leftrightarrow \left[\!\!\left[\, x,y \in \mathbb{N}_0,\ y < (f(n))^2,\ x < 2^{(f(n))^2},\ (Bw_1(x))(y) = 1 \,\right]\!\!\right] ;$$
$$\vdash_T \mathbf{H}_w(x) \leftrightarrow \left[\!\!\left[\, |w| = n \in \mathbb{N},\ x \in \mathbb{N}_0,\ x < 2^{(f(n))^2},\right.\right.$$
$$\left.\left. (Bw_1(x))(0) \circ \ldots \circ (Bw_1(x))(f(n)-1) = w \circ 0^{f(n)-n} \,\right]\!\!\right] .$$

(ii) Die Familien $\left\{\mathbf{I}_n(x)^{((M))}\right\}_{n\in\mathbb{N}_0}$, $\left\{\mathbf{J}_n(x)^{((M))}\right\}_{n\in\mathbb{N}_0}$, $\left\{\mathbf{L}_n(x)^{((M))}\right\}_{n\in\mathbb{N}_0}$ *und* $\left\{\mathbf{S}_n(x,y)^{((M))}\right\}_{n\in\mathbb{N}_0}$ *genügen den Längen- und Konstruierbarkeitsbedingungen (A),* $\left\{\mathbf{H}_w(x)^{((M))}\right\}_{w\in BW0}$ *den Bedingungen (B) aus Definition 3.3.5.*

Dann gilt *für* $f(n)$ *und* $T^{((M))}$ *unter den weiteren Voraussetzungen von Satz 3.4.1 (an* Γ, Σ_{code}, *Symb und* $\langle\cdot\rangle_{\Gamma,Symb}$*) die Annahme von Satz 3.4.1.*

[Dieser Satz entspricht—im Kontext der Aufarbeitung hier—Theorem 7, p. 9, in [FiR74].]

Das wesentliche Hilfsmittel im Beweis dieser Aussage besteht in einer Möglichkeit (die [FiR74] beim Beweis von Theorem 7, p. 9, auf p. 11, 12, angeben), Berechnungen einer 1-Band-Turingmaschine der Länge $\leq f(n)$ auf einem Eingabewort w mit $n = |w|$ durch Wörter (und letztlich später im Beweis durch Binärwörter) der Länge $(f(n))^2$ zu beschreiben.

Da eine 1-Band-Turingmaschine mit einseitig-rechtsseitig unendlichem Band ihren SLK während einer Berechnung der Länge $< f(n)$ nicht weiter nach rechts als auf das $f(n)$-te Bandkästchen bewegen kann, spielt bei einer solchen Berechnung nur der Inhalt der ersten $f(n)$ Bandkästchen eine Rolle.

[36] Diese hier und im folgenden wieder häufig verwendete abkürzende Schreibweise für sich auf natürliche Zahlen beziehende Terme ist in Definition 2.1.1 definiert worden.

Daher kann ein Berechnungspfad $C = (\alpha_0, \alpha_1, \ldots, \alpha_l)$ mit $l \in \mathbb{N}_0$, $l < f(n)$ einer Turingmaschine $M \in \mathcal{EM}_\Gamma$ für Eingabewort $w \in \Sigma^*$ mit $|w| = n$ und wobei weiters $\alpha_j = w_{j_1} q_{i_j} w_{j_2}$, $w_{j_1} \in \Gamma^*$, $q_{i_j} \in Q$, $w_{j_2} \in \Gamma^*(\Gamma \setminus \{\#\}) \cup \{\epsilon\}$ (für $0 \leq j \leq l$, $j \in \mathbb{N}_0$), $j_l = k$, und $Q = \{q_1, \ldots, q_k\}$, $\Gamma = \{S_0, \ldots, S_m\}$ $(k, m \in \mathbb{N})$ gelten, durch Wörter $U_j \in \{0, 1, \ldots, k\}^{f(n)}$, $W_j \in \{0, 1, \ldots, m\}^{f(n)}$ der Länge $f(n)$ mit

$$W_j := w_{j_1}^{(N)} \circ w_{j_2}^{(N)} \circ 0^{f(n) - \left|w_{j_1}^{(N)}\right| - \left|w_{j_2}^{(N)}\right|}$$
$$U_j := 0^{\left|w_{j_1}^{(N)}\right|} \circ i_j \circ 0^{f(n) - \left|w_{j_1}^{(N)}\right| - 1}$$
$$(j \in \mathbb{N}_0,\ 0 \leq j \leq l)$$

erfaßt werden (hierbei und im folgenden bezeichnet für ein Wort $w \in \Sigma^*$ mit $|w| = n$ und $w = S_{l_1} \circ S_{l_2} \circ \ldots \circ S_{l_n}$ $(l_j \in \{0, \ldots, m\}$ für $j \in \{1, \ldots, n\})$ der Ausdruck $w^{(N)}$ das aus natürlichen Zahlen bestehende Wort $l_1 \circ l_2 \circ \ldots \circ l_n$). W_j erfaßt dabei den Bandzustand der ersten $f(n)$ Bandkästchen zum Zeitpunkt j im Berechnungspfad C und U_j den aktuellen Zustand, in dem sich M zu diesem Zeitpunkt befindet, und die Position des SLKes von M auf dem betrachteten Teil des Turingbandes zur Zeit j.

Eine abbrechende Berechnung C von M auf Eingabe w der Länge $l < f(n)$ kann nun durch zwei Wörter $U \in \{0, 1, \ldots, k\}^{(f(n))^2}$, $W \in \{0, 1, \ldots, n\}^{(f(n))^2}$ der Länge $(f(n))^2$ mit

$$W := W_0 \circ W_1 \circ \ldots \circ W_l \circ (W_l)^{f(n)-l-1}$$
$$U := U_0 \circ U_1 \circ \ldots \circ U_l \circ (U_l)^{f(n)-l-1}$$

beschrieben werden, wobei in diese Beschreibung die Annahme eingeht, daß in den auf die Termination der Berechung folgenden Zeittakten $j \in \{l+1, l+2, \ldots, f(n)-1\}$ der Endzustand der Maschine beibehalten wird.

Das folgende Lemma enthält in einer solchen Situation notwendige und hinreichende Bedingungen an $U \in \{0, 1, \ldots, k+1\}^{f(n)^2}$ und $W \in \{0, 1, \ldots, n\}^{(f(n))^2}$ dafür, daß es sich dabei um eine Beschreibung der vorgestellten Art eines *akzeptierenden* Berechnungspfades von M auf w der Länge $< f(n)$ $(n = |w|)$ handelt. Dabei ist das Alphabet für U um eine Zahl vergrößert worden (aus formal-technischen Gründen der Darstellung von abbrechenden, nicht akzeptierenden Berechnungen) und weiters tritt darin (gegenüber der in [FiR74] verwendeten, vergleichbaren Aussage) noch ein zusätzliches Binärwort $V \in \{0, 1\}^{(f(n))^2}$ mit $V = (10^{f(n)-1})^{f(n)}$ auf, das Anfang und Ende der Wörter U_j nd W_j $(j \in \{0, 1, \ldots, f(n)-1\})$ innerhalb von U und W erkennen hilft und es erlaubt, die Bedingungen an U und W klarer verstehbar zu machen, und das außerdem zur Klärung der Beschreibung in einigen besonderen Situationen nötig ist (etwa in dem Fall, daß eine Berechnung abbricht, falls die Turingmaschine versucht, den SLK über das links-äußerste Bandkästchen hinaus weiter nach links zu bewegen).

Lemma 3.4.5. *$M = (Q, \Sigma, \Gamma, \delta, q_1, \#, F)$ sei eine 1-Band-Turingmaschine $M \in \mathcal{EM}_\Gamma$ mit $Q = \{q_1, \ldots, q_k\}$, $\Gamma = \{S_0, \ldots, S_m\}$ $(k, n \in \mathbb{N})$, $\# = S_0$, $\Sigma \subseteq \Gamma \setminus \{S_0\}$, $F = \{q_k\}$, $\delta\colon (Q \setminus F) \times \Gamma \to 2^{Q \times \Gamma \times \{L,R\}}$ partielle Funktion.*
$f : \mathbb{N}_0 \to \mathbb{N}_0$ eine Funktion mit $(\forall n \in \mathbb{N})\,(f(n) > \max\{n, 1\})$.

Dann gilt *für alle $w \in \Sigma^*$, $w_1 \in (\Gamma \setminus \{\#\})^*$ und $w_2 \in \Gamma^*(\Gamma \setminus \{\#\}) \cup \{\epsilon\}$, wobei $|w| = n$ und $n \in \mathbb{N}_0$:*

$$\begin{aligned}
&\big[\,(\,\exists\, l \in \{0, 1, \ldots, f(n)-1\}\,)\,(\,\exists\, w_1 \in \Gamma^*,\, w_2 \in \Gamma^*(\Gamma \setminus \{\#\}) \cup \{\epsilon\}\,) \\
&\qquad\qquad (\; q_1 w \vdash_M^{(l)} w_1 q_k w_2 \;)\,\big] \\
&\big(\iff \mathit{Min\text{-}RZ}_M(w) < f(n)\ \&\ M \text{ akzeptiert } w\big) \\
&\quad\iff \big(\exists\, U \in \{0, 1, \ldots, k+1\}^{(f(n))^2},\, V \in \{0,1\}^{(f(n))^2},\, W \in \{0, 1, \ldots, m\}^{(f(n))^2}\,\big) \\
&\qquad\qquad \big(\forall\, i \in \{0, 1, \ldots, (f(n))^2 - 1\}\big) \\
&\qquad\qquad\qquad \big(\text{es gelten die an } U, V, W, i \text{ und } w \\
&\qquad\qquad\qquad\qquad \text{gerichteten Bedingungen (B1)-(B9)}\big)
\end{aligned}$$

wobei:

(B1):: $$\begin{aligned} W(0)\,W(1)\,\ldots\,W(f(n)-1) &= w^{(N)}\,0^{f(n)-|w|}\,, \\ U(0)\,U(1)\,\ldots\,U(f(n)-1) &= 1\,0^{f(n)-1}\,, \\ V(0)\,V(1)\,\ldots\,V(f(n)-1) &= 1\,0^{f(n)-1}\,; \end{aligned}$$

(B2):: $U(i) = 0\ \&\ i + f(n) < |W| \ \Rightarrow\ W(i + f(n)) = W(i)$;

(B3):: $i + f(n) < |V| \ \Rightarrow\ V(i + f(n)) = V(i)$;

(B4):: *siehe Formel 3.4.1* ;

(B5):: $i + f(n) < |V|\ \&\ V(i+1) = 1 \ \rightarrow\ U(i) = 0$;

(B6):: $$\begin{aligned} &i + f(n) - 1 < |U|, |W|\ \&\ V(i) = 1\ \Rightarrow \\ &\qquad \Rightarrow\ (\,\exists!\, j \in \mathbb{N}_0\,)\,(\,i \le j < i + f(n)\ \&\ U(j) \neq 0\,)\,; \end{aligned}$$

(B7):: $$\begin{aligned} &i + f(n) < |U|, |W|\ \&\ U(i) = k\ \Rightarrow \\ &\qquad \Rightarrow\ U(i + f(n)) = k\ \&\ W(i + f(n)) = W(i)\,; \end{aligned}$$

(B8):: $$\begin{aligned} &i + f(n) < |U|, |W|\ \&\ U(i) = k+1\ \Rightarrow \\ &\qquad \Rightarrow\ U(i + f(n)) = k+1\ \&\ W(i + f(n)) = W(i)\,; \end{aligned}$$

Formel 3.4.1 Die Bedingung (B4):

$$i + f(n) + 1 < |U|, |V|, |W| \;\&\; \&\!\!\&_{\substack{i_1 \in \{1,\ldots,k-1\},\\ l_1 \in \{0,\ldots,m\}}} \Big[U(i) = i_1 \;\&\; W(i) = l_1 \;\Rightarrow$$

$$\Rightarrow \left\{ \begin{array}{l} W(i+f(n)) = W(i) \;\&\; U(i+f(n)) = k+1 \\ \qquad\qquad \ldots\ldots\ldots\; \delta(q_{i_1}, S_{l_1}) = \emptyset \\ \big[\big(V(i) = 1 \Rightarrow W(i+f(n)) = W(i) \;\&\; U(i+f(n)) = k+1 \big) \\ \quad \&\; \big(V(i) = 0 \Rightarrow \bigvee\limits_{(q_{i_2}, S_{l_2}, L) \in \delta(q_{i_1}, S_{l_1})} W(i+f(n)) = l_2 \;\&\; U(i+f(n)-1) = i_2 \big) \big] \\ \qquad\qquad \ldots\ldots\ldots\; \delta(q_{i_1}, S_{l_1}) \neq \emptyset \;\& \\ \qquad\qquad\qquad\qquad \&\text{ es gibt kein } (q_{i_2}, S_{l_2}, R) \in \delta(q_{i_1}, S_{l_1}) \\ \Big(\bigvee\limits_{(q_{i_2}, S_{l_2}, R) \in \delta(q_{i_1}, S_{l_1})} W(i+f(n)) = l_2 \;\&\; U(i+f(n)+1) = i_2 \Big) \;\vee \\ \vee \Big(\bigvee\limits_{(q_{i_2}, S_{l_2}, L) \in \delta(q_{i_1}, S_{l_1})} V(i) = 0 \;\&\; W(i+f(n)) = l_2 \;\&\; U(i+f(n)-1) = i_2 \Big) \\ \qquad\qquad \ldots\ldots\ldots \text{ sonst} \end{array} \right\} \Big] \;;$$

(B9):: $(\exists\, i_0 \in \mathbb{N}_0)\,(\, i_0 < f(n) \;\;\&\;\; U(i_0) = k\,)$.

[Dieses Lemma entspricht im Rahmen und im Kontext der Aufarbeitung hier einer in [FiR74] beim Beweis von Theorem 7, p. 9, auf p. 11, 12, eingearbeiteten, vergleichbaren Aussage[37]]

Erläuterungen zu den Bedingungen (B1)–(B9).

(B1): Beschreibt den Anfangszustand einer Berechnung von M auf w, das Hilfswort V wird durch $V_0 := 10^{f(n)-1}$ initialisiert.

(B2): Formalisiert die Bedingung, daß der Bandinhalt eines Bandkästchens, auf dem sich der SLK von M zu einem Zeitpunkt j nicht befindet, im folgenden Berechnungsschritt (der zum Zeitpunkt $j+1$ führt) nicht verändert wird.

(B3): Setzt das Hilfswort V als $V = V_0 \circ V_1 \circ \ldots \circ V_{f(n)-1}$ mit $V_j := V_0$ für alle Zeitpunkte $j \in \{0, 1, \ldots, f(n)-1\}$ durch induktive Definition aus V_0 fest.

(B4): Formalisiert einen Berechnungsschritt der Maschine M (das Drucken eines Symbols, das Bewegen des SLKes auf ein benachbartes Bandkästchen), wenn so ein Schritt möglich ist. Wenn so ein Schritt unmöglich ist (weil entweder die Übergangsfunktion für eine beschriebene Konfiguration keine Nachfolgerkonfiguration ermöglicht oder weil der SLK über das linke Bandende hinausbewegt werden würde), geht die Beschreibung in den undefinierten Maschinenzustand $k+1$ über.

(B5): Formalisiert für Augenblicksbeschreibungen $U = U_0 \circ U_1 \circ \ldots \circ U_j$ mit $|U_i| = f(n)$ $(0 \leq i \leq j)$, mit $j < f(n)$, daß das $f(n)$-te Bandkästchen zu allen Zeitpunkten $0, 1, \ldots, j-1$ vom SLK der Turingmaschine nicht erreicht werden kann. (Das ist erst zum Zeitpunkt $f(n)-1$ möglich.)

(B6): Fordert, daß in der Beschreibung $U_j \in \{0, 1, \ldots, k+1\}^{f(n)}$ die Position des SLKes eindeutig festgelegt ist.

(B7): Ist bei einer Berechnung ein Endzustand erreicht worden, so wird die Position des SLKes und der Endzustand der Maschine auch im nächstfolgenden Zeittakt beibehalten und der Bandinhalt wird an dieser Stelle nicht mehr verändert.

(B8): Ist eine Berechnung abgebrochen worden, so wird in einem folgenden Zeittakt der SLK nicht mehr bewegt, der Bandinhalt an der Position des SLKes unverändert belassen und der undefinierte Maschinenzustand $k+1$ beibehalten.

[37] Diese in [FiR74] dabei verwendete Aussage, die hier in den Kontext dieser Aufarbeitung übertragen wurde, sollte [m.E., C.G.] an einigen Stellen (v.a. die Bedingung (ϵ) auf p. 12 betreffend) noch geringfügig abgeändert werden, damit sie im Zusammenhang, in dem [FiR74] diese Aussage einsetzen, exakt beweisbar ist.

(B9): Die Augenblicksbeschreibung U_j irgend eines Zeitpunktes $j \in \{0, 1, \dots, f(n)-1\}$ enthält den Endzustand, d.h. diese Beschreibung erfaßt eine Endkonfiguration.

Beweisskizze für Lemma 3.4.5. M und f seien wie in der Annahme des Lemmas.

(1) Der Hauptteil des Beweises kann im Nachweis liegen, daß für alle $w \in \Sigma^*$, $w_1 \in \Gamma^*$, $w_2 \in \{\Gamma^*(\Gamma \setminus \{\#\}) \cup \{\epsilon\}$, $n \in \mathbb{N}_0$, $|w| = n$, $i_1 \in \{1, \dots, k+1\}$ und $l \in \{0, 1, \dots, f(n)-1\}$ die folgende Aussage $A(l; w, w_1, w_2, i_1)$

$$
\begin{aligned}
&\{\, q_1 w \vdash_M^{(l)} w_1 q_{i_1} w_2 \;\vee \\
&\qquad \vee\, (\exists\, l_0 \in \mathbb{N}_0)\,(\exists i_2 \in \{1, \dots, k\}) \\
&\qquad\qquad [\, l_0 < l \;\&\; q_1 w \vdash_M^{(l_0)} w_1 q_{i_2} w_2 \;\& \\
&\qquad\qquad\qquad \&\; \big(i_2 = i_1 = k \;\vee\; i_2 \neq k \;\&\; w_1 q_{i_2} w_2 \text{ besitzt keine} \\
&\qquad\qquad\qquad\qquad \text{Nachfolgekonfiguration bzgl. } M, \delta \;\&\; i_1 = k+1\big)\,]\,\} \\
\iff\; &\big(\exists\, U \in \{0, 1, \dots, k+1\}^{(l+1)f(n)}, \\
&\qquad\qquad V \in \{0,1\}^{(l+1)f(n)},\, W \in \{0, 1, \dots, m\}^{(l+1)f(n)}\big) \\
&\qquad (\forall\, i \in \{0, 1, \dots, (l+1)f(n)-1\}\,) \\
&\qquad\qquad \big(\text{ es gelten die an } U, V, W, w \text{ gerichteten Bedingungen} \\
&\qquad\qquad\quad \text{(B1),(B2), } \dots \text{,(B}\underline{8}\text{)} \;\& \\
&\qquad\qquad\quad \&\; U(l\, f(n))\, U(l\, f(n)+1) \dots U((l+1)\, f(n)-1) = \\
&\qquad\qquad\qquad\qquad = 0^{|w_1|}\, i_1\, 0^{f(n)-|w_1|-1} \\
&\qquad\qquad\quad \&\; W(l\, f(n))\, W(l\, f(n)+1) \dots W((l+1)\, f(n)-1) = \\
&\qquad\qquad\qquad\qquad = w_1^{(N)}\, w_2^{(N)}\, 0^{f(n)-|w_1|-|w_2|} \\
&\qquad\qquad\quad \&\; V(l\, f(n))\, V(l\, f(n)+1) \dots V((l+1)\, f(n)-1) = \\
&\qquad\qquad\qquad\qquad = 1\, 0^{f(n)-1}\,\big)
\end{aligned}
\tag{3.46}
$$

gilt. Diese $\iff$ Beziehung von Teilaussagen drückt aus, daß sich alle Berechnungspfade (und nicht nur akzeptierende Berechnungspfade) der Länge $l < f(n)$ von M für Eingabewort $w \in \Sigma^*$, $n = |w|$, auf die früher dargestellte Weise durch (entsprechende) Wörter U, V, W der Länge $(l+1)f(n)$ (und im weiteren Beweis dann durch Wörter der Länge $(f(n))^2$) exakt beschreiben lassen.

Die Gültigkeit der Aussage $A(l; w, w_1, w_2, i_1)$ kann für beliebige $w \in \Sigma^*$, $w_1 \in \Gamma^*$, $w_2 \in \Gamma^*(\Gamma \setminus \{\#\}) \cup \{\epsilon\}$, $n \in \mathbb{N}_0$, $|w| = n$ $i_1 \in \{1, \dots, k+1\}$ und $l \in \{0, 1, \dots, f(n)-1\}$ durch den Nachweis der beiden $\Longrightarrow$-Richtungen in der Äquivalenz $\iff$ darin jeweils mittels Induktion über l gezeigt werden. Dabei muß

jeweils ausführlich auf die genaue formale Definition von 1-Band-Turingmaschinen aus Abschnitt 3 (die dort aus [HoUl79] entnommen wurde) zurückgegriffen werden. Wegen des großen Umfangs unterbleibt dieser (detailreiche, jedoch nicht schwierige) Beweisteil hier.

(2) Ausgehend von (1) kann nun nun die Aussage des Lemmas gezeigt werden, also für alle $w \in \Sigma^*$ die Aussage:

$$\begin{aligned}
&\big[\,(\,\exists l \in \{0,1,\ldots,f(n)-1\}\,)\,(\,\exists w_1 \in \Gamma^*,\, w_2 \in \Gamma^*(\Gamma\setminus\{\#\})\cup\{\epsilon\}\,) \\
&\qquad\qquad (\; q_1 w \vdash_M^{(l)} w_1 q_k w_2 \;)\,\big] \\
&\iff \big(\exists U \in \{0,1,\ldots,k+1\}^{(f(n))^2},\, V \in \{0,1\}^{(f(n))^2},\, W \in \{0,1,\ldots,m\}^{(f(n))^2}\,\big) \\
&\qquad \big(\exists i \in \{0,1,\ldots,(f(n))^2-1\}\big) \\
&\qquad\quad \big(\text{es gelten die an } U,\, V,\, W,\, i \text{ und } w \\
&\qquad\qquad \text{gerichteten Bedingungen (B1)–(B9)}\,\big)
\end{aligned}$$

Sei dazu $w \in \Sigma^*$, $|w| = n$ beliebig, fest: Zeige unter Benützung der in (1) erzielten Aussage für w die obige Äquivalenz durch den Nachweis der Gültigkeit beider Richtungs-Implikationen.

„$\Rightarrow$“: Nach Annahme existieren $l \in \mathbb{N}_0$, $l \in \{0,1,\ldots,f(n)-1\}$, $w_1 \in \Gamma^*$ und $w_2 \in \Gamma^*(\Gamma\setminus\{\#\})\cup\{\epsilon\}$ mit

$$q_1 w \vdash_M^{(l)} w_1 q_k w_2\,. \tag{3.47}$$

Seien l, w_1, w_2 so gewählt, im folgenden fest.
Aus (3.47) folgt wegen der in (1) erzielten Aussage (3.46) (in der Anwendung für $l := f(n)-1$) die Existenz von $U \in \{0,1,\ldots,k+1\}^{(f(n))^2}$, $V \in \{0,1\}^{(f(n))^2}$ und $W \in \{0,1,\ldots,m\}^{(f(n))^2}$, die für alle $i \in \{0,1,\ldots,(f(n))^2-1\}$ (B1)–(B8) erfüllen und für die außerdem gilt:

$$\begin{aligned}
&U((f(n)-1)\,f(n))\,U((f(n)-1)\,f(n)+1)\ldots U((f(n))^2-1) = \\
&\qquad = 0^{|w_1|}\,k\,0^{f(n)-|w_1|-1} \\
&W((f(n)-1)\,f(n))\,W((f(n)-1)\,f(n)+1)\ldots W((f(n))^2-1) = \\
&\qquad = w_1^{(N)}\,w_2^{(N)}\,0^{f(n)-|w_1|-|w_2|} \\
&V((f(n)-1)\,f(n))\,V((f(n)-1)\,f(n)+1)\ldots V((f(n))^2-1) = \\
&\qquad = 1\,0^{f(n)-1}
\end{aligned}$$

Da hieraus $U(((f(n)-1)\,f(n)+|w_1|)=k$ folgt, ist für U auch (B9) erfüllt und insgesamt erfüllen daher U,V,W,w für alle $i\in\{0,1,\ldots,(f(n))^2-1\}$ die Bedingungen (B1)–(B9). Damit ist aber der Nachweis der Implikation „$\Rightarrow$“ gelungen.

„$\Leftarrow$“: Seien umgekehrt $U\in\{0,1,\ldots,k+1\}^{(f(n))^2}$, $V\in\{0,1\}^{(f(n))^2}$ und $W\in\{0,1,\ldots,m\}^{(f(n))^2}$ nach Annahme so gewählt und im folgenden fest, daß U,V,W,w für alle $i\in\{0,1,\ldots,(f(n))^2-1\}$ die Bedingungen (B1)–(B9) erfüllen.

Wegen (B9) existiert ein $i_0\in\{0,1,\ldots,(f(n))^2-1\}$ mit

$$U(i_0)=k \tag{3.48}$$

Sei $l_1\in\{0,1,\ldots,f(n)-1\}$ von i_0 abhängig so gewählt, daß

$$l_1\,f(n)\le i_0<(l_1+1)\,f(n) \tag{3.49}$$

gilt. Durch Induktion aus (B1) mit Hilfe von (B3) ist leicht zu sehen, daß

$$\begin{aligned}&V(l_1\,f(n))\,V_0(l_1\,f(n)+1)\ldots V_0((l_1+1)\,f(n)-1)=\\&\qquad=1\,0^{f(n)-1}\end{aligned} \tag{3.50}$$

gilt. Damit sind wegen außerdem (3.48), (3.49) und (B6) $w_1\in\Gamma^*$ und $w_2\in\Gamma^*(\Gamma\setminus\{\#\})\cup\{\epsilon\}$ wählbar, so, daß

$$\begin{aligned}&U(l_1\,f(n))\,U(l_1\,f(n)+1)\ldots U((l_1+1)\,f(n)-1)=\\&\qquad=0^{|w_1|}\,k\,0^{f(n)-|w_1|-1}\\&W(l_1\,f(n))\,W(l_1\,f(n)+1)\ldots W((l_1+1)\,f(n)-1)=\\&\qquad=w_1^{(N)}\,w_2^{(N)}\,0^{f(n)-|w_1|-|w_2|}\end{aligned} \tag{3.51}$$

gilt.

Seien nun $U_0\in\{0,1,\ldots,k+1\}^{(f(n))^2}$, $V_0\in\{0,1\}^{(f(n))^2}$ und $W_0\in\{0,1,\ldots,m\}^{(f(n))^2}$ definiert durch

$$\begin{aligned}U_0(i):=U(i),\quad V_0(i):=V(i),\quad W_0(i):=W(i)\\(i_0\in\{0,1,\ldots,(l_1+1)\,(f(n))-1\})\end{aligned} \tag{3.52}$$

die Einschränkungen von U,V,W auf Wörter der Länge $(l_1+1)\,f(n)$. U_0,V_0,W_0,w erfüllen nun weiter die Bedingungen (B1)–(B8) [38] für alle $i\in\mathbb{N}_0$,

[38] Ebenso natürlich auch noch (B9), das aber für den folgenden Schluß, der sich auf die in (1) erhaltene Aussage bezieht, nicht mehr nötig ist.

$0 \leq i < (l_1+1)\,f(n)$ und es gilt wegen (3.50), (3.51) und (3.52)

$$\begin{aligned} &U_0(l_1\,f(n))\,U_0(l_1\,f(n)+1)\ldots U_0((l_1+1)\,f(n)-1) = \\ &\qquad = 0^{|w_1|}\,k\,0^{f(n)-|w_1|-1} \\ &W_0(l_1\,f(n))\,W_0(l_1\,f(n)+1)\ldots W_0((l_1+1)\,f(n)-1) = \\ &\qquad = w_1^{(N)}\,w_2^{(N)}\,0^{f(n)-|w_1|-|w_2|} \\ &V_0(l_1\,f(n))\,V_0(l_1\,f(n)+1)\ldots V_0((l_1+1)\,f(n)-1) = \\ &\qquad = 1\,0^{f(n)-1}\,. \end{aligned}$$

Wegen der in (1) erzielten Aussage (3.46) (in der Anwendung für $l := l_1$) existiert daher nun ein $l_0 \in \mathbb{N}_0$, $l_0 \leq l_1$ mit $q_1 w \vdash_M^{(l_0)} w_1 q_k w_2$. Sei nun $l := l_0$.
Insgesamt existieren daher $l \in \mathbb{N}_0$, $l < f(n)$, $w_1 \in \Sigma^*$, $w_2 \in \Gamma^*(\Gamma\backslash\{\#\}) \cup \{\epsilon\}$ mit $q_1 w \vdash_M^{(l)} w_1 q_k w_2$.
Damit ist aber der Nachweis der Gültigkeit des Sukzedens der Implikation „$\Leftarrow$“ in diesem Fall und, weil dieser Schritt für beliebige, aber feste $w \in \Sigma^*$ ausgeführt wurde, allgemein geglückt.

$\Diamond$

Beweis von Satz 3.4.4. Sei $f(n)$ nun eine der beiden im Satz vorausgesetzten Funktionen 2^n oder 2^{2^n}, $T = Th(\langle A; 0, 1, +, \ldots\rangle)$ für ein Universum A mit $\mathbb{N}_0 \subseteq A$;
$T^{((M))} = (\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ die als System formaler Sprachen mit informatisch-sinnvoller Formelsyntax erfaßte Theorie T;
sei $Bw_1 : \mathbb{N}_0 \to BW1$, $n \mapsto Bw_1(n) := ((n)_2)^R$.

Weiters seien für $T^{((M))}$ und $f(n)$ die weiteren Voraussetzungen von Satz 3.4.1 erfüllt, d.h. Γ sei ein endliches Alphabet mit $\Gamma \supseteq \Sigma_{T^{((M))}} \cup \Sigma_{\text{code}} \cup \{\#\}$, wobei Σ_{code} wie in Definition 3.3.2, $\#$ dabei ein Leersymbol, $\# \notin \Sigma_{T^{((M))}}$, $Symb\colon \{0, 1, \ldots, |\Gamma| - 1\} to \Gamma$ eine bijektive Funktion mit $Symb(0) = \#$, $\langle\cdot\rangle\colon \mathcal{EM}_\Gamma \to (\Gamma\backslash\{\#\})^+$ eine Kodierung für $\mathcal{EM}_\Gamma$-Turingmaschinen, die wie in Definition 3.3.1 festgelegt ist.

Sei nun weiters die Annahme von Satz 3.4.4 gültig. Danach seien nun $c_1, \ldots, c_5 \in \mathbb{N}$ und $g_1, \ldots, g_4\colon DZW \to Fo_{T^{((M))}}$ und $g_5\colon BW0 \to Fo_{T^{((M))}}$ mit $g_1, \ldots, g_5 \in DFTime(POL)$

so gewählt und im folgenden fest, daß für alle $n \in \mathbb{N}_0$ und $w \in BW0$

$$\begin{aligned}
g_1((n)_{10}) &= \mathbf{I}_n(x)^{((M))} & \left|(\mathbf{I}_n(x))^{((M))}\right| &\leq c_1\, n \\
g_2((n)_{10}) &= \mathbf{J}_n(x)^{((M))} & \left|(\mathbf{J}_n(x))^{((M))}\right| &\leq c_2\, n \\
g_3((n)_{10}) &= \mathbf{L}_n(x)^{((M))} & \left|(\mathbf{L}_n(x))^{((M))}\right| &\leq c_3\, n \\
g_4((n)_{10}) &= \mathbf{S}_n(x,y)^{((M))} & \left|(\mathbf{S}_n(x,y))^{((M))}\right| &\leq c_4\, n \\
g_5(w) &= \mathbf{H}_w(x)^{((M))} & \left|(\mathbf{H}_w(x))^{((M))}\right| &\leq c_5\, n
\end{aligned} \tag{3.53}$$

gelten, wobei die hierin auftretenden Formeln $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$, $\mathbf{L}_n(x)$, $\mathbf{S}_n(x,y)$ und $\mathbf{H}_w(x)$ für alle $n \in \mathbb{N}_0$ und $w \in BW0$ jeweils den in der Annahme (i) des Satzes aufgeführten inhaltlichen Bedingungen genügen. $g_1, \ldots, g_5$ können dabei weiters als so gewählt angenommen werden, daß $g_1, \ldots, g_5 \in DFTime_{\mathcal{EM}_\Gamma}(POL)$ gilt (eine solche Wahl von $g_1, \ldots, g_5$ macht höchstens eine zuvor nötige Anwendung des Alphabet-Reduktions-Satzes erforderlich).

Um unter diesen Voraussetzungen die Annahme von Satz 3.4.1 zu zeigen, ist die Existenz von $d \in \mathbb{R}$, $d > 0$ und Funktionen $e\colon \mathbb{N}_0 \to \mathbb{N}_0$ und $g\colon (\Gamma\backslash\{\#\})^* \to \Sigma_T^*$ mit $g \in DFTime_{\mathcal{EM}_\Gamma}(POL)$ zu zeigen, so, daß für alle $M \in \mathcal{EM}_\Gamma$ und $w \in (\Gamma\backslash\{\#\})^*$ eine geschlossene Formel $\mathbf{F}_{M,w} \in Fo_{T^{((M))}}$ so existiert, daß

$$\begin{aligned}
\mathbf{F}_{M,w} \in Thm_{T^{((M))}} \iff\ & w \in (\Sigma(M))^* \ \&\ \ M \text{ akzeptiert } w \ \& \\
& \& \ Min\text{-}RZ_M(w) < f(|w|)\,; && (3.54)\\
\left|\mathbf{F}_{M,w}\right| \leq\ & e(\left|\langle M\rangle_{\Gamma,Symb}\right|) + d\cdot|w|\ ; && (3.55)\\
g(\langle M\rangle_{\Gamma,Symb} \circ w) =\ & \mathbf{F}_{M,w} && (3.56)
\end{aligned}$$

gelten.

