Beschränkte Arithmetik
in
scharf beschränkten Theorien zweiter Stufe

von
Arnold Beckmann
aus Lünen

Dem Institut für
mathematische Logik und Grundlagenforschung
am Fachbereich 15 - Mathematik
der Westfälischen Wilhelms-Universität Münster
als Diplomarbeit eingereicht

im September 1992

„Unsere größte Schwäche ist die Verschwendung an Zeit, für die der Mangel an Mut verantwortlich ist, das als unwesentlich Erkannte auch für unwesentlich zu erklären.“

Hinrich Seidel,
Präsident der Europäischen Rektorenkonferenz

Inhalt

Einleitung

Aus der theoretischen Informatik kommt die Fragestellung nach dem effizientesten Algorithmus, um ein gegebenes Problem zu lösen. In diesem Zusammenhang wird die von Meyer-Stockmeyer in [Stockmeyer 1976] eingeführte Polynomiale Hierarchie $\mathbf{PH} = \bigcup_i \mathbf{\Delta_i^p}$ von Prädikaten auf natürlichen Zahlen betrachtet, deren bekannteste Vertreter die Klassen $\mathbf{P} = \mathbf{\Delta_1^p}$ und $\mathbf{NP} = \mathbf{\Sigma_1^p}$ sind. **P** enthält alle Prädikate, die durch eine Turingmaschine in polynomialer Zeit berechenbar sind, und **NP** alle diejenigen, für die eine nicht-deterministische Turingmaschine analoges leistet.
Wichtige offene Probleme sind die Fragen

(i) $\mathbf{P} = \mathbf{NP}$?

oder weitergehend

(ii) kollabiert **PH** ?

Zudem gibt es die Klassen **PSPACE**, die aus allen durch eine Turingmaschine mit polynomialen Platzbedarf berechenbaren Prädikaten besteht, und **EXPTIME**, in der genau die durch eine Turingmaschine in exponentieller Zeit berechenbaren Prädikate liegen. Damit schließen sich weitere offene Fragen an:

(iii) $\mathbf{PSPACE} = \mathbf{PH}$?

(iv) $\mathbf{PSPACE} = \mathbf{EXPTIME}$?

S. Buss ist in [Buss 1986] ein wichtiger Schritt zur mathematisch-logischen Beschreibung des aufgezeigten Problemkreises gelungen, indem er in der Beschränkten Arithmetik die mathematischen Theorien $\mathbf{S_2^i}$, $\mathbf{T_2^i}$, $\mathbf{U_2^i}$ und $\mathbf{V_2^i}$ eingeführt hat. $\mathbf{S_2^i}$ und $\mathbf{T_2^i}$ sind Theorien erster Stufe, die in enger Beziehung zu $\mathbf{\Delta_i^p}$ und $\mathbf{\Delta_{i+1}^p}$ stehen. $\mathbf{U_2^i}$ und $\mathbf{V_2^i}$ sind Theorien zweiter Stufe, die mit **PSPACE** und **EXPTIME** eng verknüpft sind.
Die für die eingangs erwähnten Probleme relevanten Fragestellungen in der Beschränkten Arithmetik sind:

(i) Ist $\mathbf{S_2^i} = \mathbf{T_2^i}$ oder $\mathbf{S_2^{i+1}} = \mathbf{T_2^i}$ für ein i ?

(ii) Kollabiert die Hierarchie der Beschränkten Arithmetik ?

(iii) Ist $\mathbf{U_2^1}$ eine konservative Erweiterung von $\mathbf{S_2} := \bigcup_i \mathbf{S_2^i}$?

(iv) $\mathbf{U_2^1} = \mathbf{V_2^1}$?

Die bisher gefundenen Resultate über Zusammenhänge zwischen den beiden Problemgruppen sind:

(a) $\mathbf{S_2^{i+1}} = \mathbf{T_2^i}$ impliziert $\mathbf{\Sigma_{i+2}^p} = \mathbf{\Pi_{i+2}^p}$ und damit den Kollabs von **PH**. Zudem wird in [Krajíček-Pudlák-Takeuti 1991] $\mathbf{S_2^{i+1}}(\mathcal{A}) \neq \mathbf{T_2^i}(\mathcal{A})$ für $i \geq 1$ gezeigt, wobei $\mathbf{S_2^{i+1}}(\mathcal{A})$ und $\mathbf{T_2^i}(\mathcal{A})$ aus $\mathbf{S_2^{i+1}}$ bzw. $\mathbf{T_2^i}$ durch Hinzufügen von freien Mengenvariablen hervorgehen.

(b) $\mathbf{S_2^0} \neq \mathbf{T_2^0}$ wird in [Takeuti 1990a] bewiesen.

(c) In [Takeuti 1988] und [Takeuti 1990b] wird gezeigt, daß $\mathbf{V_2^1}$ keine konservative Erweiterung von $\mathbf{S_2^1}$ ist.

(d) Außerdem hat P. Pudlák gezeigt, daß für $i = 1$ und $i = 2$ $\mathbf{S_2^i}(\mathcal{A}) \neq \mathbf{T_2^i}(\mathcal{A})$ gilt. (S. Buss hat dies für $i = 1$ bewiesen.)

Ziel dieser Arbeit ist es, Theorien $\mathbf{U_2^{i,w^\star}}$ anzugeben, so daß sich in $\mathbf{U_2^{w^\star}} = \bigcup_i \mathbf{U_2^{i,w^\star}}$ die Polynomiale Hierarchie **PH** charakterisieren und $\mathbf{U_2^{w^\star}}$ von $\mathbf{U_2^1}$ separieren läßt. Also ist $\mathbf{U_2^1}$ zwar eine Erweiterung von $\mathbf{U_2^{w^\star}}$, aber keine konservative. Mithin läßt sich das auf die Theorien $\mathbf{U_2^{i,w^\star}}$, die im wesentlichen zu $\mathbf{S_2^i}$ äquivalent sind, übertragene Problem (iii) aus der Beschränkten Arithmetik lösen, und es liegt die Vermutung nahe, daß $\mathbf{U_2^1}$ keine konservative Erweiterung von $\mathbf{S_2}$ ist.

Im Folgenden skizzieren wir die wichtigen Ideen auf dem Weg zu dem gerade beschriebenen Ziel, die dann in der Arbeit ausführlich behandelt werden.
Wir geben die Theorien $\mathbf{U_2^{i,w^\star}}$ an, indem wir zuerst schwache zweitstufige Formelmengen $\mathbf{\Sigma_i^{1,w^\star}}$ und $\mathbf{\Pi_i^{1,w^\star}}$ definieren, die im wesentlichen zweitstufige Versionen von $\mathbf{\Sigma_i^b}$ und $\mathbf{\Pi_i^b}$ sind. Dazu werden beschränkte erststufige Quantoren $Qx{\leq}t\, F(x)$ in den von Buss eingeführten Formelmengen $\mathbf{\Sigma_i^b}$ und $\mathbf{\Pi_i^b}$ durch scharf beschränkte zweitstufige Quantoren $Q\phi\, G(\phi^{|t|})$ ersetzt. Dabei ist $|t|$, die Länge von t, ungefähr $\log_2(t)$. Einen Hinweis auf die gleiche Ausdrucksstärke von $\mathbf{\Sigma_i^b}/\mathbf{\Pi_i^b}$ und $\mathbf{\Sigma_i^{1,w^\star}}/\mathbf{\Pi_i^{1,w^\star}}$ erhalten wir, indem wir ein scharf beschränktes Anfangsstück einer Menge $\alpha^{|t|} = \{u < |t| : u \in \alpha\}$ als Binärdarstellung der Zahl

$$\sum_{i<|t|} (i)_\alpha \cdot 2^i \quad \text{mit} \quad (i)_\alpha = \begin{cases} 0 & : \quad i \notin \alpha \\ 1 & : \quad i \in \alpha \end{cases}$$

auffassen ($\sum_{i<|t|}(i)_\alpha \cdot 2^i \leq 2^{|t|} \approx t$).
Sei Ψ eine Formelmenge, dann haben die uns interessierenden polynomialen Induktionen die Gestalt

$$(\Psi\text{-PIND}) \quad A(0) \wedge \forall x\, (A(\lfloor \tfrac{1}{2}x \rfloor) \rightarrow A(x)) \rightarrow A(t)$$

oder äquivalent

$$(\Psi\text{-LIND}) \quad A(0) \wedge \forall x\, (A(x) \rightarrow A(\mathrm{S}x)) \rightarrow A(|t|)$$

mit $A \in \Psi$. Die scharf beschränkte Komprehension hat die Gestalt

$$(\mathrm{w}\Psi\text{-CA}) \quad \exists X\, \forall x{\leq}|t|\, \Big(x \in \phi^{|t|} \leftrightarrow A(x)\Big)$$

mit $A \in \Psi$.
($\mathbf{\Sigma^b_i}$-PIND) aus $\mathbf{S^i_2}$ wird in $\mathbf{U^{i,w^\star}_2}$ durch ($\mathbf{\Sigma^{1,w^\star}_i}$-LIND) und (w$\mathbf{\Sigma^{1,w^\star}_0}$-CA) ersetzt. Diese Komprehension reicht, da sich damit (w$\mathbf{\Sigma^{1,w^\star}_i}$-CA) in $\mathbf{U^{i,w^\star}_2}$ beweisen läßt.
Über den Hauptsatz der Beschränkten Arithmetik

$$\mathrm{A} \in \mathbf{\Delta^p_i} \iff \text{A ist in } \mathbf{\Delta^b_i} \text{ bezüglich } \mathbf{S^i_2}$$

erhalten wir als wesentliche Charakterisierung von $\mathbf{U^{i,w^\star}_2}$

$$\mathrm{A} \in \mathbf{\Delta^p_i} \iff \text{A ist in } \mathbf{\Delta^{1,w^\star}_i} \text{ bezüglich } \mathbf{U^{i,w^\star}_2}\,.$$

Insofern ist $\mathbf{U^{w^\star}_2} = \bigcup_i \mathbf{U^{i,w^\star}_2}$ im wesentlichen äquivalent zu $\mathbf{S_2} = \bigcup_i \mathbf{S^i_2}$.