Hierfür wird im folgenden die äußere Gestalt der Konstruktion von g vermittels

$$g\colon (\Gamma\backslash\{\#\})^* \to \Sigma^*_{T^{((M))}} \tag{3.57}$$

$$x \mapsto g(x) := \begin{cases}
\epsilon & \ldots \text{ falls } x \neq \langle M\rangle_{\Gamma,Symb} \circ w \\
& \quad \text{für alle } M \in \mathcal{EM}_\Gamma,\ w \in (\Gamma\backslash\{\#\})^* \\
1 = 0 & \ldots \text{ falls } x = \langle M\rangle_{\Gamma,Symb} \circ w \\
& \quad \text{und } w \notin (\Sigma(M))^* \text{ für} \\
& \quad \text{und } M \in \mathcal{EM}_\Gamma,\ w \in (\Gamma\backslash\{\#\})^* \\
\mathbf{F}_{M,w} & \ldots \text{ sonst (d.h. falls } x = \langle M\rangle_{\Gamma,Symb} \circ w \\
& \quad \text{und } w \in (\Sigma(M))^* \text{ für} \\
& \quad \text{und } M \in \mathcal{EM}_\Gamma,\ w \in (\Gamma\backslash\{\#\})^*)
\end{cases}$$

bezüglich noch zu konstruierender Formeln $\mathbf{F}_{M,w} \in Fo_{T^{((M))}}$ (für $M \in \mathcal{EM}_\Gamma$, und $w \in (\Sigma(M))^*$) grundlegend sein. Ausgehend von so einer Setzung und (nach der genauen Beschreibung der Formeln $\mathbf{F}_{M,w}$ im letzten Fall:) Definition von g werden danach $d \in \mathbb{R}$, $d > 0$ und $e\colon \mathbb{N}_0 \to \mathbb{N}_0$ wie oben angegeben werden können.

Es soll schon an dieser Stelle bemerkt werden, daß die in der Definition von g nötige Fallunterscheidung in deterministischer polynomialer Rechenzeit von $\mathcal{EM}_\Gamma$-Maschinen durchgeführt werden kann und daß dies dann also auch auf die Berechnung von g in den ersten beiden Alternativen in der Definition von g zutrifft. Dies folgt zuerst aus Lemma 3.3.3, wonach die Kodes $x = \langle M\rangle_{\Gamma,Symb}$ von $\mathcal{EM}_\Gamma$-Maschinen M in $DTime_{\mathcal{EM}_\Gamma}(POL)$ liegen (hier gilt ja nach Annahme $\Gamma \cup \Sigma_{\text{code}} = \Gamma$), und dann daraus, daß ausgehend von $\langle M\rangle_{\Gamma,Symb} \circ w$ ($M \in \mathcal{EM}_\Gamma$, $w \in (\Gamma\setminus\{\#\})^*$) natürlich auch in deterministischer polynomialer Rechenzeit von einer $\mathcal{EM}_\Gamma$-Maschine festgestellt werden kann, ob $w \in (\Sigma(M))^*$ gilt (: durch Vergleich der einzelnen Symbole von w mit dem in $\langle M\rangle_{\Gamma,Symb}$ ja als Liste enthaltenen Eingabealphabet $\Sigma(M)$ von M).

Die für die letztgültige Definition von g notwendigen Formeln $\mathbf{F}_{M,w} \in Fo_{T^{((M))}}$ müssen für alle $M \in \mathcal{EM}_\Gamma$ und $w \in (\Sigma(M))^*$ wegen (3.54) nun jedenfalls so definiert werden, daß gilt:

$$\mathbf{F}_{M,w} \in Thm_{T^{((M))}} \iff M \text{ akzeptiert } w \ \&\ Min\text{-}RZ_M(w) < f(|w|) \tag{3.58}$$

Die rechte Seite in (3.58) kann nun aber mit der Aussage von Lemma 3.4.5 in Beziehung gebracht werden, die Anwendung von Lemma 3.4.5 führt dabei dann auf eine Charakterisierung der rechten Seite von (3.58), die dann zur Konstruktion von $\mathbf{F}_{M,w}$ mit Hilfe der hier vorausgesetzten Hilfsformeln in T dienen kann.

Für beliebiges $M \in \mathcal{EM}_\Gamma$ und $w \in (\Sigma(M))^*$ mit Zustandsmenge $Q = \{q_1, \ldots, q_k\}$ ($k \in \mathbb{N}$) und den Bezeichnungen $\Gamma = \{S_0, S_1, \ldots, S_m\}$, $m := |\Gamma| - 1$ mit $S_i := Symb(i)$ ($0 \le i \le m$) folgt nämlich aus Lemma 3.4.5:

$$\begin{aligned} &M \text{ akzeptiert } w \,\&\, Min\text{-}RZ_M(w) < f(|w|) \iff \\ &\quad\iff \big(\exists U \in \{0,1,\ldots,k+1\}^{(f(n))^2}\ \exists V \in \{0,1\}^{(f(n))^2}\ \exists W \in \{0,1,\ldots,m\}^{(f(n))^2}\big) \\ &\qquad \big(\forall i \in \{0,1,\ldots,(f(n))^2 - 1\}\big) \\ &\qquad\quad \big(\text{es gelten die an } U,V,W,i,w \text{ gerichteten} \\ &\qquad\quad \text{Bedingungen (B1), } \ldots \text{,(B9) (wie in Lemma 3.4.5 angegeben)}\big) \end{aligned} \tag{3.59}$$

Da sich die in der Annahme vorausgesetzten Formeln $\mathbf{S}_n(x,y)$ und $\mathbf{H}_w(x)$ aber auf die Beschreibung von *Binärwörtern* der Länge $(f(n))^2$ beziehen, müssen, damit diese Hilfsformeln in Beziehung zu (3.58) und mit (3.57) zur Konstruktion von $\mathbf{F}_{M,w}$ verwendet werden können, die in (3.59) erscheinenden

Wörter $U \in \{0,1,\ldots,k+1\}^{(f(n))^2}$ und $W \in \{0,1,\ldots,m\}^{(f(n))^2}$ in Binärwörter $U'_1,\ldots,U'_p \in \{0,1\}^{(f(n))^2}$ und $W'_1,\ldots,W'_q \in \{0,1\}^{(f(n))^2}$ mit $p := \lfloor \log_2(k+1) \rfloor + 1$ und $q := \lfloor \log_2 m + 1 \rfloor + 1$ und z.B. mit

$$\begin{aligned} U(i) &= U'_1(i) + U'_2(i)\,2^1 + \ldots + U'_p(i)\,2^{p-1}\,, \\ W(i) &= W'_1(i) + W'_2(i)\,2^1 + \ldots + W'_q(i)\,2^{q-1}\,, \\ &\qquad (i \in \mathbb{N}_0,\ 0 \le i < (f(n))^2) \end{aligned} \tag{3.60}$$

geteilt werden. Zur Konstruktion von $\mathbf{F}_{M,w} \in Fo_T$ für $M \in \mathcal{EM}_\Gamma$ und $w \in (\Sigma(M))^*$ mit $Q = \{q_1,\ldots,q_k\}$ $(k \in \mathbb{N})$, $\Gamma = \{S_0,\ldots,S_m\}$, $m := |\Gamma| - 1$, $S_i := Symb(i)$ $(0 \le i < m)$ kann dann wegen (3.58), (3.57)

$$\begin{aligned} \mathbf{F}_{M,w} \in Thm_T \iff \big(\exists\, U'_1,\ldots,U'_p,V,W'_1,\ldots,W'_q &\in \{0,1\}^{(f(n))^2}\big) \\ \big(\ \text{für } U \in \{0,1,\ldots,k+1\}^{(f(n))^2},\ W \in \{0,1,\ldots,m\}^{(f(n))^2} & \\ \text{mit (3.60) und } V \text{ und alle } i \in \{0,1,\ldots,(f(n))^2-1\} & \\ \text{gelten die an } U,V,W,w,i \text{ gerichteten} & \\ \text{Bedingungen (B1), ... ,(B9).}\ \big) & \end{aligned} \tag{3.61}$$

mit $p := \lfloor \log_2(k+1) \rfloor + 1$ und $q := \lfloor \log_2 m + 1 \rfloor + 1$ dienen.

Seien dafür nun $M, w, Q, \Gamma, S_0, \ldots, S_m$ wie oben beliebig, aber vorerst fest gewählt. Seien $p := \lfloor \log_2(k+1) \rfloor + 1$, $q := \lfloor \log_2 m \rfloor + 1$.

Die Berechtigtheit einer nun nötigen Übertragung der rechten Seite in (3.61) zu einer Formel $\mathbf{F}_{M,w}$, die die Gültigkeit dieser Ausage in T via der Beziehung (3.61) ausdrückt, beruht nun auf Überlegungen wie etwa der folgenden Art (die gesamte Übertragung kann wegen ihres Umfangs hier nämlich nicht im einzelnen gerechtfertigt werden):

Aus den angenommenen Eigenschaften von $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$ und $\mathbf{S}_n(x,y)$ folgt unmittelbar

$$\begin{aligned} \vdash_T\ & \mathbf{L}_n(x)\ \&\ \mathbf{I}_n(y)\ \&\ \neg\,\mathbf{S}_n(x,y) \\ & \leftrightarrow [\![\, x,y \in \mathbb{N}_0,\ x < 2^{(f(n))^2},\ y < (f(n))^2,\ Bw_1(a)(y) = 0 \,]\!] \end{aligned} \tag{3.62}$$

Seien nun $\tilde{m} \in \mathbb{N}$, $i_1,\ldots,i_{\tilde{m}} \in \{0,1,\ldots,(f(n))^2-1\}$ und $a_1,\ldots,a_{\tilde{m}} \in \{0,1\}$ beliebig, aber fest gewählt. Weiters seien für $n \in \mathbb{N}_0$ und $a \in \{0,1\}$ Formeln $\mathbf{T}_{a,n}(x,y)$ durch

$$\mathbf{T}_{a,n}(x,y) ::= \begin{cases} \mathbf{S}_n(x,y) & \ldots\ a = 1 \\ \neg\,\mathbf{S}_n(x,y) & \ldots\ a = 0 \end{cases} \tag{3.63}$$

definiert. Aus (3.62) folgt nun mit der vorausgesetzten inhaltlichen Eigenschaft von $\mathbf{S}_n(x,y)$ (durch Induktion)

$$\begin{aligned}\vdash_T \mathbf{L}_n(x) \;\&\; \mathop{\&}_{j=1}^{\tilde{m}} \mathbf{T}_{a_j,n}(x,\underline{\underline{i_j}}) \\ \leftrightarrow \left[\!\!\left[x \in \mathbb{N}_0,\, x < 2^{(f(n))^2}, (Bw_1(x))(i_j) = a_j \;(j \in \mathbb{N},\, 1 \le j \le m) \right]\!\!\right],\end{aligned} \tag{3.64}$$

woraus weiter

$$\begin{aligned}\vdash_T \; \exists x \left(\mathbf{L}_n(x) \;\&\; \mathop{\&}_{j=1}^{\tilde{m}} \mathbf{T}_{a_j,n}(x,\underline{\underline{i_j}}) \right) \iff \\ \iff \left(\exists X \in \{0,1\}^{(f(n))^2} \right) \\ \left(X(i_j) = a_j \;\; (\text{für alle } j \in \mathbb{N},\, j \in \{1,\ldots,m\}) \right),\end{aligned} \tag{3.65}$$

(3.65) kann nun aber so verstanden werden, daß dadurch die Existenz eines Binärwortes $X \in \{0,1\}^{(f(n))^2}$, das bestimmten Bedingungen genügt (nämlich den einfachen Aussagen $X(i_j) = a_j$ für alle $j \in \{1,\ldots,\tilde{m}\}$) mit der Ableitbarkeit einer bestimmten Formel in T verknüpft worden ist. (Ähnliche Aussagen wie (3.65) können auch unter der Beteiligung einer Formel $\mathbf{H}_w(x)$, die die ersten $f(n)$ der von x beschriebenen Symbole als $w\,0^{f(n)-|w|}$ festsetzt, gezeigt werden (wobei $n = |w|$)).

In weit komplizierterem Ausmaß ist eine solche Verknüpfung im Hinblick auf (3.61) die Grundlage der folgenden vorläufigen Festlegung $\mathbf{F}^*_{M,w}$ in (3.66) von $\mathbf{F}_{M,w}$ (und kann ausführlich prinzipiell ganz ähnlich gezeigt und eingesehen werden). Vorläufig erfolgt die Definition von $\mathbf{F}_{M,w}$ in $\mathbf{F}^*_{M,w}$ deshalb, weil $\mathbf{F}^*_{M,w}$ der Längenbedingung (ii) in Satz 3.4.1 noch nicht genügt, ein solcher Zwischenschritt aber notwendig ist, um den Beweis—halbwegs—nachvollziehbar zu gestalten.

$$\begin{aligned}\mathbf{F}^*_{M,w} ::= \\ \exists x_1 \ldots \exists x_p \, \exists y \, \exists z_1 \ldots \exists z_q \\ \forall x \left(\mathbf{L}_n(x_1) \;\&\; \ldots \;\&\; \mathbf{L}_n(x_p) \;\&\; \mathbf{L}_n(y) \;\&\; \mathbf{L}_n(z_1) \;\&\; \ldots \mathbf{L}_n(z_q) \right) \\ \&\; \forall y' \forall z' \left(\mathbf{I}_n(y') \;\&\; \mathbf{J}_n(z') \to \mathbf{E}^*_{(\mathrm{B1})} \;\&\; \mathbf{E}^*_{(\mathrm{B2})} \;\&\; \ldots \;\&\; \mathbf{E}^*_{(\mathrm{B9})} \right)\end{aligned} \tag{3.66}$$

wobei (mit später erklärten Hilfsformeln) gilt:

$$\begin{aligned}\mathbf{E}^*_{(\mathrm{B1})} ::= \mathbf{H}_{10^{n-1}}(x_1) \;\&\; \mathbf{H}_{0^n}(x_2) \;\&\; \ldots \;\&\; \mathbf{H}_{0^n}(x_p) \\ \mathbf{H}_{10^{n-1}}(y) \\ \mathbf{H}_{w_1}(z_1) \;\&\; \mathbf{H}_{w_2}(z_2) \;\&\; \ldots \;\&\; \mathbf{H}_{w_q}(z_p)\,,\end{aligned}$$

wobei $w_1, \dots, w_q \in \{0,1\}^n$ so, daß

$$w_j(i) := Bw_1(w(i))(j-1) \qquad (i \in \mathbb{N}_0,\ 0 \le i < q,\ 1 \le j \le q)\,;$$

es gilt dann für alle $i \in \mathbb{N}_0,\ 0 \le i < q$

$$w(i) = w_1(i) + w_2(i) \cdot 2^1 + \ldots + w_q(i) \cdot 2^{q-1}\,;$$

$$\mathbf{E}^*_{(\mathrm{B2})} ::= \mathbf{I}_n(y'+z') \,\&\, \mathbf{U}^*_{0,p,n}(x_1, \dots, x_p, y') \to \mathbf{WE}^*_{q,n}(z_1, \dots, z_q, y', y'+z')\,;$$

$$\mathbf{E}^*_{(\mathrm{B3})} ::= \mathbf{I}_n(y'+z') \to \big(\mathbf{S}_n(y,y') \leftrightarrow \mathbf{S}_n(y, y'+z')\big)\,;$$

$$\mathbf{E}^*_{(\mathrm{B4})} ::= \mathbf{I}_n(y'+z'+1)$$

$$\to \mathop{\&}_{\substack{i_1 \in \{1,\dots,k-1\} \\ l_1 \in \{0,\dots,m\}}} \big[\, \mathbf{U}^*_{i,p,n}(x_1, \dots, x_p, y') \,\&\, \mathbf{W}^*_{l_1,q,n}(z_1, \dots, z_q, y') \to \mathbf{B^*}_{i_1,l_1,p,q,n}(x_1, \dots, x_p, z_1, \dots, z_q, y', z')\,\big]\,,$$

wobei $\mathbf{B^*}_{i_1,l_1,p,q,n}(\dots)$ wie in Formel 3.4.2 ;

$$\mathbf{E}^*_{(\mathrm{B5})} ::= \mathbf{I}_n(y'+z') \to \mathbf{S}_n(y, y'+1) \to \mathbf{U}^*_{0,p,n}(x_1, \dots, x_p, y')\,;$$

$$\mathbf{E}^*_{(\mathrm{B6})} ::= \exists z'' \big(\mathbf{I}_n(z'') \,\&\, z''+1 = z' \,\&\, \mathbf{I}_n(y'+z'')\big) \,\&\, \mathbf{S}_n(y,y')$$
$$\to \exists z_0 \big[\, \mathbf{SJ}_n(z_0) \,\&\, \neg\, \mathbf{U}^*_{0,p,n}(x_1, \dots, x_p, y'+z_0)$$
$$\&\, \forall z'' \big(\mathbf{SJ}_n(z'') \,\&\, \neg\, z'' = z_0 \to \mathbf{U}^*_{0,p,n}(x_1, \dots, x_p, y'+z'')\big)\,\big]\,,$$

wobei die Formeln $\mathbf{SJ}_n(z)$ die Eigenschaft

$$\vdash_T \mathbf{SJ}_n(z) \leftrightarrow [\![\, z \in \mathbb{N}_0,\ z < f(n)\,]\!]$$

besitzen und wie folgt definiert sind:

$$\mathbf{SJ}_n(z) ::= \exists z' \exists z''' \big(\mathbf{J}_n(z') \,\&\, \mathbf{I}_n(z) \,\&\, \mathbf{I}_n(z''') \,\&\, z + z''' + 1 = z'\big)$$

$$\mathbf{E}^*_{(\mathrm{B7})} ::= \mathbf{I}_n(y'+z') \to \mathbf{U}^*_{k,p,n}(x_1, \dots, x_p, y')$$
$$\to \mathbf{U}^*_{k,p,n}(x_1, \dots, x_p, y'+z') \,\&\, \mathbf{WE}^*_{q,n}(z_1, \dots, z_q, y', y'+z')\,;$$

$$\mathbf{E}^*_{(\mathrm{B8})} ::= \mathbf{I}_n(y'+z') \to \mathbf{U}^*_{k+1,p,n}(x_1, \dots, x_p, y')$$
$$\to \mathbf{U}^*_{k+1,p,n}(x_1, \dots, x_p, y'+z') \,\&\, \mathbf{WE}^*_{q,n}(z_1, \dots, z_q, y', y'+z')\,;$$

$$\mathbf{E}^*_{(\mathrm{B9})} ::= \exists y'' \big(\mathbf{I}_n(y'') \,\&\, \mathbf{U}^*_{k,p,n}(x_1, \dots, x_p, y'')\big)\,.$$

Die in $\mathbf{E}^*_{(\mathrm{B1})}, \dots, \mathbf{E}^*_{(\mathrm{B9})}$ (für feste $p, q, n \in \mathbb{N}$ und bestimmte $i \in \mathbb{N}_0$) auftretenden Formeln $\mathbf{U}^*_{i,p,n}(\dots)$, $\mathbf{W}^*_{i,q,n}(\dots)$, $\mathbf{WE}^*_{q,n}(\dots)$ seien für allgemeine Parameter $i, n \in \mathbb{N}_0,\ p, q \in \mathbb{N}$

Formel 3.4.2 Die Formel $\mathbf{B^*}_{i_1,l_1,p,q,n}(x_1,\dots,x_p,z_1,\dots,z_q,y',z')$:

$$
\begin{aligned}
&\mathbf{B^*}_{i_1,l_1,p,q,n}(x_1,\dots,x_p,z_1,\dots,z_q,y',z') ::= \\
&\begin{cases}
\mathbf{U}^*_{k+1,p,n}(x_1,\dots,x_p,y'+z') \;\&\; \mathbf{WE}^*_{q,n}(z_1,\dots,z_q,y',y'+z') \\
\qquad\qquad \dots\dots\dots\; \delta(q_{i_1},S_{l_1}) = \emptyset \\
\big[\,\mathbf{S}_n(y,y') \to \mathbf{U}^*_{k+1,p,n}(x_1,\dots,x_p,y'+z') \;\&\; \mathbf{WE}^*_{q,n}(z_1,\dots,z_q,y',y'+z')\,\big] \;\& \\
\;\&\; \Big[\,\neg\,\mathbf{S}_n(y,y') \to \bigvee_{(q_{i_2},S_{l_2},L)\in\delta(q_{i_1},S_{l_1})} \big(\,\mathbf{W}^*_{l_2,q,n}(z_1,\dots,z_q,y'+z') \;\& \\
\qquad\qquad\qquad\qquad \&\; \exists y''\big(\,y''+1 = y'+z' \;\&\; \mathbf{U}^*_{i_2,p,n}(x_1,\dots,x_p,y'')\,\big)\,\Big] \\
\qquad\qquad \dots\dots\dots\; \delta(q_{i_1},S_{l_1}) \neq \emptyset \;\&\; \text{es gibt kein } (q_{i_2},S_{l_2},R) \in \delta(q_{i_1},S_{l_1}) \\
\Big[\bigvee_{(q_{i_2},S_{l_2},R)\in\delta(q_{i_1},S_{l_1})} \mathbf{U}^*_{i_2,p,n}(x_1,\dots,x_p,y'+z'+1) \;\&\; \mathbf{W}^*_{l_2,q,n}(z_1,\dots,z_q,y'+z')\Big] \;\& \\
\;\&\; \Big[\bigvee_{(q_{i_2},S_{l_2},L)\in\delta(q_{i_1},S_{l_1})} \neg\,\mathbf{S}_n(y,y') \;\&\; \exists y''\,\big(\,y''+1 = y'+z' \;\&\; \mathbf{U}^*_{i_2,p,n}(x_1,\dots,x_p,y'')\,\big) \;\& \\
\qquad\qquad\qquad \&\; \mathbf{W}^*_{l_2,q,n}(z_1,\dots,z_q,y'+z')\,\Big] \\
\qquad\qquad \dots\dots\dots\; \text{sonst}
\end{cases}
\end{aligned}
$$

dabei so definiert:

$$\mathbf{U}^*_{i,p,n}(x_1,\ldots,x_p,y') ::= \mathop{\&}_{j=1}^{p} \mathbf{T}_{(Bw_1(i))(j-1),n}(x_j,y)$$

(für $i,n \in \mathbb{N}_0$, $p \in \mathbb{N}$,
und wobei $\mathbf{T}_{a,n}(x,y)$ $(a \in \{0,1\},\ n \in \mathbb{N})$ wie in (3.63)) ;

$$\mathbf{W}^*_{i,q,n}(z_1,\ldots,z_q,y') ::= \mathbf{U}^*_{i,q,n}(z_1,\ldots,z_q,y')$$

(für $i,n \in \mathbb{N}_0$, $q \in \mathbb{N}$) ;

$$\mathbf{WE}^*_{q,n}(z_1,\ldots,z_q,y',y'') ::= \mathop{\&}_{i=1}^{q} \big(\mathbf{S}_n(z_i,y') \leftrightarrow \mathbf{S}_n(z_i,y'')\big)$$

(für $n \in \mathbb{N}_0$, $q \in \mathbb{N}$) .

Eine zu $M \in \mathcal{EM}_\Gamma$ und $w \in (\Sigma(M))^*$ so definierte Formel $\mathbf{F}^*_{M,w}$ kann aber die Längenbedingung (3.56) nicht erfüllen, denn es gilt jedenfalls:

$$\begin{aligned}\big|\mathbf{F}^*_{M,w}\big| &> \big|\mathbf{E}^*_{(\mathrm{B4})}\big| \\ &> (k-1)\cdot m\cdot\big(\big|\mathbf{U}^*_{\cdot,p,n}(x_1,\ldots,x_p,y')\big| + \big|\mathbf{W}^*_{\cdot,q,n}(z_1,\ldots,z_p,y')\big|\big) \\ &\geq (k-1)\cdot m\cdot\big(p\cdot\big|\mathbf{S}_n(x,y)\big| + q\cdot\big|\mathbf{S}_n(x,y)\big|\big) \\ &> (k-1)\cdot m\cdot p\cdot\big|\mathbf{S}_n(x,y)\big| = (k-1)\cdot m\cdot p\cdot c_4\cdot n\end{aligned} \tag{3.67}$$

Hierin hängen nun aber sowohl k als auch p von $\big|\langle M\rangle_{\Gamma,Symb}\big|$ ab (k ist die Anzahl der Zustände von M, $p = \lfloor \log_2(k+1)\rfloor + 1)$ und nur $n = |w|$ von w, sodaß dadurch eine Abschätzung von $\big|\mathbf{F}_{M,w}\big|$ nach oben vermittels einer getrennten Summe von zwei Anteilen, die nur von $\big|\langle M\rangle_{\Gamma,Symb}\big|$ bzw. von $|w|$ abhängen, unmöglich wird[39].

Ähnliches gilt sogar auch in Beziehung zu (z.B.) $\mathbf{E}^*_{(\mathrm{B2})}$, nämlich:

$$\begin{aligned}\big|\mathbf{F}^*_{M,w}\big| &> \big|\mathbf{E}^*_{(\mathrm{B2})}\big| > \big|\mathbf{U}^*_{0,p,n}(x_1,\ldots,x_p,y')\big| \\ &\geq p\cdot\big|\mathbf{S}_n(x,y)\big|\end{aligned} \tag{3.68}$$

und p hängt erneut von $\big|\langle M\rangle_{\Gamma,Symb}\big|$ ab (zwar nur sehr schwach, es gilt jedenfalls $p \leq \lfloor \log_2(\, g_{10}(\,\big|\langle M\rangle_{\Gamma,Symb}\big|\,) + 1)\rfloor + 1$ mit $g_{10}(n)$ wie in Definition 3.3.6 erklärt; es gilt jedoch $g_{10}(n) \leq n$ für alle $n \in \mathbb{N}$).

[39] Das könnte unter der zusätzlichen Annahme $(n \mapsto |\mathbf{S}_n(x,y)|) \in \Theta(n)$ (die zwar über die in der Annahmebedingung (ii) von Satz 3.4.4 an $\{\mathbf{S}_n(x,y)\}_{n\in\mathbb{N}_0}$ enthaltene Forderung $(n \mapsto |\mathbf{S}_n(x,y)|) \in O(n)$ hinausgeht, im Kontext der Komplexitätsbeweise hier für die in den einzelnen Theorien entwickelten Formeln $\mathbf{S}_n(x,y)$ aber zutrifft) exakt bewiesen werden.

Genau dieses Längenproblem tritt aber *eigentlich* auch schon in [FiR74] auf (dort bei der Formulierung von E_γ, vgl. p. 13), wird dort aber nicht weiter behandelt: Die dort für $\mathbf{U}^*_{0,p,n}(x_1, \ldots, x_p, y)$ verwendete Formel

$$\neg\, \mathbf{S}_n(x_1, y)\ \&\ \ldots\ \&\ \neg\, \mathbf{S}_n(x_p, y) \tag{3.69}$$

gestattet sicherlich *nicht* den Nachweis der in der Voraussetzung von Theorem 6 in [FiR74] geforderten Längenbedingung (b) von der Form

$$\left|\mathbf{F}^*_{M,w}\right| \leq d \cdot \left(\left|\langle M\rangle\right| + |w|\right) \qquad \text{(für alle } M,\ w) \tag{3.70}$$

für ein $d \in \mathbb{R}$, $d > 0$ [leichte Anpassung dieser Bedingung an die hier verwendeten Symbole von mir, C.G.]; im Beweis nötige Formeln der Gestalt (3.69) sind auch der Grund, warum eine Längenbedingung der Form (3.70) sehr wahrscheinlich—dort wie auch hier—nicht erzielt werden kann. Denn es ist zwar eine Verkürzung von (3.69) zu

$$\forall x \left(x = x_1 \vee \ldots \vee x = x_p \rightarrow \neg\, \mathbf{S}_n(x, y)\right), \tag{3.71}$$

möglich, also zu einer Formel, deren Länge durch eine Summe von getrennten Anteilen bestimmt ist, die von p (und also von $\left|\langle M\rangle_{\Gamma,Symb}\right|$) bzw. von n (und also von $|w|$) abhängen (das Wachstumsverhalten der Länge von (3.71) liegt in $O(n) + \Theta(p \log_{10} p)$). Zur Formulierung von E_δ im Beweis von Theorem 7 in [FiR74] bzw. von (B4) hier aus Lemma 3.4.5 ist es aber nötig, zu jedem Kodezeichen in $\langle M\rangle_{\Gamma,Symb}$, das einer Zustandsnummer angehört, eine der Variablen $x_1, \ldots, x_p$ in $\mathbf{F}_{M,w}$ zu verwenden. Deshalb kann das Wachstumsverhalten von $\mathbf{F}_{M,w}$ bezüglich der hier verwendeten Konstruktion dieser Formel wohl nur etwa durch $O(\left|\langle M\rangle_{\Gamma,Symb}\right| \log p) + O(|w|)$ (p hängt wie oben beschrieben von M und $\left|\langle M\rangle_{\Gamma,Symb}\right|$ ab) begrenzt werden.

Aus diesem Grund kann die Formel $\mathbf{F}_{M,w}$ entlang der hier verwendeten (dem Beweis von Theorem 7 in [FiR74] folgenden) Vorgehensweise [wohl, C.G.] nur so gewählt werden daß dafür eine Abschätzung von etwa der Qualität

$$\begin{aligned}\left|\mathbf{F}^*_{M,w}\right| \leq d \cdot \Big(\left|\langle M\rangle_{\Gamma,Symb}\right| \cdot \log\log g_{10}(\left|\langle M\rangle_{\Gamma,Symb}\right|)\ +\ |w|\Big)\\ \text{(für alle } M \in \mathcal{EM}_\Gamma,\ w \in (\Sigma(M))^* \subseteq (\Gamma\setminus\{\#\})^*)\end{aligned} \tag{3.72}$$

möglich wird (k läßt sich nämlich durch $g_{10}(\left|\langle M\rangle_{\Gamma,Symb}\right|)$ und davon ausgehend p durch $\lfloor \log_2(g_{10}(\left|\langle M\rangle_{\Gamma,Symb}\right|) + 1)\rfloor + 1$ abschätzen).

Im folgenden wird die schon definierte Formel $\mathbf{F}^*_{M,w}$ so zu einer Formel $\mathbf{F}_{M,w}$ übertragen werden, daß dafür eine Längenabschätzung der Gestalt (3.72) erzielbar ist. Dabei werden in der Hauptsache logische Umformungsmöglichkeiten zur verkürzten Schreibweise von Formeln—wie zwischen (3.69) und (3.71) verwendet—benützt; damit können v.a. die in $\mathbf{E}^*_{(B1)}$, ... ,$\mathbf{E}^*_{(B9)}$ auftretenden Teilformeln $\mathbf{U}^*_{i,p,n}(\ldots)$, $\mathbf{W}^*_{i,q,n}(\ldots)$ und $\mathbf{WE}^*_{q,n}(\ldots)$ in

entsprechend kürzere Formeln $\mathbf{U}_{i,p,n}(\dots)$, $\mathbf{W}_{i,q,n}(\dots)$ und $\mathbf{WE}_{q,n}(\dots)$ überführt werden. Lediglich die Übertragung von $\mathbf{E}^{*}_{(\mathrm{B4})}$ zur Teilformel $\mathbf{E}_{(\mathrm{B4})}$ von $\mathbf{F}_{M,w}$ erfordert eine (um einiges) kompliziertere Übertragung.