Abschließend geben wir in dieser Arbeit mehrere Beispiele an, die $\mathbf{U^{w^\star}_2}$ von $\mathbf{U^1_2}$ separieren.

(i) Das volle Induktionsaxiom ist nicht in $\mathbf{U^{w^\star}_2}$ herleitbar, während $\mathbf{U^1_2}$ es beweist.

(ii) Eine Formulierung des Fermatschen Satzes ist nicht in $\mathbf{U^{w^\star}_2}$ herleitbar, während $\mathbf{U^1_2}$ sie beweist.

(iii) Eine Formulierung des Wilsonschen Satzes ist nicht in $\mathbf{U^{w^\star}_2}$ herleitbar, während $\mathbf{U^1_2}$ sie beweist.

(iv) $\mathbf{U^{w^\star}_2}$ leitet nicht

$$\exists x{\leq}2\cdot c\, \forall y{<}|c|\, (\mathrm{Bit}(y,x) = 1 \leftrightarrow y \in \alpha)$$

her, während $\mathbf{U^1_2}$ dies beweist.

Wir zeigen sogar noch mehr, indem wir eine Erweiterung $\mathbf{U^w_2}$ von $\mathbf{U^{w^\star}_2}$ betrachten, die sich von $\mathbf{U^1_2}$ separieren läßt. Dazu erweitern wir $\mathbf{\Sigma^{1,w^\star}_i}$ zu $\mathbf{\Sigma^{1,w}_i}$ vermöge Ersetzung der scharf beschränkten Mengenquantoren in $\mathbf{\Sigma^{1,w^\star}_i}$ $\mathrm{Q}\phi\, F(\phi^{|t|})$ durch beliebige Mengenquantoren. Damit ist $\mathbf{\Sigma^{1,w}_i}$ abgeschlossen unter $\mathrm{Q}x{\leq}|t|$ und $\exists\phi$; es werden also die Alternationen der Mengenquantoren gezählt. Dann sei $\mathbf{\Sigma^{1,w}} := \bigcup_i \mathbf{\Sigma^{1,w}_i}$.
G. Takeuti hat in seinem, dieser Arbeit zugrundeliegenden Artikel [Takeuti 1991] aus $\mathbf{U^{i,w^\star}_2}$ mittels Ersetzen von ($\mathbf{\Sigma^{1,w^\star}_i}$-LIND) und (w$\mathbf{\Sigma^{1,w^\star}_0}$-CA) durch ($\mathbf{\Sigma^{1,w}}$-LIND) bzw. ($\mathbf{\Sigma^{1,w}_1}$-CA) $\mathbf{U^w_2}$ erhalten. Diese Wahl des Komprehensionsaxioms ist begründet in der Notwendigkeit, in $\mathbf{U^w_2}$ Schnitte zu eliminieren, wozu Takeuti sein Verfahren aus [Takeuti 1987] für ($\mathbf{\Sigma^1_1}$-CA) verwendet. Wie wir sehen werden, wird so mit Kanonen auf Spatzen geschossen.
Es ist bekannt ([Buss 1986] §9), daß zweitstufige Beschränkte Arithmetik nicht stärker ist als Peano Arithmetik. Somit liegt die Vermutung nahe, daß ein kombinatorisch so

aufwendiges Verfahren, wie es für die Bewältigung der Schnittelimination von ($\mathbf{\Sigma^1_1}$-CA) benötigt wird, zu umgehen sein müßte.
Wir tuen dies, indem wir Takeutis Definition von $\mathbf{U^w_2}$ in bezug auf die Komprehension zu

($\mathbf{\Sigma^{1,w}}$-CA)

erweitern, und durch einen Trick die vollständige Schnittelimination in einem halbformalen Kalkül prädikativ beweisen. (Ähnliche halbformale Systeme werden ausführlich zum Beispiel in [Pohlers 1989] vorgestellt.) In dem halbformalen Kalkül werden nur beschränkte, erststufig geschlossene Formeln hergeleitet, also solche ohne freie Individuenvariablen; er formalisiert im erststufigen Bereich mit Hilfe einer beschränkten ω-Regel

$$\Gamma, F(\underline{n}) \quad \text{für alle } n \leq t \quad \Longrightarrow \quad \Gamma, \forall x{\leq}t\, F(x)$$

die Wahrheit im Standardmodell. Im zweitstufigen Bereich benötigen wir wegen der Verwendung freier Mengenvariablen weiterhin ($\mathbf{\Sigma^{1,w}_0}$-CA). Der Trick besteht nun darin, ($\mathbf{\Sigma^{1,w}}$-CA) in dem halbformalen System zu beweisen.

Um die Vorgehensweise zur Begründung der Unbeweisbarkeit obiger Aussagen in $\mathbf{U^{w^\star}_2}$ zu erläutern, betrachten wir zuerst eine minimale Teilmenge der natürlichen Zahlen, die für die Gültigkeit solch einer Aussage benötigt wird. Aufgrung der Vollständigkeit des halbformalen Kalküls sind damit im wesentlichen diejenigen Zahlen gemeint, die in einem halbformalen Beweis der festgehaltenen Aussage auftauchen müssen. Wir werden sehen, daß diese Menge polynomial in den Parametern der Aussage wächst.
Gäbe es im Zusammenhang mit solch einer Aussage einen formalen Beweis, in dem jeder ($\forall$)-Schluß die Gestalt

$$\Gamma, a \not\leq |t|, A(a) \quad \Longrightarrow \quad \Gamma, \forall x{\leq}|t|\, A(x)$$

mit $a \notin \mathsf{FV}(\Gamma, \forall x{\leq}|t|\, A(x))$ und jeder Induktionsschluß die Gestalt

$$\Gamma, \neg A(a), A(\mathrm{S}a) \quad \Longrightarrow \quad \Gamma, \neg A(0), A(|t|)$$

mit $a \notin \mathsf{FV}(\Gamma, A(|t|))$ hat. Dann werden die Prämissen dieser Schlüsse bei Einbettung in den halbformalen Kalkül nur für $a{\leq}|t|{\leq}\mathrm{p}_t(|\vec{a}|)$ mit $\mathsf{FV}(t) \subset \{\vec{a}\}$ und einem Polynom p_t benötigt. Übertragen wir diese Beobachtung auf den gesammten Beweis, so folgt, daß die Anzahl der in dem halbformalen Kalkül benutzten natürlichen Zahlen durch ein Polynom in der Länge der Parametervariablen des Beweises beschränkt ist. Da aber, wie wir oben gesehen haben, mindestens polynomial in den Parametern, was gleichbedeutend ist mit exponentiell in der Länge der Parameter, viele Zahlen benötigt werden, führt ein Vergleich der Wachstumsraten zum Widerspruch.
Dies zeigt die Unbeweisbarkeit jener Aussagen.

Zum Abschluß dieser einführenden Worte bleibt mir noch all denen zu danken, die mit dem Gelingen meiner Arbeit verbunden sind. Da sind ganz allgemein die Mitarbeiter des Instituts für mathematische Logik und Grundlagenforschung zu erwähnen, die mich in ihren Kreis aufgenommen haben. Speziell hat Thomas Glaß mit seiner konstruktiven Kritik das Ende der Arbeit in absehbare Nähe gerückt.
Mein besonderer Dank gilt Herrn Prof. Dr. Pohlers für die Anregung und Betreuung dieser Arbeit.

Teil A

Beschränkte Arithmetik

1 Die Polynomiale Hierarchie

In diesem ersten Paragraphen tragen wir die wesentlichen Begriffe, die zum Aufbau der Polynomialen Hierarchie benötigt werden, zusammen. Wir wählen den mathematisch logischen Zugang und erwähnen den berechenbarkeitstheoretischen nur dort, wo es nötig ist. Die Äquivalenz beider Wege wird unter anderem in dem ersten Teil in [Buss 1986] ausgeführt.

Die Grundidee hinter der Polynomialen Hierarchie ist die, das Berechenbarkeitskonzept von „rekursiven“ auf „polynomiale-Zeit“ Berechnungen abzuschwächen, um so zu Funktionen zu gelangen, die nicht nur intuitiv (also durch einen Algorithmus), sondern darüberhinaus auch durchführbar („feasible“) berechenbar sind. In „polynomialer Zeit“ heißt, daß die Rechenzeit, also die Anzahl der zur Berechnung des Ergebnisses benötigten Rechenschritte, durch ein Polynom in der Länge der Eingabe, die als Anzahl der Bits in der Binärdarstellung der Eingabe definiert ist, beschränkt ist. Durch die Einschränkung des Berechenbarkeitsbegriffs ergibt sich automatisch eine polynomiale Wachstumsrate der berechneten Funktion, da die polynomiale Zeitschranke auch eine obere Schranke der von dem Ergebnis belegten Bandfelder einer Turingmaschine, also der Länge des Ergebnisses, ist.

1.1 Definition

(a) Die *Länge* $|n|$ *einer natürlichen Zahl* n ist die Anzahl der Bits in ihrer Binärdarstellung:

$$|n| := \lceil \log_2(n+1) \rceil$$

(für reelle Zahlen r ist $\lceil r \rceil$ die kleinste ganze Zahl z mit $z \geq r$).
Für Tupel $\vec{n} = (n_1, \ldots, n_k)$ schreiben wir

$$|\vec{n}| := (|n_1|, \ldots, |n_k|) .$$

(b) p ist ein *geeignetes Polynom*, wenn p nur nichtnegative Koeffizienten hat.

(c) Eine Funktion $f : \mathbb{N}^k \to \mathbb{N}$ hat eine *polynomiale Wachstumsrate*, wenn es ein geeignetes Polynom p gibt mit

$$\forall \vec{n} \in \mathbb{N}^k \Big(|f(\vec{n})| \leq p(|\vec{n}|) \Big) .$$

(d) Sei f eine Funktion. Eine Turingmaschine M_f *berechnet* f *in polynomialer Zeit*, wenn sie f berechnet und die Anzahl der Rechenschritte $\overline{\mathbf{RZ}}_{M_f}$ zur Berechnung von f durch ein Polynom p in der Länge der Eingabe beschränkt ist:

$$\forall \vec{n} \in \mathbb{N}^k \Big(\overline{\mathbf{RZ}}_{M_f}(\vec{n}) \leq p(|\vec{n}|) \Big) .$$

Es gibt verschiedene Möglichkeiten, polynomiale-Zeit-Turingmaschinen mit Orakeln für Funktionen exakt zu definieren. Die in [Buss 1986] gewählte zählt eine Orakelanfrage als einen Rechenschritt und fügt eine a priori Beschränkung an den Platzbedarf der Turingmaschine.

P sei die Menge aller Funktionen, die durch eine Turingmaschine in polynomialer Zeit berechnet werden.
PSPACE sei die Menge aller Funktionen f mit polynomialer Wachstumsrate, so daß für eine Turingmaschine M_f, die f berechnet, die Anzahl der benutzbaren Bandfelder durch ein Polynom in der Länge der Eingabe beschränkt ist.
Zum Beispiel sind folgende Funktionen aus **P**:

- die Konstante Nullfunktion 0 ,
- die Nachfolgerfunktion $n \mapsto \mathrm{S}n$,
- die Addition $(m,n) \mapsto m+n$,
- die Multiplikation $(m,n) \mapsto m \cdot n$,
- die „shift right“-Funktion $n \mapsto \lfloor \frac{1}{2} n \rfloor$, die jeder natürlichen Zahl n das größte Ganze kleinergleich n zuweist,
- die Funktion $n \mapsto |n|$, die jeder natürlichen Zahl n ihre Länge zuweist,
- die „smash“-Funktion $(m,n) \mapsto m\#n \quad = 2^{|m|\cdot|n|}$,
- die arithmetische Subtraktion

$$(m,n) \mapsto m \dot{-} n \quad = \begin{cases} m-n & : \quad m-n \geq 0 \\ 0 & : \quad m-n < 0 \end{cases} ,$$

- die Funktionen $(m,n) \mapsto \mathrm{MSP}(m,n)$ und $(m,n) \mapsto \mathrm{LSP}(m,n)$, die den höherwertigen Teil („more significant part“) und den niederwertigen Teil („less significant part“) einer Zahl m berechnen. Sie sind eindeutig bestimmt durch

$$m = \mathrm{MSP}(m,n) \cdot 2^n + \mathrm{LSP}(m,n)$$

und

$$|\mathrm{LSP}(m,n)| \leq n \qquad \text{oder äquivalent dazu} \qquad \mathrm{LSP}(m,n) < 2^n ,$$

- die Funktion $(m,n) \mapsto \mathrm{Bit}(m,n)$, die das m-te Bit in der Binärdarstellung von n berechnet,

– Kodier- und Dekodierfunktionen für Gödelnummern $\langle n_1, \ldots, n_k \rangle$ von endlichen Sequenzen natürlicher Zahlen:

$$\beta(i, \langle n_1, \ldots, n_k \rangle) = \begin{cases} k & : \quad i = 0 \\ n_i & : \quad 0 < i \leq k \end{cases}$$

$$n_0 * \langle n_1, \ldots, n_k \rangle = \langle n_0, n_1, \ldots, n_k \rangle \,,$$

– die Funktion $(m, n) \mapsto \mathrm{Rem}(m, n)$, die den Rest berechnet, der bei der ganzzahligen Division von m durch n auftritt. Es gilt

$$\mathrm{Rem}(m, n) < n$$

und

$$\exists k \in \mathbb{N}\Big(m = k \cdot n + \mathrm{Rem}(m, n)\Big) \,.$$

Die Klasse der in polynomialer Zeit berechenbaren Funktionen läßt sich induktiv erzeugen. Wir benötigen dazu ein schwächeres Konzept als die primitive Rekursion, nämlich die limitierte Iteration.

1.2 Definition

Seien $k \geq 0$, $g : \mathbb{N}^k \to \mathbb{N}$, $h : \mathbb{N}^{k+2} \to \mathbb{N}$ beliebige Funktionen und p, q geeignete Polynome. $f : \mathbb{N}^k \to \mathbb{N}$ heißt *definiert durch limitierte Iteration von g und h mit Zeitschranke p und Platzschranke q*, wenn folgendes gilt:

Sei $\tau := \mathcal{R}(g, h)$, also $\tau : \mathbb{N}^{k+1} \to \mathbb{N}$ mit

$$\begin{aligned} \tau(\vec{m}, 0) &= g(\vec{m}) \\ \tau(\vec{m}, n+1) &= h(\vec{m}, n, \tau(\vec{m}, n)) \,, \end{aligned}$$

so daß

$$\forall \vec{m} \in \mathbb{N}^k \Big[\forall n \leq p(|\vec{m}|) \Big(|\tau(\vec{m}, n)| \leq q(|\vec{m}|)\Big)\Big]$$

ist. Dann ist f definiert durch

$$\forall \vec{m} \in \mathbb{N}^k \Big(f(\vec{m}) = \tau(\vec{m}, p(|\vec{m}|))\Big) \,.$$

Für den formalen induktiven Aufbau einer Funktionenklasse benötigen wir im ersten Schritt eine Menge von Grundfunktionen, die ihrer Bezeichnung entsprechend möglichst einfach sein sollen. Eine erzeugende Menge einfacher Funktionen, wie sie auch in [Buss 1986] steht, ist die Menge B:

1.3 Definition

(a) B sei die Menge folgender Funktionen:

(1) die Nullfunktion 0,

(2) die Nachfolgerfunktion S,

(3) die „shift right“-Funktion $\lfloor \frac{1}{2}.\rfloor$,

(4) die “shift left“-Funktion $n \mapsto 2 \cdot n$,

(5) die Funktion $(m,n) \mapsto m \leq n \quad = \begin{cases} 1 & : \quad m \leq n \\ 0 & : \quad m > n \end{cases}$

(6) die Funktion $(l,m,n) \mapsto Choise(l,m,n) \quad = \begin{cases} m & : \quad l > 0 \\ n & : \quad l = 0 \end{cases}$

(b) Sei C eine Menge von Funktionen mit polynomialer Wachstumsrate. Der *polynomiale Zeitabschluß von* C, $\mathrm{PTC}(C)$, ist die kleinste Menge von Funktionen, die

(1) C und B enthält und

(2) abgeschlossen ist unter Komposition und limitierter Iteration.

Die Begründung dafür, daß der gerade definierte mathematische Begriff des polynomialen Zeitabschlusses mit dem zuvor definierten berechenbarkeitstheoretischen Begriff übereinstimmt, ist die folgende Aussage, die in [Buss 1986] §1.2 Theorem 2 und Korollar 3 begründet werden.

1.4 Satz

Sei C eine Menge von Funktionen mit polynomialer Wachstumsrate. f ist in $\mathrm{PTC}(C)$ genau dann, wenn eine Turingmaschine mit Orakel für endlich viele Funktionen aus C in polynomialer Zeit f berechnet. □

1.5 Korollar

$\mathbf{P} = \mathrm{PTC}(\emptyset)$ □

Eine *arithmetische Formel* ist eine Formel der Logik erster Stufe, die die logischen Symbole $=, \neq, \wedge, \vee, \exists, \forall$ und die nichtlogischen Symbole 0, S, $+$, $\cdot$, $|.|$, $\lfloor \frac{1}{2}.\rfloor$, $\#$, $\leq$, $\not\leq$ enthalten kann. Die Funktionszeichen repräsentieren die entsprechende Funktion und die nichtlogischen Relationszeichen stehen für

$\leq$ kleinergleich

$\not\leq$ nicht kleinergleich.