$\mathbf{F}_{M,w}$ sei nun insgesamt folgendermaßen definiert:

$$
\begin{aligned}
&\mathbf{F}_{M,w} ::= \\
&\quad \exists x_1 \dots \exists x_p \, \exists y \, \exists z_1 \dots \exists z_q \\
&\qquad \forall x \left(x = x_1 \vee \dots \vee x = x_p \vee x = y \vee x = z_1 \vee \dots \vee x = z_q \to \mathbf{L}_n(x) \right) \\
&\qquad \& \, \forall y' \forall z' \left[\exists x \left(x = y' \,\&\, \mathbf{I}_n(x) \right) \,\&\, \exists x \left(x = z' \,\&\, \mathbf{J}_n(x) \right) \right. \\
&\qquad\qquad \left. \to \mathbf{E}_{(\mathrm{B1})} \,\&\, \mathbf{E}_{(\mathrm{B2})} \,\&\, \dots \mathbf{E}_{(\mathrm{B9})} \right]
\end{aligned}
\tag{3.73}
$$

wobei

$$
\begin{aligned}
\mathbf{E}_{(\mathrm{B1})} ::= \; & \exists x \left(x = x_1 \,\&\, \mathbf{H}_{10^{n-1}}(x) \right) \\
& \& \, \forall x \left(x = x_2 \vee \dots \vee x = x_p \to \mathbf{H}_{0^n}(x) \right) \\
& \& \, \exists x \left(x = y \,\&\, \mathbf{H}_{10^{n-1}}(x) \right) \\
& \& \, \exists x \left(x = z_1 \,\&\, \mathbf{H}_{w_1}(x) \right) \,\&\, \dots \,\&\, \exists x \left(x = z_q \,\&\, \mathbf{H}_{w_q}(x) \right)
\end{aligned}
$$

wobei $w_1, \dots, w_q \in \{0,1\}^n$ so, daß

$$w(i) = w_1(i) + w_2(i) \cdot 2^1 + \dots + w_q(i) \cdot 2^{q-1} ;$$

für $i \in \mathbb{N}_0$, $0 \le i < q$; das führt auf die Setzungen

$$w_j(i) := B w_1(w(i))(j-1) \qquad (i \in \mathbb{N}_0,\ 0 \le i < q,\ 1 \le j \le q) ;$$

$$
\begin{aligned}
\mathbf{E}_{(\mathrm{B2})} ::= \; & \exists x \, (\, x = y' + z' \,\&\, \mathbf{I}_n(x) \,) \,\&\, \mathbf{U}_{0,p,n}(x_1, \dots, x_p, y') \\
& \longrightarrow \mathbf{WE}_{q,n}(z_1, \dots, z_q, y', y' + z') ;
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{E}_{(\mathrm{B3})} ::= \; & \exists x \, (\, x = y' + z' \,\&\, \mathbf{I}_n(x) \,) \\
& \to \exists x \left[\, x = y \right. \\
& \qquad \left. \& \, \left(\exists y \, (\, y = y' \,\&\, \mathbf{S}_n(x,y) \,) \right) \leftrightarrow \left(\exists y \, (\, y = y' + z' \,\&\, \mathbf{S}_n(x,y) \,) \right) \right] ;
\end{aligned}
$$

$\mathbf{E}_{(\mathrm{B4})}$: vgl. Formel 3.4.3 ;

$$
\begin{aligned}
\mathbf{E}_{(\mathrm{B5})} ::= \; & \exists x \, (\, x = y' + z' \,\&\, \mathbf{I}_n(x) \,) \\
& \longrightarrow \exists x \left(x = y \,\&\, \exists y \, (\, y = y' \,\&\, \mathbf{S}_n(x,y) \,) \right) \to \mathbf{U}_{0,p,n}(x_1, \dots, x_p, y') ;
\end{aligned}
$$

$$\begin{aligned}
\mathbf{E}_{(\mathrm{B6})} ::= \;& \exists z''\,\big(\,\exists x\,(\,x = z'' \;\&\; \mathbf{I}_n(x)\,)\;\&\; z''+1 = z'\;\&\;\exists x\,(\,x = z''\;\&\;\mathbf{I}_n(x)\,)\,\big)\\
& \&\;\exists x\,\big(x = y\;\&\;\exists y\,(\,y = y'\;\&\;\mathbf{S}_n(x,y)\,)\,\big)\\
& \longrightarrow \exists z_0\,\big[\,\mathbf{SJ}'_n(z_0)\;\&\;\neg\,\mathbf{U}_{0,p,n}(x_1,\ldots,x_p,y'+z_0)\\
& \qquad \&\;\forall z''\,\big(\mathbf{SJ}'_n(z'')\;\&\;\neg\,z'' = z_0\\
& \qquad\qquad \rightarrow \mathbf{U}_{0,p,n}(x_1,\ldots,x_p,y'+z'')\,\big)\,\big]
\end{aligned}$$

$$\begin{aligned}
\text{wobei } \mathbf{SJ}'_n(z) ::= \;& \exists z'\,\exists z'''\\
& \big(\,\exists x\,(\,x = z'\;\&\;\mathbf{J}_n(x)\,)\;\&\;\exists x\,(\,x = z\;\&\;\mathbf{I}_n(x)\,)\\
& \;\&\;\exists x\,(\,x = z'''\;\&\;\mathbf{I}_n(x)\,)\;\&\; z + z''' + 1 = z'\,\big)
\end{aligned}$$

$$\begin{aligned}
\mathbf{E}_{(\mathrm{B7})} ::= \;& \exists x\,\big(x = y'+z'\;\&\;\mathbf{I}_n(x)\big)\;\&\;\mathbf{U}_{k,p,n}(x_1,\ldots,x_p,y')\\
& \longrightarrow \mathbf{U}_{k,p}(x_1,\ldots,x_p,y'+z')\;\&\;\mathbf{WE}_{q,n}(x_1,\ldots,x_p,y'')\,;
\end{aligned}$$

$$\begin{aligned}
\mathbf{E}_{(\mathrm{B8})} ::= \;& \exists x\,\big(x = y'+z'\;\&\;\mathbf{I}_n(x)\big)\;\&\;\mathbf{U}_{k+1,p,n}(x_1,\ldots,x_p,y')\\
& \longrightarrow \mathbf{U}_{k+1,p}(x_1,\ldots,x_p,y'+z')\;\&\;\mathbf{WE}_{q,n}(x_1,\ldots,x_p,y'')\,;
\end{aligned}$$

$$\mathbf{E}_{(\mathrm{B9})} ::= \exists y''\,\big(\,\exists x\,(\,x = y''\;\&\;\mathbf{I}_n(x)\,)\;\&\;\mathbf{U}_{k,p,n}(x_1,\ldots,x_p,y'')\,\big)\,;$$

Die in $\mathbf{E}_{(\mathrm{B1})}, \ldots, \mathbf{E}_{(\mathrm{B9})}$ (für feste $p, q, n \in \mathbb{N}$ und bestimmte $i \in \mathbb{N}_0$ in der obigen Formulierung von $\mathbf{F}_{M,w}$ auftretenden Formeln $\mathbf{U}_{i,p,n}(\ldots)$, $\mathbf{W}_{i,q,n}(\ldots)$ und $\mathbf{WE}_{q,n}$ (diese werden im folgenden als verkürzt geschriebene, den Formeln $\mathbf{U}^*_{i,p,n}(\ldots)$, $\mathbf{W}^*_{i,q,n}(\ldots)$ und $\mathbf{WE}^*_{q,n}(\ldots)$ äquivalente Entsprechungen definiert werden) und $\mathbf{A}_{i,p}(\ldots)$, $\mathbf{UB}_{p,n}(\ldots)$ sowie $\mathbf{WB}_{q,n}(\ldots)$ seien für allgemeine Parameter $i, n \in \mathbb{N}_0$, $p, q \in \mathbb{N}$ dabei nun so definiert:

$$\begin{aligned}
& \mathbf{U}_{i,p,n}(x_1,\ldots,x_p,y') ::=\\
& \quad \forall x\,\forall w\,\big[\,x = x_1\;\&\; w = \underline{\underline{Bw_1(i)(0)}}\;\vee\; x = x_p\;\&\; w = \underline{\underline{Bw_1(i)(p-1)}}\\
& \qquad\qquad \rightarrow \exists y\,\big(\,y = y'\;\&\;\mathbf{S}_n(x,y) \leftrightarrow w = 1\,\big)\,\big]
\end{aligned}$$

(für $i, n \in \mathbb{N}_0$, $p \in \mathbb{N}$);

$$\mathbf{W}_{i,q,n}(z_1,\ldots,z_q,y') ::= \mathbf{U}_{i,p,n}(x_1,\ldots,x_p,y')$$

(für $i, n \in \mathbb{N}_0$, $q \in \mathbb{N}$);

$$\begin{aligned}
& \mathbf{WE}_{q,n}(z_1,\ldots,z_q,y',y'') ::=\\
& \quad \forall z\,\big\{\,z = z_1 \vee \ldots \vee z = z_q\\
& \qquad \rightarrow \exists x\,\big[\,x = z\\
& \qquad\qquad \&\;\big(\,\exists y\,(\,y = y'\;\&\;\mathbf{S}_n(x,y)\,) \leftrightarrow \exists y\,(\,y = y''\;\&\;\mathbf{S}_n(x,y)\,)\,\big)\,\big]\,\big\}
\end{aligned}$$

(für $n \in \mathbb{N}_0$, $q \in \mathbb{N}$);

Formel 3.4.3 Die Formel $\mathbf{E}_{(\mathrm{B4})}$:

$$
\begin{aligned}
\mathbf{E}_{(\mathrm{B4})} ::= {} & \exists x \left(x = y' + z' + 1 \;\&\; \mathbf{I}_n(x) \right) \\
& \rightarrow \forall w_1^{(U)} \ldots w_p^{(U)}\, w_1^{(W)} \ldots w_q^{(W)} \\
& \quad \Big\{ \Big[\bigvee_{\substack{i_1 \in \{1,\ldots,k-1\} \\ l_1 \in \{0,\ldots,m\}}} \left(\mathbf{A}_{i_1,p}(w_1^{(U)}, \ldots, w_p^{(U)}) \;\&\; \mathbf{A}_{l_1,q}(w_1^{(U)}, \ldots, w_q^{(U)}) \right) \\
& \qquad \&\; \mathbf{UB}_{p,n}(x_1, \ldots, x_p, w_1^{(U)}, \ldots, w_p^{(U)}, y') \\
& \qquad \&\; \mathbf{WB}_{q,n}(z_1, \ldots, z_p, w_1^{(U)}, \ldots, w_q^{(U)}, y') \Big] \\
& \quad \rightarrow \exists w_1^{(U)\prime} \ldots \exists w_p^{(U)\prime}\, \exists w_1^{(W)\prime} \ldots \exists w_q^{(W)\prime}\, \exists y''\, \exists w \\
& \qquad \Big[\Big((w = 0 \vee w = 1) \\
& \qquad\quad \&\; \left\{ w = 1 \leftrightarrow \exists x \left[x = y \;\&\; \exists y \left(y = y' \;\&\; \mathbf{S}_n(x, y) \right) \right] \right\} \Big) \\
& \qquad\quad \&\; \bigvee_{\substack{i_1 \in \{1,\ldots,k-1\} \\ l_1 \in \{0,\ldots,m\}}} \left(\mathbf{A}_{i_1,p}(w_1^{(U)}, \ldots, w_p^{(U)}) \;\&\; \mathbf{A}_{l_1,q}(w_1^{(U)}, \ldots, w_q^{(U)}) \right. \\
& \qquad\qquad\qquad \left. \&\; \mathbf{B}_{i_1,l_1,p,q}(w_1^{(W)}, \ldots\ldots, w_q^{(W)\prime}, y', z'', y'', w) \right) \\
& \qquad\quad \&\; \mathbf{UB}_{q,n}(x_1, \ldots, x_p, w_1^{(U)\prime}, \ldots, w_p^{(U)\prime}, y'') \\
& \qquad\quad \&\; \mathbf{WB}_{q,n}(z_1, \ldots, z_p, w_1^{(W)\prime}, \ldots, w_q^{(W)\prime}, y' + z') \Big] \Big\}
\end{aligned}
$$

wobei die Formel

$$
\begin{aligned}
& \mathbf{B}_{i_1,l_1,p,q}(w_1^{(W)}, \ldots, w_q^{(W)}, \\
& \qquad w_1^{(U)\prime}, \ldots, w_p^{(U)\prime}, w_1^{(W)\prime}, \ldots, w_q^{(W)\prime}, y', z'', y'', w)
\end{aligned}
$$

wie in Formel 3.4.4 definiert ist.

Formel 3.4.4 Die Formel
$\mathbf{B}_{i_1,l_1,p,q}(w_1^{(W)},\ldots,w_q^{(W)},w_1^{(U)\prime},\ldots,w_p^{(U)\prime},w_1^{(W)\prime},\ldots,w_q^{(W)\prime},y',z'',y'',w)$:

$$\mathbf{B}_{i_1,l_1,p,q}(w_1^{(W)},\ldots,w_q^{(W)},w_1^{(U)\prime},\ldots,w_p^{(U)\prime},w_1^{(W)\prime},\ldots,w_p^{(W)\prime},y',z'',y'',w) ::=$$

$$\begin{cases}
y'' = y' + z' \;\&\; \mathbf{A}_{k+1,p}(w_1^{(U)\prime},\ldots,w_p^{(U)\prime}) \;\&\; w_1^{(W)\prime} = w_1^{(W)} \;\&\; \ldots \;\&\; w_p^{(W)\prime} = w_p^{(W)} \\
\qquad\qquad \ldots\ldots\ldots\ \delta(q_{i_1},S_{l_1}) = \emptyset) \\
\big[\, w = 1 \to y'' = y' + z' \;\&\; \mathbf{A}_{k+1,p}(w_1^{(U)\prime},\ldots,w_p^{(U)\prime}) \\
\qquad\quad \&\; w_1^{(W)\prime} = w_1^{(W)} \;\&\; \ldots \;\&\; w_p^{(W)\prime} = w_p^{(W)} \,\big] \\
\&\; \big[\, w = 0 \to y'' + 1 = y' + z' \\
\qquad\quad \&\; \bigvee_{(q_{i_2},S_{l_2},L)\in\delta(q_{i_1},S_{l_1})} \big(\mathbf{A}_{i_2,p}(w_1^{(U)\prime},\ldots,w_p^{(U)\prime}) \;\&\; \mathbf{A}_{l_2,q}(w_1^{(W)\prime},\ldots,w_q^{(W)\prime})\big) \,\big] \\
\qquad\qquad \ldots\ldots\ldots\ \delta(q_{i_1},S_{l_1}) \neq \emptyset \;\&\; \text{es gibt kein } (q_{i_2},S_{l_2},R) \in \delta(q_{i_1},S_{l_1}) \\
\big[\, y'' = y' + z' + 1 \;\&\; \bigvee_{(q_{i_2},S_{l_2},R)\in\delta(q_{i_1},S_{l_1})} \big(\mathbf{A}_{i_2,p}(w_1^{(U)\prime},\ldots,w_p^{(U)\prime}) \;\&\; \mathbf{A}_{l_2,q}(w_1^{(W)\prime},\ldots,w_q^{(W)\prime})\big) \,\big] \\
\vee \big[\, y'' + 1 = y' + z' \;\&\; w = 0 \\
\quad \&\; \bigvee_{(q_{i_2},S_{l_2},L)\in\delta(q_{i_1},S_{l_1})} \big(\mathbf{A}_{i_2,p}(w_1^{(U)\prime},\ldots,w_p^{(U)\prime}) \;\&\; \mathbf{A}_{l_2,q}(w_1^{(W)\prime},\ldots,w_q^{(W)\prime})\big) \,\big] \\
\qquad\qquad \ldots\ldots\ldots\ \text{sonst}
\end{cases}$$

$$\mathbf{A}_{i,p}(x_1,\ldots,x_p) ::= \; x_1 = \underline{\underline{Bw_1(i)(0)}} \;\&\; \ldots \;\&\; x_p = \underline{\underline{Bw_1(i)(p-1)}}$$

(für $i,n \in \mathbb{N}_0$, $p \in \mathbb{N}$);

$$\mathbf{UB}_{p,n}(x_1,\ldots,x_p,w_1,\ldots,w_p,y') ::=$$
$$\forall w \left(w = w_1 \vee \ldots \vee w = w_p \rightarrow w = 0 \vee w = 1 \right)$$
$$\& \; \forall x \forall w \left[x = x_1 \;\&\; w = w_1 \vee \ldots \vee x = x_p \;\&\; w = w_p \right.$$
$$\left. \rightarrow \left(\exists y \left(y = y' \;\&\; \mathbf{S}_n(x,y) \right) \leftrightarrow w = 1 \right) \right]$$

(für $p \in \mathbb{N}$, $n \in \mathbb{N}_0$);

$$\mathbf{WB}_{q,n}(z_1,\ldots,z_q,w_1,\ldots,w_q,y') ::= \; \mathbf{UB}_{q,n}(z_1,\ldots,z_q,w_1,\ldots,w_q,y')$$

(für $q \in \mathbb{N}$, $n \in \mathbb{N}_0$).

Es läßt sich leicht einsehen, daß

$$\vdash_T \mathbf{U}_{i,p,n}(x_1,\ldots,x_p,y') \leftrightarrow \mathbf{U}^*_{i,p,n}(x_1,\ldots,x_p,y')$$

und (Analoges für $\mathbf{W}_{i,q,n}$ und $\mathbf{W}^*_{i,q,n}$:)

$$\vdash_T \mathbf{WE}_{q,n}(z_1,\ldots,z_q,y',y'') \leftrightarrow \mathbf{WE}^*_{q,n}(z_1,\ldots,z_q,y',y'')$$

(für alle $i,n \in \mathbb{N}_0$, $p,q \in \mathbb{N}$) gelten, diese Formeln also jeweils in T äquivalent sind, daß jedoch von $\mathbf{U}^*_{i,p,n}(\ldots)$ zu $\mathbf{U}_{i,p,n}(\ldots)$ und von $\mathbf{WE}^*_{q,n}(\ldots)$ zu $\mathbf{WE}_{q,n}(\ldots)$ insofern eine „Verkürzung“ stattgefunden hat, als in $\mathbf{U}_{i,p,n}(\ldots)$ die Formel $\mathbf{S}_n(x,y)$ nur mehr einmal und in $\mathbf{WE}_{q,n}(\ldots)$ nur mehr zweimal vorkommt, $\mathbf{S}_n(x,y)$ in $\mathbf{U}^*_{i,p,n}(\ldots)$ aber p-mal und in $\mathbf{WE}^*_{q,n}(\ldots)$ $2q$-mal vorgekommen ist[40]. Insbesondere gilt

$$\left|\mathbf{U}_{i,p,n}(x_1,\ldots,x_p,y')\right| = 7p + 13 + |\mathbf{S}_n(x,y)| + |x_1| + \ldots + |x_p| + \left|y'\right| \;,$$

hingegen

$$\left|\mathbf{U}^*_{i,p,n}(x_1,\ldots,x_p,y')\right| \geq p \cdot |\mathbf{S}_n(x,y)| + p - 1 \;.$$

Es muß an dieser Stelle darauf hingewiesen werden, daß die Formulierung von $\mathbf{F}_{M,w}$ hier noch nicht direkt in einer fixierten informatisch-sinnvollen Formelsyntax erfolgt ist, wenngleich aber augenscheinlich ist, welche geringfügigen Änderungen z.B. bezüglich der für die Theorien der Presburger Arithmetik gegebenen LR(1)-Formelsprache in

[40] Im Fall von $\mathbf{W}^*_{i,q,n}(\ldots)$ und $\mathbf{WE}^*_{q,n}(\ldots)$ ist die Durchführung einer Verkürzung im Beweis hier eigentlich unnötig, geschieht aber aus Symmetriegründen trotzdem.

Grammatik 2.6.1 notwendig wären: (1) Die Formel muß in pränexe Schreibweise umgebaut werden, (2) die Indizierung der Variablen ist genau festzulegen, insbesondere müssen die hier (der Lesbarkeit wegen und um die Beziehung zum Beweis von Theorem 7 in [FiR74]—so gut es geht—aufrechtzuerhalten) benutzten einzelnen unär indizierten Variablen durch dezimal indizierte Variable ersetzt werden und $x_1, \ldots, x_p$ müssen als Zeichenketten $x_{(1)_{10}}, \ldots, x_{(p)_{10}}$ (mit dezimaler subscript-Indizierung), $z_1, \ldots, z_q$, $w_1^{(U)}, \ldots, w_p^{(U)}$, $w_1^{(U)\prime}, \ldots, w_p^{(U)\prime}$, $w_1^{(W)}, \ldots, w_q^{(W)}$, $w_1^{(W)\prime}, \ldots, w_q^{(W)\prime}$ beispielsweise als $z_{(1)_{10}}, \ldots, z_{(q)_{10}}$, $w_{(2q+1)_{10}}, \ldots, w_{(2q+p)_{10}}$, $w_{(2q+p+1)_{10}}, \ldots, w_{(2q+2p)_{10}}$, $w_{(1)_{10}}, \ldots, w_{(q)_{10}}$, $w_{(q+1)_{10}}, \ldots, w_{(2q)_{10}}$ (jeweils also mit zur Variablen als Wort symbolweise beitragender dezimaler subscript-Indizierung).

Es ist nun direkt überprüfbar, daß in $\mathbf{F}_{M,w}$ die Formel $\mathbf{I}_n(x)$ nur mehr genau 14-mal, $\mathbf{J}_n(x)$ 3-mal, $\mathbf{L}_n(x)$ einmal, $\mathbf{S}_n(x,y)$ 22-mal und eine Formel $\mathbf{H}_{\tilde{w}}(x)$ (für jeweils ein $\tilde{w} \in \{0,1\}^*$, $|\tilde{w}| = |w| = n$) genau $3+q$-mal vorkommt und daß der übrige Teil von $\mathbf{F}_{M,w}$ in seiner Länge von $n = |w|$ nicht mehr abhängt, sondern nur von q ($q = \lfloor \log_2 m + 1 \rfloor + 1$, $m = |\Gamma| - 1$, Γ ist nach Annahme fest), von k (Anzahl der Zustände von M), von p ($p = \lfloor \log_2(k+1) \rfloor + 1$) und von der konkreten Wahl der in $\mathbf{F}_{M,w}$ vorkommenden Variablen (und alle diese Größen sind von $n = |w|$ unabhängig und auch die Freiheit in der Variablenwahl hat nichts mit n zu tun). Genau läßt sich durch Abzählen[41] einsehen[42]:

$$\begin{aligned}|\mathbf{F}_{M,w}| \leq\ & 14\,\left|\mathbf{I}_n(x)^{((M))}\right| + 3\,\left|\mathbf{J}_n(x)^{((M))}\right| + \left|\mathbf{L}_n(x)^{((M))}\right| + 22\,\left|\mathbf{S}_n(x,y)^{((M))}\right| + \\ & + (3+q)\,\left|\mathbf{H}_w(x)^{((M))}\right| + \\ & + 90\,p + 46\,q + 630 + \\ & + 13\,(\,|x_1| + \ldots + |x_p|\,) + 7\,(\,|z_1| + \ldots + |z_p|\,) + \\ & + 3\,(\,\left|w_1^{(U)}\right| + \ldots + \left|w_p^{(U)}\right|\,) + 3\,(\,\left|w_1^{(W)}\right| + \ldots + \left|w_q^{(W)}\right|\,)\end{aligned}$$

[41] [*Geringfügiges* Mich-Verzählt-Haben kann ich nicht ganz zu 100 % ausschließen (though I've tried hard), C.G.]

[42] Die Längen von unär indizierten Variablen wurden jeweils symbolweise gezählt, z.B. $|x'''| = 3$; weiters wurde dabei von der in pränexer Schreibweise angeschriebenen Formel $\mathbf{F}_{M,w}$ ausgegangen, logische Symbole $\forall$, $\leftrightarrow$, & wurden—entsprechend z.B. der Formelgrammatik Grammatik 2.6.1 in Kapitel 2 für *PreAN*—als einfache Symbole gezählt und wurden nicht wie in [Shoe67] als definierte Symbole aufgefaßt (sodaß diese weiter eliminiert werden müßten und $\mathbf{F}_{M,w}$ nur mit den logischen Symbolen $\exists$, $\vee$ und $\neg$ aufgebaut würde). – Es sollte hier jedoch ausdrücklich bemerkt und angefügt werden (und kann an der hier festgelegten Gestalt von $\mathbf{F}_{M,w}$ leicht überprüft werden), daß die Verwendung einer solchen, etwas erweiterten logischen Syntax für Formeln aus Theorien 1. Ordnung für die Durchführung dieses Beweises keineswegs wesentlich ist. Wenn nämlich—wie in den Abschnitten 5, 6 und 7 dargestellt—die in der Annahme dieses Satzes vorausgesetzten Formeln $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$, $\mathbf{L}_n(x)$, $\mathbf{S}_n(x,y)$ und $\mathbf{H}_w(x)$ in den jeweils behandelten Theorien immer so konstruiert werden können, daß sie der zusätzlichen Bedingung genügen, nur $\exists$, $\vee$ und $\neg$ (neben $=$ wie in [Shoe67]) als logische Symbole zu enthalten, so kann (durch die einfache logische Ersetzung der Symbole $\rightarrow$, &, $\leftrightarrow$ in $\mathbf{F}_{M,w}$ wie hier definiert) eine entsprechende Formel $\mathbf{F}'_{M,w}$ mit den hier gewünschten Eigenschaften gefunden werden, die ebenfalls dieser weiteren Bedingung genügt, d.h. die ebenfalls nur mit den logischen Symbolen $\exists$, $\vee$ und $\neg$ (neben natürlich $=$) aufgebaut ist.

$$
\begin{aligned}
&+ 3\,(\,|w_1^{(U)\prime}| + \ldots + |w_p^{(U)\prime}|\,) + 3\,(\,|w_1^{(W)\prime}| + \ldots + |w_q^{(W)\prime}|\,) \\
&+ k\,(m+1)\,\big[\,9\,p + 11\,q + 31 + \\
&\qquad + 2\,(\,|w_1^{(U)}| + \ldots + |w_p^{(U)}|\,) + 3\,(\,|w_1^{(W)}| + \ldots + |w_q^{(W)}|\,) + \\
&\qquad + (\,|w_1^{(U)\prime}| + \ldots + |w_p^{(U)\prime}|\,) + 2\,(\,|w_1^{(W)\prime}| + \ldots + |w_q^{(W)\prime}|\,)\,\big] + \\
&+ \sum_{\substack{i_2 \in \{1,\ldots,k\},\ \text{wobei} \\ (q_{i_2}, S_{l_2}, M) \in \delta(q_{i_1}, S_{l_1}) \\ \text{für } i_1 \in \{1,\ldots,k-1\},\ l_1 \in \{0,\ldots,m\}, \\ l_2 \in \{0,\ldots,m\},\ M \in \{L,R\}.}} \Big|\mathbf{A}_{i_2,p}(w_1^{(U)\prime}, \ldots, w_p^{(U)\prime})\Big| \qquad (3.74)
\end{aligned}
$$

Der letzte Summand in (3.74) läßt sich (jedenfalls) durch

$$|\langle M\rangle_{\Gamma,Symb}| \cdot (\,3\,p - 1 + |w_1^{(U)\prime}| + \ldots + |w_p^{(U)\prime}|\,) \qquad (3.75)$$

abschätzen, ist aber zusammen mit einem Ausdruck der Gestalt $k \cdot (\,|w_1^{(U)\prime}| + \ldots + |w_p^{(U)\prime}|\,)$ (vgl. im vorletzten Summanden) die wesentliche Ursache dafür, daß $\mathbf{F}_{M,w}$ nicht auch von $|\langle M\rangle_{\Gamma,Symb}|$ (wie von $|w|$) linear abhängt (sondern leicht super-linear von $|\langle M\rangle_{\Gamma,Symb}|$ abhängt (und damit der Beweis von Theorem 6 in [FiR74] nicht weitgehend direkt übernommen werden konnte).

Die Variablen $x_1, \ldots, x_p$, $z_1, \ldots, z_q$, $w_1^{(U)\prime}, \ldots, w_p^{(U)\prime}$, $w_1^{(W)}, \ldots, w_q^{(W)}$ und $w_1^{(W)\prime}, \ldots, w_q^{(W)\prime}$ können auf früher angedeutete Weise jedenfalls so gewählt werden, daß von $n = |w|$ und $\langle M\rangle_{\Gamma,Symb}$ unabhängige, fixe Zahlen $C, D \in \mathbb{N}$ so existieren, daß

$$
\begin{aligned}
|x_1| + \ldots + |x_p| &\leq C\,p\,\log p\,, \\
|w_1^{(U)}| + \ldots + |w_p^{(U)}| &\leq C\,p\,\log p\,, \\
|w_1^{(U)\prime}| + \ldots + |w_p^{(U)\prime}| &\leq C\,p\,\log p
\end{aligned}
$$

(die Möglichkeit, C so wählen zu können, beruht v.a. auf der Aussage von Lemma 3.3.7, (ii)) und

$$|z_1| + \ldots + |z_q|\,,\ |w_1^{(W)}| + \ldots + |w_q^{(W)}|\,,\ |w_1^{(W)\prime}| + \ldots + |w_q^{(W)\prime}| \leq D$$

gelten (die Wahl von D hängt natürlich von q ab, da jedoch $q = \lfloor \log_2 |\Gamma| \rfloor + 1$ und Γ im Beweis fest gewählt wurde, kann D fest und unabhängig von $n = |w|$ und $|\langle M\rangle_{\Gamma,Symb}|$ angenommen werden). (Durch nähere Analyse der verwendeten Strategie bei der konkreten Festlegung der Variablen könnten C und D natürlich auch ganz konkret gefunden werden. Im Beweis hier ist dabei zuerst aber nur die Möglichkeit nötig, daß Zahlen C und D mit diesen Eigenschaften gefunden werden *können*.)

Davon ausgehend kann nun $|\mathbf{F}_{M,w}|$ unter Aufspaltung der von $n = |w|$ und von $\big|\langle M\rangle_{\Gamma,Symb}\big|$ abhängigen Längenanteile der Formel $\mathbf{F}_{M,w}$ durch

$$\begin{aligned}|\mathbf{F}_{M,w}| \leq \big\{\, & 90\,p + 46\,q + 630 \\ & + 19 + C\,p\,\log p + 16\,D \\ & + k\,(m+1)\,(9\,p + 11\,q + 31 + 3\,C\,p\,\log p + 5\,D \\ & + \big|\langle M\rangle_{\Gamma,Symb}\big|\,(3\,p - 1 + C\,\log p)\,\big\} \\ & + \big\{\, 14\,c_1 + 3\,c_2 + c_3 + 22\,c_4 + (3+q)\,c_5\,n\,\big\}\end{aligned} \tag{3.76}$$

abgeschätzt werden ($c_1, \ldots, c_5 \in \mathbb{N}$ sind dabei die am Anfang des Beweises angenommenen, für die Abschätzungen der Längen von $\mathbf{I}_n(x)^{((M))}, \ldots, \mathbf{H}_w(x)^{((M))}$ in (3.53) maßgeblichen Konstanten).

Hieraus ergibt sich aber nun direkt eine Längenabschätzung der Gestalt (3.55) und zwar mit

$$d := 14\,c_1 + 32\,c_2 + c_3 + 22\,c_4 + (3+q)\,c_5$$

(wobei $c_1, \ldots, c_5$ wie in (3.53)) und (da sich k durch $g_{10}(\big|\langle M\rangle_{\Gamma,Symb}\big|$ und $p := \lfloor \log_2(k+1)\rfloor + 1$ davon ausgehend durch $\log_2(g_{10}(\big|\langle M\rangle_{\Gamma,Symb}\big| + 1) + 1$ abschätzen läßt) einer Funktion $e\colon \mathbb{N}_0 \to \mathbb{N}$ mit

$$\begin{aligned}e(i) := & \, 90\,\tilde{p}(i) + q + 649 \\ & + C\,p\,\log \tilde{p}(i) + 16\,D \\ & + \tilde{k}(i)\,(m+1)\,(\,9\,\tilde{p}(i) + 11\,q + 31 + 3\,C\,\tilde{p}(i)\,log\,\tilde{p}(i)\, + 5\,D\,) \\ & + l\,(\,3\,\tilde{p}(i) - 1 + 3\,C\,\tilde{p}(i)\,log\,\tilde{p}(i)\,)\end{aligned}$$

wobei

$$\begin{aligned}\tilde{p}(i) &:= \log_2(g_{10}(i) + 1) + 1 && (i \in \mathbb{N}_0)\,, \\ \tilde{k}(i) &:= g_{10}(i) && (i \in \mathbb{N}_0)\,, \\ m &= |\Gamma| - 1 && (\text{wie früher festgelegt})\,, \\ q &= \lfloor \log_2(m+1) + 1\rfloor && (\text{wie früher festgelegt})\,.\end{aligned}$$

Es ist leicht einzusehen, daß gilt

$$e(l) \in O(\,l\,\log g_{10}(l)\,\log\log g_{10}(l)\,) \subsetneqq O(\,l\,\log l\,\log\log l\,)\,,$$

daß also $e(l)$ nur ganz leicht super-linear wächst.

Der Bedingung (3.54) ist durch die wie oben erfolgte (inhaltlich motivierte und entwickelte) Festlegung von $\mathbf{F}_{M,w}$ entsprochen worden.

Die Bedingung (3.56), also die Existenz einer die Formeln $\mathbf{F}_{M,w}$ für alle $M \in \mathcal{EM}_\Gamma$ und $w \in (\Gamma \setminus \{\#\})^*$ herstellenden Funktion $g \in DFTime_{\mathcal{EM}_\Gamma}(POL)$ kann ausführlich über den hier dargestellten Aufbau der Formeln $\mathbf{F}_{M,w}$ gerechtfertigt werden, wobei als nötige Teilkonstruktionen die vorausgesetzten Funktionen $g_1, \ldots, g_5 \in DFTime_{\mathcal{EM}_\Gamma}(POL)$ eingehen, die Herstellungsprozesse für $\mathbf{I}_n(x)$, ... , $\mathbf{H}_w(x)$ beschreiben.

Der einzige Schritt im Aufbau der Formeln $\mathbf{F}_{M,w}$, der hier noch einer näheren Überprüfung bedarf, ist die Konstruktion der Teilformeln $\mathbf{E}_{(\mathrm{B4})}$ (ausgehend von $\langle M \rangle_{\Gamma,Symb}$ und w), wobei nämlich explizit auf den Maschinenkode $\langle M \rangle_{\Gamma,Symb}$ von M zurückgegriffen werden muß. Die Durchführbarkeit der Konstruktion von $\mathbf{E}_{(\mathrm{B4})}$ durch eine $\mathcal{EM}_\Gamma$-Turingmaschine in polynomialer Rechenzeit kann aber prinzipiell sehr ähnlich wie in der Beweisskizze zu Lemma 3.3.3 dargestellt erfolgen und unterbleibt hier, da ein solcher Nachweis analog zu dort wirklich sehr naheliegt, auch aus Umfangsgründen.

Insgesamt kann dadurch der Beweis dieses Satzes aber als geglückt angesehen werden. □

Es soll an dieser Stelle darauf hingewiesen werden, daß unter den Voraussetzungen und Annahmen von Satz 3.4.4 die Annahmen von Satz 3.4.3 eigentlich einfacher als (wie hier bewiesen) diejenigen von Satz 3.4.1 nachgewiesen werden könnten bzw. [von mir hier, C.G.] nachgewiesen hätten werden können. Die in Satz 3.4.3 geforderte, schwächere Längenbedingung (ii) in dessen Annahme würde es nämlich in einem sehr analog zu oben zu führenden Beweis möglich machen, schon bei den hier konstruierten Formeln $\mathbf{F}^*_{M,w}$ Halt zu machen und diese nicht noch—wie hier—weiter (bzgl. der Wachstumsordnung dieser Länge) verkürzen zu müssen, um eine Abschätzung der Länge von $\mathbf{F}_{M,w}$ durch eine Summe getrennter, von $\left|\langle M \rangle_{\Gamma,Symb}\right|$ bzw. von $|w|$ abhängiger Anteile zu erreichen. – Da [FiR74] ihre Komplexitätsbeweise jedoch auf eine Satz 3.4.1 vergleichbare Aussage (nämlich auf Theorem 6, p. 7, in [FiR74]) gestützt haben, wollte hier deutlich gemacht werden, welcher Beweisweg und -umfang zur Präzisierung des in [FiR74] nur angedeuteten Beweises (allem Anschein nach) wahrscheinlich unumgänglich ist.

Allerdings hat dieser etwas längere Beweisweg auch die Vorteile, (1) daß sich der Beweis nicht (wie jener von Satz 3.4.3) auf eine hier nicht bewiesene Aussage über Zeithierarchien für nichtdeterministische Turingmaschinen stützen muß und daß sich der Nachweis der in [FiR74] erzielten Komplexitätsaussagen hier deshalb zur Gänze überschauen läßt, sowie, (2) daß daran wirklich konstruktiv nachvollzogen werden kann, wie für jede hier in Frage kommende Theorie $T^{((M))}$ und eine hier vorausgesetzte Funktion $f\colon \mathbb{N}_0 \to \mathbb{N}$ mit $f(n) := 2^n$ oder $f(n) := 2^{2^n}$ wenigstens zu jeder $\mathcal{EM}_\Gamma$-Turingmaschine M_E, die $Thm_{T^{((M))}}$ oder $\mathrm{co}-Thm_{T^{((M))}}$ akzeptiert, *tatsächlich effektiv* immer Theoreme $\mathbf{F} \in Thm_{T^{((M))}}$ gefunden werden können, so, daß $Min-RZ_{M_E}(\mathbf{F}) > f(c\,|\mathbf{F}|)$ gilt.

Diese Konstruktivität bzw. Effektivität der vorgestellten Beweise ist eine bemerkenswerte Eigenschaft, die zur wissenschaftlichen Qualität und—zum Zeitpunkt der Veröffentlichung—Neuheit und auch Neuartigkeit der erzielten Aussagen in der Arbeit [FiR74]

noch in wesentlichem Ausmaß hinzukommt.