Die Wahl der Funktionszeichen ist nicht willkürlich. Zu jedem geeigneten Polynom p gibt es einen Term t, der neben freien Variablen höchstens die Funktionen $0, \mathrm{S}, \lfloor \frac{1}{2}.\rfloor, \cdot, \#$

enthält, mit

$$\forall \vec{n} \in \mathbb{N}^k \Big[t(\vec{n}) = 2^{p(|\vec{n}|)} \Big] .$$

Also hat f eine polynomiale Wachstumsrate genau dann, wenn es einen Term t mit

$$\forall \vec{n} \in \mathbb{N}^k \Big[f(\vec{n}) \leq t(\vec{n}) \Big]$$

gibt.
Zur Übersicht schreiben wir abkürzend

$$\forall x{\leq}t \, (\ldots) \quad \text{für} \quad \forall x \, (x \not\leq t \vee \ldots)$$

und

$$\exists x{\leq}t \, (\ldots) \quad \text{für} \quad \exists x \, (x \leq t \wedge \ldots) .$$

Die Quantoren dieser Gestalt heißen *beschränkt*. Sie heißen *scharf beschränkt*, falls es einen Term s mit $t \equiv |s|$ gibt.
Mit obiger Bemerkung sieht man, daß beschränkte Quantoren den polynomial beschränkten Quantoren

$$\mathrm{Q}x{\leq}2^{p(|\vec{n}|)} \, (\ldots)$$

und scharf beschränkte Quantoren den logarithmisch beschränkten Quantoren

$$\mathrm{Q}x{\leq}p(|\vec{n}|) \, (\ldots)$$

entsprechen, mit denen auf dem berechenbarkeitstheoretischen Weg, wie zum Beispiel in [Buss 1986], die Polynomiale Hierarchie konstruiert wird.
Wir definieren nun eine Hierarchie von beschränkten arithmetischen Formeln analog zur arithmetischen Hierarchie, wobei hier die beschränkten bzw. scharf beschränkten Quantoren die Rolle der unbeschränkten resp. beschränkten in der arithmetischen Hierarchie übernehmen.

1.6 Induktive Definition der Formelmengen $\mathbf{\Sigma^b_i}$ und $\mathbf{\Pi^b_i}$

(a) $\mathbf{\Sigma^b_0} = \mathbf{\Pi^b_0}$ sei die Menge aller arithmetischen Formeln, deren Quantoren scharf beschränkt sind.

(b) $\mathbf{\Sigma^b_{k+1}}$ sei die kleinste Menge mit
   (1) $\mathbf{\Sigma^b_{k+1}} \supseteq \mathbf{\Pi^b_k}$
   (2) $A(a) \in \mathbf{\Sigma^b_{k+1}} \implies \exists x{\leq}t \, A(x), \forall x{\leq}|t| \, A(x) \in \mathbf{\Sigma^b_{k+1}}$
   (3) $A, B \in \mathbf{\Sigma^b_{k+1}} \implies A \wedge B, A \vee B \in \mathbf{\Sigma^b_{k+1}} .$

(c) $\mathbf{\Pi^b_{k+1}}$ sei in dualer Weise definiert.

Damit sind wir in der Lage, die Polynomiale Hierarchie zu entwickeln. Wir nutzen dabei neben der Definition in [Buss 1986] §1.4 noch [Buss 1986] §1.6 Theorem 8 aus. Für eine Klasse von Funktionen C sei $\mathrm{Pred}(C)$ die Menge aller charakteristischen Funktionen, also Funktionen f mit $rng(f) \subseteq \{0,1\}$, in C.

1.7 Induktive Definition der Polynomialen Hierarchie

(a) $\mathbf{\Sigma_k^p}$ sei die Menge aller Prädikate, die durch eine $\mathbf{\Sigma_k^b}$-Formel definiert werden.

(b) $\mathbf{\Pi_k^p}$ sei die Menge aller Prädikate, die durch eine $\mathbf{\Pi_k^b}$-Formel definiert werden.

(c) $\mathbf{\Delta_0^p} := \mathbf{\Sigma_0^p} (= \mathbf{\Pi_0^p})$

(d) $\mathbf{\square_{k+1}^p} := \mathrm{PTC}(\mathbf{\Sigma_k^p})$

(e) $\mathbf{\Delta_{k+1}^p} := \mathrm{Pred}(\mathbf{\square_{k+1}^p})$

(f) $\mathbf{PH} := \bigcup_k \mathbf{\Sigma_k^p}$

Bemerkung

Wie schon oben festgestellt ist $\mathbf{P} = \mathrm{PTC}(\emptyset)$. Zusätzlich halten wir fest:

$$\mathbf{\square_1^p} = \mathbf{P} \,,$$

da mit $\mathbf{\Delta_0^p} \subset \mathbf{P}$, der Monotonie von PTC und Korollar 1.5

$$\mathbf{\square_1^p} = \mathrm{PTC}(\mathbf{\Delta_0^p}) \subset \mathrm{PTC}(\mathbf{P}) = \mathbf{P}$$

und

$$\mathbf{P} = \mathrm{PTC}(\emptyset) \subset \mathrm{PTC}(\mathbf{\Delta_0^p}) = \mathbf{\square_1^p}$$

gilt.

Die Schichten der Polynomialen Hierarchie lassen sich in mathematischen Theorien der Logik erster Stufe beschreiben. Deren Formulierung bestimmt die Richtung der folgenden Schritte.

2 Grundlagen der Beschränkten Arithmetik

Ziel dieses Abschnitts ist es, den sprachlichen Rahmen der Beschränkten Arithmetik festzulegen und durch Tait-Kalküle die verschiedenen Fragmente anzugeben, die für diese Arbeit von Interesse sind.

Wir beginnen, indem wir eine Sprache für die Beschränkte Arithmetik definieren. Sie ist eine Sprache der Prädikatenlogik mit Gleichheit und entspricht im wesentlichen der in [Buss 1986] und [Takeuti 1991] benutzten. Anstatt mehrstelliger Prädikatenvariablen benutzen wir analog zu [Pohlers 1989] und [Schwichtenberg 1977] einstellige Mengenvariablen und die Prädikatszeichen $\in, \notin$. Die mit den zweitstufigen Variablen gebildeten atomaren Formeln haben also die Gestalt $t \in \alpha, t \notin \alpha$ anstatt $\alpha(t_1, \ldots, t_n), \neg\alpha(t_1, \ldots, t_n)$. Um die Polynomiale Hierarchie im „Bootstrap"-Verfahren zu entwickeln, sind gewisse Grundfunktionen notwendig, die unter anderem Funktionen von polynomialer Wachstumsrate beschränken. In [Buss 1986] wird gezeigt, daß hierfür die Funktionen S, $+$, $\cdot$, $\lfloor \frac{1}{2} . \rfloor$, $|.|$ und $\#$ ausreichen. Für das schwache zweitstufige Fragment der Beschränkten Arithmetik, welches in der Folge vorgestellt wird, wird es auf Grund der schwächeren erststufigen Axiomatisierung notwendig sein, zusätzliche Funktionen aus $\mathbf{P}$ hinzuzunehmen. Deshalb betrachten wir Erweiterungen der Sprache aus [Buss 1986] um zusätzliche Funktionszeichen aus einer Menge $\mathcal{F}$, die eine Teilmenge von Funktionen aus $\mathbf{P}$ repräsentiert. Neben $\in$ und $\notin$ gibt es noch die Prädikatszeichen $=, \neq, \leq$ und $\not\leq$.

2.1 Definition der Sprache $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$

Die Sprache $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ der beschränkten Arithmetik enthält

- abzählbar viele freie Individuenvariablen $a_0, a_1, a_2, \ldots$
- abzählbar viele gebundene Individuenvariablen $x_0, x_1, x_2, \ldots$
- abzählbar viele freie Mengenvariablen $\alpha_0, \alpha_1, \alpha_2, \ldots$
- abzählbar viele gebundene Mengenvariablen $\phi_0, \phi_1, \phi_2, \ldots$
- logische Symbole $\in, \notin, =, \neq, \wedge, \vee, \forall, \exists$
- Funktionszeichen
  - 0 als Zeichen für die Null
  - $\mathrm{S}, |.|, \lfloor \frac{1}{2} . \rfloor$ als Zeichen für die Nachfolger-, die Binärlängen- und die „shift-right"-Funktion, die in Abschnitt 1 definiert wurden
  - $+, \cdot, \#$ als Zeichen für die Addition, die Multiplikation und die „smash"-Funktion wie in Abschnitt 1 definiert
  - f für jedes $f \in \mathcal{F}$
- Prädikatszeichen $\leq, \not\leq$

– Hilfszeichen $(,)$.

Die Menge aller Mengenvariablen wird mit $\mathcal{A}$ bezeichnet.

Über diese Sprache werden in gewohnter Weise Terme und Formeln definiert. Die Negation ist hierbei kein logisches Symbol, sondern eine syntaktische Operation auf den Formeln, die entsprechend den de Morganschen Regeln ausgerechnet wird.

2.2 Induktive Definition der *Terme* aus $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$

(a) 0 ist ein Term.

(b) Ist t ein Term, so sind auch $(\mathrm{S}t), (\lfloor\frac{1}{2}.\rfloor t), (|.|t)$ Terme.

(c) Sind s, t Terme, so sind auch $(+st), (\cdot st), (\#st)$ Terme.

(d) Sind $t_1, \ldots, t_n$ Terme, f ein Funktionszeichen aus $\mathcal{F}$ mit Stellenzahl n, so ist auch $(ft_1 \ldots t_n)$ ein Term.

Für einen Term t sei die Menge $\mathsf{FV}(t)$ seiner freien Variablen definiert als die Menge aller in t auftretenden *freien* Individuenvariablen.

Wenn klar ist, um welches $\mathcal{F}$ es sich handelt, wird kurz $\mathbf{L}_{\mathbf{BA}}$ statt $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ geschrieben.
Für eine bessere Lesbarkeit werden im folgenden überflüssige Klammern weggelassen. Außerdem schreiben wir kurz $\lfloor\frac{1}{2}t\rfloor$ statt $(\lfloor\frac{1}{2}.\rfloor t)$, $s+t$ statt $(+st)$ etc.
Ist A eine Zeichenreihe, a und α freie Variablen, dann sei $A_a(t)$ bzw. $A_a(x)$ die Zeichenreihe, die aus A entsteht, indem jedes Auftreten von a durch den Term t resp. die gebundene Variable x ersetzt wird. Entsprechend sei $A_\alpha(\beta)$ bzw. $A_\alpha(\phi)$ die Ersetzung von α durch die freie Mengenvariable β resp. die gebundene ϕ in A.
Tritt zum erstenmal in einem Kontext $A(a)$ oder $A(\alpha)$ auf, so wird damit die freie Variable a bzw. α angegeben, für die nachfolgend in demselben Kontext in A ersetzt wird. Wir verwenden dann abkürzend $A(t)$, $A(x)$, $A(\beta)$ und $A(\phi)$.
Die Angabe mehrerer freier Variablen sei in natürlicher Weise definiert.

2.3 Induktive Definition der *Formeln* aus $\mathbf{L}_{\mathbf{BA}}$

(a) Für Terme s, t aus $\mathbf{L}_{\mathbf{BA}}$ sind $(t=s)$, $(t\neq s)$, $(t\leq s)$, $(t\not\leq s)$, $(t\in\alpha)$, $(t\notin\alpha)$ Formeln.

(b) Sind A und B Formeln, so auch $(A\vee B)$, $(A\wedge B)$.

(c) Ist A eine Formel, t ein Term, a eine freie und x eine gebundene Variable, so daß x nicht in A auftaucht, so sind auch $(\forall x\, A_a(x))$, $(\exists x\, A_a(x))$, $(\forall x{\leq}t\, A_a(x))$ und $(\exists x{\leq}t\, A_a(x))$ Formeln.

(d) Ist A eine Formel, α eine freie und ϕ eine gebundene Mengenvariable, die nicht in A auftaucht, so sind auch $(\forall\phi\, A_\alpha(\phi))$ und $(\exists\phi\, A_\alpha(\phi))$ Formeln.

Die Formeln unter (a) heißen auch *Primformeln*. Die Menge $\mathsf{FV}(A)$ der freien Variablen einer Formel A wird definiert als die Menge aller in A auftretenden *freien*

Individuen- und Mengenvariablen. Analog sei $\mathsf{BV}(A)$ die Menge aller in A auftretenden *gebundenen* Individuen- und Mengenvariablen. Einschränkend sei $\mathsf{FV_1}(A)$ die Menge aller Individuenvariablen in $\mathsf{FV}(A)$, also die Menge aller in A auftretenden *freien* Individuenvariablen.

Wir definieren nun die Länge und die Negation einer Formel wie in [Pohlers 1989] bzw. [Schwichtenberg 1977].

2.4 Definition der *Länge* $\mathsf{L}(F)$ einer Formel F aus $\mathbf{L_{BA}}$

Die Definition erfolgt durch Rekursion nach dem Aufbau von F:

(a) Ist F eine Primformel, so sei $\mathsf{L}(F) := 0$.

(b) Ist $F \equiv A \circ B$ mit $\circ \in \{\wedge, \vee\}$, dann sei $\mathsf{L}(F) := Max\{\mathsf{L}(A), \mathsf{L}(B)\} + 1$.

(c) Ist $F \equiv \mathrm{Q}x\, A(x)$ oder $F \equiv \mathrm{Q}x{\leq}t\, A(x)$ mit $\mathrm{Q} \in \{\forall, \exists\}$, dann sei $\mathsf{L}(F) := \mathsf{L}(A(a)) + 1$.

(d) Ist $F \equiv \mathrm{Q}\phi\, A(\phi)$ mit $\mathrm{Q} \in \{\forall, \exists\}$, dann sei $\mathsf{L}(F) := \mathsf{L}(A(\alpha)) + 1$.

2.5 Definition der *Negation* $\neg A$ einer Formel A aus $\mathbf{L_{BA}}$

Die Definition erfolgt durch Rekursion nach $\mathsf{L}(A)$:

(a) Für Primformel definieren wir $\neg(t{=}s) :\equiv t{\neq}s$, $\neg(t{\neq}s) :\equiv t{=}s$, $\neg(t{\leq}s) :\equiv t \not\leq s$, $\neg(t \not\leq s) :\equiv t \leq s$, $\neg(t \in \alpha) :\equiv t \notin \alpha$, $\neg(t \notin \alpha) :\equiv t \in \alpha$.

(b) Ist A keine Primformel, so sei $\neg A$ entsprechend den de Morganschen Regeln definiert.

Also ist $\neg$ kein Zeichen der Sprache, sondern eine syntaktische Operation. Mit A ist auch $\neg A$ eine Formel und es gilt $\neg\neg A \equiv A$.

2.6 Definition

Für eine Formel $A(a)$ heißt $\{u : A(u)\}$ *Klassenterm*. Wir definieren für Formeln $F(\alpha)$ die *Substitution von Klassentermen* $F(A(.)) :\equiv F(\{u : A(u)\})$ durch Rekursion nach der Länge von F.

Dabei ist $F(A(.)) \equiv F$ für $\alpha \notin \mathsf{FV}(F)$ und $F(A(.)) \equiv A(t)/\neg A(t)$ für $F \equiv t \in \alpha / t \notin \alpha$. In den übrigen Fällen ist $F(A(.))$ homomorph definiert.

Wir verwenden folgende Abkürzungen und Bezeichnungen:

(i) Sind A, B Formeln, Γ eine endliche Formelmenge und s, t Terme, so sei abkürzend definiert:

$$t < s \quad :\equiv \quad s \not\leq t$$

$$
\begin{array}{rcl}
t \not< s & :\equiv & s \leq t \\
A \to B & :\equiv & \neg A \vee B \\
A \leftrightarrow B & :\equiv & (A \to B) \wedge (B \to A) \\
\forall x{<}t\, A(x) & :\equiv & \forall x{\leq}t\, (t < x \to A(x)) \\
\exists x{<}t\, A(x) & :\equiv & \exists x{\leq}t\, (t < x \wedge A(x)) \\
\emptyset & :\equiv & \{u : u \neq u\} \\
\mathsf{FV}(\Gamma) & :\equiv & \bigcup\{\mathsf{FV}(F) : F \in \Gamma\} \\
\mathsf{BV}(\Gamma) & :\equiv & \bigcup\{\mathsf{BV}(F) : F \in \Gamma\} \\
\mathsf{FV}_1(\Gamma) & :\equiv & \bigcup\{\mathsf{FV}_1(F) : F \in \Gamma\}\,.
\end{array}
$$

(ii) Wir unterscheiden folgende erststufigen Quantoren:

- $\forall x\ ,\ \exists x$ *unbeschränkte Quantoren*
- $\forall x{\leq}t\ ,\ \exists x{\leq}t$ *beschränkte Quantoren*
- $\forall x{\leq}|t|\ ,\ \exists x{\leq}|t|$ *scharf beschränkte Quantoren.*

Eine *beschränkte Formel* enthält nur beschränkte Quantoren.

(iii) Wie auch schon oben mehrmals verwandt, sollen im weiteren

- $a, b, c \ldots$ freie Individuenvariablen
- $x, y, z \ldots$ gebundene Individuenvariablen
- $\alpha, \beta, \gamma \ldots$ freie Mengenvariablen
- $\phi, \psi, \chi \ldots$ gebundene Mengenvariablen

bezeichnen.

(iv) Eine Formel heißt *erststufig*, wenn sie keine Mengenvariablen enthält.

(v) Eine Formel F ist vom $\vee$-*Typ*, wenn sie eine *negative* Primformel, also der Gestalt $(t \neq s)$, $(t \not\leq s)$, $(t \notin \alpha)$, oder von der Gestalt $(A \vee B)$, $(\exists x\, A_a(x))$, $(\exists x{\leq}t\, A_a(x))$ oder $(\exists \phi\, A_\alpha(\phi))$ ist.

Nach diesen grundlegenden Definitionen werden Formelmengen $\mathbf{\Sigma^b_i}$, $\mathbf{\Sigma^b_i}(\mathcal{A})$, $\mathbf{\Sigma^{1,b}_i}$, $\mathbf{\Sigma^{1,w^\star}_i}$ und $\mathbf{\Sigma^{1,w}_i}$ definiert. Die ersten drei sind in [Buss 1986] definiert, $\mathbf{\Sigma^{1,w^\star}_i}$ und $\mathbf{\Sigma^{1,w}_i}$ in [Takeuti 1991]. Bei den Bezeichnungen steht das „b“ für „bounded“ und das „w“ für „weak“. Dementsprechend sind $\mathbf{\Sigma^b_i}$ und $\mathbf{\Sigma^b_i}(\mathcal{A})$ bzw. $\mathbf{\Sigma^{1,b}_i}$ beschränkte Analoga zur arithmetischen Hierarchie $\mathbf{\Sigma_i}$ resp. analytischen Hierarchie $\mathbf{\Sigma^1_i}$.

In $\mathbf{\Sigma_i^b}$, als „beschränktes“ Pendant zur arithmetischen Hierarchie $\mathbf{\Sigma_i}$, entsprechen die scharf beschränkten Quantoren den beschränkten Quantoren in $\mathbf{\Sigma_i}$ und die beschränkten, nicht scharf beschränkten Quantoren den unbeschränkten Quantoren in $\mathbf{\Sigma_i}$. In [Buss 1986] wird gezeigt, daß die Formelmengen $\mathbf{\Sigma_i^b}$ genau die zur Charakterisierung der polynomialen Hierarchie $\mathbf{\square_i^p}$ benötigten sind.