Für den im Abschnitt 7 zu erbringenden Nachweis einer doppelt-exponentiell-linearen unteren Schranke bzgl. nichtdeterministischer Turing-Rechenzeit auch für die Theorie TAZ bzw. für $Th(\langle\mathbb{Z};0,1,+\rangle)$ ist folgende Variante von Satz 3.4.4 nötig. Dies v.a. deshalb, weil dabei eine andere Kodierungsfunktion für Binärwörter verwendet wird, nämlich die Funktion Bw_2 aus (3.42), für die bezüglich $x \in \mathbb{Z}$ und $y \in \mathbb{N}_0$ die Aussage $(Bw_2(x))(y) = 1$ genau dann gilt, falls $x \neq 0$ und p_{y+1} (die $(y+1)$-t-kleinste Primzahl) x teilt. Diese Funktion läßt sich nicht ganz genauso durch Formeln $\mathbf{I}_n(x)$, ... ,$\mathbf{H}_w(x)$ beschreiben wie Bw_1. Es gilt aber:

Satz 3.4.6. *Sei $f(n) := 2^{2^n}$* [43]*. T sei gleich TAZ oder $Th(\langle\mathbb{Z};0,1,+\rangle)$, $T^{((M))}$ eine informatisch-sinnvolle Formelsyntax für T, Bw_2 sei wie in (3.42); $\mathfrak{Z}$ sei das Modell $\langle\mathbb{Z};0,1,+\rangle$ von T.*

Angenommen, *es existieren für alle $n \in \mathbb{N}_0$ Formeln $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$, $\mathbf{S}_n(x,y)$ und für alle $w \in BW0$ Formeln $\mathbf{H}_w(x)$ in T so, daß die beiden Bedingungen (i) und (ii) gelten, wobei:*

(i) Für alle $n \in \mathbb{N}_0$ und $w \in BW0$ mit $|w| = n$ gilt:

$$\vdash_T \mathbf{I}_n(x) \leftrightarrow [\![\, x \in \mathbb{N}_0,\ x < (f(n))^2 \,]\!] \ ;$$
$$\vdash_T \mathbf{J}_n(x) \leftrightarrow x = \underline{\underline{f(n)}} \ ;$$

Für alle $a \in \mathbb{Z}$ ist die Formel

$$\mathbf{S}_n(\mathbf{i}_a, y) \leftrightarrow \Big[\!\!\Big[\, y \in \mathbb{N}_0,\ y < (f(n))^2,\ (Bw_2(a))(y) = 1 \,\Big]\!\!\Big]$$

in $\mathfrak{Z}$ gültig ;

Für alle $a \in \mathbb{Z}$ gilt:

$$\mathbf{H}_w(\mathbf{i}_a) \text{ ist gültig in } \mathfrak{Z} \iff$$
$$\iff (Bw_2(a))(0) \circ \ldots \circ (Bw_2(a))(f(n)-1) = w \circ 0^{f(n)-n} \,.$$

(Wobei hierin $\mathbf{i}_a$ immer als „Name“ [44] *in $L(\mathfrak{Z})$ für das entsprechende „Individuum“* [44] *$a \in |\mathfrak{Z}| = \mathbb{Z}$ zu verstehen ist.)*

(ii) Die Familien $\{\mathbf{I}_n(x)\}_{n\in\mathbb{N}_0}$, $\{\mathbf{J}_n(x)\}_{n\in\mathbb{N}_0}$ und $\{\mathbf{S}_n(x,y)\}_{n\in\mathbb{N}_0}$ genügen den Längen- und Konstruierbarkeitsbedingungen (A), $\{\mathbf{H}_w(x)\}_{w\in BW0}$ den Bedingungen (B) aus Definition 3.3.5.

Dann gilt *für $f(n)$ und $T^{((M))}$ unter den weiteren Voraussetzungen von Satz 3.4.1 (an Γ, Σ_{code}, Symb und $\langle\cdot\rangle_{\Gamma,Symb}$) die Annahme von Satz 3.4.1.*

[43] Vgl. Fußnote 35 zu Satz 3.4.4.
[44] Vgl. diese Begriffsbildung in [Shoe67].

Beweis. Der Beweis dieses Satzes kann mit einer geringfügingen Änderung (die den Verzicht auf die hier nicht vorhandenen und nicht benötigten Formeln $\mathbf{L}_n(x)$ betrifft) so gut wie völlig analog zum Beweis von Satz 3.4.4 erfolgen.

Hierfür ist entscheidend, daß die Übertragung von an Binärwörter der Länge $(f(n))^2$ gerichteten Bedingungen zu äquivalenten, an Kodierungen dieser Binärwörter (via der Funktion Bw_2) in ganzen Zahlen mittels der hier vorausgesetzten Formeln gestellten Forderungen sehr ähnlich wie dort durchgeführt werden kann.

Sei zur Darstellung einer dazu erforderlichen vereinfachten Überlegung hier $n \in \mathbb{N}_0$ nun beliebig, vorerst dabei jedoch fest.

Aus den in der Annahme von Satz 3.4.6 enthaltenen Eigenschaften der Formeln $\mathbf{I}_n(x)$ und $\mathbf{S}_n(x,y)$ folgt zuerst eine (3.62) hier entsprechende Aussage, nämlich die Gültigkeit von

$$\mathbf{I}_n(y) \,\&\, \neg\, \mathbf{S}_n(\mathbf{i}_a, y) \leftrightarrow [\![\, y \in \mathbb{N}_0,\, y < (f(n))^2,\, Bw_2(a)(y) = 0 \,]\!]$$

für alle $a \in \mathbb{Z}$ im Modell $\mathfrak{Z}$ von TAZ. Daraus und aus der in der Annahme des Satzes geforderten inhaltlichen Kodierungseigenschaft von $\mathbf{S}_n(x,y)$ folgt weiters bezüglich den in (3.63) zu $\mathbf{S}_n(x,y)$ definierten Formeln $\mathbf{T}_{a,n}(x,y)$ (für $a \in \{0,1\}$) für alle $\tilde{m} \in \mathbb{N}$, $i_1, \ldots, i_{\tilde{m}} \in \{0,1,\ldots,(f(n))^2 - 1\}$ und $a_1, \ldots, a_{\tilde{m}} \in \{0,1\}$, sowie für alle $a \in \mathbb{Z}$

$$\begin{aligned} &\mathop{\&}_{j=1}^{\tilde{m}} \mathbf{T}_{a_j,n}(\mathbf{i}_a, \underline{\underline{i_j}}) \quad \text{ist gültig in } \mathfrak{Z} \iff \\ &\qquad \iff \quad Bw_2(a)(i_j) = a_j \quad (\text{für alle } j \in \mathbb{N},\, j \in \{1,\ldots,m\}), \end{aligned}$$

eine zu (3.64) analoge Aussage; hieraus folgt nun weiters

$$\begin{aligned} \vdash_T \; \exists x \Big(\mathop{\&}_{j=1}^{\tilde{m}} \mathbf{T}_{a_j,n}(x, \underline{\underline{i_j}}) \Big) \iff \\ \iff \big(\exists X \in \{0,1\}^{(f(n))^2} \big) \\ \big(X(i_j) = a_j \quad (\text{f.a. } j \in \mathbb{N},\, j \in \{1,\ldots,\tilde{m}\}) \big), \end{aligned} \tag{3.77}$$

eine (3.65) hier entsprechende Aussage. (3.77) kann nun erneut als eine Möglichkeit aufgefaßt werden, die Aussage der Existenz eines Binärwortes $X \in \{0,1\}^{(f(n))^2}$, das den (einfachen) Bedingungen $X(i_j) = a_j$ $(1 \le j \le \tilde{m})$ genügt, durch die dazu äquivalente Aussage der Beweisbarkeit der Formel $\exists x \Big(\mathop{\&}_{j=1}^{\tilde{m}} \mathbf{T}_{a_j,n}(x, \underline{\underline{i_j}}) \Big)$ in TAZ (bzw. deren Gültigkeit im Modell $\mathfrak{Z}$ von TAZ) zu ersetzen (wobei wie oben $\tilde{m} \in \mathbb{N}$, $i_1, \ldots, i_{\tilde{m}} \in$ $\in \{0,1,\ldots,(f(n))^2 - 1\}$ und $a_1, \ldots, a_{\tilde{m}} \in \{0,1\}$).

Nun kann auf prinzipiell wieder ganz ähnliche, allerdings weit umfangreichere Weise die Konstruktion der Formel $\mathbf{F}_{M,w}$ für $M \in \mathcal{EM}_\Gamma$ und $w \in (\Sigma(M))^*$, $|w| = n \in \mathbb{N}$ gerechtfertigt werden, so, daß dabei die Beweisbarkeit von $\mathbf{F}_{M,w}$ in TAZ entlang von (3.61) äquivalent zur Existenz von Binärwörtern $U'_1, \ldots, U'_p,\ V,\ W'_1, \ldots, W'_q \in \{0,1\}^{(f(n))^2}$ ist, die bzgl. U, W wie in (3.60) und w, sowie für alle $i \in \{0, 1, \ldots, (f(n))^2 - 1\}$ den Bedingungen (B1), ... ,(B9) von Lemma 3.4.5 genügen.

$\mathbf{F}_{M,w}$ kann dabei nun analog wie im Beweis von Satz 3.4.4 festgelegt werden, z.B. erneut schrittweise, zuerst durch die Definition von $\mathbf{F}^*_{M,w}$ analog zu (3.66) nun als die Formel

$$\begin{array}{l} \mathbf{F}^*_{M,w} ::= \\ \quad \exists x_1 \ldots \exists x_p\, \exists y\, \exists z_1 \ldots \exists z_q \\ \qquad \forall y' \forall z' \left(\mathbf{I}_n(y') \,\&\, \mathbf{J}_n(z') \rightarrow \mathbf{E}^*_{(\mathrm{B1})} \,\&\, \mathbf{E}^*_{(\mathrm{B2})} \,\&\, \ldots \,\&\, \mathbf{E}^*_{(\mathrm{B9})} \right), \end{array}$$

wobei als $\mathbf{E}^*_{(\mathrm{B1})}, \ldots, \mathbf{E}^*_{(\mathrm{B9})}$ genau dieselben Formeln wie die im Beweis von Satz 3.4.4 definierten verwendet werden können (darin kommen die Formeln $\mathbf{L}_n(x)$ nämlich nicht vor); und dann im (bezüglich der Längeneigenschaft dieser Formel:) Verfeinerungsschritt der zu (3.73) analogen Definition von $\mathbf{F}_{M,w}$ als Formel

$$\begin{array}{l} \mathbf{F}_{M,w} ::= \\ \quad \exists x_1 \ldots \exists x_p\, \exists y\, \exists z_1 \ldots \exists z_q \\ \qquad \,\&\, \forall y' \forall z' \left[\exists x \left(x = y' \,\&\, \mathbf{I}_n(x) \right) \,\&\, \exists x \left(x = z' \,\&\, \mathbf{J}_n(x) \right) \right. \\ \qquad\qquad \left. \rightarrow \mathbf{E}_{(\mathrm{B1})} \,\&\, \mathbf{E}_{(\mathrm{B2})} \,\&\, \ldots \mathbf{E}_{(\mathrm{B9})} \right], \end{array} \tag{3.78}$$

mit $\mathbf{E}_{(\mathrm{B1})}, \ldots, \mathbf{E}_{(\mathrm{B9})}$ ebenfalls wie im Beweis von Satz 3.4.4. (Hierbei mußten also jeweils nur die sich auf die Formeln $\mathbf{L}_n(x)$ bzw. auf deren Instanzen beziehenden Teilformeln weggelassen werden.)

Die übrigen Beweisteile können von früher direkt übernommen werden, wenn man davon absieht, daß in einer nun für $\mathbf{F}_{M,w}$ analog zu (3.74) zu erzielenden Längenabschätzung der sich auf das Auftreten der Teilformel

$$\forall x \left(x = x_1 \vee \ldots \vee x = x_p \vee x = y \vee x = z_1 \vee \ldots \vee x = z_q \rightarrow \mathbf{L}_n(x) \right)$$

in (3.74) und (3.76) beziehende Längenanteil in $\mathbf{F}_{M,w}$ nun wegfällt und die entlang von (3.78) hier festgelegte Formel $\mathbf{F}_{M,w}$ also jeweils sogar kürzer ist und eine Längenbedingung (3.55) danach dafür sogar eher erfüllt werden kann.

□

3.5 Beweis von Satz 3.1.3 (Spezieller Beweisteil in [FiR74] bei der Erzielung von $RA \notin NTime(2^{cn})$ für ein $c \in \mathbb{R}$, $c > 0$)

Sei T im folgenden die vollständige und entscheidbare Theorie 1. Ordnung (im Sinn von [Shoe67]) $RA = Th(\langle \mathbb{R}; 0, 1, + \rangle)$ oder eine dazu äquivalente axiomatisierte Theorie und L deren Sprache (also jene Sprache einer Theorie 1. Ordnung, die als Konstantensymbole 0 und 1 und als 2-stelliges Funktionssymbol das Symbol + und sonst keine weiteren nichtlogischen Symbole besitzt; = ist im Sinn von [Shoe67] ja immer Teil der Sprache und ein *logisches* Symbol). $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ die als System formaler Sprachen aufgefaßte Theorie T, wobei dieses hier z.B. mit dem Verweis auf G aus Grammatik 2.6.1 und deren Terminalalphabet Σ durch die Setzungen

$$\begin{aligned} &\Sigma_{T^{((M))}} := \Sigma \setminus \{ <, \leq, \equiv, \equiv^N, U_{IZN}, \textcircled{1}, \oplus, \otimes \} ; \\ &Fo_{T^{((M))}} := L(G) \mid \Sigma_{T^{((M))}} ; \\ &Thm_{T^{((M))}} := \{ \boldsymbol{\mathcal{A}} \in Fo_{T^{((M))}} / \vdash_T \mathbf{A}^{(\boldsymbol{\mathcal{A}})} \} ; \end{aligned} \tag{3.79}$$

präzis gemacht werden könnte[45]. ($T^{((M))}$, wie hier präzisiert, ist für beide Wahlmöglichkeiten von T wie oben dasselbe System, da diese beiden Theorien äquivalent sind.)

Um nun die von Satz 3.1.3 für die Entscheidungskomplexität von T behauptete exponentiell-lineare untere Schranke, d.h. allgemeiner sogar die Aussage

$$Thm_{T^{((M))}}, \text{co}-Thm_{T^{((M))}} \notin NTime(2^{cn}) \text{ (für ein } c \in \mathbb{R},\, c > 0) , \tag{3.80}$$

zu zeigen (die in der Überschrift dieses Abschnittes unpräzise zu $RA \notin NTime(2^{cn})$ für ein $c \in \mathbb{R}$, $c > 0$ verkürzt worden ist), kann nun so argumentiert werden: Wäre für $f(n) := 2^{cn}$ und T, $T^{((M))}$ wie hier vorausgesetzt und Bw_1 wie in (3.41) die Annahme von Satz 3.4.4 erfüllt, so würde aus der Folgerung dieses Satzes die Erfülltheit der Annahme von Satz 3.4.1 unter seinen Voraussetzungen folgen. Nun könnte deshalb aber auch Korollar 3.4.2 angewendet werden und es würde sich damit (3.80) als Folgerung ergeben.

Aus diesem Grund reduziert sich der an dieser Stelle noch nötige Beweis auf den Nachweis der Erfülltheit der Annahme von Satz 3.4.4 bezüglich $f(n) := 2^{cn}$ und T, $T^{((M))}$, also den konstruktiven Nachweis für die Existenz von Formeln $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$, $\mathbf{L}_n(x)$, $\mathbf{S}_n(x, y)$ (für alle $n \in \mathbb{N}_0$) und Formeln $\mathbf{H}_w(x)$ (für alle $w \in BW0$) von T mit den inhaltlichen Eigenschaften

$$\vdash_T \mathbf{I}_n(x) \leftrightarrow [\![x \in \mathbb{N}_0,\, x < 2^{2n}]\!] , \tag{3.81}$$

[45] Das Vorhandensein des Symbols $\leftrightarrow$ in $\Sigma_{T^{((M))}}$ hier ist für die erzielten Aussagen nicht unbedingt erforderlich.

$$\vdash_T \mathbf{J}_n(x) \leftrightarrow x = \underline{\underline{2^n}}^{\,46}\,, \tag{3.82}$$

$$\vdash_T \mathbf{L}_n(x) \leftrightarrow \left[\!\left[x \in \mathbb{N}_0,\ x < 2^{2^{2n}} \right]\!\right]\,, \tag{3.83}$$

$$\vdash_T \mathbf{S}_n(x,y) \leftrightarrow \left[\!\left[x,y \in \mathbb{N}_0,\ y < 2^{2n},\ x < 2^{2^{2n}},\ (Bw_1(x))(y) = 1 \right]\!\right] \tag{3.84}$$

(jeweils für alle $n \in \mathbb{N}_0$), sowie

$$\begin{aligned} \vdash_T \mathbf{H}_w(x) \leftrightarrow \Big[\!\Big[\ & |w| = n \in \mathbb{N},\ x \in \mathbb{N}_0,\ x < 2^{2^{2n}}, \\ & (Bw_1(x))(0) \circ \ldots \circ (Bw_1(x))(2^n - 1) = w \circ 0^{2^n - n} \Big]\!\Big] \end{aligned} \tag{3.85}$$

(für alle Binärwörter $w \in BW0$) und den Längen- und Konstruierbarkeitseigenschaften (A) (für $\left\{\mathbf{I}_n(x)\right\}_{n\in\mathbb{N}_0}$, $\left\{\mathbf{J}_n(x)\right\}_{n\in\mathbb{N}_0}$, $\left\{\mathbf{L}_n(x)\right\}_{n\in\mathbb{N}_0}$ und $\left\{\mathbf{S}_n(x,y)\right\}_{n\in\mathbb{N}_0}$) und (B) (für $\left\{\mathbf{H}_w(x)\right\}_{w\in BW0}$) aus Definition 3.3.5.

Diese Formeln werden nun in diesem Abschnitt nach und nach definiert und deren oben geforderte Eigenschaften nachgewiesen. Ein wesentlicher Schritt dabei ist die Konstruktion von Formeln $\mathbf{M}_n(x,y,z)$ in T, die es erlauben, die Multiplikation $z = x \cdot y$ zweier Zahlen x und y, wobei $x \in \mathbb{N}_0$ und $x < 2^{2^n}$, in T zu formalisieren und die weiters auch noch den hier immer betrachteten Längen- und Konstruierbarkeitsbedingungen genügen. Die Existenz solcher Formeln wird im folgenden Satz behauptet und ihre Konstruktion im Beweis dafür aufgeführt.

Satz 3.5.1. *Seien T und $T^{((M))}$ wie in diesem Abschnitt angenommen.*

Es existieren für alle $n \in \mathbb{N}_0$ Formeln $\mathbf{M}_n(x,y,z)$ von T so, daß einerseits

$$\vdash_T \mathbf{M}_n(x,y,z) \leftrightarrow \left[\!\left[x \in \mathbb{N}_0,\ x < 2^{2^n},\ x \cdot y = z \right]\!\right] \tag{3.86}$$

für alle $n \in \mathbb{N}_0$ gilt und weiters bezüglich der Familie $\left\{\mathbf{M}_n(x,y,z)\right\}_{n\in\mathbb{N}_0}$ die (Längen- und Konstruierbarkeits-) Bedingungen (A) aus Definition 3.3.5 erfüllt sind. (Die Formeln $\mathbf{M}_n(x,y,z)$ erlauben jedenfalls *die Beschreibung der Multiplikation auf $\mathbb{N}_0$ von durch 2^{2^n} beschränkten Zahlen mittels $O(n)$-längenbeschränkten und in (von der Eingabe $(n)_{10}$ abhängigem) POLYLIN-Aufwand herstellbaren Formeln).*

[Dieser Satz entspricht Theorem 8, p. 14, in [FiR74].]

Beweis. Seien T, $T^{((M))}$ wie in diesem Abschnitt vorausgesetzt.

Die Definition und Konstruktion der Formeln $\mathbf{M}_n(x,y,z)$ erfolgt hier per Induktion über $n \in \mathbb{N}_0$. Für $n = 0$ kann $\mathbf{M}_n(x,y,z)$ als

$$\mathbf{M}_0(x,y,z) ::= \ x = 0 \ \&\ z = 0 \ \ \vee \ \ x = 1 \ \&\ z = y \tag{3.87}$$

[46] Diese abkürzende Schreibweise für auf Zahlen aus $\mathbb{N}_0$ verweisende Terme aus Definition 2.1.1 wird hier auch im folgenden—erneut—öfter verwendet werden.

gewählt bzw. festgesetzt werden und erfüllt damit jedenfalls die inhaltliche Forderung (3.86).

Sei nun $n \in \mathbb{N}_0$ beliebig so, daß Formeln $\mathbf{M}_j(x,y,z)$ für alle $j \in \mathbb{N}_0$, $j \leq n$ schon gewählt wurden und mit $n \to j$ jeweils (3.86) erfüllen.

Als Hilfsmittel zur Definition von $\mathbf{M}_{n+1}(x,y,z)$ unter Verwendung von $\mathbf{M}_n(x,y,z)$ dient nun v.a. die Aussage über natürliche Zahlen

$$\begin{aligned}&(\forall k \in \mathbb{N}_0)\,(\forall x \in \mathbb{N}_0)\\ &\quad\big[\, x < 2^{2^{k+1}} \iff \big(\exists x_1,x_2,x_3,x_4 \in \mathbb{N}_0,\ x_1,x_2,x_3,x_4 < 2^{2^k}\big)\\ &\qquad\qquad \big(x = x_1 \cdot x_2 + x_3 + x_4\big)\,\big]\,,\end{aligned} \tag{3.88}$$

von der man sich auf einfache Weise überzeugen kann, die weiters auf die im folgenden verwendete Aussage

$$\begin{aligned}&(\forall k \in \mathbb{N}_0)\,(\forall x,y,z \in \mathbb{N}_0)\\ &\quad\big[\, x < 2^{2^{k+1}} \,\&\, z = x \cdot y \iff \big(\exists x_1,x_2,x_3,x_4 \in \mathbb{N}_0,\ x_1,x_2,x_3,x_4 < 2^{2^k}\big)\\ &\qquad\qquad \big(\, x = x_1 \cdot x_2 + x_3 + x_4 \,\&\\ &\qquad\qquad\ z = x_1 \cdot (x_2 \cdot y) + x_3 \cdot y + x_4 \cdot y\,\big)\,\big]\end{aligned} \tag{3.89}$$

führt. (3.89) kann nun zur Definition von $\mathbf{M}_{n+1}(x,y,z)$ mit Hilfe von $\mathbf{M}_n(x,y,z)$ dienen. Um für $n+1$ der inhaltlichen Forderung (3.86) gerecht zu werden, könnte $\mathbf{M}_{n+1}(x,y,z)$ als

$$\begin{aligned}&\exists x_1\,\exists x_2\,\exists x_3\,\exists x_4\,\exists x_5 \exists z_1\,\exists z_2\,\exists z_3\,\exists z_4\\ &\quad\big(\mathbf{M}_n(x_2,y,z_2)\,\&\,\mathbf{M}_n(x_1,z_2,z_1)\,\&\,\mathbf{M}_n(x_3,y,z_3)\\ &\qquad\&\,\mathbf{M}_n(x_4,y,z_4)\,\&\,\mathbf{M}_n(x_1,x_2,x_5)\\ &\qquad\&\, x = x_5 + x_3 + x_4\,\&\, z = z_1 + z_3 + z_4\big)\end{aligned} \tag{3.90}$$

gewählt werden (das ist ausführlich leicht nachzuprüfen). Eine Definition von $\mathbf{M}_{n+1}(x,y,z)$ durch die Formel (3.90) ist jedoch deshalb nicht möglich, da in diesem Fall eine Längenabschätzung $|\mathbf{M}_{n+1}(x,y,z)| \geq 5 \cdot |\mathbf{M}_n(x,y,z)|$ folgen würde und damit höchstens $(\tilde{n} \mapsto \big|\mathbf{M}_{\tilde{n}}(x,y,z)^{((M))}\big|) \in O(5^{\tilde{n}})$ als Längenabschätzung zu gewinnen wäre, im Gegensatz zur gewünschten Aussage

$$(\tilde{n} \mapsto \big|\mathbf{M}_{\tilde{n}}(x,y,z)^{((M))}\big|) \in O(\tilde{n}) \tag{3.91}$$

Zur Erzielung dieser Längenabschätzung ist sinnvollerweise nur eine Abschätzung der Gestalt

$$\Big|\mathbf{M}_{\tilde{n}+1}(x,y,z)^{((M))}\Big| \leq C + \Big|\mathbf{M}_{\tilde{n}}(x,y,z)^{((M))}\Big| \qquad (\tilde{n} \in \mathbb{N}_0) \tag{3.92}$$

bezüglich eines von $\tilde{n}$ unabhängigem $C \in \mathbb{R}$, $C > 0$ verwendbar. Eine solche Abschätzung kann jedoch dann erzielt werden, wenn (3.90) durch logische Umformungen so umgeschrieben wird, daß darin nur mehr eine Instanz von $\mathbf{M}_n(x,y,z)$ vorkommt, etwa der Aussage

$$\begin{aligned} \vdash_{\tilde{T}} & \mathbf{F}(x_1,y_1) \,\&\, \mathbf{F}(x_2,y_2) \,\&\, \mathbf{F}(x_3,y_3) \\ \longleftrightarrow \quad & \forall x \forall y \, \big(x = x_1 \,\&\, y = y_1 \quad \vee \quad x = x_2 \,\&\, y = y_2 \\ & \qquad \vee \quad x = x_3 \,\&\, y = y_3 \quad \rightarrow \quad \mathbf{F}(x,y) \big) \end{aligned} \tag{3.93}$$

(für alle Theorien $\tilde{T}$ und Formeln $\mathbf{F}(x,y)$ von $\tilde{T}$) folgend (die [FiR74] als einfaches Beispiel einer viel allgemeineren „Verkürzungsaussage“ von Formeln anführen (vgl. hierzu jedoch (3) im Beweis zu Satz 3.7.2, Abschnitt 7)); in diesem Fall agiert $\mathbf{F}(x,y)$ auf der rechten Seite der Äquivalenz $\leftrightarrow$ in (3.93) als „Unterprogramm“, das dreimal „aufgerufen“ wird, im Gegensatz zu einem dreimal zu verschiedenen „Eingaben“ auf der linken Seite „ausgeführten“ „Programmcode“ $\mathbf{F}$ (diese Analogie ist aus [HoU179], p. 346, übernommen).

Zur Erzielung von (3.92) für $\tilde{n} \rightarrow n$ ist weiters nötig, daß die Definition von $\mathbf{M}_{n+1}(x,y,z)$ auch wirklich auf $\mathbf{M}_n(x,y,z)$ zurückgreift und nicht auf eine (andere) Instanz von $\mathbf{M}_n(x,y,z)$. Um das zu erreichen, sind logische Umformungen, wie etwa in der Aussage

$$\vdash \mathbf{A}_{\mathbf{x}}[\mathbf{a}] \leftrightarrow \exists \mathbf{x} \, (\, \mathbf{x} = \mathbf{a} \,\&\, \mathbf{A} \,)$$

(Corollary 3, Chapt. 3.5, [Shoe67]) ausgedrückt, nötig. Solche Umformungen führen ausgehend von (3.90) auf eine Definition von $\mathbf{M}_{n+1}(x,y,z)$ durch

$$\begin{aligned} & \mathbf{M}_{n+1}(x,y,z) ::= \\ & \quad \exists x_1 \, \exists x_2 \, \exists x_3 \, \exists x_4 \, \exists x_5 \exists z_1 \, \exists z_2 \, \exists z_3 \, \exists z_4 \\ & \qquad \big\{ \, x = x_5 + x_3 + x_4 \,\&\, z = z_1 + z_3 + z_4 \\ & \qquad\quad \&\, \forall x_0 \, \forall y_0 \, \forall z_0 \\ & \qquad\qquad \big[\, x_0 = x_2 \,\&\, y_0 = y \,\&\, z_0 = z_2 \quad \vee \quad x_0 = x_1 \,\&\, y_0 = z_2 \,\&\, z_0 = z_1 \\ & \qquad\qquad\quad \vee \quad x_0 = x_3 \,\&\, y_0 = y \,\&\, z_0 = z_3 \quad \vee \quad x_0 = x_4 \,\&\, y_0 = y \,\&\, z_0 = z_4 \\ & \qquad\qquad\quad \vee \quad x_0 = x_1 \,\&\, y_0 = x_2 \,\&\, z_0 = x_5 \\ & \qquad\qquad\quad \rightarrow \quad \exists x \, \exists y \, \exists z \\ & \qquad\qquad\qquad\quad \big(x = x_0 \,\&\, y = y_0 \,\&\, z = z_0 \,\&\, \mathbf{M}_n(x,y,z) \big) \, \big] \big\} \, . \end{aligned} \tag{3.94}$$

Hieraus erhellt deutlich, daß nun mit $\tilde{n} \rightarrow n$ (3.92) gilt und zwar im weiteren für ein bestimmtes (aus (3.94) leicht zu ermittelndes), von n unabhängiges $C \in \mathbb{R}$, $C > 0$[47] für die hier direkt ablesbare Unabhängigkeit der Konstante C von n ist auch entscheidend, daß

[47] Abzählung in dieser Formel ergibt (bzgl. pränexer Formelschreibweise) $C := 166$.

bei der induktiven Definition von $\mathbf{M}_n(x,y,z)$ dieselben 15 Variablen aus logischen Gründen (daß der „Geltungs-“ oder „Einflußbereich“ einer gebundenen Variablen $\mathbf{x}$ in einer Formel $(Q\mathbf{x})\mathbf{A}$ sich nicht auf eine Teilformel $(Q'\mathbf{x})\mathbf{B}$ von $\mathbf{A}$ erstreckt, in dieser Formel $(Q'\mathbf{x})\mathbf{B}$ jedoch ein neuer solcher Bereich für die Variable $\mathbf{x}$ entsteht bzw. möglich ist, der vom äußeren unabhängig ist $(Q,Q' \in \{\exists,\forall\})$), immer wieder verwendet werden konnten. Dabei kommen zu x,y,z 12 weitere Variablen hinzu, wie auch [FiR74] bemerken; es wäre aber sogar möglich, mit 10 neuen Variablen auszukommen, denn die Verwendung x_0 und z_0 könnte durch deren Ersetzung durch x bzw. z umgangen werden.

Insgesamt ist dadurch (3.92) gezeigt, woraus (3.91) wegen der Unabhängigkeit eines in Frage kommenden $C \in \mathbb{R}$, $C > 0$ von n unmittelbar durch Induktion folgt (da $\mathbf{M}_n(x,y,z)^{((M))}$ der Formel $\mathbf{M}_n(x,y,z)$ direkt entspricht; die Verwendung von Klammerungsschreibweise anstatt pränexer Schreibweise erfolgt ja—wie in [Shoe67]—nur um die Lesbarkeit der Formel zu erhalten, während von den Formeln selbst immer angenommen wird, daß es sich eigentlich um pränex geschriebene Ausdrücke handelt).

Die die Formeln aus der Familie $\left\{\mathbf{M}_n(x,y,z)^{((M))}\right\}_{n\in\mathbb{N}_0}$ betreffende Forderung der $POLYLIN$-Konstruierbarkeit, d.h. die Eigenschaft (β) der dafür zu zeigenden Bedingung (A) bezüglich dieser Familie, ergibt sich direkt aus der induktiven Form der Definition der Formeln $\mathbf{M}_n(x,y,z)$ hier vermittels (3.87) und (3.94) (und könnte auf verschiedene Weise präziser bewiesen werden; das unterbleibt hier jedoch).

Insgesamt sind damit Formeln $\mathbf{M}_n(x,y,z)$ für alle $n \in \mathbb{N}_0$ mit den im Lemma geforderten Eigenschaften gefunden und definiert worden.

□

Formeln $\mathbf{J}_n(x)$ mit (3.82) und der Eigenschaft (A) können durch die induktive Setzung

$$\begin{aligned} \mathbf{J}_0(x) &::= \; x = 1\,; \\ \mathbf{J}_{n+1}(x) &::= \; \exists x_0 \left(\exists x \left(x = x_0 \;\&\; \mathbf{J}_n(x) \right) \;\&\; x = x_0 + x_0 \right) \qquad (n \in \mathbb{N}_0)\,; \end{aligned} \tag{3.95}$$

gefunden und definiert werden (diese induktive Definition ist—verglichen mit der für $\mathbf{M}_n(x,y,z)$ in (3.94) vorgenommenen—von besonders einfacher Gestalt, da hierbei keine „Verkürzung“ vorgenommen, sondern nur sichergestellt werden mußte, daß die gleichen Variablen x_0, x in jedem neuen Definitionsschritt wieder verwendet werden können).

Unter Verwendung der Formeln $\mathbf{M}_n(x,y,z)$ könnte $\mathbf{I}_n(x)$ nun als

$$\exists x_1 \, \exists z \big(\mathbf{J}_{2n}(x_1) \;\&\; \mathbf{M}_n(x,1,x) \;\&\; \mathbf{M}_n(z,1,z) \;\&\; x + z + 1 = x_1 \big) \tag{3.96}$$

(wegen $2^{2n} \leq 2^{2^n}$ (für alle $n \in \mathbb{N}_0$)) definiert werden, um die Bedingungen (A) an $\mathbf{I}_n(x)$ jedoch besser einsehen zu lassen (d.h. durch Bildung von Instanzen der Formeln $\mathbf{M}_n(x,y,z)$, $\mathbf{J}_{2n}(x)$ die Längen dieser Formeln nicht durch dann vielleicht nötige Umbenennung gebundener Variablen darin zu verändern bzw. dadurch nicht mehr direkt auf Turingmaschinen

für deren Herstellung zugreifen zu können), ist folgende vorsichtigere, aber aufwendigere Setzung sinnvoll:

$$\begin{aligned}\mathbf{I}_n(x) ::= \\ \exists x_1\,\exists z\big\{\,&\exists x\,(\,x = x_1\ \&\ \mathbf{J}_n(x)\,)\ \&\ x + z + 1 = x_1 \\ &\&\ \forall x_1\,\forall y\,\forall z_1 \\ &\quad\big[\,\big(\,x_1 = x\ \&\ z_1 = x\ \ \vee\ \ x_1 = z\ \&\ z_1 = z\,\big)\ \&\ y = 1 \\ &\qquad\rightarrow\ \ \exists x\,\exists z\big(\,x = x_1\ \&\ z = z_1\ \&\ \mathbf{M}_n(x,y,z)\,\big)\,\big]\,\big\}\,. \end{aligned} \tag{3.97}$$

(Aus Gründen der Bedingung (A), (α) allein wäre hier die Ersetzung des zweimaligen Auftretens von $\mathbf{M}_n(x,y,z)$ durch ein einziges Auftreten dieser Formel nicht erforderlich gewesen, da es sich hier ja *nicht* um eine induktive Definition von $\mathbf{I}_n(x)$ unter Rückgriff auf Formeln $\mathbf{I}_{\tilde{n}}(x)$ für $\tilde{n} < n$ handelt, sondern um eine für alle $n \in \mathbb{N}_0$ gleichartige Festsetzung von $\mathbf{I}_n(x)$ mit Hilfe von (unabhängig hiervon definierten) Formeln $\mathbf{M}_n(x,y,z)$ und $\mathbf{J}_n(x)$.) — Solche aufwendig anzuschreibenden exakten Definitionen würden auch im folgenden öfter benötigt werden, um die Bedingungen (A) oder (B) jeweils genau einsehbar oder nachprüfbar zu machen; diese ins einzelne gehenden Festlegungen werden dann aber zumeist unterbleiben, da anhand der Beispiele hier deutlich geworden sein sollte, wie sie auf leichtem und direktem Weg immer auf analoge Weise gefunden und fixiert werden können.

Für $\mathbf{L}_n(x)$ kann nun

$$\mathbf{L}_n(x) ::=\ \exists y\,\exists z\,\big(\,y = 1\ \&\ z = x\ \&\ \mathbf{M}_{2n}(x,y,z)\,\big) \tag{3.98}$$

gesetzt werden.