2.7 Induktive Definition der Formelmengen $\mathbf{\Sigma_i^b}$ und $\mathbf{\Pi_i^b}$

(a) $\mathbf{\Sigma_0^b = \Pi_0^b}$ sei die Menge aller Formeln aus $\mathbf{L_{BA}^{\emptyset}}$, deren Quantoren erststufig und scharf beschränkt sind und die keine Mengenvariablen enthalten.

(b) $\mathbf{\Sigma_{k+1}^b}$ sei die kleinste Menge mit

(1) $\mathbf{\Sigma_{k+1}^b \supseteq \Pi_k^b}$

(2) $A(a) \in \mathbf{\Sigma_{k+1}^b} \implies \exists x{\leq}t\, A(x), \forall x{\leq}|t|\, A(x) \in \mathbf{\Sigma_{k+1}^b}$

(3) $A, B \in \mathbf{\Sigma_{k+1}^b} \implies A \wedge B, A \vee B \in \mathbf{\Sigma_{k+1}^b}$.

(c) $\mathbf{\Pi_{k+1}^b}$ sei in dualer Weise definiert.

Außerdem sei $\mathbf{\Sigma^b} := \mathbf{\Pi^b} := \bigcup_i \mathbf{\Sigma_i^b}$.

Entsprechend seien auch Formelmengen $\mathbf{\Sigma_i^b}(\mathcal{A})$ und $\mathbf{\Pi_i^b}(\mathcal{A})$ definiert, bei denen das Auftreten freier Mengenvariablen erlaubt ist.

So wie $\mathbf{\Sigma_i^b}$ der arithmetischen Hierarchie $\mathbf{\Sigma_i}$ entspricht, steht $\mathbf{\Sigma_i^{1,b}}$ mit der analytischen Hierarchie $\mathbf{\Sigma_i^1}$ in Zusammenhang. Die beschränkten erststufigen Quantoren in $\mathbf{\Sigma_i^{1,b}}$ entsprechen den unbeschränkten erststufigen in $\mathbf{\Sigma_i^1}$, die zweitstufigen Quantoren in $\mathbf{\Sigma_i^{1,b}}$ entsprechen den zweitstufigen Quantoren in $\mathbf{\Sigma_i^1}$. In [Buss 1986] wird gezeigt, daß die Formelmenge $\mathbf{\Sigma_1^{1,b}}$ genau die zur Charakterisierung von **PSPACE** benötigte ist.

2.8 Induktive Definition der Formelmengen $\mathbf{\Sigma_i^{1,b}}$ und $\mathbf{\Pi_i^{1,b}}$

(a) $\mathbf{\Sigma_0^{1,b} = \Pi_0^{1,b}}$ sei die Menge aller Formeln aus $\mathbf{L_{BA}^{\emptyset}}$, deren Quantoren erststufig und beschränkt sind.

(b) $\mathbf{\Sigma_{k+1}^{1,b}}$ sei die kleinste Menge mit

(1) $\mathbf{\Sigma_{k+1}^{1,b} \supseteq \Pi_k^{1,b}}$

(2) $A(a) \in \mathbf{\Sigma_{k+1}^{1,b}} \implies \exists x{\leq}t\, A(x), \forall x{\leq}t\, A(x) \in \mathbf{\Sigma_{k+1}^{1,b}}$

(3) $A, B \in \mathbf{\Sigma_{k+1}^{1,b}} \implies A \wedge B, A \vee B \in \mathbf{\Sigma_{k+1}^{1,b}}$

(4) $A(\alpha) \in \mathbf{\Sigma_{k+1}^{1,b}} \implies \exists \phi\, A(\phi) \in \mathbf{\Sigma_{k+1}^{1,b}}$.

(c) $\mathbf{\Pi_{k+1}^{1,b}}$ sei in dualer Weise definiert.

Außerdem sei $\mathbf{\Sigma^{1,b}} := \mathbf{\Pi^{1,b}} := \bigcup_i \mathbf{\Sigma_i^{1,b}}$.

Für einen Klassenterm $U \equiv \{u : A(u)\}$ sei $U^{|t|}$ eine endliche Approximation an U:

$$U^{|t|} :\equiv \{u \leq |t| : A(u)\} :\equiv \{u : u \leq |t| \wedge A(u)\}\,.$$

Die Formelmengen $\mathbf{\Sigma_i^{1,w^\star}}$ sind wesentlich schwächer als $\mathbf{\Sigma_i^{1,b}}$. Sie sind abgeschlossen unter scharf beschränkter Quantifikation. Für Komplexitätssteigerung sorgen hier Quantifikationen über endliche, scharf beschränkte Approximationen an Mengenvariablen. Diese ersetzt die fehlende beschränkte, nicht scharf beschränkte Quantifikation, denn

$$\mathrm{Q}\phi\, F(\{u \leq |t| : u \in \phi\})$$

ist in geeigneter Weise äquivalent zu

$$\mathrm{Q}x{\leq}(2^{|t|+1} \dot{-} 1)\, F(\{u : \mathrm{Bit}(u,x) = 1\})\,,$$

da $\{u \leq |t| : u \in \phi\}$ der Binärdarstellung von $\sum_{i\leq|t|} 1_\phi(i) \cdot 2^i$ entspricht.
Die bisher definierten Formelmengen sind über der Sprache $\mathbf{L_{BA}^{\emptyset}}$ gegeben, da sich alle wichtigen Funktionen durch ein Bootstrap-Verfahren definieren lassen, wie in [Buss 1986] Abschnitt 2.4 und Abschnitt 2.5 gezeigt. Durch die Verschiebung der Quantoren in $\mathbf{\Sigma_i^{1,w^\star}}$ verlagert sich das Bootstrap-Verfahren zu Funktionen auf scharf beschränkten Klassentermen, die aber nicht durch unsere sprachlichen Mittel beschrieben werden können. Darum gehen wir in $\mathbf{\Sigma_i^{1,w^\star}}$ von einer größeren Menge $\mathcal{F}^{\mathrm{w}}$ von Grundfunktionen aus.
Wir setzten $\mathcal{F}^{\mathrm{w}} :\equiv \{\mathrm{MSP}, \mathrm{LSP}, \mathrm{Bit}, \dot{-}, \beta, *\}$.

2.9 Induktive Definition der Formelmengen $\mathbf{\Sigma_i^{1,w^\star}}$ und $\mathbf{\Pi_i^{1,w^\star}}$

(a) $\mathbf{\Sigma_0^{1,w^\star} = \Pi_0^{1,w^\star}}$ sei die Menge aller Formeln aus $\mathbf{L_{BA}^{\mathcal{F}^{\mathrm{w}}}}$, deren Quantoren erststufig und scharf beschränkt sind.

(b) $\mathbf{\Sigma_{k+1}^{1,w^\star}}$ sei die kleinste Menge mit

(1) $\mathbf{\Sigma_{k+1}^{1,w^\star} \supseteq \Pi_k^{1,w^\star}}$

(2) $A(a) \in \mathbf{\Sigma_{k+1}^{1,w^\star}} \implies \exists x{\leq}|t|\, A(x), \forall x{\leq}|t|\, A(x) \in \mathbf{\Sigma_{k+1}^{1,w^\star}}$

(3) $A, B \in \mathbf{\Sigma_{k+1}^{1,w^\star}} \implies A \wedge B, A \vee B \in \mathbf{\Sigma_{k+1}^{1,w^\star}}$

(4) $A(\alpha) \in \mathbf{\Sigma_{k+1}^{1,w^\star}} \implies \exists \phi\, A(\phi^{|t|}) \in \mathbf{\Sigma_{k+1}^{1,w^\star}}$.

(c) $\mathbf{\Pi_{k+1}^{1,w^\star}}$ sei in dualer Weise definiert.

Außerdem sei $\mathbf{\Sigma^{1,w^\star} := \Pi^{1,w^\star} := \bigcup_i \Sigma_i^{1,w^\star}}$.

$\mathbf{\Sigma_i^{1,w}}$ ist eine über $\mathbf{\Sigma_i^{1,b}}$ hinausgehende Beschränkung der analytischen Hierarchie. Hier sind nur scharf beschränkte erststufige Quantoren zugelassen, die also den beschränkten erststufigen Quantoren in $\mathbf{\Sigma_i^{1,b}}$ und den unbeschränkten erststufigen in $\mathbf{\Sigma_i^1}$ entsprechen.

2.10 Induktive Definition der Formelmengen $\mathbf{\Sigma_i^{1,w}}$ und $\mathbf{\Pi_i^{1,w}}$

(a) $\mathbf{\Sigma_0^{1,w} = \Pi_0^{1,w}}$ sei die Menge aller Formeln aus $\mathbf{L_{BA}^{P}}$, deren Quantoren erststufig und scharf beschränkt sind.

(b) $\mathbf{\Sigma_{k+1}^{1,w}}$ sei die kleinste Menge mit

(1) $\mathbf{\Sigma_{k+1}^{1,w} \supseteq \Pi_k^{1,w}}$

(2) $A(a) \in \mathbf{\Sigma_{k+1}^{1,w}} \implies \exists x{\leq}|t|\, A(x), \forall x{\leq}|t|\, A(x) \in \mathbf{\Sigma_{k+1}^{1,w}}$

(3) $A, B \in \mathbf{\Sigma_{k+1}^{1,w}} \implies A \wedge B, A \vee B \in \mathbf{\Sigma_{k+1}^{1,w}}$

(4) $A(\alpha) \in \mathbf{\Sigma_{k+1}^{1,w}} \implies \exists \phi\, A(\phi) \in \mathbf{\Sigma_{k+1}^{1,w}}$.

(c) $\mathbf{\Pi_{k+1}^{1,w}}$ sei in dualer Weise definiert.

Außerdem sei $\mathbf{\Sigma^{1,w} := \Pi^{1,w} := \bigcup_i \Sigma_i^{1,w}}$. Die Formel aus $\mathbf{\Sigma^{1,w}}$ heißen *scharf beschränkt im weiten Sinne.*

Die soeben definierten Formelmengen lassen sich für eine Menge neuer Funktionszeichen $\mathcal{F}$ auf $\mathbf{L_{BA}^{\mathcal{F}}}$ verallgemeinern. Die entstehenden Formelmengen werden mit $\mathbf{\Sigma_i^b}(\mathcal{F})$, $\mathbf{\Sigma_i^b}(\mathcal{A}, \mathcal{F})$, $\mathbf{\Sigma_i^{1,b}}(\mathcal{F})$, etc. bezeichnet. Analoges gilt für Mengen neuer Prädikatszeichen $\mathcal{P}$.

Für die $\mathbf{\Sigma}$-Mengen $\mathbf{\Sigma_i^b}$, $\mathbf{\Sigma_i^b}(\mathcal{A})$, $\mathbf{\Sigma_i^{1,b}}$, $\mathbf{\Sigma_i^{1,w^\star}}$ und $\mathbf{\Sigma_i^{1,w}}$ und den entsprechenden $\mathbf{\Pi}$-Mengen gilt:

– $A \in \mathbf{\Sigma} \iff \neg A \in \mathbf{\Pi}$

– $A \in \mathbf{\Sigma}, B \in \mathbf{\Pi} \implies (A \to B) \in \mathbf{\Pi}, (B \to A) \in \mathbf{\Sigma}$.

Nun sind wir in der Lage, Tait-Kalküle für $\mathbf{L_{BA}^{\mathcal{F}}}$ zu definieren, wie sie in ähnlicher Form in [Schwichtenberg 1977], [Pohlers 1989] etc. vorgestellt werden. Sie sind Kalküle für Logik mit Gleichheit, die speziell an die beschränkten Formeln angepaßt sind.
Wir definieren logische Axiome und Gleichheitsaxiome für $\mathbf{L_{BA}^{\mathcal{F}}}$. Dabei sei $\Gamma \subset \mathbf{L_{BA}^{\mathcal{F}}}$ eine endliche Formelmenge. Γ ist ein

logisches Axiom, falls $A, \neg A \in \Gamma$ für eine Primformel A gilt.

Gleichheitsaxiom, falls

(a) $t = t \in \Gamma$ ist, oder

(b) $t_1 \neq s_1, \ldots, t_n \neq s_n,\ f\,\vec{t} = f\,\vec{s} \in \Gamma$ für ein n-stelliges Funktionssymbol f gilt, oder

(c) $t_1 \neq s_1, \ldots, t_n \neq s_n, \neg\, p\,\vec{t},\ p\,\vec{s} \in \Gamma$ für ein n-stelliges Prädikatssymbol p gilt.

Dabei seien $t, t_1, \ldots, t_n, s_1, \ldots, s_n$ beliebige Terme.

Ein Axiom Γ heißt *erststufig*, wenn alle Formeln in Γ erststufig sind, also keine Mengenvariablen enthalten.

Nun definieren wir logische Schlüsse für $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$. Dabei sind $A, B, F(a), G(\alpha)$ $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$-Formeln, s, t $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$-Terme und $\Gamma \subset \mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ eine endliche Formelmenge.

$$
\begin{array}{rlcl}
(\wedge) & \vdash \Gamma, A \text{ und } \vdash \Gamma, B & \Longrightarrow & \vdash \Gamma, A \wedge B \\
(\vee) & \vdash \Gamma, A_i \text{ für } i = 1 \text{ oder } i = 2 & \Longrightarrow & \vdash \Gamma, A_1 \vee A_2 \\
(\forall) & \vdash \Gamma, F(a) \text{ und } a \notin \mathsf{FV}(\Gamma, \forall x\, F(x)) & \Longrightarrow & \vdash \Gamma, \forall x\, F(x) \\
(\exists) & \vdash \Gamma, F(t) & \Longrightarrow & \vdash \Gamma, \exists x\, F(x) \\
(\forall\leq) & \vdash \Gamma, a \not\leq t, F(a) \text{ und } a \notin \mathsf{FV}(\Gamma, \forall x{\leq}t\, F(x)) & & \\
 & & \Longrightarrow & \vdash \Gamma, \forall x{\leq}t\, F(x) \\
(\exists\leq) & \vdash \Gamma, F(t) & \Longrightarrow & \vdash \Gamma, t \not\leq s, \exists x{\leq}s\, F(x) \\
\text{(Schnitt)} & \vdash \Gamma, A \text{ und } \vdash \Gamma, \neg A & \Longrightarrow & \vdash \Gamma \\
(\forall^2) & \vdash \Gamma, G(\alpha) \text{ und } \alpha \notin \mathsf{FV}(\Gamma, \forall \phi\, G(\phi)) & \Longrightarrow & \vdash \Gamma, \forall \phi\, G(\phi) \\
(\exists^2) & \vdash \Gamma, G(\alpha) & \Longrightarrow & \vdash \Gamma, \exists \phi\, G(\phi)
\end{array}
$$

$(\forall)$, $(\forall\leq)$ und $(\forall^2)$ sind Schlüsse mit *Variablenbedingung* an die *Eigenvariablen* a bzw. α. $(\forall^2)$ und $(\exists^2)$ heißen *zweitstufige Schlüsse*, die restlichen heißen *erststufige Schlüsse*.

Ein *erststufiges Fragment* der Beschränkten Arithmetik zur Sprache $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ ist eine Menge von erststufigen Formeln aus $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$, die alle erststufigen logischen Axiome und Gleichheitsaxiome für $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ enthält und abgeschlossen unter allen erststufigen logischen Schlüssen für $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ ist. Ein *zweitstufiges Fragment* der Beschränkten Arithmetik für $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ ist eine Menge von Formeln aus $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$, die alle logischen Axiome und Gleichheitsaxiome für $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ enthält und abgeschlossen unter allen logischen Schlüssen für $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ ist.

Wir geben nun die verschiedenen mathematischen Axiome und Schlüsse für $\mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ an, die für uns von Interesse sind.
Eine endliche Formelmenge $\Gamma \subset \mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ ist ein *mathematisches Axiom*, falls eine Substitutionsinstanz einer Formel aus $\textsc{Basic}(\mathcal{F})$ in Γ liegt. Dabei ist $\textsc{Basic}(\mathcal{F})$ eine genügend große Menge von Formeln aus $\mathbf{\Sigma^b_0}$, die ausreicht, um die Bedeutung der verwendeten Funktionssymbole festzulegen. Die Menge $\textsc{Basic}(\emptyset)$ ist in Tabelle 1 angegeben. Sie unterscheidet sich von der in [Buss 1986] verwendeten, insofern sie einfachere Multiplikationsaxiome benutzt und überflüssige Axiome ausschließt. Dabei ist gewährleistet, daß die Axiome in [Buss 1986] hier in einer minimalen Theorie beweisbar sind. Für beliebige $\mathcal{F}$ ist die über $\textsc{Basic}(\emptyset)$ hinausgehende Wahl der Axiome für unser weiteres Vorgehen ohne Bedeutung, solange sie die Funktionen passend axiomatisieren.
Es werden verschiedene Induktionen und Komprehensionen betrachtet. Wir geben immer Axiome und äquivalente Schlüsse an.
Seien $\Psi, \Gamma \subset \mathbf{L}^{\mathcal{F}}_{\mathbf{BA}}$ Formelmengen, $A(t) \in \Psi$ und $a \notin \mathsf{FV}(\Gamma, A(0))$, wobei Γ endlich ist.

(a)	$0 \leq a$
(b)	$b \leq a \vee a \leq b$
(c)	$a \leq b \wedge b \leq a \to a = b$
(d)	$a \leq b \wedge b \leq c \to a \leq c$
(e)	$b \leq a \leftrightarrow b < \mathrm{S}a$
(f)	$a < b \to \mathrm{S}(2 \cdot a) < 2 \cdot b$
(g)	$a = \lfloor \frac{1}{2} b \rfloor \leftrightarrow (2 \cdot a = b \vee \mathrm{S}(2 \cdot a) = b)$
(h)	$\lvert 0 \rvert = 0$
(i)	$a \neq 0 \to \lvert a \rvert = \mathrm{S}(\lvert \lfloor \frac{1}{2} a \rfloor \rvert)$
(j)	$a \leq b \to \lvert a \rvert \leq \lvert b \rvert$
(k)	$0 \# a = 1$
(l)	$a \neq 0 \to 1 \# a = 2 \cdot (1 \# \lfloor \frac{1}{2} a \rfloor)$
(m)	$a \neq 0 \to a \# b = (\lfloor \frac{1}{2} a \rfloor \# b) \cdot (1 \# b)$
(n)	$a \# b = b \# a$
(o)	$\lvert a \rvert = \lvert b \rvert \to a \# c = b \# c$
(p)	$a + 0 = a$
(q)	$a + \mathrm{S}b = \mathrm{S}(a + b)$
(r)	$a + b = b + a$
(s)	$(a + b) + c = a + (b + c)$
(t)	$b < c \to a + b < a + c$
(u)	$a \cdot 0 = 0$
(v)	$a \cdot (\mathrm{S}b) = (a \cdot b) + a$
(w)	$a \cdot b = b \cdot a$
(x)	$(a \cdot b) \cdot 2 = a \cdot (b \cdot 2)$

Tabelle 1: Die Menge $\textsc{Basic}(\emptyset)$

Ein Induktionsaxiom liegt vor, wenn eine der folgenden Formeln in Γ ist.