Zur Konstruktion von $\mathbf{S}_n(x,y)$ mit (3.84) sind neben den bisher definierten Formeln noch solche nötig, die in T die Exponentiation für natürliche Zahlen $< 2^{2^n}$ ausdrücken, und daneben noch den Bedingungen (A) genügen; diese Formeln werden mit $\mathbf{Pow}_n(x,y,z)$ bezeichnet werden.

Satz 3.5.2. *Seien T und $T^{((M))}$ wie in diesem Abschnitt angenommen.*

Es existieren für alle $n \in \mathbb{N}_0$ Formeln $\mathbf{Pow}_n(x,y,z)$ von T so, daß einerseits für alle $n \in \mathbb{N}_0$

$$\vdash_T \mathbf{Pow}_n(x,y,z)\ \leftrightarrow\ [\![\, x,y,z \in \mathbb{N}_0,\ x,y,z < 2^{2^n},\ z = y^x\,]\!] \tag{3.99}$$

gilt und weiters die bezüglich diesen Formeln definierte Familie $\{\mathbf{Pow}_n(x,y,z)^{((M))}\}_{n\in\mathbb{N}_0}$ auch der (Längen- und Konstruierbarkeits-) Eigenschaft (A) aus Definition 3.3.5 genügt. (Die Formeln $\mathbf{Pow}_n(x,y,z)$ erlauben die Beschreibung der Exponentiation von Zahlen aus $\mathbb{N}_0$ der Größe $< 2^{2^n}$ in T durch $O(n)$-längenbeschränkte und in POLYLIN-Aufwand (bezüglich Eingabe $(n)_{10}$) mechanisch generierbaren Formeln).

[Dieser Satz entspricht Theorem 10, p. 16, in [FiR74].]

Beweis. T, $T^{((M))}$ seien erneut wie in diesem Abschnitt vorausgesetzt.

Die Definition der Formeln $\mathbf{Pow}_n(x,y,z)$ erfolgt für alle $n \in \mathbb{N}_0$ gesondert, jedoch analog durch die Verwendung von Formeln $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ für $k \in \mathbb{N}_0$, $k \leq n$, die inhaltlich die Eigenschaft

$$\begin{aligned} \vdash_T \mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0) \leftrightarrow \Big[\!\Big[x,y,z \in \mathbb{N}_0,\ x < 2^{2^k},\ y,z < 2^{2^n},\ z = y^x \Big]\!\Big] \\ \&\ \mathbf{M}_n(x_0,y_0,z_0) \end{aligned} \tag{3.100}$$

formalisieren; dabei soll die Festlegung dieser Formeln auch so erfolgen, daß die abschließende Setzung

$$\begin{aligned} &\mathbf{Pow}_n(x,y,z) ::= \\ &\quad \exists x_0\, \exists y_0\, \exists z_0 \left(x_0 = 0\ \&\ y_0 = 0\ \&\ z_0 = 0\ \&\ \mathbf{E}_{n,n}(x,y,z,x_0,y_0,z_0) \right) \end{aligned} \tag{3.101}$$

(von der man leicht sieht, daß sie unter der Voraussetzung eines konstruktiven Nachweises der Existenz von Formeln $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ mit (3.100) auf $\mathbf{Pow}_n(x,y,z)$ mit den inhaltlichen Eigenschaften (3.99) führt) auch die Längen- und Konstruierbarkeitsbedingung (A) an $\mathbf{Pow}_n(x,y,z)$ zu erreichen ermöglicht.

Eine derartige Definition der Formeln $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ für alle $n \in \mathbb{N}_0$ kann nun jeweils induktiv über $k \in \mathbb{N}_0$, $k \leq n$ unter Benützung der Formeln $\mathbf{M}_n(x,y,z)$ aus Satz 3.5.1 erfolgen. Es wird dabei die in T durch die Formeln $\mathbf{M}_n(x,y,z)$ beschriebene, auf natürliche Zahlen $< 2^{2^n}$ beschränkte Multiplikation zur induktiven Definition von Formeln, die immer größere Teile der Exponentiation auf diesen Zahlen (und schließlich in $\mathbf{Pow}_n(x,y,z)$ die Exponentation für natürliche Zahlen $< 2^{2^n}$ allgemein) formalisieren, verwendet.

Für $n \in \mathbb{N}_0$ und $k = 0$ kann nun $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ von der Gestalt

$$\big(x = 0\ \&\ z = 1\ \vee\ x = 1\ \&\ z = y \big)\ \&\ \mathbf{M}_n(y,1,y)\ \&\ \mathbf{M}_n(x_0,y_0,z_0) \tag{3.102}$$

gewählt werden (hierin sollten $\mathbf{M}_n(z,1,z)$ und $\mathbf{M}_n(x_0,y_0,z_0)$ noch durch direkt auf $\mathbf{M}_n(x,y,z)$ Bezug nehmende äquivalente Formeln ersetzt werden; wie früher ist das aber leicht zu erreichen).

Seien nun $n \in \mathbb{N}_0$ und $k \in \mathbb{N}_0$, $k < n$ beliebig, im folgenden fest.

Der Induktionsschritt $k \to k+1$ in der Festlegung von $\mathbf{E}_{k+1,n}(x,y,z,x_0,y_0,z_0)$ mit Hilfe von zuvor definierten Formeln $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ macht nun von der früher verwendeten Aussage (3.88) Gebrauch und zwar dadurch, daß für $x \in \mathbb{N}_0$ mit $x < 2^{2^{k+1}}$ danach $x_1,x_2,x_3,x_4 \in \mathbb{N}_0$, $x = x_1 \cdot x_2 + x_3 + x_4$ existieren, so, daß sich die Zahl y^x durch

$$y^x = y^{x_1 \cdot x_2 + x_3 + x_4} = (y^{x_1})^{x_2} \cdot y^{x_3} \cdot y^{x_4}$$

darstellen läßt. Diese Überlegung führt zusammen mit der Induktionsannahme über $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$, (3.100) zu erfüllen, auf eine vorläufige Setzung für die Formel $\mathbf{E}_{k+1,n}(x,y,z,x_0,y_0,z_0)$ von der folgenden Gestalt:

$$\begin{aligned}
&\exists x_1 \ldots \exists x_5\, \exists z_1 \ldots \exists z_5 \\
&\quad \big[\, \mathbf{E}_{k,n}(x_1,y,z_1,0,0,0) \;\&\; \mathbf{E}_{k,n}(x_2,z_1,z_2,0,0,0) \\
&\qquad \&\; \mathbf{E}_{k,n}(x_3,y,z_3,0,0,0) \;\&\; \mathbf{E}_{k,n}(x_4,y,z_4,0,0,0) \\
&\qquad \&\; \mathbf{E}_{k,n}(0,1,1,x_1,x_2,x_5) \;\&\; x = x_5 + x_3 + x_4 \\
&\qquad \&\; \mathbf{E}_{k,n}(0,1,1,z_3,z_4,z_5) \;\&\; \mathbf{E}_{k,n}(0,1,1,z_2,z_5,z) \\
&\qquad \&\; \mathbf{E}_{k,n}(0,1,1,z,1,z) \;\&\; \mathbf{E}_{k,n}(0,1,1,x_0,y_0,z_0) \,\big] \,. \qquad (3.103)
\end{aligned}$$

Um eine im folgenden nötige Längenabschätzung

$$\big|\mathbf{E}_{k+1,n}(x,y,z,x_0,y_0,z_0)^{((M))}\big| \le C + \big|\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)^{((M))}\big| \quad (\text{für alle } n \in \mathbb{N}_0) \qquad (3.104)$$

zu erzielen, wobei C von k unabhängig sein soll (von n jedoch abhängen dürfte, wenngleich das nicht der Fall sein wird), ist eine logische Umformung von (3.103)—analog wie die die Definition von $\mathbf{M}_n(x,y,z)$ betreffende zwischen (3.89) und (3.94)—nötig, so, daß darin $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ nur mehr einmal und weiters auch nur in genau dieser Gestalt auftritt. Eine solche führt etwa zur ausführlichen Festsetzung:

$$\begin{aligned}
&\mathbf{E}_{k+1,n}(x,y,z,x_0,y_0,z_0) ::= \\
&\quad \exists x_1 \ldots \exists x_5\, \exists z_1 \ldots \exists z_5 \\
&\qquad \big\{\, x = x_5 + x_3 + x_4 \\
&\qquad\quad \&\; \forall x_{11}\, \forall y_{11}\, \forall z_{11}\, \forall x_{10}\, \forall y_{10}\, \forall z_{10} \\
&\qquad\qquad \big[\, x_{11} = x_1 \;\&\; y_{11} = y \;\&\; z_{11} = z_1 \;\&\; x_{10} = 0 \;\&\; y_{10} = 0 \;\&\; z_{10} = 0 \\
&\qquad\qquad\quad \vee \;\; x_{11} = x_2 \;\&\; y_{11} = z_1 \;\&\; z_{11} = z_2 \;\&\; x_{10} = 0 \;\&\; y_{10} = 0 \;\&\; z_{10} = 0 \\
&\qquad\qquad\quad \vdots \\
&\qquad\qquad\quad \vee \;\; x_{11} = 0 \;\&\; y_{11} = 1 \;\&\; z_{11} = 1 \;\&\; x_{10} = x_0 \;\&\; y_{10} = y_0 \;\&\; z_{10} = z_0 \\
&\qquad\qquad\quad \to \;\; \exists x\, \exists y\, \exists z\, \exists x_0\, \exists y_0\, \exists z_0 \big(\, x = x_{11} \;\&\; y = y_{11} \;\&\; z = z_{11} \\
&\qquad\qquad\qquad\qquad\qquad\qquad \&\; x_0 = x_{10} \;\&\; y_0 = y_{10} \;\&\; z_0 = z_{10} \\
&\qquad\qquad\qquad\qquad\qquad\qquad \&\; \mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0) \big) \,\big] \,\big\} \,. \qquad (3.105)
\end{aligned}$$

(Hierbei beziehen sich die vertikalen Punkte im Teil der Disjunktionen innerhalb der eckigen Klammern [...] in (3.105) auf Erfassungen der übrigen 6 Instanzen der Formel $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ in (3.103)[48] hierin durch Fixierungen der Variablen x_{11}, y_{11}, z_{11},

[48](nämlich übrigen 6 Instanzen $\mathbf{E}_{k,n}(x_3,y,z_3,0,0,0)$, $\mathbf{E}_{k,n}(x_4,y,z_4,0,0,0)$, $\mathbf{E}_{k,n}(0,1,1,x_1,x_2,x_5)$, $\mathbf{E}_{k,n}(0,1,1,z_3,z_4,z_5)$, $\mathbf{E}_{k,n}(0,1,1,z_2,z_5,z)$ und $\mathbf{E}_{k,n}(0,1,1,z,1,z)$)

x_{10}, y_{10} und z_{10}.) Hieraus ist leicht abzulesen, daß damit (3.104) gilt (erneut gestattet es diese induktive Setzung, daß für alle $k \in \mathbb{N}_0$ dieselben 16 zusätzlichen neuen Variablen immer wieder verwendet werden können). Aus (3.104) ergibt sich nun zusammen mit (3.102) und der Eigenschaft von $\mathbf{M}_n(x,y,z)^{((M))}$, $O(n)$-längenbeschränkt zu sein, auf einfache Weise durch Induktion

$$\left(n \mapsto \left|\mathbf{E}_{n,n}(x,y,z,x_0,y_0,z_0)^{((M))}\right|\right) \in O(n)\ . \tag{3.106}$$

(Der Übergang von einer Formel in T zu einer Formel in $T^{((M))}$ findet hier eigentlich nicht statt, da diese Formeln schon mit dezimaler Variablenindizierung, jedoch in Klammerungs- und nicht in pränexer Schreibweise angegeben wurden, vgl. Bemerkung über die hier verwendete Unschärfe im Gebrauch des Formalismus für Theorien 1. Ordnung aus [Shoe67] am Ende von Abschnitt 3). Entlang der induktiven Setzungen von $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ für $k \in \mathbb{N}_0$, $k \leq n$ (zu vorgegebenem $n \in \mathbb{N}_0$) entlang von (3.102) und (3.105) läßt sich auch ziemlich deutlich die $POLYLIN$-Generierbarkeit von $\mathbf{E}_{n,n}(x,y,z,x_0,y_0,z_0)^{((M))}$ für Eingabe $(n)_{10}$ einsehen bzw. diese ließe sich damit ausführlich beweisen. Wesentlich dafür ist natürlich die entsprechende, im Beweis zu Satz 3.5.1 begründete Eigenschaft von $\mathbf{M}_n(x,y,z)^{((M))}$, da $\mathbf{M}_n(x,y,z)^{((M))}$ ja in den Induktionsanfang für $k = 0$ eingeht. Für den in in (3.105) ausgedrückten Induktionsschritt $k \to k+1$ in der Festlegung von $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ (zu vorgegebenem $n \in \mathbb{N}_0$) wird die Formel $\mathbf{M}_n(x,y,z)$ als *explizite Teilformel* jedoch nicht mehr benötigt, obwohl sie dabei *inhaltlich* eine große Rolle in der Form von Instanzen von $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$, auf die dabei verwiesen wird, spielt, wobei solche Verweise wegen der Induktionsannahme in diesem Induktionsschritt möglich sind (d.h. letztlich deshalb, weil dann $\mathbf{M}_n(x,y,z)$ als direkte Teilformel in $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ schon enthalten ist.)

Insgesamt ergibt sich damit zusammen mit (3.106) und wegen der schon anfangs angekündigten Setzungen (3.101) für $\{\mathbf{Pow}_n(x,y,z)^{((M))}\}_{n\in\mathbb{N}_0}$ auch die Gültigkeit der Bedingung (A). Damit sind für alle $n \in \mathbb{N}_0$ Formeln $\mathbf{Pow}_n(x,y,z)$ mit den im Satz behaupteten Eigenschaften gefunden bzw. konstruiert worden.

□

Nun können Formeln $\mathbf{S}_n(x,y)$ in T, die für alle $n \in \mathbb{N}_0$ (3.84) erfüllen und bzgl. derer die Familie $\{\mathbf{S}_n(x,y)^{((M))}\}_{n\in\mathbb{N}_0}$ den Bedingungen (A) genügt, unter Zuhilfenahme der bereits definierten Formeln und der folgenden, leicht nachzuprüfenden Aussage gefunden

werden:

$$
\begin{aligned}
&(\forall x, y \in \mathbb{N}_0) \\
&\quad \big[\, (Bw_1(x))(y) = 1 \iff ((x)_2)^R(y) = 1 \iff \\
&\qquad \iff (\exists z \in \mathbb{N}) \big(2^y \leq z < 2^{y+1} \;\&\; z \leq x \;\&\; 2^{y+1} \mid x - z \big) \\
&\qquad \iff (\exists z \in \mathbb{N}_0)\, (\exists w \in \mathbb{N}_0) \\
&\qquad\qquad \big(2^y \leq z < 2^{y+1} \;\&\; x = z + w \cdot 2^{y+1} \big) \,\big] \,. \qquad (3.107)
\end{aligned}
$$

Satz 3.5.3. *T, $T^{((M))}$ wie in diesem Abschnitt angenommen.*

Es existieren für alle $n \in \mathbb{N}_0$ Formeln $\mathbf{S}_n(x,y)$ in T, die der inhaltlichen Forderung (3.84) genügen, und bzgl. denen die Familie $\big\{\mathbf{S}_n(x,y)^{((M))}\big\}_{n\in\mathbb{N}_0}$ den Längen- und Konstruierbarkeitsbedingungen (A) aus Definition 3.3.5 genügt.

[Dieser Satz entspricht Theorem 11, p.17, in [FiR74].]

Beweisskizze. $\mathbf{S}_n(x,y)$ können für alle $n \in \mathbb{N}_0$ durch Formalisierung von (3.107) mit Hilfe von $\mathbf{I}_n(x)$, $\mathbf{L}_n(x)$, $\mathbf{Pow}_{2n}(x,y,z)$ und $\mathbf{M}_{2n}(x,y,z)$ von der Gestalt

$$
\begin{aligned}
&\mathbf{L}_n(x) \;\&\; \mathbf{I}_n(y) \\
&\;\&\; \exists z\, \exists w\, \exists y_0\, \exists y_1\, \exists z_1\, \exists z_2\, \exists w_1 \\
&\qquad \big(\mathbf{Pow}_{2n}(y, \underline{\underline{2}}, y_0) \;\&\; y_1 = y_0 + y_0 \;\&\; \mathbf{M}_{2n}(z,1,z) \\
&\qquad\quad \;\&\; y_0 + z_1 = z \;\&\; z + z_2 + 1 = y_1 \\
&\qquad\quad \;\&\; \mathbf{M}_{2n}(w, y_1, w_1) \;\&\; x = z + w_1 \big) \qquad (3.108)
\end{aligned}
$$

gewählt werden. Das Auftreten der Instanz $\mathbf{M}_{2n}(z,1,z)$ von $\mathbf{M}_{2n}(x,y,z)$ hierin ist eigentlich nicht notwendig, denn die Forderung an z, eine Zahl aus $\mathbb{N}_0$ zu sein, ergibt sich aus den anderen Teilen der Formel, ebenso wie das auf einfacher zu erkennende Weise auch für die übrigen Variablen gilt; aus Gründen der einfacheren Nachvollziehbarkeit der inhaltlichen Eigenschaften von (3.108) ist dieses Auftreten von $\mathbf{M}_{2n}(z,1,z)$ darin aber hier dennoch beibehalten worden). Wie früher sollte (3.108) logisch äquivalent zu einer Formel umgeformt werden, die gerade $\mathbf{I}_n(x)$, $\mathbf{Pow}_{2n}(x,y,z)$ und $\mathbf{M}_{2n}(x,y,z)$ als Teilformeln besitzt, und die dann als exakte Setzung für $\mathbf{S}_n(x,y)$ verwendet werden kann, um die Forderungen des Satzes (direkter) einsehen bzw. nachprüfen zu können. $\diamondsuit$

Es sind nun noch Formeln $\mathbf{H}_w(x)$ mit (3.85) und den Eigenschaften (A) bezüglich $\big\{\mathbf{H}_w(x)^{((M))}\big\}_{w\in BW0}$ zu konstruieren, also Formeln, die an x die Forderung stellen, daß $x \in \mathbb{N}_0$ ist und daß die ersten 2^n Buchstaben des x durch $Bw_1(x)$ zugeordneten Binärwortes auch dieselben Buchstaben des Wortes $w \circ 0^{2^n - n}$ $(n = |w|)$ sind.

Satz 3.5.4. *T, $T^{((M))}$ wie in diesem Kapitel vorausgesetzt.*

Für alle $w \in BW0$ existieren Formeln $\mathbf{H}_w(x)$ in T mit der inhaltlichen Eigenschaft (3.85) und bzgl. denen die Familie $\{\mathbf{H}_w(x)^{((M))}\}_{w\in BW0}$ den Eigenschaften (B) aus Definition 3.3.5 genügt.

[Dieser Satz entspricht Theorem 12, p. 18, in [FiR74].]

Beweis. Die Konstruktion der Formeln $\mathbf{H}_w(x)$ in [FiR74] benutzt Formeln $\mathbf{K}_w(x)$ in T mit der inhaltlichen Eigenschaft

$$\vdash_T \mathbf{K}_w(x) \leftrightarrow \Big[\!\Big[\ |w| = n \in \mathbb{N},\ x \in \mathbb{N}_0,\ x < 2^{2^{2n}},\\ (Bw_1(x))(0) \circ \ldots \circ (Bw_1(x))(|w|-1) = w \Big]\!\Big]\ ,$$

bzw.—was dieselbe Forderung ist—

$$\vdash_T \mathbf{K}_w(x) \leftrightarrow x = \underline{\underline{\textstyle\sum_{i=0}^{|w|-1} w(i)\cdot 2^i}}\,,$$

und der Bedingung an $\{\mathbf{K}_w(x)^{((M))}\}_{w\in BW0}$, (B) zu erfüllen.

Für beliebige $w \in BW0$ können die Formeln $\mathbf{K}_w(x)$ mit diesen Eigenschaften entlang der rekursiven Definitionen

$$\begin{aligned} \mathbf{K}_0(x) &::= \ x = 0\ ;\\ \mathbf{K}_1(x) &::= \ x = 1\ ; \end{aligned}$$

für $|w| = 1$, sowie für $|w| > 1$, $w = Su$ ($S \in \{0,1\}$, $u \in BW0$) als

$$\begin{aligned} \mathbf{K}_{0u}(x) &::= \ \exists x_0\big(\,\exists x\,(\,x = x_0\ \&\ \mathbf{K}_u(x)\,)\ \&\ x = x_0 + x_0\,\big)\ ;\\ \mathbf{K}_{1u}(x) &::= \ \exists x_0\big(\,\exists x\,(\,x = x_0\ \&\ \mathbf{K}_u(x)\,)\ \&\ x = x_0 + x_0 + 1\,\big)\ ; \end{aligned}$$

definiert werden. (Diese Setzungen für $\mathbf{K}_w(x)$ bezüglich $|w| > 1$ unterscheiden sich (geringfügig) von der in [FiR74] dafür auf p. 18 explizit gemachten Gestalt dieser Formeln, sind jedoch [m.E., C.G.] *so* hier richtig und sollten dort auch so stehen). Es dürfte klar sein, daß sich entlang den obigen Rekursionsformeln eine Turingmaschine konstruieren läßt, die für jede Eingabe $w \in BW0$ in polynomialer deterministischer Rechenzeit und linear beschränktem Speicherplatzaufwand $\mathbf{K}_w(x)$ bzw. $\mathbf{K}_w(x)^{((M))}$ konstruiert.

Ausgehend von diesen Formeln $\mathbf{K}_w(x)$ können nun unter zusätzlicher Verwendung der Formeln $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$ und $\mathbf{S}_n(x,y)$ die Formeln $\mathbf{H}_w(x)$ entlang von

$$\begin{aligned} \mathbf{L}_n(x)\ \&\ \exists x_0\,\exists z\big\{\,&\mathbf{K}_w(x_0)\ \&\ \mathbf{J}_n(z)\\ &\&\ \forall y\big[\,\mathbf{I}_n(y)\ \&\ \exists z_0\,(\,y + z_0 + 1 = z\,)\\ &\qquad\to\ \ \big(\,\mathbf{S}_n(x,y) \leftrightarrow \mathbf{S}_n(x_0,y)\,\big)\,\big]\,\big\} \end{aligned} \tag{3.109}$$

(: $\sim$ die ersten 2^n Buchstaben eines durch von $Bw_1(x)$ beschriebenen Wortes entsprechen den ersten 2^n Buchstaben von $Bw_1(x_0)$ mit x_0 so, daß $K_w(x_0)$ gilt) festgelegt werden. Eine exakte Setzung für $\mathbf{H}_w(x)$ entlang von (3.109) sollte—früheren Beispielen folgend—leicht präzisierbar sein und ebenso sollten danach weitergehende Nachweise der Eigenschaft von $\left\{\mathbf{H}_w(x)^{((M))}\right\}_{w\in BW0}$, die Bedingungen (B) zu erfüllen, einfach zu führen sein. □

Es sind hiermit also nun insgesamt für alle $n \in \mathbb{N}_0$ und $w \in BW0$ Formeln $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$, $\mathbf{L}_n(x)$, $\mathbf{S}_n(x,y)$ und $\mathbf{H}_w(x)$ konstruiert worden, die (3.81)–(3.85) sowie den jeweils zugehörigen Längen- und Konstruierbarkeitsbedingungen (A) bzw. (B) aus Definition 3.3.5 genügen. Damit ist für T, $T^{((M))}$ wie angenommen und $f(n) := 2^n$ die Annahme von Satz 3.4.4 erfüllt. Nach der zu Beginn dieses Abschnittes dargestellten Argumentation folgt dann (mit bzw. aus Sätzen des Abschnitts 3.4) die Behauptung von Satz 3.1.3 bzw. ist dieser Satz dadurch bewiesen.

3.6 Beweis von Satz 3.1.1 (Spezieller Beweisteil in [FiR74] bei der Erzielung von $Th(\langle \mathbb{N}_0; 0, 1, + \rangle) \notin NTime(2^{2^{cn}})$ für ein $c \in \mathbb{R}$, $c > 0$)

Sei T in diesem Abschnitt entweder die per definitionem vollständige, semantisch definierte Theorie $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ oder die dazu äquivalente, axiomatisierte Theorie $PreAN_1$ aus Abschnitt 2.3 (Definition 2.3.2) (die sich auf definitorischem Weg durch die Einführung von $<$ zur „Presburger Arithmetik natürlicher Zahlen“ $PreAN$ aus Abschnitt 2.3 erweitern läßt) und L deren Sprache (wie in Abschnitt 5 also eine Sprache einer Theorie 1. Ordnung mit den Konstantensymbolen 0 und 1 sowie weiters noch dem zweistelligen Funktionssymbol + als deren nichtlogische Symbole). $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ sei die als System formaler Sprachen mit informatisch-sinnvoller Formelsyntax aufgefaßte Theorie T [49], wobei diese hier mit dem Verweis auf Grammatik 2.6.1 und deren Terminalalphabet Σ durch die Setzungen (3.79) aus Abschnitt 5 (jedoch bezüglich T wie hier vorausgesetzt) präzisieren ließe (völlig analog wie dort für RA geschehen)[50].

Der hier darzulegende Komplexitätsbeweis bezieht sich also zuerst auf Theorien der Presburger Arithmetik natürlicher Zahlen, die kein Ordnungssymbol in ihrer Sprache enthalten; dies v.a. deshalb, weil dabei das (jedenfalls theoretisch:) allgemeinere Komplexitätsresultat erzielt wird (damit ist gemeint, daß die Entscheidungskomplexität einer definitorischen Erweiterung $\tilde{T}'$ einer Theorie $\tilde{T}$ immer mindestens ebenso hoch ist wie die der Theorie $\tilde{T}$ selber[51]). Der Beweis hier könnte aber ebenso für $T = PreAN$ durchgeführt werden und würde darin sogar einfacher sein, wie sich auch daran zeigt (d.h. sehen lassen wird), daß bei der vorläufigen Festlegung von zu konstruierenden Formeln hier dennoch öfter Ordnungssymbole verwendet werden (weil die Lesbarkeit und Verständlichkeit dieser Formeln damit eher gewährleistet wird), die erst bei einer präzisen Festlegung dieser Formeln (auf die oft aus Analogiegründe verzichtet wird) eliminiert werden müßten. Etwa durch die Konstruktion von Translationsformeln und die Verwendung definitorischer Axiome wie etwa die Axiome

$$x \leq y \leftrightarrow \exists z \, (\, x + z = y \,) \, ,$$
$$x < y \leftrightarrow \exists z \, (\, x + z + 1 = y \,)$$

zur definitorischen Einführung von $\leq$ bzw. $<$ in T.

In einer darüber etwas hinausgehenden Weise könnte der hier dargelegte Beweis(-teil) auch für $PreAZ$, die Theorie der Presburger Arithmetik ganzer Zahlen aus Abschnitt 2.2,

[49] Da $Th(\langle \mathbb{N}_0; 0, 1, + \rangle)$ und $PreAN_1$ äquivalente Theorien sind, ist das hier nun betrachtete und definierte Sprachsystem $T^{((M))}$ in beiden Fällen das selbe.

[50] Das Vorhandensein des Symbols $\leftrightarrow$ in $\Sigma_{T^{((M))}}$ hier ist für die erzielten Aussagen (wie in Abschnitt 3.5) ebenfalls nicht unbedingt erforderlich.

[51] Diese Aussage gilt natürlich auch für allgemeine konservative Erweiterungen $\tilde{T}'$ einer Theorie $\tilde{T}$.

ganz analog geführt werden. Dabei müßten nur die hier zu konstruierenden Formeln bezüglich der Formel $0 = x \;\&\; 0 < x$ „relativiert“ werden, d.h. im Sinn von Definition 2.4.1 jeweils von Formeln $\mathbf{A}$ zu Formeln $\mathbf{A}^R$ übergegangen werden. Es ist leicht, sich davon zu überzeugen, daß dadurch die Längen- und Konstruierbarkeitseigenschaften von zu konstruierenden Formeln *qualitativ* (und d.h.: bezüglich der Festsetzung dieser Eigenschaften in Definition 3.3.5, auf die in diesem Zusammenhang hier immer verwiesen wird) erhalten bleiben. – Eine solche Beweisverallgemeinerung für $PreAZ$ ist jedoch gerade auch im Lichte von Satz 2.6.4 und Lemma 2.6.3 eigentlich unnötig.

Eine entsprechende Übertragung des Beweises hier ist jedoch für die Theorie TAZ aus Abschnitt 2.1 (gerade wegen des *substantiellen* Fehlens eines Ordnungssymbols darin, d.h. der Nicht-Definierbarkeit eines Ordnungssymbols in dessen gebräuchlicher Bedeutung in TAZ) nicht möglich, jedenfalls nicht direkt (vgl. jedoch Abschnitt 7; dort wird eine analog-hohe untere Schranke für die Entscheidungskomplexität von TAZ auf—etwas—andere Weise erzielt).

Im folgenden sei hier außerdem noch das Standardmodell für T mit $\mathfrak{N} := \langle \mathbb{N}_0; 0, 1, + \rangle$ bezeichnet bzw. festgelegt.

Durch eine völlig analoge Argumentation mittels Sätzen aus dem Abschnitt 4 wie zu Beginn des Abschnitts 5 läßt sich nun ein Beweis für Satz 3.1.1, also für die Existenz einer doppelt-exponentiell-linearen Schranke für die Entscheidungskomplexität von T, und weiters sogar von

$$Thm_{T^{((M))}},\ \mathrm{co}{-}Thm_{T^{((M))}} \notin NTime(2^{2^{cn}}) \ \text{(für ein } c \in \mathbb{R},\ c > 0) \tag{3.110}$$

zum Nachweis der Erfülltheit der Annahme von Satz 3.4.1, bezüglich $f(n) := 2^{2^n}$ und T, $T^{((M))}$ wie angenommen, reduzieren. Also zum Nachweis der Existenz von Formeln $\mathbf{I}^*_n(x)$, $\mathbf{J}^*_n(x)$, $\mathbf{L}^*_n(x)$, $\mathbf{S}^*_n(x,y)$ für alle $n \in \mathbb{N}_0$ mit (ebenfalls für alle $n \in \mathbb{N}_0$:)

$$\vdash_T \mathbf{I}^*_n(x) \leftrightarrow \left[\!\!\left[x \in \mathbb{N}_0,\ x < 2^{2^{n+1}} \right]\!\!\right], \tag{3.111}$$

$$\vdash_T \mathbf{J}^*_n(x) \leftrightarrow x = \underline{\underline{2^{2^n}}}\ ^{52}, \tag{3.112}$$

$$\vdash_T \mathbf{L}^*_n(x) \leftrightarrow \left[\!\!\left[x \in \mathbb{N}_0,\ x < 2^{2^{2^{n+1}}} \right]\!\!\right], \tag{3.113}$$

$$\vdash_T \mathbf{S}^*_n(x,y) \leftrightarrow \left[\!\!\left[x, y \in \mathbb{N}_0,\ y < 2^{2^{n+1}},\ x < 2^{2^{2^{n+1}}},\ (Bw_1(x))(y) = 1 \right]\!\!\right], \tag{3.114}$$

und Formeln $\mathbf{H}^*_w(x)$ in T für alle $w \in BW0$ und $|w| = n$ mit

$$\begin{aligned} \vdash_T \mathbf{H}^*_w(x) \leftrightarrow \Big[\!\!\Big[& x \in \mathbb{N}_0,\ x < 2^{2^{2^{n+1}}}, \\ & (Bw_1(x))(0) \circ \ldots \circ (Bw_1(x))(2^{2^n} - 1) = w \circ 0^{2^{2^n} - n} \Big]\!\!\Big] \end{aligned} \tag{3.115}$$

[52] Für die genaue Definition dieser sich auf Zahlen aus $\mathbb{N}_0$ beziehenden Schreibweise für Terme in T sei hier wieder (wie auch im folgenden immer) auf Definition 2.1.1 verwiesen.

bezüglich denen die Familien $\{\mathbf{I}^*_n(x)\}_{n\in\mathbb{N}_0}$, $\{\mathbf{J}^*_n(x)\}_{n\in\mathbb{N}_0}$, $\{\mathbf{L}^*_n(x)\}_{n\in\mathbb{N}_0}$, $\{\mathbf{S}^*_n(x,y)\}_{n\in\mathbb{N}_0}$ die (Längen- und Konstruierbarkeits) Bedingungen (A) und $\{\mathbf{H}^*_w(x)\}_{w\in BW0}$ die Bedingungen (B) aus Definition 3.3.5 erfüllen.

Hierbei sind diese Formeln (gegenüber ihrem Auftreten in Satz 3.4.4) durch * indiziert worden, da bei der hier folgend nach und nach durchgeführten Konstruktion dieser Formeln auf die Formeln $\mathbf{I}_n(x)$, $\mathbf{J}_n(x)$, $\mathbf{K}_w(x)$, $\mathbf{M}_n(x,y,z)$ und $\mathbf{Pow}_n(x,y,z)$ aus Abschnitt 5 zurückgegriffen wird. Dies ist deshalb möglich, weil (wie sich leicht überprüfen läßt) Satz 3.5.1 und Satz 3.5.2 auch für T, $T^{((M))}$ wie hier vorausgesetzt gültig sind; diese Tatsache bezieht sich auch auf die übrigen Sätze aus Abschnitt 5, von denen hier aber nur noch die Formeln $\mathbf{K}_w(x)$ (für $w \in BW0$) aus dem Beweis von Satz 3.5.4 bei der Konstruktion von $\mathbf{H}^*_w(x)$ ins Spiel kommen.

Nun können hier für alle $n \in \mathbb{N}_0$ die Formeln $\mathbf{I}^*_n(x)$ und $\mathbf{J}^*_n(x)$ direkt durch die Verwendung von Formeln $\mathbf{M}_{\tilde{n}}(x,y,z)$, $\mathbf{J}_{\tilde{n}}(x)$ und $\mathbf{Pow}_{\tilde{n}}(x,y,z)$ (für geeignete $\tilde{n} \in \mathbb{N}_0$) ausgedrückt werden, und zwar kann gesetzt werden:

$$\mathbf{I}^*_n(x) ::= \exists y\, \exists z \left(y = 1 \;\&\; z = x \;\&\; \mathbf{M}_{n+1}(x,y,z) \right) ; \tag{3.116}$$

$\mathbf{J}^*_n(x)$ kann von der Gestalt

$$\exists x_0 \left(\mathbf{J}_n(x_0) \;\&\; \mathbf{Pow}_{n+1}(x_0, \underline{\underline{2}}, x) \right) \tag{3.117}$$

gewählt werden (jeweils für alle $n \in \mathbb{N}_0$); (3.117) sollte—wie im Abschnitt 5 öfter durchgeführt und hier in (3.116) für $\mathbf{I}^*_n(x)$ schon analog erreicht—noch logisch so umgeformt werden, daß darin $\mathbf{J}_n(x)$ und $\mathbf{Pow}_{n+1}(x,y,z)$ als Teilformeln auftreten, jedoch keine (anderen) Instanzen dieser Formeln. Die inhaltlichen Eigenschaften von $\mathbf{I}^*_n(x)$ und $\mathbf{J}^*_n(x)$ sowie die Erfülltheit von (A) für die zugehörigen Familien sind nun leicht auf die aus Abschnitt 5 bekannten Eigenschaften der Formeln $\mathbf{M}_{n+1}(x,y,z)$, $\mathbf{J}_n(x)$ und $\mathbf{Pow}_{n+1}(x,y,z)$ (bzw. der zugehörigen Familien) zurückzuführen.

Bei der noch ausstehenden Festlegung von $\mathbf{L}^*_n(x)$, $\mathbf{S}^*_n(x,y)$ und $\mathbf{H}^*_w(x)$ übernehmen nun weitgehend neue Formeln $\mathbf{Prod}_n(x,y,z)$ von T die vergleichbare Rolle von $\mathbf{M}_n(x,y,z)$ bei der Definition der Formeln $\mathbf{I}_n(x), \ldots, \mathbf{H}_w(x)$ in Abschnitt 5. Diese Formeln $\mathbf{Prod}_n(x,y,z)$ von T gestatten es dabei, die Multiplikation natürlicher Zahlen $< 2^{2^{2^{n+1}}}$ in T zu formalisieren, und zwar erneut als $O(n)$-längenbeschränkte und $POLYLIN$-konstruierbare Formeln.

Lemma 3.6.1. *T und $T^{((M))}$ seien wie in diesem Abschnitt vorausgesetzt.*
Es existiert eine Funktion $g : \mathbb{N}_0 \to \mathbb{N}_0$ so, daß für alle $n \in \mathbb{N}_0$

$$g(n) \geq 2^{2^{2^{n+1}}} \tag{3.118}$$

gilt und weiters damit für alle $n \in \mathbb{N}_0$ Formeln $\mathbf{Prod}_n(x,y,z)$ von T existieren, die einerseits die Eigenschaft

$$\vdash_T \mathbf{Prod}_n(x,y,z) \leftrightarrow [\![\, x,y,z, \in \mathbb{N}_0,\ x,y,z < g(n),\ x \cdot y = z \,]\!] \tag{3.119}$$

(für alle $n \in \mathbb{N}_0$) erfüllen und bezüglich denen für die Familie $\left\{\mathbf{Prod}_n(x,y,z)^{((M))}\right\}_{n\in\mathbb{N}_0}$ die (Längen- und Konstruierbarkeits-) Bedingungen (A) aus Definition 3.3.5 gültig sind. (Die Formeln $\mathbf{Prod}_n(x,y,z)$ erlauben die Beschreibung der Multiplikation auf $\mathbb{N}_0$ in T bis Zahlen der Größe $g(n)$ durch $O(n)$-längenbeschränkte und in (bzgl. der Eingabe $(n)_{10}$ zu verstehendem) POLYLIN-Aufwand herstellbaren Formeln von T).

[Dieser Satz entspricht Theorem 12, p.20, in [FiR74].]

Beweis. (1) Die Funktion

$$g(n) := \prod_{\substack{p\in\mathbb{P},\\ p<2^{2^{n+2}}}} p \tag{3.120}$$

erfüllt (3.118) (und kann daher im weiteren als Ausgangspunkt für die spätere Konstruktion von Formeln $\mathbf{Prod}_n(x,y,z)$ mit wie im Lemma in Beziehung zu g behaupteten Eigenschaften dienen):

Zum Nachweis dieser Behauptung kann eine schwächere Version des Primzahlsatzes $\lim\limits_{x\to\infty} \pi(x)\dfrac{\ln x}{x} = 1$ (bzw. $\pi(x) \sim \frac{x}{\ln x}$) (wobei $\pi(x) :=$ Anzahl der Primzahlen $\leq x$ (für $x \in \mathbb{R}$)) verwendet werden, und zwar ein Satz von Tschebyscheff, wonach es konstante positive Zahlen $a, b \in \mathbb{R}^+$ gibt, sodaß

$$a \cdot \frac{x}{\ln x} < \pi(x) < b \cdot \frac{x}{\ln x} \qquad (x \in \mathbb{R}^+,\ x \geq 2) \tag{3.121}$$

gilt. Nach [NZ76], Band II, S. 242, (und einem dort dargestellten Beweis dafür) können a und b *jedenfalls* als

$$a := \frac{\ln 2}{4} \qquad \text{und} \qquad b := 32 \cdot \ln 2 \tag{3.122}$$

gewählt werden; nach [NZ76] handelt es sich dabei aber *nicht* um besonders gute oder gar um nahezu-bestmögliche Werte für a und b in Beziehung zur Gültigkeit von

(3.121) (im Vergleich mit dem Supremum aller für a in (3.121) möglichen bzw. dem Infimum aller für b bzgl. (3.121) zulässigen reellen Zahlen).

Wegen (3.121) und (3.122) kann nun die Anzahl der Primzahlen bis höchstens $2^{2^{n+2}}$ durch

$$\pi(2^{2^{n+2}}) > \frac{\ln 2}{4} \cdot \frac{2^{2^{n+2}}}{2^{n+2} \cdot \ln 2} = 2^{2^{n+2}-n-4} \qquad (n \in \mathbb{N}_0) \tag{3.123}$$

abgeschätzt werden. Durch Induktion läßt sich nun leicht

$$2^{2^{n+2}-n-4} > 2^{2^{n+1}} \qquad (\text{für } n \in \mathbb{N},\ n \geq 2)$$

nachprüfen, woraus mit (3.123)

$$\pi(2^{2^{n+2}}) > 2^{2^{n+1}} \qquad (\text{für } n \in \mathbb{N},\ n \geq 2) \tag{3.124}$$

folgt. Da (3.124) auch für $n = 0$ und $n = 1$ gilt (wie sich einfach nachprüfen läßt), gilt damit sogar

$$\pi(2^{2^{n+2}}) > 2^{2^{n+1}} \qquad (\text{für alle } n \in \mathbb{N}_0)\,. \tag{3.125}$$

Für g wie in (3.120) ergibt sich nun danach insgesamt

$$g(n) = \prod_{\substack{p \in \mathbb{P}\,, \\ p < 2^{2^{n+2}}}} p \; > 2^{\pi(2^{2^{n+2}})} \underset{(3.125)}{>} 2^{2^{2^{n+1}}} \qquad (n \in \mathbb{N}_0)\,, \tag{3.126}$$

also die für g gewünschte Abschätzung (in sogar schärferer Gestalt).

(2) Zur Konstruktion von Formeln $\mathbf{Prod}_n(x, y, z)$ in T zu g wie in (1) definiert und mit den im Lemma behaupteten Eigenschaften werden im folgenden (dabei weiter den Beweisweg in [FiR74] auf p. 20, 21 beschreitend) Hilfsformeln $\mathbf{P}_n(x)$, $\mathbf{Res}_n(x, y, z)$ und $\mathbf{G}_n(x)$ (für jedes $n \in \mathbb{N}_0$) benötigt, für die die zugehörigen Familien den Bedingungen (A) genügen und die weiters den folgenden inhaltlichen Forderungen genügen:

$$\vdash_T \mathbf{P}_n(x) \leftrightarrow \left[\!\left[\, x \in \mathbb{N},\ x < 2^{2^n},\ x \text{ ist Primzahl} \,\right]\!\right]\,, \tag{3.127}$$

Für jedes $a \in \mathbb{N}_0$ gilt im Modell $\mathfrak{N}$ von T die Formel:

$$\mathbf{Res}_n(\mathbf{i}_a, y, z) \leftrightarrow \left[\!\left[\, y, z \in \mathbb{N}_0,\ 2 \leq y < 2^{2^n},\ a \equiv_y z,\ z < y \,\right]\!\right]$$

(wobei $\mathbf{i}_a$ als „Name“ von a in $L(\mathfrak{N})$ für das „Individuum“ $a \in |\mathfrak{N}| = \mathbb{N}_0$ steht)\,,

$\vdash_T \mathbf{G}_n(x) \leftrightarrow x = \underline{\underline{g(n)}}$\,.

$\mathbf{P}_n(x)$ beschreibt dabei also in T die Eigenschaft, Primzahl $< 2^{2^n}$ zu sein, $\mathbf{G}_n(x)$ beschreibt inhaltlich $g(n)$ als Formel in T, und $\mathbf{Res}_n(x,y,z)$ dient zur (beschränkten) Kongruenzresiduenbildung in T.

Diese Formeln können nun mit Hilfe der in Abschnitt 5 konstruierten Formeln $\mathbf{M}_n(x,y,z)$ und $\mathbf{I}_n(x)$ einfach formuliert werden, sodaß sowohl die inhaltlichen Forderungen als auch die Längen- und Konstruierbarkeitsbedingung (A) erfüllt ist. Und zwar könnte $\mathbf{P}_n(x)$ für $n \in \mathbb{N}_0$ von der Gestalt wie

$$\begin{cases} 0 = 1 & \dots \quad n = 0 \\ \mathbf{M}_n(x,1,x) \;\&\; \neg\, x = 1 & \\ \quad \&\; \forall y \forall z \left(\mathbf{M}_n(y,z,x) \;\rightarrow\; y = 1 \;\vee\; y = x \right) & \dots \quad n \in \mathbb{N}_0,\, n \geq 1 \end{cases} \tag{3.128}$$

gewählt werden, $\mathbf{Res}_n(x,y,z)$ von der Gestalt wie

$$\underline{\underline{2}} \leq y \;\&\; \exists w_1 \exists w_2 \left(\mathbf{M}_n(y,w_2,w_1) \;\&\; x = z + w_1 \right) \;\&\; z < y$$

und davon ausgehend $\mathbf{G}_n(x)$ wie

$$\begin{aligned} &\forall y \left[\mathbf{P}_{n+2}(y) \;\rightarrow\; \exists w \left(\neg\, w = 0 \;\&\; \mathbf{M}_{n+2}(y,w,x) \right) \right] \\ &\;\&\; \forall x' \left\{ \forall y \left[\mathbf{P}_{n+2}(y) \;\rightarrow\; \exists w \left(\neg\, w = 0 \;\&\; \mathbf{M}_{n+2}(y,w,x') \right) \right] \right. \\ &\qquad \left. \rightarrow\; x \leq x' \right\} . \end{aligned}$$

(: $g(n)$ ist die *kleinste* natürliche Zahl, die durch alle $p \in \mathbb{P}$ mit $p < 2^{2^{n+2}}$ teilbar ist)[53]. Unter Benutzung der Eigenschaften von $\mathbf{I}_n(x)$ und $\mathbf{M}_n(x,y,z)$ kann leicht eingesehen werden, daß die obigen, für $\mathbf{P}_n(x)$, $\mathbf{Res}_n(x,y,z)$ und $\mathbf{G}_n(x)$ (vorläufig) gewählten Formeln den anfangs geforderten inhaltlichen Bedingungen genügen. Allerdings treten in diesen auch Ordnungssymbole auf, die nicht in $L(T)$ vorkommen (die allerdings durch den Übergang zu Translationsformeln zwischen (etwa) $PreAN$ (das definitorische Erweiterung von $PreAN_1$ ist) und $PreAN_1$ leicht eliminiert werden können). und weiters ist auch wegen der geforderten Gültigkeit der Bedingungen (A) eine etwas vorsichtigere Wahl dieser Formel sinnvoll. Diese Überlegung führt im

[53] Für diese Festlegung von $\mathbf{G}_n(x)$ ist das Vorhandensein eines Ordnungssymbol $<$ bzw. $\leq$ in T entscheidend und eine analoge Definition ist in TAZ daher nicht möglich. Es ist sogar denkbar, daß diese Formel $G(x)$—mit den hier zusätzlich immer geforderten Längen- und Konstruierbarkeitseigenschaften—in TAZ überhaupt nicht definierbar ist. – Jedenfalls scheitert eine direkte Übertragung dieses Beweises auf TAZ zum ersten Mal an dieser Stelle. (Bei der Definition von $\mathbf{Res}_n(x,y,z)$ kann das Symbol $<$ ja—im dafür nur benötigten, eingeschränkten Umfang seiner inhaltlichen Bedeutung—sehr leicht unter Verwendung von Formeln $\mathbf{M}_n(x,y,z)$ ausgedrückt werden.)

Fall von $\mathbf{Res}_n(x,y,z)$ auf die etwas aufwendige Setzung

$$\begin{aligned}
&\mathbf{Res}_n(x,y,z) ::= \\
&\quad \exists w\,(\, y = \underline{\underline{2}} + w\,) \\
&\quad \&\ \exists w_1\,\exists w_2\,\{\,\exists y_0\,[\, y_0 = y\ \& \\
&\qquad\qquad \exists x\,\exists y\,\exists z\,\big(x = y_0\ \&\ y = w_2\ \&\ z = w_1\ \&\ \mathbf{M}_n(x,y,z)\big)\,] \\
&\qquad\qquad \&\ x = z + w_1\,\} \\
&\quad \&\ \exists w\,(\, y = z + w + 1\,)\,,
\end{aligned}$$

die es allerdings erlaubt, direkt auf die Definition von $\mathbf{M}_n(x,y,z)$ in Abschnitt 5 zurückzugreifen und auch deren Herstellung bei der Konstruktion von $\mathbf{Res}_n(x,y,z)$ als Teilprogramm in Dienst stellen zu können (womit die Erfülltheit der Bedingungen (A) an $\{\mathbf{Res}_n(x,y,z)^{((M))}\}_{n\in\mathbb{N}_0}$ mit $\mathbf{Res}_n(x,y,z)$ wie oben definiert—damit mehr oder weniger—direkt ablesbar ist). – Gleichartige exakte Setzungen können nun auch für $\mathbf{P}_n(x)$ und $\mathbf{G}_n(x)$ durchgeführt werden (diese liegen aber nahe und unterbleiben hier deshalb).

(3) Unter Zuhilfenahme der Formeln $\mathbf{P}_n(x)$, $\mathbf{Res}_n(x,y,z)$ und $\mathbf{G}_n(x)$ aus (2) kann nun für jedes $n \in \mathbb{N}_0$ eine Formel $\mathbf{Prod}_n(x,y,z)$ mit wie im Lemma behaupteten Eigenschaften gefunden werden:

Hierfür ist wegen der Wahl von $g(n)$ wie in (3.120) ausschlaggebend, daß für drei Zahlen $x,y,z \in \mathbb{N}_0$ mit $x,y,z < g(n)$ das Vorliegen der Eigenschaft $x \cdot y = z$ nach dem Chinesischen Restsatz durch die Überprüfung der Aussagen $[\,[x]_p \cdot [y]_p\,]_p = [z]_p$ für alle $p \in \mathbb{P}$ mit $p < 2^{2^{n+2}}$ ($[\tilde{x}]_m :=$ Restklasse von $\tilde{x}$ bei der Division durch m ($m \in \mathbb{N}$, $m \geq 2$)) geschehen kann; d.h. weil gilt:

$$\begin{aligned}
&\big(\forall x,y,z \in \mathbb{N}_0, x,y,z < g(n)\big) \\
&\quad \big\{\, x \cdot y = z \iff \big(\forall p \in \mathbb{P},\, p < 2^{2^{n+2}}\big)\big(\,[\,[x]_p \cdot [y]_p\,]_p = [z]_p\big)\,\big\}\,.
\end{aligned}$$

Diese Aussage kann zur Grundlage einer Definition von $\mathbf{Prod}_n(x,y,z)$ entlang von

$$\begin{aligned}
&\exists x'\,\big(\,\mathbf{G}_n(x')\ \&\ x < x'\ \&\ y < x'\ \&\ z < x'\,\big) \\
&\ \&\ \forall y'\,[\,\mathbf{P}_{n+2}(y')\ \rightarrow \\
&\qquad \exists x_0\,\exists y_0\,\exists z_0\,\exists z_1 \\
&\qquad\quad \big(\ \mathbf{Res}_{n+2}(x,y',x_0)\ \&\ \mathbf{Res}_{n+2}(y,y',y_0)\ \&\ \mathbf{Res}_{n+2}(z,y',z_0) \\
&\qquad\quad\ \ \&\ \mathbf{M}_{n+2}(x_0,y_0,z_1)\ \&\ \mathbf{Res}_{n+2}(z_1,y',z_0)\,\big)\,]
\end{aligned}$$

werden; dabei müßten, um zu einer genauen und vorsichtigen Setzung für die Formeln $\mathbf{Prod}_n(x,y,z)$ zu gelangen, (a) die atomaren Formeln mit Ordnungssymbol $<$

durch Formeln von $L(T)$ ersetzt werden, (b) x' und y' durch dezimal indizierte Variablen ausgetauscht werden, (c) wie für $\mathbf{Res}_n(x,y,z)$ in (2) zusätzliche Teilformeln eingebaut werden, sodaß direkt auf $\mathbf{G}_n(x)$, $\mathbf{P}_{n+2}(x)$, $\mathbf{M}_{n+2}(x,y,z)$ und $\mathbf{Res}_{n+2}(x,y,z)$ verwiesen werden kann. Es ist jedoch klar, auf welche Weise das analog, wie für $\mathbf{Res}_n(x,y,z)$ in (2) durchgeführt, hier geschehen kann und unterbleibt hier v.a. auch deshalb, weil eine so präzisierte Setzung für $\mathbf{Prod}_n(x,y,z)$ zur Verständlichkeit der Konstruktion dieser Formel wegen des damit verbundenen Aufwands nichts weiteres mehr beitragen kann. – Die Erfülltheit der Bedingungen (A) für $\{\mathbf{Prod}_n{}^{((M))}(x,y,z)\}_{n\in\mathbb{N}_0}$ kann allerdings nur von einer auf beschriebene Art verfeinerten Wahl von $\mathbf{Prod}_n(x,y,z)$ direkt abgelesen werden (d.h. genau: die einfache Zurückführbarkeit der Längen- und Konstruierbarkeitsbedingungen (A) an $\{\mathbf{Prod}_n{}^{((M))}(x,y,z)\}_{n\in\mathbb{N}_0}$ auf die entsprechenden, zuvor und früher begründeten Eigenschaften von $\mathbf{G}_n(x)$, $\mathbf{P}_{n+2}(x)$, $\mathbf{M}_{n+2}(x,y,z)$ und $\mathbf{Res}_{n+2}(x,y,z)$).

□

Ausgehend von den Formeln $\mathbf{Prod}_n(x,y,z)$ $(n\in\mathbb{N}_0)$, die in T die Multiplikation natürlicher Zahlen $< g(n)$ beschreiben, können nun auf analoge Weise zum Vorgehen in Abschnitt 5 Formeln $\mathbf{Pow}^*_n(x,y,z)$ in T konstruiert werden, die die Exponentiation $z=y^x$ für natürliche Zahlen $z,y<g(n)$ und natürliche Exponenten $x<2^{2^n}$ beschreiben (und entsprechenden Längen- und Konstruierbarkeitsbedingungen, wie hier immer betrachtet, genügen). Diese Formeln $\mathbf{Pow}^*_n(x)$ sollen der inhaltlichen Forderung

$$\vdash_T \mathbf{Pow}^*_n(x,y,z) \leftrightarrow [\![\, x,y,z\in\mathbb{N}_0,\ x<2^{2^n},\ y,z<g(n),\ z=y^x \,]\!]$$

genügen und weiters soll $\{\mathbf{Pow}^*_n(x,y,z)\}_{n\in\mathbb{N}_0}$ die Bedingungen (A) erfüllen. Die Konstruktion von $\mathbf{Pow}^*_n(x,y,z)$ kann völlig analog zur Konstruktion von $\mathbf{Pow}_n(x,y,z)$ in Abschnitt 5 mit Hilfe der Formeln $\mathbf{E}_{k,n}(x,y,z,x_0,y_0,z_0)$ durchgeführt werden, wobei nun aber Formeln $\mathbf{E}^*_{k,n}(x,y,z,x_0,y_0,z_0)$ mit der inhaltlichen Eigenschaft

$$\vdash_T \mathbf{E}^*_{k,n}(x,y,z,x_0,y_0,z_0) \leftrightarrow [\![\, x,y,z\in\mathbb{N}_0,\ x<2^{2^k},\ y,z<g(n),\ z=y^x \,]\!] \\ \&\ \mathbf{Prod}_n(x_0,y_0,z_0)$$

$(n,k\in\mathbb{N}_0,\ k\le n)$ dabei verwendet werden, in denen statt den Formeln $\mathbf{M}_n(x,y,z)$ jeweils $\mathbf{Prod}_n(x,y,z)$ ins Spiel kommen. Die rekursive Festlegung von $\mathbf{E}^*_{k,n}(x,y,z,x_0,y_0,z_0)$ für $k\in\mathbb{N}_0$, $k\le n$ (zu gegebenem $n\in\mathbb{N}_0$) kann völlig analog zum Beweis von Satz 3.5.2 geschehen (wobei an einer Stelle, eine Übertragung von (3.104) betreffend, eine entsprechend auftretende Konjunktionsformel $\mathbf{E}^*_{k,n}(0,1,1,z,1,1)$ nun sogar überflüssig wäre und weggelassen werden könnte; eine solche Entfernung einer Formel zieht dann auch die Weglassung einer Konjunktionsformel (bzw. -zeile) in einem Analogon zu (3.105) als dann präzisierter Festlegung der Formeln $\mathbf{E}^*_{k+1,n}(x,y,z,x_0,y_0,z_0)$ (im Induktionsschritt $k\to k+1$ für $k+1\le n$, $k,n\in\mathbb{N}_0$) nach sich.)

Daran anschließend kann $\mathbf{Pow}^*_n(x,y,z)$ dann letztlich durch

$$\mathbf{Pow}^*_n(x,y,z) ::= \quad \exists x_0\, \exists y_0\, \exists z_0 \big(x_0 = 0 \;\&\; y_0 = 0 \;\&\; z_0 = 0 \;\&\; \mathbf{E}^*_{n,n}(x,y,z,x_0,y_0,z_0) \big)$$

für alle $n \in \mathbb{N}_0$ analog zu (3.101) festgesetzt werden.

Ausgehend von den bisher festgelegten Formeln können nun Definitionen für $\mathbf{L}^*_n(x)$, $\mathbf{S}^*_n(x,y)$, und $\mathbf{H}^*_w(x)$ mit (3.113), (3.114) und (3.115) (für alle $n \in \mathbb{N}_0$, $w \in BW0$, $|w| = n \in \mathbb{N}$) und den entsprechenden Längen- und Konstruierbarkeitseigenschaften entlang der (vorläufigen) Setzungen

$$\exists x_0 \, \big(\mathbf{J}^*_{n+1}(x_0) \;\&\; \mathbf{Pow}^*_{n+2}(x_0, \underline{\underline{2}}, x_1) \;\&\; x < x_1 \big) \tag{3.129}$$

für $\mathbf{L}^*_n(x)$ und

$$\begin{aligned} &\mathbf{L}^*_n(x) \;\&\; \mathbf{I}^*_n(y) \\ &\;\&\; \exists z\, \exists w\, \exists y_0\, \exists y_1\, \exists w \, \big(\mathbf{Pow}^*_{n+1}(y, \underline{\underline{2}}, y_0) \;\&\; y_1 = y_0 + y_0 \;\&\; y_0 \leq z \\ &\qquad\qquad \;\&\; z < y_1 \;\&\; \mathbf{Prod}_{n+2}(y_1, w, w_1) \;\&\; x = z + w_1 \big) \end{aligned} \tag{3.130}$$

für $\mathbf{S}^*_n(x,y)$ [wobei (3.130) analog zu (3.108) und unter Verwendung von (3.107) konstruiert wurde; nähere Überprüfung zeigt, daß hierbei $\mathbf{Prod}_{n+2}(y_1,w,w_1)$ durch $\mathbf{Prod}_{n+1}(y_1,w,w_1)$ ersetzt werden könnte] und

$$\begin{aligned} \mathbf{L}^*_n(x) \;\&\; \exists x_0\, \exists z \, \big\{ &\mathbf{K}_w(x_0) \;\&\; \mathbf{J}^*_n(z) \\ &\;\&\; \forall y \, \big[\, y < z \rightarrow \; \big(\mathbf{S}^*_n(x,y) \leftrightarrow \mathbf{S}^*_n(x_0,y) \big) \, \big] \, \big\} \end{aligned} \tag{3.131}$$

für $\mathbf{H}^*_w(x)$ für alle $n \in \mathbb{N}_0$ und $w \in BW0$ mit $|w| = n$ weiter präzis gemacht werden. Hierbei müssen (a) die Ordnungssymbole $<$ und $\leq$ durch den Übergang zu entsprechenden Translationsformeln beseitigt werden, und muß (b) durch logische Umformungen zu äquivalenten Formeln übergegangen werden, die direkt auf früher festgelegte Formeln wie z.B. $\mathbf{Prod}_{n+2}(x,y,z)$ oder $\mathbf{S}^*_n(x,y)$ verweisen und nicht auf Instanzen dieser Formeln. Da solche logischen Umformungen—früheren Beispielen folgend—allerdings leicht durchführbar sind und naheliegen, kann schon an dieser Stelle eingesehen werden, daß hierdurch präzise Festlegungen von $\mathbf{L}^*_n(x)$, $\mathbf{S}^*_n(x,y)$ und $\mathbf{H}^*_w(x)$ für alle $n \in \mathbb{N}_0$ und $w \in BW0$ mit $|w| = n$ entstehen, für die (3.113)–(3.115) gelten und die die weiteren an diese Formeln (zu Beginn dieses Abschnitts) geknüpften Bedingungen erfüllen.

Es ist damit nun insgesamt gelungen, für alle $n \in \mathbb{N}_0$ und $w \in BW0$ mit $|w| = n \in \mathbb{N}$ Formeln $\mathbf{I}^*_n(x)$, $\mathbf{J}^*_n(x)$, $\mathbf{L}^*_n(x)$, $\mathbf{S}^*_n(x,y)$ und $\mathbf{H}^*_w(x)$ mit (3.111)–(3.115) sowie den zugehörigen Längen- und Konstruierbarkeitsbedingungen (A) bzw. (B) aus Definition 3.3.5 zu finden bzw. zu beschreiben, wie diese exakt festgelegt sein können. Damit ist für T, $T^{((M))}$ wie angenommen und $f(n) = 2^{2^n}$ die Annahme von Satz 3.4.4 erfüllt. Wie zu Beginn dieses Abschnitts (bzw. analog zu Beginn des Abschnitts 5) erläutert, folgt daraus mit Sätzen aus dem Abschnitt 4 die Behauptung von Satz 3.1.1. Dieser Satz ist damit bewiesen.

3.7 Anwendung der Methoden und einer Idee aus [FiR74] zur Erzielung von $TAZ \notin NTime(2^{2^{cn}})$ für ein $c \in \mathbb{R}$, $c > 0$

T sei in diesem Abschnitt entweder die Theorie TAZ aus Abschnitt 2.1 (Definition 2.1.1) oder die dazu äquivalente, semantisch definierte Theorie $Th(\langle\mathbb{Z}; 0, 1, +\rangle)$ und L deren Sprache (also erneut wie in den Abschnitten 5 und 6 eine Sprache einer Theorie 1. Ordnung mit den Konstantensymbolen 0 und 1 sowie weiters noch mit dem zweistelligen Funktionssymbol + als deren nichtlogische Symbole). $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ sei die als System formaler Sprachen mit informatisch-sinnvoller Formelsyntax dargestellte Theorie T, wobei sich dieses erneut wie in Abschnitt 5 und in Abschnitt 6 mit dem Verweis auf Grammatik 2.6.1 und deren Terminalalphabet Σ durch die Setzungen (3.79) (jedoch bzgl. T wie hier vorausgesetzt) präzisieren ließe. (Erneut ist das Vorhandensein des logischen Symbols $\leftrightarrow$ in $T^{((M))}$ bzw. in $\Sigma_{T^{((M))}}$ (etwa wie das in der Präzisierung hier der Fall ist) nicht zwingend erforderlich, obwohl hier große Teile des Beweises *vorerst*[54] ausdrücklich davon Gebrauch machen.)

Im folgenden sei hier außerdem das Standardmodell für TAZ mit $\mathfrak{Z} := \langle\mathbb{Z}; 0, 1, +\rangle$ bezeichnet. Weiters werden zur Beschreibung von Eigenschaften der hier zu entwickelnden Formeln in Beziehung zu $\mathfrak{Z}$ wieder (wie schon in Abschnitt 6 vereinzelt und im Satz 3.4.4 in Abschnitt 4) „Namen" $\mathbf{i}_a$ aus $L(\mathfrak{Z})$ für Zahlen („Individuen") $a \in \mathbb{Z} = |\mathfrak{Z}|$ verwendet; $L(\mathfrak{Z})$ ist dabei die um alle Namen $\mathbf{i}_a$ (für $a \in \mathbb{Z}$) als zusätzliche Konstantensymbole erweiterte Sprache L. Diese Bezeichnungsweise korrespondiert mit der in [Shoe67] zur Beschreibung der Gültigkeit von Formeln einer Sprache $\tilde{L}$ in Strukturen für $\tilde{L}$ eingeführten Bezeichnungsweise.

Die in diesem Abschnitt ebenso wie für RA in Abschnitt 5 und für $PreAN$ in Abschnitt 6 nun für T ($\underset{\text{z.B}}{=} TAZ$) ebenso wie dort durch die Verwendung von Methoden für allgemeine Komplexitätsbeweise aus [FiR74], die in Abschnitt 4 dargestellt bzw. präzisiert wurden, zu zeigende Komplexitätsaussage besitzt dabei nun die folgende, zu den Sätzen Satz 3.1.1 und Satz 3.1.3 völlig analoge Gestalt:

[54] Vgl. jedoch Abschnitt (6) im Beweis von Satz 3.7.2.

Satz 3.7.1. *T wie hier vorausgesetzt (eine zu TAZ äquivalente Theorie 1. Ordnung); $T^{((M))}=(\Sigma_{T^{((M))}}, Fo_{T^{((M))}}, Thm_{T^{((M))}})$ die als System formaler Sprachen mit informatisch-sinnvoller Formelsyntax dargestellte Theorie T.*

Dann gilt: Es existiert ein $c \in \mathbb{R}$, $c > 0$ so, daß $2^{2^{cn}}$ eine untere Schranke für die Entscheidungskomplexität von T bzgl. nichtdeterministischer Turing-Rechenzeit ist. Darüber hinaus kann $c \in \mathbb{R}$, $c > 0$ so gewählt werden, daß

$$Thm_{T^{((M))}},\ \text{co}-Thm_{T^{((M))}} \notin NTime(2^{2^{cn}})$$

gilt.

Der *Beweis* dieses Satzes erstreckt sich über den restlichen Teil dieses Abschnitts.

Auf eine völlig analoge Weise wie zu Beginn der Abschnitte 5 und 6 läßt sich nun durch eine Argumentation mittels Sätzen aus dem Abschnitt 4 der hier noch zu erbringende Beweis von Satz 3.7.1 auf einen Nachweis der Erfülltheit der Annahme von (jetzt:) Satz 3.4.6 für T, $T^{((M))}$ und $f(n) := 2^{2^n}$ reduzieren. Also auf den Nachweis der Existenz von Formeln $\mathbf{I}_n^{**}(x)$, $\mathbf{J}_n^{**}(x)$, $\mathbf{S}_n^{**}(x,y)$ und $\mathbf{H}_w^{**}(x)$ für alle $n \in \mathbb{N}_0$ und $w \in BW0$, sodaß für alle $n \in \mathbb{N}_0$ und $w \in BW0$ mit $|w| = n$ die Aussagen

$$\vdash_T \mathbf{I}_n^{**}(x) \leftrightarrow \left[\!\!\left[x \in \mathbb{N}_0,\ x < 2^{2^{n+1}} \right]\!\!\right]; \tag{3.132}$$

$$\vdash_T \mathbf{J}_n^{**}(x) \leftrightarrow x = \underline{\underline{2^{2^n}}}\ ^{55}; \tag{3.133}$$

Für alle $a \in \mathbb{Z}$ ist in $\mathfrak{Z}$ die folgende Formel gültig:

$$\mathbf{S}_n^{**}(\mathbf{i}_a, y) \leftrightarrow \left[\!\!\left[y \in \mathbb{N}_0,\ y < 2^{2^{n+1}},\ (Bw_2(a))(y) = 1 \right]\!\!\right]; \tag{3.134}$$

Für alle $a \in \mathbb{Z}$ gilt:

$$\mathbf{H}_w^{**}(\mathbf{i}_a) \text{ ist gültig in } \mathfrak{Z} \iff$$

$$(Bw_2(a))(0) \circ \ldots \circ (Bw_2(a))(2^{2^n}-1) = w \circ 0^{2^{2^n}-n} \tag{3.135}$$

gelten und weiters die zugehörigen Formelfamilien den Bedingungen (A) bzw. (B) aus Definition 3.3.5 genügen. (Hierin sind diese Formeln gegenüber ihrem Auftreten in Satz 3.4.6 doppelt durch * indiziert worden, da bei ihrer Definition erneut auf entsprechend bezeichnete, in den Abschnitten 5 und 6 entwickelte Formeln zurückgegriffen wird und deshalb eine Unterscheidung in der Bezeichnung dieser Formeln sinnvoll ist).

Für $\mathbf{I}_n^{**}(x)$ und $\mathbf{J}_n^{**}(x)$ können nun direkt $\mathbf{I}_n^{*}(x)$ und $\mathbf{J}_n^{*}(x)$ aus (3.116) und (3.117) herangezogen werden bzw. die neuen Formeln diesen früheren gleichgesetzt werden (dies ist möglich, da $\mathbf{I}_n^{*}(x)$ und $\mathbf{J}_n^{*}(x)$ unabhängig von der Definierbarkeit der Ordnung in $PreAN_1$ gewählt wurden und diese Formeln die selben inhaltlichen Eigenschaften (3.111)

[55] Diese abkürzende Schreibweise für auf Zahlen aus $\mathbb{N}_0$ verweisende Terme aus Definition 2.1.1 wird hier wieder (wie auch schon in den früheren Abschnitten) einige Male benützt werden.

und (3.112) auch schon in $T = RA$ ausdrücken, in einer Theorie also, in der kein Ordnungssymbol vorhanden ist).

Für die Definition von $\mathbf{S}_n^{**}(x,y)$ und $\mathbf{H}_w^{**}(x)$ (für $n \in \mathbb{N}_0$ und $w \in BW0$) kann nun jedoch nicht mehr *direkt* auf die entsprechenden Formeln aus Abschnitt 5 und Abschnitt 6 zurückgegriffen werden, da hier eine andere Kodierungsfunktion für Binärwörter, nämlich die Funktion Bw_2 aus (3.42) verwendet wird. Die Idee zur Verwendung dieser Kodierungsfunktion stammt aus [FiR74], p. 23, unten, p. 24, wo damit eine Möglichkeit skizziert wird, wie eine 3-fach-exponentiell-lineare untere Schranke für $MULT$ bzw. SkA bzw. $Th(\langle \mathbb{N}; 0, 1, \cdot \rangle)$ mit ähnlichen Methoden wie den in ihrer Arbeit vorgestellten beweisbar ist.

Für den Beweis hier sind aber die Formeln $\mathbf{M}_n(x,y,z)$ aus Satz 3.5.1 wesentlich, deren inhaltliche Eigenschaft (3.86) für T wie hier angenommen erhalten bleibt; ebenso können die sich auf Primzahlen $< 2^{2^n}$ beziehenden Formeln $\mathbf{P}_n(x)$ mit (3.127) und der sich einfach aus $\mathbf{M}_n(x,y,z)$ herleitenden Gestalt (3.128) hierher übernommen werden. Damit weiter im Zusammenhang stehen hier benötigte Formeln $\mathbf{PT}_n(z,x)$ mit der Eigenschaft, daß für alle $a \in \mathbb{Z}$ und $n \in \mathbb{N}_0$

$$\mathbf{PT}_n(z, \mathbf{i}_a) \leftrightarrow [\![\, z \in \mathbb{N},\ z < 2^{2^n},\ z \text{ ist Primzahl},\ a \neq 0,\ z \text{ teilt } a \,]\!] \tag{3.136}$$

in $\mathfrak{Z}$ gültig ist. Die Formeln $\mathbf{PT}_n(z,x)$ drücken also die Eigenschaft von zwei Zahlen z und x aus, daß z Primteiler $< 2^{2^n}$ von x ist. $\mathbf{PT}_n(z,x)$ kann jeweils von der Gestalt

$$\mathbf{P}_n(z)\ \&\ \exists w \left(\neg\, w = 0\ \&\ \mathbf{M}_n(z,w,x) \right) \tag{3.137}$$

gewählt werden; bzgl. den so weitergehend präzis gemachten Formeln $\mathbf{PT}_n(x)$ erfüllt $\left\{ \mathbf{PT}_n(z,x)^{((M))} \right\}_{n \in \mathbb{N}_0}$ klarerweise auch die Bedingungen (A) aus Definition 3.3.5. – Zusätzlich zu diesen Formeln tritt noch eine durch $x \leq_n y$ abgekürzte Formel auf, die die $\leq$-Eigenschaft von natürlichen Zahlen $< 2^{2^n}$ in T ausdrückt und die durch

$$x \leq_n y \leftrightarrow [\![\, x, y \in \mathbb{N}_0,\ x, y < 2^{2^n},\ x \leq y \,]\!] \tag{3.138}$$

beschrieben und durch eine Festlegung der Gestalt

$$\mathbf{M}_n(x,0,0)\ \&\ \mathbf{M}_n(y,0,0)\ \&\ \exists z \left(\mathbf{M}_n(z,0,0)\ \&\ y = x + z \right) \tag{3.139}$$

gegeben sei. – Ähnlich dazu sei weiters auch die Formel $x <_n y$ entlang von

$$\mathbf{M}_n(x,0,0)\ \&\ \mathbf{M}_n(y,0,0)\ \&\ \exists z \left(\mathbf{M}_n(z,0,0)\ \&\ y = x + z + 1 \right) \tag{3.140}$$

festgelegt.

Satz 3.7.2. *T, $T^{((M))}$ wie in diesem Kapitel vorausgesetzt.*

Es existieren für alle $n \in \mathbb{N}_0$ Formeln $\mathbf{PZ}_{n+2}(z,y)$ in T so, daß für alle $n \in \mathbb{N}_0$

$$\vdash_T \mathbf{PZ}_{n+2}(z,y) \leftrightarrow \Big[\!\Big[z,y \in \mathbb{N}_0,\ z < 2^{2^{n+2}},\ y < 2^{2^{n+1}},\ z \text{ ist die } (y+1)\text{-te Primzahl} \Big]\!\Big]^{56} \tag{3.141}$$

gilt und weiters die Familie $\{\mathbf{PZ}_{n+2}(z,y)\}_{n\in\mathbb{N}_0}$ die Bedingungen (A) aus Definition 3.3.5 erfüllt.

Beweis. T, $T^{((M))}$ wie in diesem Kapitel vorausgesetzt. In diesem Beweis wird an einigen Stellen zuerst verwendet, daß $\leftrightarrow$ in der Sprache von $T^{((M))}$ enthalten ist (das ist nach Voraussetzung über $T^{((M))}$ der Fall). In Punkt (6) wird jedoch kurz erläutert, wie das Ergebnis auch auf den möglichen Fall übertragen werden könnte, wenn $\leftrightarrow$ nicht als Symbol der Formelsprache $Fo_{T^{((M))}}$ zugelassen wäre.

(1) Es soll bemerkt werden, daß die inhaltliche Forderung (3.141) an $\mathbf{PZ}_{n+2}(z,y)$ für alle $n \in \mathbb{N}_0$ sinnvoll ist, da nach (3.125) für alle $n \in \mathbb{N}_0$ die Aussage $\pi(2^{2^{n+2}}) > 2^{2^{n+1}}$ gilt, woraus unmittelbar

$$p_{2^{2^{n+1}}} < 2^{2^{n+2}} \qquad (\text{für alle } n \in \mathbb{N}_0)$$

(: $p_{\tilde{n}}$ bezeichnet dabei die $\tilde{n}$-te Primzahl bzw. die $\tilde{n}$-t-kleinste Primzahl) folgt.

(2) Bei der Konstruktion der Formeln $\mathbf{PZ}_{n+2}(z,y)$ für $n \in \mathbb{N}_0$ werden die folgenden, mit Hilfe von $\mathbf{PT}_n(z,x)$ aus (3.137) sowie von $\mathbf{P}_n(x)$ und von $\leq_n$, $<_n$ gebildeten Formeln $\mathbf{SmPT}_n(z,x)$, $\mathbf{GPT}_n(z,x)$, $\mathbf{SuPT}_n(z_1,z_2,x)$, $\mathbf{SuP}_n(z_1,z_2)$, $\mathbf{NoPT}_n(x)$, $\mathbf{NoSmPT}_n(x_1,x_2)$, $\mathbf{NoGPT}_n(x_1,x_2)$, $\mathbf{IntSaPT}_n(x_1,x_2)$ verwendet werden, die den entsprechenden Längen und Konstruierbarkeitseigenschaften (A) (bzgl. den zugehörigen Formelfamilien) genügen und die inhaltlich folgende Aussagen formalisieren: Für alle $a, a_1, a_2 \in \mathbb{Z}$ gelten in $\mathfrak{Z}$:

$$\mathbf{SmPT}_n(z,\mathbf{i}_a) \leftrightarrow \Big[\!\Big[z \in \mathbb{N}_0,\ a \neq 0,\ z \text{ ist kleinster Primteiler} < 2^{2^n} \text{ von } a \Big]\!\Big];$$

$$\mathbf{GPT}_n(z,\mathbf{i}_a) \leftrightarrow \Big[\!\Big[z \in \mathbb{N}_0,\ a \neq 0,\ z \text{ ist größter Primteiler} < 2^{2^n} \text{ von } a \Big]\!\Big];$$

$$\mathbf{SuPT}_n(z_1,z_2,\mathbf{i}_a) \leftrightarrow \Big[\!\Big[z_1,z_2 \in \mathbb{N}_0,\ z_1,z_2 < 2^{2^n},\ a \neq 0,\ z_1 < z_2,\ z_1,z_2 \text{ sind Primteiler von } a,\ \text{es gibt keinen weiteren Primteiler } z_3 \text{ von } a \text{ mit } z_1 < z_3 < z_2 \Big]\!\Big];$$

[56] Die Forderung $z < 2^{2^{n+2}}$ stellt hier keine zusätzliche Einschränkung dar und könnte deshalb weggelassen werden, vgl. dazu (1) im Beweis des Satzes.

$$\begin{aligned}
\mathbf{NoSmPT}_n(\mathbf{i}_{a_1}, \mathbf{i}_{a_2}) \leftrightarrow [\![\, & a_1, a_2 \neq 0,\ a_1 \text{ besitzt keinen} \\
& \text{Primteiler} < 2^{2^n}, \text{ der kleiner ist} \\
& \text{als ein Primteiler} < 2^{2^n} \text{ von } a_2 \,]\!] \\
\mathbf{NoGPT}_n(\mathbf{i}_{a_1}, \mathbf{i}_{a_2}) \leftrightarrow [\![\, & a_1, a_2 \neq 0,\ a_1 \text{ besitzt keinen} \\
& \text{Primteiler} < 2^{2^n}, \text{ der größer ist} \\
& \text{als ein Primteiler} < 2^{2^n} \text{ von } a_2 \,]\!] \\
\mathbf{IntSaPT}_n(\mathbf{i}_{a_1}, \mathbf{i}_{a_2}) \leftrightarrow [\![\, & a_1, a_2 \neq 0,\ a_1 \text{ im Intervall zwischen} \\
& \text{dem kleinsten und dem größten} \\
& \text{Primteiler} < 2^{2^n} \text{ von } a_2 \text{ besitzen} \\
& a_1 \text{ und } a_2 \text{ die gleichen Primteiler} \,]\!] \,;
\end{aligned}$$

sowie für alle $a \in \mathbb{Z}$

$$\begin{aligned}
\mathbf{NoPT}_n(\mathbf{i}_a) \text{ ist gültig in } \mathfrak{Z} \iff & a \neq 0,\ a \text{ besitzt keinen} \\
& \text{Primteiler } < 2^{2^n}
\end{aligned}$$

und

$$\begin{aligned}
\mathbf{SuP}_n(z_1, z_2) \leftrightarrow [\![\, & z_1, z_2 \in \mathbb{N}_0,\ z_1, z_2 < 2^{2^n}, \\
& z_1, z_2 \text{ sind aufeinanderfolgende Primzahlen} \,]\!] \,.
\end{aligned}$$

Nun können jedoch $\mathbf{SmPT}_n(z, x)$ und $\mathbf{GPT}_n(z, x)$ von der Gestalt

$$\begin{aligned}
& \mathbf{PT}_n(z, x) \;\&\; \forall z_1 \left(\mathbf{PT}_n(z_1, x) \rightarrow z \leq_n z_1 \right) \quad \text{bzw.} \\
& \mathbf{PT}_n(z, x) \;\&\; \forall z_1 \left(\mathbf{PT}_n(z_1, x) \rightarrow z_1 \leq_n z \right) \,,
\end{aligned}$$

$\mathbf{SuPT}_n(z_1, z_2, x)$ von der Gestalt

$$\begin{aligned}
& \mathbf{PT}_n(z_1, x) \;\&\; \mathbf{PT}_n(z_2, x) \;\&\; z_1 <_n z_2 \\
& \;\&\; \neg\, \exists z_3 \left(\mathbf{PT}_n(z_3, x) \;\&\; z_1 <_n z_3 \;\&\; z_3 <_n z_2 \right) \,,
\end{aligned}$$

$\mathbf{SuP}_n(z_1, z_2)$ von der Gestalt

$$\begin{aligned}
& \mathbf{P}_n(z_1) \;\&\; \mathbf{P}_n(z_2) \;\&\; z_1 <_n z_2 \\
& \;\&\; \neg\, \exists z_3 \left(\mathbf{P}_n(z_3) \;\&\; z_1 <_n z_3 \;\&\; z_3 <_n z_2 \right) \,,
\end{aligned}$$

$\mathbf{NoSmPT}_n(x_1, x_2)$ und $\mathbf{NoGPT}_n(x_1, x_2)$ von der Gestalt

$$\begin{aligned}
& \neg\, x_1 = 0 \;\&\; \neg\, x_2 = 0 \\
& \;\&\; \forall z_2 \left[\mathbf{SmPT}_n(z_2, x_2) \rightarrow \neg\, \exists z_1 \left(\mathbf{PT}_n(z_1, x_1) \;\&\; z_1 <_n z_2 \right) \right] \quad \text{bzw.}
\end{aligned}$$

$$\begin{aligned}&\neg\, x_1 = 0 \;\&\; \neg\, x_2 = 0\\ &\;\&\; \forall w_2 \left[\, \mathbf{GPT}_n(w_2, x_2) \rightarrow \neg\, \exists z_1 \left(\mathbf{PT}_n(z_1, x_1) \;\&\; w_2 <_n z_1 \right) \right] ,\end{aligned}$$

$\mathbf{IntSaPT}_n(x_1, x_2)$ von der Gestalt

$$\begin{aligned}&\neg\, x_1 = 0 \;\&\; \neg\, x_2 = 0\\ &\;\&\; \forall z_2\, \forall w_2 \left\{ \mathbf{SmPT}_n(z_2, x_2) \;\&\; \mathbf{GPT}_n(w_2, x_2) \right.\\ &\qquad\qquad \rightarrow \forall z \left[\, z_2 \leq_n z \;\&\; z \leq_n w_2 \right.\\ &\qquad\qquad\qquad \left. \left. \rightarrow \left(\mathbf{PT}_n(z, x_1) \leftrightarrow \mathbf{PT}_n(z, x_2) \right) \right] \right\}\end{aligned}$$

und $\mathbf{NoPT}_n(x)$ als

$$\mathbf{NoPT}_n(x) ::= \; \neg\, x = 0 \;\&\; \forall z \left(\neg\, \mathbf{PT}_n(z, x) \right)$$

gewählt werden. (Analog zu Beispielen aus Abschnitt 4 und Abschnitt 5 können diese Formeln anhand dieser vorläufigen Festlegungen leicht weiter präzisiert werden, sodaß auch die Längen- und Konstruierbarkeitsbedingungen (A) (bzgl. den entsprechenden Formelfamilien) erfüllt sind).

(3) Es wird im weiteren hier nun eine Möglichkeit zur Konstruktion von verkürzten, jedoch logisch äquivalenten Schreibweisen von Formeln zu gelangen, erforderlich sein, die über die in Abschnitt 5 z.B. beim Aufbau der Formeln $\mathbf{M}_n(x, y, z)$ benutzte Möglichkeit (die dort etwa durch das Beispiel (3.93) beschrieben ist) deutlich hinausgeht: Es soll damit hier möglich sein, eine in DNF-Gestalt $\bigvee_{i=1}^{k} \mathbf{A}_i$ gegebene Formel $\mathbf{A}$, in der in den Konjunktionsformeln in $\mathbf{A}_i$ (beliebig viele) Instanzen einer Formel $\mathbf{B}(\mathbf{x})$ ($\mathbf{x}$ eine beliebige Variable)—neben weiteren Formeln—auftreten, zu einer Formel $\mathbf{A}'$ so logisch umzuformen, daß in $\mathbf{A}'$ die Formel $\mathbf{B}(\mathbf{x})$ nur mehr einmal vorkommt und daneben keine (weitere) Instanzen von $\mathbf{B}(\mathbf{x})$ mehr auftreten. Diese im folgenden dargestellte Umformung soll weiters von der inneren Gestalt von $\mathbf{B}(\mathbf{x})$ unabhängig sein, d.h. für eine sich aus $\mathbf{A}$ durch den Austausch aller Instanzen $\mathbf{B}(\mathbf{a})$ in $\mathbf{A}$ durch $\tilde{\mathbf{B}}(\mathbf{a})$ für eine Formel $\tilde{\mathbf{B}}(\mathbf{x})$ ($\mathbf{a}$ ein Term) ergebende Formel $\tilde{\mathbf{A}}$ auf völlig analoge Weise ergeben.

Eine solche Umformungsmöglichkeit ist nun für $k \in \mathbb{N}$, $n_1, \ldots, n_k$, $m_1, \ldots, m_k \in \mathbb{N}$, $\sum_{i=1}^{k} n_i + \sum_{i=1}^{k} m_i > 0$, eine Formel $\mathbf{B}(\mathbf{x})$, Variablen $\mathbf{x}_{i,j}$ ($1 \leq i \leq k$, $1 \leq j \leq n_i$) und $\mathbf{y}_{i,j}$ ($1 \leq i \leq k$, $1 \leq j \leq m_i$) und Formeln $\mathbf{C}_1, \ldots, \mathbf{C}_k$ in TAZ z.B. durch die in Formel 3.7.1 enthaltene, (relativ:) einfach einzusehende Aussage (3.142) gegeben. Darin bezeichen $n := \max\limits_{1 \leq i \leq k} n_i$, $m := \max\limits_{1 \leq i \leq k} m_i$ und $\mathbf{x}_1, \ldots, \mathbf{x}_n$, $\mathbf{y}_1, \ldots, \mathbf{y}_m$, $\mathbf{z}, \bar{\mathbf{x}}, \mathbf{w}$ neue, paarweise verschiedene Variablen (gegenüber allen $\mathbf{x}_{i,j}$, $\mathbf{y}_{i,j}$ sowie $\mathbf{x}$ und den in einem der $\mathbf{C}_i$ frei vorkommenden Variablen).

Formel 3.7.1 Logische Umformungsmöglichkeit zur verkürzten Schreibweise von Formeln in DNF

$$
\begin{aligned}
&\vdash_{TAZ} \bigvee_{1\le i\le k} \mathbf{B}(\mathbf{x}_{i,1}) \,\&\, \ldots \,\&\, \mathbf{B}(\mathbf{x}_{i,n_i}) \,\&\, \neg\mathbf{B}(\mathbf{y}_{i,1}) \,\&\, \ldots \,\&\, \neg\mathbf{B}(\mathbf{y}_{i,m_i}) \,\&\, \mathbf{C}_i \\
&\quad\longleftrightarrow\ \exists\mathbf{x}_1 \ldots \exists\mathbf{x}_n\, \exists\mathbf{y}_1 \ldots \exists\mathbf{y}_m\, \exists\mathbf{z} \\
&\qquad \Big\{ \Big[\bigvee_{\substack{1\le i\le k \\ n_i, m_i > 0}} \big(\mathbf{z} = 0 \,\&\, \mathbf{x}_1 = \mathbf{x}_{i,1} \,\&\ldots\&\, \mathbf{x}_{n_i} = \mathbf{x}_{i,n_i} \\
&\qquad\qquad\qquad \&\, \mathbf{x}_{n_i+1} = \mathbf{x}_{i,n_i} \,\&\ldots\&\, \mathbf{x}_n = \mathbf{x}_{i,n_i} \\
&\qquad\qquad\qquad \&\, \mathbf{y}_1 = \mathbf{y}_{i,1} \,\&\ldots\&\, \mathbf{y}_{m_i} = \mathbf{y}_{i,m_i} \\
&\qquad\qquad\qquad \&\, \mathbf{y}_{m_i+1} = \mathbf{y}_{i,m_i} \,\&\ldots\&\, \mathbf{y}_m = \mathbf{y}_{i,m_i} \,\&\, \mathbf{C}_i \big) \\
&\qquad\quad \vee \bigvee_{\substack{1\le i\le k \\ n_i > 0,\, m_i = 0}} \big(\mathbf{z} = 1 \,\&\, \mathbf{x}_1 = \mathbf{x}_{i,1} \,\&\ldots\&\, \mathbf{x}_{n_i} = \mathbf{x}_{i,n_i} \\
&\qquad\qquad\qquad \&\, \mathbf{x}_{n_i+1} = \mathbf{x}_{i,n_i} \,\&\ldots\&\, \mathbf{x}_n = \mathbf{x}_{i,n_i} \,\&\, \mathbf{C}_i \big) \\
&\qquad\quad \vee \bigvee_{\substack{1\le i\le k \\ n_i = 0,\, m_i > 0}} \big(\mathbf{z} = \underline{\underline{2}} \,\&\, \mathbf{y}_1 = \mathbf{y}_{i,1} \,\&\ldots\&\, \mathbf{y}_{m_i} = \mathbf{y}_{i,m_i} \\
&\qquad\qquad\qquad \&\, \mathbf{y}_{m_i+1} = \mathbf{y}_{i,m_i} \,\&\ldots\&\, \mathbf{y}_m = \mathbf{y}_{i,m_i} \,\&\, \mathbf{C}_i \big) \\
&\qquad\quad \vee \bigvee_{\substack{1\le i\le k \\ n_i = m_i = 0}} \mathbf{z} = \underline{\underline{3}} \,\&\, \mathbf{C}_i \Big] \\
&\qquad \&\, \forall\bar{\mathbf{x}}\, \forall\mathbf{w} \\
&\qquad\qquad \big[\big((\bar{\mathbf{x}} = \mathbf{x}_1 \vee \ldots \vee \bar{\mathbf{x}} = \mathbf{x}_n) \,\&\, (\mathbf{z} = 0 \vee \mathbf{z} = 1) \,\&\, \mathbf{w} = 0 \big) \\
&\qquad\qquad\quad \vee \big((\bar{\mathbf{x}} = \mathbf{y}_1 \vee \ldots \vee \bar{\mathbf{x}} = \mathbf{y}_m) \,\&\, (\mathbf{z} = 0 \vee \mathbf{z} = \underline{\underline{2}}) \,\&\, \mathbf{w} = 1 \big) \\
&\qquad\qquad\quad \to\ \big(\exists\mathbf{x}\, (\mathbf{x} = \bar{\mathbf{x}} \,\&\, \mathbf{B}(\mathbf{x})) \leftrightarrow \mathbf{w} = 0 \big) \big] \Big\}
\end{aligned}
\tag{3.142}
$$

Für die logische Umformung, die durch diese Aussage bestimmt ist und die die Anzahl der Instanzen einer Formel $\mathbf{B}(\mathbf{x})$ bezüglich einer in DNF-Gestalt vorliegenden Formel $\mathbf{A}$ auf *eine* zu reduzieren gestattet, ist das Vorhandensein von $\leftrightarrow$ als Sprachelement (wohl) unverzichtbar. Diese Umformung selbst kann im selben Ausmaß wie für TAZ in Theorien mit 4 beweisbar verschiedenen Konstanten analog durchgeführt werden und läßt sich dann weiters sofort für alle konsistenten Theorien, die nur mindestens zweielementige Modelle besitzen, verallgemeinern.

[FiR74] deuten an einer Stelle, auf p. 16, eine solche allgemeinere Verkürzungsaussage als ein Theorem von M. Fischer und A. Meyer an, das sie jedoch bei der Darstellung ihrer Beweise nicht benötigen (sondern nur einfache Spezialfälle davon wie etwa den hier schon erwähnten, in (3.93) ausgedrückten). Eine zur hier vorgestellten Verkürzungsmöglichkeit ähnliche wird auch in [FeRa79] im Beweis von Lemma 3 auf p. 156 verwendet (die, wie [FeRa79] darstellen, gerade auf M. Fischer und A. Meyer und frühere Arbeiten von L. Stockmeyer ([FeRa79] verweisen auf [SM73]) zurückgeht; diese Möglichkeit ist etwas allgemeiner als die hier vorgestellte und bezieht sich nicht notwendigerweise nur auf in *DNF-Gestalt* vorliegende Ausgangsformeln $\mathbf{A}$ bzgl. der „zu extrahierenden“ Instanzen einer Formel $\mathbf{B}(\mathbf{x})$, jedoch ist eine entsprechende *Pränexform* von $\mathbf{A}$ in Beziehung zu den Instanzen von $\mathbf{B}(\mathbf{x})$ dafür schon auch erforderlich). – Die hier beschriebene Möglichkeit ist allerdings auch im Zusammenhang mit den schon in Satz 3.4.4 bei der Festlegung der Formeln $\mathbf{F}_{M,w}$ verwendeten Formelverkürzungen zu sehen bzw. in Analogie zu den dort entwickelten Formeln entstanden.

(3.142) läßt sich sofort auch für Formeln $\mathbf{B}(\mathbf{x}'_1, \ldots, \mathbf{x}'_n)$, in denen also mehrere freie Variable vorkommen, verallgemeinern.

(4) Die Konstruktion von Formeln $\mathbf{PZ}_{n+2}(z, y)$ in T mit den im Lemma behaupteten Eigenschaften läßt sich auf die Existenz von Formeln $\mathbf{AnzPT}_{n+2}(x, y)$ zurückführen, die in $\mathfrak{Z}$ für alle $n \in \mathbb{N}_0$ und $a \in \mathbb{Z}$ die Gültigkeit von

$$\mathbf{AnzPT}_{n+2}(\mathbf{i}_a, y) \leftrightarrow [\![\, a \neq 0,\ y \in \mathbb{N}_0,\ y < 2^{2^{n+1}},\ a \text{ besitzt genau } y \text{ verschiedene Primteiler} < 2^{2^{n+2}} \,]\!] \qquad (3.143)$$

garantieren und bzgl. denen $\left\{\mathbf{AnzPT}_{n+2}(x, y)^{((M))}\right\}_{n \in \mathbb{N}_0}$ die Bedingungen (A) erfüllen:

Unter der Annahme der Existenz solcher Formeln läßt sich nun $\mathbf{PZ}_{n+2}(z, y)$ mit Hilfe der Formeln aus (1), die Eigenschaften von ganzen Zahlen in Beziehung zu

Primteilern $< 2^{2^{n(+2)}}$ formulieren, in T durch

$$\begin{aligned}&\mathbf{M}_{n+1}(y,1,y)\ \&\ (y=0 \to z=\underline{\underline{2}})\\ &\ \&\ \{\neg\, y=0 \to \exists x\,\exists w_0\,[\,\mathbf{AnzPT}_{n+2}(x,y)\ \&\ \mathbf{SmPT}_{n+2}(\underline{\underline{2}},x)\\ &\qquad\qquad \&\ \forall z_1\,\forall z_2\,(\,\mathbf{SuPT}_{n+2}(z_1,z_2,x) \to \mathbf{SuP}_{n+2}(z_1,z_2)\,)\\ &\qquad\qquad \&\ \mathbf{GPT}_{n+2}(w_0,x)\ \&\ \mathbf{SuP}_{n+2}(w_0,z)\,]\,\}\end{aligned} \tag{3.144}$$

(: ist die (y+1)-te Primzahl p_{y+1} gesucht, so kommt in (3.144) als für $y \neq 0$, $y < 2^{2^{n+1}}$, $y \in \mathbb{N}$ etwa die Zahl $x := \underbrace{p_1}_{=2} \cdot \underbrace{p_2}_{=3} \cdot \ldots \cdot p_y$ ins Spiel (oder aber jede andere Zahl $\neq 0$, die genau nur diese Primteiler $< 2^{2^{n+2}}$ besitzt)). Durch—wie in Abschnitt 5 öfter durchgeführten Übergang zu einer „vorsichtigeren“ Wahl dieser Formel, in der direkt auf die beteiligten Hilfsformeln verwiesen wird—kann dann $\mathbf{PZ}_{n+2}(z,y)$ exakt so festgelegt werden, daß sich die Bedingungen (A) auf ablesbare Weise aus den entsprechenden, früher erwiesenen Eigenschaften der verwendeten Hilfsformeln erkennen lassen.

(5) Es reicht nun für den Beweis dieses Lemmas im weiteren aus, die Formeln $\mathbf{AnzPT}_{n+2}(x,y)$ (wie in (4) beschrieben) zu konstruieren:

Dazu werden im folgenden für alle Zahlen $n,k \in \mathbb{N}_0$ mit $k \leq n+1$ die Formeln $\mathbf{NumPT}_{k,n+2}(x,y,x_0,y_0,z_0)$ konstruiert, die für alle $a \in \mathbb{Z}$, $k,n \in \mathbb{N}_0$, $k \leq n+1$ in $\mathfrak{Z}$ die Gültigkeit von

$$\begin{aligned}\mathbf{NumPT}_{k,n+2}(\mathbf{i}_a,y,x_0,y_0,z_0) \leftrightarrow [\![\, &a \neq 0,\ y \in \mathbb{N}_0,\ y < 2^{2^k},\\ &a \text{ besitzt genau } y \text{ verschiedene}\\ &\text{Primteiler} < 2^{2^{n+2}}\,]\!]\\ \&\ &\mathbf{M}_{n+2}(x_0,y_0,z_0)\end{aligned} \tag{3.145}$$

ausdrücken, sowie für die gilt:

$$\begin{aligned}&\left|\mathbf{NumPT}_{k+1,n+2}(x,y,x_0,y_0,z_0)^{((M))}\right| \leq\\ &\quad C + \left|\mathbf{NumPT}_{k,n+2}(x,y,x_0,y_0,z_0)^{((M))}\right| \quad (\text{für alle } k,n \in \mathbb{N}_0,\ k \leq n)\end{aligned} \tag{3.146}$$

mit einem von k (und sogar auch von n) unabhängigen $C \in \mathbb{N}$ und für die

$$\left(n \mapsto \left|\mathbf{NumPT}_{0,n+2}(x,y,x_0,y_0,z_0)^{((M))}\right|\right) \in O(n) \tag{3.147}$$

und diese Formel auch $POLYLIN$-konstruierbar ist (bzgl. Eingabe $(n)_{10}$).

Damit lassen sich nämlich dann die Formeln $\mathbf{AnzPT}_{n+2}(x, y, x_0, y_0, z_0)$ durch

$$\begin{aligned}&\mathbf{AnzPT}_{n+2}(x, y) ::= \\ &\quad \exists x_0\, \exists y_0\, \exists z_0 \big(x_0 = 0 \;\&\; y_0 = 0 \;\&\; z_0 = 0 \\ &\qquad\qquad \&\; \mathbf{NumPT}_{n+1,n+2}(x, y, x_0, y_0, z_0) \big)\end{aligned} \tag{3.148}$$

angeben und insbesondere die Eigenschaft (A) (α) dafür durch Induktion mittels (3.146), (3.147) leicht einsehen; (A) (β) kann durch den im folgenden geschilderten Aufbau von $\mathbf{NumPT}_{k,n+2}(\dots)$ als rekursive Definition über $k \in \mathbb{N}$, $k \leq n$ eingesehen bzw. präzis gemacht werden. – Das hier und im folgenden geschilderte Vorgehen bei der Definition der Formeln $\mathbf{AnzPT}_{n+2}(x, y)$ mit Hilfe der Formeln $\mathbf{NumPT}_{k,n+2}(x, y, x_0, y_0, z_0)$ für $k, n \in \mathbb{N}_0$, $k \leq n+1$ ist sehr analog zu dem bei der Konstruktion von $\mathbf{Pow}_n(x, y, z)$ mit Hilfe der Formeln $\mathbf{E}_{k,n}(x, y, z, x_0, y_0, z_0)$ in Satz 3.5.2 (bzw. von [FiR74] beim Beweis von Theorem 8, p. 14 darin) benutzten.

Für $n \in \mathbb{N}_0$ und $k = 0$ kann $\mathbf{NumPT}_{0,n+2}(x, y, x_0, y_0, z_0)$ nun von der Gestalt

$$\begin{aligned}&\big\{ \big(\neg\, x = 0 \;\&\; y = 0 \;\&\; \mathbf{NoPT}_{n+2}(x) \big) \\ &\quad \vee \big[y = 1 \;\&\; \exists z \big(\mathbf{SmPT}_{n+2}(z, x) \;\&\; \mathbf{GPT}_{n+2}(z, x) \big) \big] \big\} \\ &\& \; \mathbf{M}_{n+2}(x_0, y_0, z_0)\end{aligned} \tag{3.149}$$

gewählt werden. (3.147) folgt aus dieser Gestalt unmittelbar, ebenso die Konstruierbarkeit dieser Formel in von der Eingabe $(n)_{10}$ abhängigem $POLYLIN$-Aufwand.

Die im folgenden dargestellte rekursive Gestalt der Definition der Formel $\mathbf{NumPT}_{k+1,n+2}(x, y, x_0, y_0, z_0)$ für alle Zahlen $n, k \in \mathbb{N}_0$, $k \leq n+1$ unter der Annahme der bereits gefundenen Form der Formel $\mathbf{NumPT}_{k,n+2}(x, y, x_0, y_0, z_0)$ geht dabei von der folgenden Überlegung aus: Besitzt $x \in \mathbb{Z}$, $x \neq 0$ genau $y \in \mathbb{N}_0$, $y < 2^{2^{k+1}}$ verschiedene Primteiler $< 2^{2^{n+2}}$, so läßt sich, da dann wegen (3.88) $y_1, y_2, y_3, y_4 \in \mathbb{N}_0$ mit $y_1, y_2, y_3, y_4 < 2^{2^k}$ und $y = y_1 \cdot y_2 + y_3 + y_4$ existieren, zuerst im Fall, daß $y_1, \dots, y_4 > 0$ gilt, x als

$$x = \bar{x} \cdot x_3 \cdot x_4 \tag{3.150}$$

auffassen, wobei (a) $\bar{x}, x_3$ bzw. x_4 genau $y_1 \cdot y_2$, y_3 bzw. y_4 Primteiler $< 2^{2^{n+2}}$ besitzen und (b) alle Primteiler $< 2^{2^{n+2}}$ von $\bar{x}$ kleiner als die Primteiler $< 2^{2^{n+2}}$ von x_3, sowie alle Primteiler $< 2^{2^{n+2}}$ von x_3 kleiner als jene von x_4 sind. $\bar{x}$ kann nun (jedenfalls immer dann, wenn $y_1 \cdot y_2 > 0$ gilt) weiters als

$$\bar{x} = \bar{\bar{x}} \cdot x_2 \tag{3.151}$$

aufgefaßt werden, wobei x_2 genau y_2 Primteiler $< 2^{2^{n+2}}$ besitzt und zwischen (in der Reihe der Primzahlen) aufeinanderfolgenden Primteilern von x_2, sowie vor deren

kleinstem genau noch immer $(y_1 - 1)$ weitere Primteiler von $\bar{x}$ (und damit auch von x) liegen. – Umgekehrt läßt sich natürlich auch von einem in der Gestalt (3.150), (3.151) (bzgl. $y_1, y_2, y_3, y_4 \in \mathbb{N}_0$, $y_1, y_2, y_3, y_4 < 2^{2^k}$, $y = y_1 \cdot y_2 + y_3 + y_4$) vorliegenden $x \in \mathbb{Z}$, $x \neq 0$ (und den beschriebenen Eigenschaften von $\bar{x}$, $\bar{\bar{x}}$, x_2, x_3, x_4 bzgl. y_1, y_2, y_3,y_4) die Aussage, daß x dann genau y Primteiler $< 2^{2^{n+2}}$ besitzt, schließen.

Die im folgenden dargestellte (und zuerst vorläufige durchgeführte) Festlegung von $\mathbf{NumPT}_{k+1,n+2}(x, y, x_0, y_0, z_0)$ geht von dieser Überlegung aus, wobei als x_1 noch (für $y_1 \neq 0$) eine Zahl aus $\mathbb{Z}$ ins Spiel kommt, die genau die ersten y_1 Primteiler $< 2^{2^{n+2}}$ von x (und $\bar{x}$ wie oben) besitzt und wobei weiters $z_1, \ldots, z_4$ jeweils für die kleinsten Primteiler $< 2^{2^{n+2}}$ und $w_1, \ldots, w_4$ für die größten Primteiler $< 2^{2^{n+2}}$ von x_1 bzw. x_2 bzw. x_3 bzw. x_4 stehen (falls für das jeweils zugehörige $y_i \neq 0$ gilt und x_i überhaupt Primteiler $< 2^{2^{n+2}}$ besitzt)[57]. Weiters sind bezüglich der obigen Überlegung noch abhängig davon, ob eine oder mehrere der Zahlen y_1, y_2, y_3, y_4 mit $y = y_1 \cdot y_2 + y_3 + y_4$ oder $y_5 := y_1 \cdot y_2$ gleich Null sind, einige Spezialfälle dabei zu beachten; deren Anzahl wird aber durch die zur Vereinfachung benutzte, höchstens eine Vertauschung von y_3 und y_4 als Folge erfordernde Bedingung $y_4 \leq y_3$ verringert.

$\mathbf{NumPT}_{k+1,n+2}(x, y, x_0, y_0, z_0)$ kann nun mit Hilfe von in (1) entwickelten Hilfsformeln und $\mathbf{M}_{n+2}(x, y, z)$ so ausgedrückt werden:

$$
\begin{aligned}
&\exists x_1 \ldots \exists x_4 \, \exists y_0 \ldots \exists y_5 \, \exists z_1 \ldots \exists z_4 \, \exists w_1 \ldots \exists w_4 \\
&\quad \big\{ \mathbf{NumPT}_{k,n+2}(x_1, y_1, 0, 0, 0) \;\&\; \mathbf{NumPT}_{k,n+2}(x_2, y_2, 0, 0, 0) \\
&\qquad \&\; \mathbf{NumPT}_{k,n+2}(x_3, y_3, 0, 0, 0) \;\&\; \mathbf{NumPT}_{k,n+2}(x_4, y_4, 0, 0, 0) \\
&\qquad \&\; \big(\neg\, y_1 = 0 \rightarrow \mathbf{SmPT}_{n+2}(z_1, x_1) \;\&\; \mathbf{GPT}_{n+2}(w_1, x_1)\big) \;\&\; \ldots \\
&\qquad \ldots \;\&\; \big(\neg\, y_4 = 0 \rightarrow \mathbf{SmPT}_{n+2}(z_4, x_4) \;\&\; \mathbf{GPT}_{n+2}(w_4, x_4)\big) \\
&\qquad \&\; \mathbf{M}_{n+2}(y_1, y_2, y_5) \;\&\; y = y_5 + y_3 + y_4 \;\&\; y_4 \leq_{n+2} y_3 \\
&\qquad \&\; \mathbf{B}(x, x_1, x_2, y_1, y_5, z_2, w_1) \;\&\; \mathbf{C}_1(x, x_3, x_4, y_4, y_5, z_3, z_4, w_2, w_3) \\
&\qquad \&\; \mathbf{C}_2(x, x_3, y_3, y_4, y_5, z_3, w_2) \;\&\; \mathbf{C}_3(x, x_2, y_3, y_5) \;\&\; \mathbf{C}_4(x, x_3, x_4, y_4, y_5, z_4) \\
&\qquad \&\; \mathbf{C}_5(x, x_3, y_3, y_4, y_5) \;\&\; \mathbf{C}_6(x, y_3, y_5) \,\big\} \\
&\;\&\; \mathbf{M}_{n+2}(x_0, y_0, z_0)
\end{aligned}
\tag{3.152}
$$

Hierbei bezieht sich $\mathbf{B}(x, x_1, x_2, y_1, y_5, z_2, w_1)$ auf die ersten $y_5 = y_1 \cdot y_2$ Primzahlen

[57] Die Verwendung von z_1 und w_4 in der im folgenden zu entwickelnden rekursiven Festlegung von $\mathbf{NumPT}_{k+1,n+2}(x, y, x_0, y_0, z_0)$ in (3.152) ist dabei nicht unbedingt nötig und könnte vermieden werden, wobei damit dann in (3.152) zugleich auch $\mathbf{SmPT}_{n+2}(z_1, x_1)$ und $\mathbf{GPT}_{n+2}(w_4, x_4)$ weggelassen werden müßten; aus Symmetrie- und Verständlichkeitsgründen wurde das Auftreten dieser Variablen hier aber beibehalten.

von x (falls $y_5 > 0$) und ist durch

$$\begin{aligned}\neg\, y_5 = 0 \rightarrow\ & \mathbf{NoSmPT}_{n+2}(x, x_1)\ \&\ \mathbf{IntSaPT}_{n+2}(x, x_1)\ \&\ w_1 = z_2 \\ & \&\ \forall z_{21}\, \forall z_{22} \\ & \quad \big[\, \mathbf{SuPT}_{n+2}(z_{21}, z_{22}, x_2) \\ & \quad\ \rightarrow \exists x_5\, \exists z_5 \\ & \quad\quad \big(\mathbf{NumPT}_{k,n+2}(x_5, y_1, 0, 0, 0)\ \&\ \mathbf{SmPT}_{n+2}(z_5, x_5) \\ & \quad\quad\ \&\ \mathbf{SuPT}_{n+2}(z_{21}, z_5, x)\ \&\ \mathbf{IntSaPT}_{n+2}(x, x_5) \\ & \quad\quad\ \&\ \mathbf{GPT}_{n+2}(z_{22}, x_5) \big)\, \big]\end{aligned}$$

festgelegt. Die Formeln $\mathbf{C}_1(\dots)$, $\dots$, $\mathbf{C}_6(\dots)$ beziehen sich auf die bezüglich den Zahlen y_1, y_2, y_3, y_4 auftretenden 6 Fällen

$y_1, y_2, y_3, y_4 > 0$	bzw.
$y_1, y_2, y_3 > 0,\ y_4 = 0$	bzw.
$y_1, y_2 > 0,\ y_3 = y_4 = 0$	bzw.
$y_1 \cdot y_2 = 0,\ y_3, y_4 > 0$	bzw.
$y_1 \cdot y_2 = 0,\ y_3 > 0,\ y_4 = 0$	bzw.
$y_1 \cdot y_2 = y_3 = y_4 = 0$	

und dabei ist $\mathbf{C}_1(x, x_3, x_4, y_4, y_5, z_3, z_4, w_2, w_3)$ als

$$\begin{aligned}\neg\, y_5 = 0\ \&\ \neg\, y_4 = 0 \rightarrow\ & \mathbf{SuPT}_{n+2}(w_2, z_3, x)\ \&\ \mathbf{IntSaPT}_{n+2}(x, x_3) \\ & \&\ \mathbf{SuPT}_{n+2}(w_3, z_4, x)\ \&\ \mathbf{IntSaPT}_{n+2}(x, x_4) \\ & \&\ \mathbf{NoGPT}_{n+2}(x, x_4)\ ,\end{aligned}$$

$\mathbf{C}_2(x, x_3, y_3, y_4, y_5, z_3, w_2)$ als

$$\begin{aligned}\neg\, y_5 = 0\ \&\ \neg\, y_3 = 0\ \&\ y_4 = 0 & \\ \rightarrow\ & \mathbf{SuPT}_{n+2}(w_2, z_3, x)\ \&\ \mathbf{IntSaPT}_{n+2}(x, x_3) \\ & \&\ \mathbf{NoGPT}_{n+2}(x, x_3)\ ,\end{aligned}$$

$\mathbf{C}_3(x, x_2, y_3, y_5)$ als

$$\neg\, y_5 = 0\ \&\ y_3 = 0 \rightarrow \mathbf{NoGPT}_{n+2}(x, x_2)\ ,$$

$\mathbf{C}_4(x, x_3, x_4, y_4, y_5, z_4)$ als

$$\begin{aligned}y_5 = 0\ \&\ \neg\, y_4 = 0 \rightarrow\ & \mathbf{NoSmPT}_{n+2}(x, x_3)\ \&\ \mathbf{IntSaPT}_{n+2}(x, x_3) \\ & \&\ \mathbf{SuPT}_{n+2}(w_3, z_4)\ \&\ \mathbf{IntSaPT}_{n+2}(x, x_4) \\ & \&\ \mathbf{NoGPT}_{n+2}(x, x_4)\ ,\end{aligned}$$

$\mathbf{C}_5(x, x_3, y_3, y_4, y_5)$ als

$$\begin{aligned} y_5 = 0 \;\&\; \neg\, y_3 = 0 \;\&\; y_4 = 0 \\ \rightarrow \mathbf{NoSmPT}_{n+2}(x, x_3) \;\&\; \mathbf{IntSaPT}_{n+2}(x, x_3) \\ \&\; \mathbf{NoGPT}_{n+2}(x, x_3) \end{aligned}$$

und $\mathbf{C}_6(x, y_3, y_5)$ als

$$y_5 = 0 \;\&\; y_3 = 0 \rightarrow \mathbf{NoPT}_{n+2}(x)$$

festgelegt.

Ausgehend von (3.152) läßt sich nun eine der Längenbedingung (3.146) genügende Festlegung von $\mathbf{NumPT}_{k+1,n+2}(x, y, x_0, y_0, z_0)$ (wegen des *jedenfalls* 5-maligen Auftretens von $\mathbf{NumPT}_{k,n+2}(x, y, x_0, y_0, z_0)$ in (3.152) kann (3.146) nicht gelten) durch folgendes Vorgehen finden:

(a) In (3.152) werden alle darin verwendeten Hilfsformeln aus (1) bzw. deren Instanzen sowie auch $\leq_{n+2}$ und alle Formeln $\mathbf{P}_{n+2}(x)$ und $\mathbf{PT}_{n+2}(z, x)$ bzw. deren Instanzen in diesen Definitionen durch die Formel $\mathbf{M}_{n+2}(x, y, z)$ bzw. durch entsprechende Instanzen dieser Formeln ausgedrückt (vgl. dazu die einzelnen früher erfolgten Festlegungen dieser Hilfsformeln). Nun werden alle Instanzen von $\mathbf{M}_{n+2}(x, y, z)$ im weiteren als Instanzen von $\mathbf{NumPT}_{k,n+2}(x, y, x_0, y_0, z_0)$ (vgl. dazu (3.145)) aufgefaßt (z.B. läßt sich dabei eine Instanz $\mathbf{M}_{n+2}(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ als die Instanz $\mathbf{NumPT}_{k,n+2}(1, 0, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3)$ formulieren).

(b) Die durch diese Umbezeichnung von Teilformeln gewonnene Gestalt von (3.152) wird nun weiters durch Pränexoperationen logisch zu einer Formel in DNF-Gestalt

$$\exists x_1 \ldots \exists x_4 \ldots \exists w_1 \ldots \exists w_4\, (Q_1 \mathbf{x}_1) \ldots (Q_l \mathbf{x}_l) \bigvee_{i=1}^{m} \mathbf{A}_i \tag{3.153}$$

umgeformt, wobei die Formeln $\mathbf{A}_i$ Konjunktionen von atomaren Formeln mit Prädikatssymbol $=$ oder Instanzen von $\mathbf{NumPT}_{k,n+2}(x, y, x_0, y_0, z_0)$ oder einfache Negationen von Formeln einer dieser beiden Formelarten sind und $\mathbf{x}_1, \ldots, \mathbf{x}_l$ $(l \in \mathbb{N})$ die dabei zusätzlich auftretenden Variablen sind.

(c) Unter Verwendung der in (3) dargestellten Methode zur längenverkürzten Schreibweise von Formeln kann nun eine zu $\bigvee_{i=1}^{m} \mathbf{A}_i$ in TAZ äquivalente Formel $\mathbf{A}'$ gefunden werden, in der $\mathbf{NumPT}_{k,n+2}(x, y, x_0, y_0, z_0)$ nur mehr einmal (und keine (andere) Instanz dieser Formel sonst mehr) auftritt.

(d) Nun kann die Setzung

$$\begin{aligned}&\mathbf{NumPT}_{k+1,n+2}(x,y,x_0,y_0,z_0) ::= \\ &\quad \exists x_1 \ldots \exists x_4 \ldots \exists w_1 \ldots \exists w_4 (Q_1 \mathbf{x}_1) \ldots (Q_l\, \mathbf{x}_l)\, \mathbf{A}'\end{aligned} \tag{3.154}$$

erfolgen und anhand dieser Festsetzung und der dabei in (c) verwendeten Umformung analog zu (3.142) kann das Erfülltsein von (3.146) (bzgl. eines auch von n unabhängigen $C \in \mathbb{N}$) leicht eingesehen werden.

Ebenso kann weiters anhand der in (3.154) erfolgten, wegen des damit verbundenen Aufwands nicht weiter explizit gemachten, rekursiven Festsetzung der Formel $\mathbf{NumPT}_{k+1,n+2}(x,y,x_0,y_0,z_0)$ bzgl. der Formel $\mathbf{NumPT}_{k,n+2}(x,y,x_0,y_0,z_0)$ die $POLYLIN$-Konstruierbarkeit von $\mathbf{NumPT}_{n+1,n+2}(x,y,x_0,y_0,z_0)$ (und damit wegen (3.148) im weiteren von $\mathbf{AnzPT}_{n+2}(x,y)$) für Eingabe $(n)_{10}$ eingesehen werden.

(6) Die Festlegung von $\mathbf{NumPT}_{k+1,n+2}(x,y,x_0,y_0,z_0)$ machte beim Umformungsschritt zwischen (3.153) und (3.154) und also bei der Anwendung der Methode zur längenverkürzten Schreibweise von Formeln aus (3) wesentlichen Gebrauch vom Vorhandensein des logischen Symbols $\leftrightarrow$ in $T^{((M))}$. Dies könnte auf folgende Weise umgangen werden: Statt $\mathbf{NumPT}_{k,n+2}(x,y,x_0,y_0,z_0)$ würden nun Formeln $\mathbf{NumPT}'_{k,n+2}(x,y,x_0,y_0,z_0,x_1,y_1,x_{10},y_{10},z_{10})$ für alle $k,n \in \mathbb{N}_0$, $k \leq n+1$ mit der Eigenschaft der Gültigkeit von

$$\begin{aligned}&\mathbf{NumPT}'_{k,n+2}(\mathbf{i}_a,y,x_0,y_0,z_0,\mathbf{i}_b,y_1,x_{10},y_{10},z_{10}) \\ &\quad \longleftrightarrow\ \mathbf{NumPT}_{k,n+2}(\mathbf{i}_a,y,x_0,y_0,z_0) \\ &\qquad \&\ \big(\neg\,\mathbf{NumPT}_{k,n+2}(\mathbf{i}_b,y_1,0,0,0)\ \vee\ \neg\,\mathbf{M}_{n+2}(x_{10},y_{10},z_{10})\big)\end{aligned} \tag{3.155}$$

in $\mathfrak{Z}$ für alle $a,b \in \mathbb{Z}$ rekursiv unter nun zweimaliger Verwendung von (3.152) (einmal zusätzlich in negierter Form als Formulierung von $\neg\,\mathbf{NumPT}_{k,n+2}(x_1,y_1,0,0,0)$ bzgl. (3.155), wobei jedoch *dabei* die Konjunktionsformel $\mathbf{M}_{n+2}(x_0,y_0,z_0)$ in (3.152) nicht beteiligt ist) konstruiert (die Formel $\mathbf{M}_{n+2}(x_{10},y_{10},z_{10})$ tritt aber in der entstehenden Formel entsprechend (3.155) auf). Nach dem Übergang zu einer DNF-Gestalt in einer dann für $\mathbf{NumPT}'_{k+1,n+2}(\ldots)$ gefundenen rekursiven Festlegung unter ausschließlicher Verwendung von Instanzen der Formeln $\mathbf{M}_{n+2}(x,y,z)$ und $\mathbf{NumPT}_{k,n+2}(x,y,x_0,y_0,z_0)$ (sowie weiters nur noch verneinten oder unverneinten atomaren Formeln von T mit Prädikatssymbol $=$) können aber dann alle darin auftretenden Instanzen bzw. negierten Instanzen von $\mathbf{M}_{n+2}(x,y,z)$ und $\mathbf{NumPT}_{k,n+2}(x,y,x_0,y_0,z_0)$ durch unnegierte Instanzen von $\mathbf{NumPT}'_{k,n+2}(\ldots)$ ausgedrückt werden. Und zwar können die Instanzen $\mathbf{NumPT}_{k,n+2}(\mathbf{a},\mathbf{b},\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0)$, $\neg\,\mathbf{NumPT}_{k,n+2}(\mathbf{a},\mathbf{b},\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0)$, $\mathbf{M}_{n+2}(\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0)$ und $\neg\,\mathbf{M}_{n+2}(\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0)$ als die Instanzen

$$\mathbf{NumPT}'_{k,n+2}(\mathbf{a},\mathbf{b},\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0,1,1,0,0,1) \quad \text{bzw.}$$

$$\mathbf{NumPT}'_{k,n+2}(1,0,0,0,0,\mathbf{a},\mathbf{b},\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0) \text{ bzw.}$$
$$\mathbf{NumPT}'_{k,n+2}(1,0,\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0,1,1,0,0,1) \text{ bzw.}$$
$$\mathbf{NumPT}'_{k,n+2}(1,0,0,0,0,1,1,\mathbf{a}_0,\mathbf{b}_0,\mathbf{c}_0)$$

von $\mathbf{NumPT}'_{k,n+2}(x,y,x_0,y_0,z_0,x_1,y_1,x_{10},y_{10},z_{10})$ aufgefaßt bzw. formuliert werden.

Da weiters zur in (3.142) ausgedrückten logischen Umformung im Fall, daß keine negierte Instanz $\neg\mathbf{B}(\mathbf{y}_{i,j})$ vorhanden ist, $\leftrightarrow$ nicht benötigt wird, gilt das dann auch für eine zur genauen rekursiven Festlegung von $\mathbf{NumPT}'_{k+1,n+2}(\dots)$ (bezüglich der Erreichung einer (3.146) entsprechenden Längenbedingung) nötigen logischen Umformung. Wie in (5) kann damit dann eine solche genaue Definition von $\mathbf{NumPT}'_{k,n+2}(\dots)$ für alle $k \in \mathbb{N}_0$, $k \leq n+1$ so vorgenommen werden, daß später die abschließende und zu (3.148) analoge Setzung

$$\begin{aligned}
&\mathbf{AnzPT}_{n+2}(x,y) ::= \\
&\quad \exists x_0\, \exists y_0\, \exists z_0\, \exists x_1\, \exists y_1\, \exists x_{10}\, \exists y_{10}\, \exists z_{10} \\
&\qquad \big(x_0 = 0 \;\&\; y_0 = 0 \;\&\; z_0 = 0 \;\&\; x_1 = 1 \;\&\; y_1 = 1 \\
&\qquad\quad \&\; x_{10} = 0 \;\&\; y_{10} = 0 \;\&\; z_{10} = 1 \\
&\qquad\quad \mathbf{NumPT}'_{n+1,n+2}(x,y,x_0,y_0,z_0,x_1,y_1,x_{10},y_{10},z_{10}) \big)
\end{aligned}$$

auf wie in (4) gesuchte Formeln $\mathbf{AnzPT}_{n+2}(x,y)$ ($n \in \mathbb{N}_0$) führt, in denen das logische Symbol $\leftrightarrow$ letztlich nicht mehr enthalten ist.

□

Ausgehend von $\mathbf{PZ}_{n+2}(z,y)$ aus Satz 3.7.1 kann nun $\mathbf{S}^{**}_n(x,y)$ für alle $n \in \mathbb{N}_0$ als

$$\mathbf{S}^{**}_n(x,y) ::= \exists z \left(\mathbf{PZ}_{n+2}(z,y) \;\&\; \mathbf{PT}_{n+2}(z,x) \right) \tag{3.156}$$

explizit gemacht werden. Die so gebildeten Formeln entsprechen (3.134) und den entsprechenden Längen- und Konstruierbarkeitsbedingungen (A) bzgl. $\left\{\mathbf{S}^{**}_n(x,y)^{((M))}\right\}_{n\in\mathbb{N}_0}$.

Die Konstruktion von Formeln $\mathbf{H}^{**}_w(x)$ für $w \in BW0$ wird im folgenden nur in groben Zügen geschildert. Hierfür werden Formeln $\mathbf{K}^{**}_{w,n}(x,y_0)$ aus T für alle $n \in \mathbb{N}$ und $w \in BW0$ mit $|w| \leq n$ verwendet mit der inhaltlichen Eigenschaft, daß für alle solchen n und w und für alle $a \in \mathbb{Z}$ in $\mathfrak{Z}$

$$\mathbf{K}^{**}_{w,n}(\mathbf{i}_a,y_0) \leftrightarrow \left[\left[y_0 = |w|\,,\ (Bw_2(a))(0) \circ \dots \circ (Bw_2(a))(2^{2^n}-1) = w \circ 0^{2^{2^n}-|w|} \right]\right]$$

gültig ist. Solche Formeln $\mathbf{K}^{**}_{w,n}(x,y_0)$ erlauben im Fall, daß die Familie $\left\{\mathbf{K}^{**}_{w,|w|}(x,y_0)\right\}_{w\in BW0}$ auch den Bedingungen (B) aus Definition 3.3.5 genügt, die Festlegung der gesuchten Formeln $\mathbf{H}^{**}_w(x)$ für alle $w\in BW0$ als

$$\mathbf{H}^{**}_w(x) ::= \exists y_0\left(y_0 = \underline{\underline{|w|}} \;\&\; \mathbf{K}^{**}_{w,|w|}(x,y_0)\right).$$

Unter Benützung von Formeln $\mathbf{SJ}^{**}_n$ mit

$$\vdash_T \mathbf{SJ}^{**}_n(x) \leftrightarrow \left[\!\left[\, x\in\mathbb{N}_0,\; x<2^{2^n}\,\right]\!\right],$$

die von der Gestalt

$$\mathbf{I}^{**}_n(x)\;\&\;\exists z\,\exists y\left(\mathbf{J}^{**}_n(z)\;\&\;\mathbf{I}^{**}_n(y)\;\&\;x+y+1=z\right)$$

gewählt werden können, ist nun für beliebig, aber fest angenommenes $n\in\mathbb{N}$ folgende rekursive Definition bzgl. $w\in BW0$, $|w|\leq n$ für die gesuchten Formeln $\mathbf{K}^{**}_{w,n}(x,y_0)$ möglich, die auf zuvor hier schon konstruierte Formeln zurückgreift:

Für $w\in BW0$ mit $|w|=1$ und $n\in\mathbb{N}$ sei $\mathbf{K}^{**}_{w,n}(x,y_0)$ im Fall von $w=0$ von der Gestalt

$$y_0=1\;\&\;\forall y\,\forall z\left(\mathbf{SJ}^{**}_n(y)\;\&\;\mathbf{PZ}_{n+2}(z,y)\rightarrow\neg\,\mathbf{PT}_{n+2}(z,x)\right)$$

und im Fall $w=1$ von der Gestalt

$$\begin{aligned} &y_0=1\;\&\;\mathbf{PT}_{n+2}(\underline{\underline{2}})\\ &\&\;\forall y\,\forall z\left(\mathbf{SJ}^{**}_n(y)\;\&\;\neg\,y=0\;\&\;\mathbf{PZ}_{n+2}(z,y)\rightarrow\neg\,\mathbf{PT}_{n+2}(z,x)\right)\end{aligned}$$

gewählt.

Für $w\in BW0$ mit $|w|>1$ und $n\in\mathbb{N}$ sei für $w=w'0$, $w'\in BW0$ die Formel $\mathbf{K}^{**}_{w,n}(x,y_0)$ rekursiv durch eine Formel der Gestalt

$$\exists y'_0\left(\mathbf{K}^{**}_{w',n}(x,y'_0)\;\&\;y_0=y'_0+1\right)$$

definiert; für $w=w'1$ für $w'\in BW0$ sei

$$\begin{aligned}\exists x_0\,\exists y'_0\,\exists z_1\,\{\,&\mathbf{K}^{**}_{w',n}(x_0,y'_0)\;\&\;y_0=y'_0+1\;\&\;\mathbf{PZ}_{n+2}(z_1,y'_0)\\ &\&\;\forall y\,\forall z\left[\,\mathbf{SJ}^{**}_n(y)\;\&\;y<_{n+2}y'_0\;\&\;\mathbf{PZ}_{n+2}(z,y)\right.\\ &\qquad\left.\rightarrow\left(\mathbf{PT}_{n+2}(z,x)\leftrightarrow\mathbf{PT}_{n+2}(z,x_0)\right)\right]\\ &\&\;\mathbf{PT}_{n+2}(z_1,x)\\ &\&\;\forall y\,\forall z\left[\,\mathbf{SJ}^{**}_n(y)\;\&\;y_0\leq_{n+2}y\;\&\;\mathbf{PZ}_{n+2}(z,y)\rightarrow\neg\,\mathbf{PT}_{n+2}(z,x)\right]\,\}.\end{aligned}$$

Die genaue Festlegung dieser rekursiven Definition der Formel $\mathbf{K}^{**}_{w,n}(x, y_0)$ (die die entsprechende Längen- und Konstruierbarkeitsbedingungen zu erreichen gestattet) erfordert jedoch in jedem dieser Schritte ein „Mitschleppen" der Formeln $\mathbf{M}_{n+2}(x_0, y_0, z_0)$, $\mathbf{SJ}^{**}_n(x)$ und $\mathbf{PZ}_{n+2}(z, y)$ und weiters die Anwendung von logischen Umformungen zur Formelverkürzung wie in (5) im Beweis zu Satz 3.7.2. Aus Umfangsgründen unterbleibt an dieser Stelle aber eine weitergehende Schilderung dieses zu (5) im Beweis von Satz 3.7.2 sehr ähnlichen, hier nötigen Vorgehens.

Insgesamt sind damit nun Formeln $\mathbf{I}^{**}_n(x)$, $\mathbf{J}^{**}_n(x)$, $\mathbf{S}^{**}_n(x, y)$ und $\mathbf{H}^{**}_w(x)$ für alle $n \in \mathbb{N}_0$ und $w \in BW0$ mit den gewünschten inhaltlichen Eigenschaften (3.132)–(3.135) und den (bzgl. den zugehörigen Formelfamilien definierten) entsprechenden Längen- und Konstruierbarkeitsbedingungen aufgebaut worden.

Unter Zuhilfenahme der früher angedeuteten, sich auf Satz 3.4.6 und die Sätze des Abschnitts 4 stützenden Argumentation kann damit dann eingesehen und genau nachvollzogen werden, daß die Aussage von Satz 3.7.1 gilt. Dieser Satz ist deshalb bewiesen.

Anhang A: Die Arbeit [FiR74]

Literaturverzeichnis

[Be80] Berman, L.: "The Complexity of Logical Theories", *Theoretical Computer Science 11*, 1980, 71–77.

[BKR84] Ben-Or, M., Kozen, D., Reif, J.: "The Complexity of Elementary Algebra and Geometry", *Proceedings of the 16th ACM Symposium on the Theory of Computing*, 1984, 457–464.

[BoJe74] Boolos, G., Jeffrey, R.: *Computability and Logic*, Cambridge University Press, Cambridge – New York – Melbourne, 1974, 1980, ... , 1987.

[CKS81] Chandra, A.K., Kozen, D.C., Stockmeyer, L.J.: "Alternation", *Journal of the ACM 28*, 1981, 114–133.

[Cob64] Cobham, A.: "The Intrinsic Computational Difficulty of Functions", *Proc. Internat. Congr. Logic, Method. and Philos. Sci.*, 1964, 24–30.

[Co73] Cook, S.A.: "A Hierarchy for Nondeterministic Time Complexity", *Journal of Computer and System Sciences 7*, 4, 1973, 343–353.

[Coo72] Cooper, D.C.: "Theorem Proving in Arithmetic without Multiplication", *Machine Intelligence 7*, Univ. Edinburgh Press, 1972, 91–100.

[FeRa73] Ferrante, J., Rackoff, Ch.W.: "A Decision Procedure for the First Order theory of Real Addition with Order", in:
(a) *MAC Technical Memorandum 33*, May 1973, MIT, Project MAC, Cambridge, Mass. 02139;
(b) *SIAM Journal for Computing 1*, 4, 1975, 67–76.

[FeRa79] Ferrante, J., Rackoff, Ch.W.: *The Computational Complexity of Logical Theories*, Springer-Verlag, Berlin – Heidelberg – New York, 1979.

[FiR74] Fischer, M.J., Rabin, M.O.: "Super-Exponential Complexity of Presburger Arithmetic",

(a) *MAC Technical Memorandum 43*, MIT, Project MAC, Cambridge, Mass. 02139;
(b) in: *Proceedings of the AMS Symposium on the Complexity of Computational Processes*, 1974, vol. VII, erschienen: New York, 1974.

[GG81] Grattan-Guinness, I.: "On the Development of Logics between the two World Wars", *Amer. Math. Monthly 88*, 1981, no. 7, p. 495–509.

[Ga94] Gandy, R. [ed.]: „The Confluence of Ideas in 1936", in: Herken, R.: *The Universal Turing Machine – A Half-Century Survey*, Springer Verlag, Wien – New York, 1994.

[Gö31] Gödel, K.: „Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme", *Monatshefte für Mathematik und Physik 38*, 1931, S. 173–198.

[HA28] Hilbert, D., Ackermann, W.: *Grundzüge der theoretischen Logik*, Springer-Verlag, Berlin, 1928.

[HiBe68] Hilbert, D., Bernays, P.: *Grundlagen der Mathematik I*, Zweite Auflage, Springer Verlag, Berlin – Heidelberg – New York, 1968.

[Hi1900] Hilbert, D.: „Mathematische Probleme", Vortrag gehalten auf dem Internationalen Mathematikerkongreß, Paris 1900, (Abschnitt 2: „Die Widerspruchslosigkeit der arithmetischen Axiome"); abgedruckt in: *Nachr. Ges. Wiss., Göttingen, Math.-Phys.-Kl.*, 1900, S. 253–297 (mit Zusätzen des Verfassers), und im *Archiv d. Math. u. Phys.*, 3. Reihe, Bd. I, 1901, S. 44–63, 213–237, 299–301.

[HoUl69] Hopcroft, J.E., Ullman, J.D.: *Formal Languages and their Relation to Automata*, Addison-Wesley, Publishing Company, Reading, Mass. – Menlo Park, Cal. – Don Mills, Ont., 1969.

[HoUl79] Hopcroft, J.E., Ullman, J.D.: *Introduction to Automata Theory, Languages and Computation*, Addison-Wesley Publishing Company, Reading, Mass. – Menlo Park, Cal. – London – Amsterdam – Don Mills, Ont. – Sydney, 1979.

[Jo90] Johnson, D.S.: "A Catalogue of Complexity Classes", Chapter 2 in: van Leeuwen, J. [ed.]: *Algorithms and Complexity*, Elsevier, Amsterdam – New York – Oxford – Tokyo, 1990.

[KrKr72] Kreisel, G., Krivine, J.-L.: *Modelltheorie*, Springer-Verlag, Berlin – Heidelberg – New York, 1972.

[NZ76] Niven, I., Zuckerman, H.I.: *Einführung in die Zahlentheorie*, Band I, Band II, B.I. Hochschultaschenbuch (Band 47), B.I. Wissenschaftsverlag, Mannheim – Wien – Zürich, 1976, unveränderter Nachdruck, 1987.

[Opp73] Oppen, D.C.: "Elementary Bounds for Presburger Arithmetic", *Proceedings of the 5th ACM Symposium on the Theory of Computing*, 1973, 34–37.

[PaHa77] Paris, J.B., Harrington, L.: „A Mathematical Incompleteness in Peano Arithmetic", in: *Handbook of Mathematical Logic*, North-Holland 1977, pp. 1133–1142.

[Pet67] Peter, R.: *Recursive Functions*, Academic Press, 1967.

[Pre29] Presburger, M.: „Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt", in: Sprawozdanie z I Kongresu Matematykow Krajow Slowjanskich - Warsaw 1929 (*Comptes-rendus du premier Congres des Mathemaciens des Pays Slaves, Warsaw 1929*), Warschau 1930, S. 92-101, 395.

[Ra77] Rabin, M.O.: "Decidable Theories", in: *Handbook of Mathematical Logic*, North-Holland Publishing Company, 1977.

[Rei90] Reischuk, K.R.: *Einführung in die Komplexitätstheorie*, B. G. Teubner, Stuttgart, 1990.

[Rem84] Remmert, R.: *Funktionentheorie I*, Reihe Grundwissen Mathematik, 5, Springer-Verlag, Berlin – Heidelberg – New York – London – Paris, 1984 (Zweite, überarbeitete und ergänzte Auflage, 1989).

[Rit63] Ritchie, R.W.: "Classes of Predictable Computable Functions", *Transactions of the AMS 106*, 1963, 139–173.

[Riv90] Rivest, R.: "Cryptography", Chapter 13 in: van Leeuwen, J. [ed.]: *Algorithms and Complexity*, Elsevier, Amsterdam – New York – Oxford – Tokyo, 1990.

[SFM73] Seiferas, J.I., Fischer, M.J., Meyer, A.R.: "Refinements of the Nondeterministic Time and Space Hierarchies", *Proceedings of the 14th IEEE Symposium on Switching and Automata Theory*, 1973, 130–137.

[SFM78] Seiferas, J.I., Fischer, M.J., Meyer, A.R.: "Separating Nondeterministic Time Complexity Classes", *Journal of the ACM 25*, 1978, 146–167.

[Shoe67] Shoenfield, J.R.: *Mathematical Logic*, Addison-Wesley Publishing Company, Reading, Mass. – Menlo Park, Cal. – London – Don Mills, Ont. , 1967, 1973.

[Sko31] Skolem, Th.: „Über einige Satzfunktionen in der Arithmetik“, *Skrifter Norske Vid. Akad. Oslo I. Klasse no. 7*, Oslo, 1930.

[SM73] Stockmeyer, L.J., Meyer, A.R.: “Word Problems Requiring Exponential Time: Preliminary Report”, *Proceedings of the 5th ACM Symposium on the Theory of Computing*, 1973, 1–9.

[Sto74] Stockmeyer, L.J.: “The Complexity of Decision Problems in Automata Theory and Logic”, *Project MAC Technical Report 133*, 1974.

[Tar28] Tarski, A.: Remarques sur les notions fondamentales de la Méthodologie des Mathématiques, *Annales de la Société Polonaise des Mathématique*, Tome VII. Année 1928, 270–272.

[Th95] Thiel, Ch.: *Philosophie und Mathematik* (eine Einführung in ihre Wechselwirkungen und in die Philosophie der Mathematik), Wissenschaftliche Buchgesellschaft, Darmstadt, 1995.

[vD94] van Dalen, D.: „Der Grundlagenstreit zwischen Brouwer und Hilbert“, in: Eichhorn, E., Thiele, E.J. [Hrsg.]: *Vorlesungen zum Gedenken an Felix Hausdorff*, Berliner Schriftenreihe zur Mathematik, Band 5, Heldermann Verlag Berlin, 1994.

[vEB90] van Emde Boas, P.: “Machine Models and Simulations”, Chapter 1 in: van Leeuwen, J. [ed.]: *Algorithms and Complexity*, Elsevier, Amsterdam – New York – Oxford – Tokyo, 1990.

[vN27] von Neumann, J.: „Zur Hilbertschen Beweistheorie“, *Math. Zentralbl. 26*, 1927, S. 1–46; neu abgedruckt in: Taub, A.H. [ed.]: *Collected Works*, vol. I, Pergamon Press, Oxford, 1961.

[Z83] Zak, S.: “A TM Time Hierarchy”, *Theoretical Computer Science 26*, 1983, 327–333.