(Ψ-IND)	$A(0) \wedge \forall x \, (A(x) \to A(\mathrm{S}x)) \to A(t)$
(Ψ-PIND)	$A(0) \wedge \forall x \, (A(\lfloor \frac{1}{2} x \rfloor) \to A(x)) \to A(t)$
(Ψ-LIND)	$A(0) \wedge \forall x \, (A(x) \to A(\mathrm{S}x)) \to A(\lvert t \rvert)$

Die äquivalenten Schlüsse lauten

(Ψ-IND)	$\Gamma, \neg A(a), A(\mathrm{S}a)$	$\Longrightarrow$	$\Gamma, \neg A(0), A(t)$
(Ψ-PIND)	$\Gamma, \neg A(\lfloor \frac{1}{2} a \rfloor), A(a)$	$\Longrightarrow$	$\Gamma, \neg A(0), A(t)$
(Ψ-LIND)	$\Gamma, \neg A(a), A(\mathrm{S}a)$	$\Longrightarrow$	$\Gamma, \neg A(0), A(\lvert t \rvert)$

Die Axiome und Schlüsse sind in jedem Fragment der Beschränkten Arithmetik äquivalent.

(Ψ-PIND) und (Ψ-LIND) sind schwächer als (Ψ-IND), denn in (Ψ-PIND) schließt man von einer stärkeren Prämisse auf die gleiche Konklusion von (Ψ-IND), in (Ψ-LIND) von der

gleichen Prämisse auf eine schwächere Konklusion. Für Formelmenge Ψ mit geringen Abschlußeigenschaften, wie zum Beispiel die oben definierten, läßt sich über einer schwachen Theorie zeigen, daß (Ψ-PIND) und (Ψ-LIND) äquivalent sind.

Im Vergleich zur üblichen Komprehension ($\mathbf{\Sigma_0^{1,b}}$-CA) ist (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) im doppelten Sinne abgeschwächt. Zum einen werden nur Klassen aus der schwachen Hierarchie $\mathbf{\Sigma_i^{1,w^\star}}$ betrachtet, und zum anderen davon auch nur endliche, scharf beschränkte Anfangsstücke. Die in [Takeuti 1991] gewählte Formulierung

$$\exists X\, \forall x{\leq}|t|\, \Big(x \in \phi^{|t|} \leftrightarrow A(x)\Big)$$

ist so schwach, daß sich folgende Ersetzung i. allg. nicht beweisen läßt:

$$\vdash \Gamma \quad \Longrightarrow \quad \vdash \Gamma_\alpha\, (\{u \leq |t| : A(u)\})\ .$$

Der Knackpunkt ist, daß $\phi = \{u \leq |t| : A(u)\}$ die Menge ϕ vollständig festlegt, also $\forall x\, (x > |t| \rightarrow x \notin \phi)$ impliziert, was durch das obige Axiom nicht gewährleistet wird.
Trotzdem wird eine partielle Schnittelimination möglich sein, da das oben angegebene Komprehensionsaxiom für $A \in \mathbf{\Sigma_i^{1,w^\star}}$ eine Formel aus $\mathbf{\Sigma_{i+1}^{1,w^\star}}$ darstellt und somit als Schnittformel erlaubt sein wird.

Dies führt zu folgenden Formulierungen. Seien $\Psi, \Gamma \subset \mathbf{L_{BA}^{\mathcal{F}}}$ Formelmengen, $F(\alpha) \in \mathbf{L_{BA}^{\mathcal{F}}}$ und $A \in \Psi$, wobei Γ endlich ist.
Ein Komprehensionsaxiom liegt vor, wenn eine der folgenden Formeln in Γ ist.

(Ψ-CA)	$\exists\phi\, \forall x\, (x \in \phi \leftrightarrow A(x))$
(wΨ-CA)	$\exists\phi\, \forall x{\leq}|t|\, (x \in \phi^{|t|} \leftrightarrow A(x))$

Die äquivalenten Schlüsse lauten

(Ψ-CA)	$\Gamma, F(\{u : A(u)\})$	$\Longrightarrow$	$\Gamma, \exists\phi\, F(\phi)$
(wΨ-CA)	$\Gamma, F(\{u \leq |t| : A(u)\})$	$\Longrightarrow$	$\Gamma, \exists\phi\, F(\phi^{|t|})$.

Auch hier sind Axiome und Schlüsse in jedem Fragment der Beschränkten Arithmetik äquivalent.

Standardbegriffe wie „Schnittformel“, „Hauptformel eines Schlusses“ etc. seien wie üblich definiert.
Wir definieren nun Fragmente $\mathbb{F}$ aufbauend auf die obige allgemeine Fragmentdefinition durch Angabe von mathematischen Axiomen $\mathbf{Ax}$ und nichtlogischen Schlüssen $\mathbf{S_1}$, …, $\mathbf{S_k}$ in der Form

$$\mathbb{F} = \mathbf{Ax} + \mathbf{S_1} + \ldots + \mathbf{S_k}\ .$$

$\mathbb{F}$ ist dann das kleinste allgemeine Fragment, das abgeschlossen ist unter $\mathbf{Ax}$, $\mathbf{S_1}$, …, $\mathbf{S_k}$ der entsprechenden Stufe (Axiome werden dabei als Schlüsse ohne Prämissen aufgefaßt).

2.11 Definition der Fragmente $\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}$, $\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A})$, $\mathbf{U}^{\mathbf{i}}_{\mathbf{2}}$, $\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}}$ und $\mathbf{U}^{\mathbf{w}}_{\mathbf{2}}$

Wir definieren ein erststufiges Fragment zur Sprache $\mathbf{L}^{\emptyset}_{\mathbf{BA}}$:

$$\mathbf{S}^{\mathbf{i}}_{\mathbf{2}} \coloneqq \textsc{Basic}(\emptyset) + (\mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{i}}\text{-PIND})\,.$$

Wir definieren zweitstufige Fragmente zur Sprache $\mathbf{L}^{\emptyset}_{\mathbf{BA}}$:

$$\begin{aligned}\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A}) &\coloneqq \textsc{Basic}(\emptyset) + (\mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{i}}(\mathcal{A})\text{-PIND})\,,\\ \mathbf{U}^{\mathbf{i}}_{\mathbf{2}} &\coloneqq \textsc{Basic}(\emptyset) + (\mathbf{\Sigma}^{\mathbf{1,b}}_{\mathbf{i}}\text{-PIND}) + (\mathbf{\Sigma}^{\mathbf{1,b}}_{\mathbf{0}}\text{-CA})\,,\end{aligned}$$

zur Sprache $\mathbf{L}^{\mathcal{F}^{\mathrm{w}}}_{\mathbf{BA}}$:

$$\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \coloneqq \textsc{Basic}(\mathcal{F}^{\mathrm{w}}) + (\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{i}}\text{-LIND}) + (\mathrm{w}\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{0}}\text{-CA})$$

und zur Sprache $\mathbf{L}^{\mathbf{P}}_{\mathbf{BA}}$:

$$\mathbf{U}^{\mathbf{w}}_{\mathbf{2}} \coloneqq \textsc{Basic}(\mathbf{P}) + (\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}}\text{-LIND}) + (\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}}\text{-CA})\,.$$

Dann seien

$$\begin{aligned}\mathbf{S_2} &\coloneqq \textstyle\bigcup_i \mathbf{S}^{\mathbf{i}}_{\mathbf{2}}\,,\\ \mathbf{S_2}(\mathcal{A}) &\coloneqq \textstyle\bigcup_i \mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A})\,,\\ \mathbf{U_2} &\coloneqq \textstyle\bigcup_i \mathbf{U}^{\mathbf{i}}_{\mathbf{2}}\,,\\ \mathbf{U}^{\mathbf{w}^\star}_{\mathbf{2}} &\coloneqq \textstyle\bigcup_i \mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}}\,.\end{aligned}$$

Es sei noch bemerkt, daß $\mathbf{S}^{\mathbf{1}}_{\mathbf{2}}$ die in [Buss 1986] verwendeten mathematischen Axiome beweist, also die oben erwähnte minimale Theorie ist. Als nächstes tragen wir, neben Ergebnissen über die Gleichwertigkeit der verschiedenen mathematischen Axiome, die Hauptsätze der Beschränkten Arithmetik aus [Buss 1986] zusammen. Letztere verknüpfen die in den hier vorgestellten Fragmenten definierbaren Funktionen mit den in Abschnitt 1 angegebenen Schichten der Polynomialen Hierarchie.

3 Ergebnisse aus der Beschränkten Arithmetik

Wir fassen die für unser weiteres Vorgehen wichtigen Ergebnisse aus [Buss 1986] zusammen, die $\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}$, $\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A})$ und $\mathbf{U}^{\mathbf{i}}_{\mathbf{2}}$ charakterisieren.

Wie schon erwähnt, sind (Ψ-PIND) und (Ψ-LIND) über einer schwachen Theorie äquivalent. Dabei heißen zwei Theorien äquivalent, wenn sie dieselben Formeln beweisen. In diesem Sinne wird in [Buss 1986] §2.9 Theorem 24 gezeigt:

3.1 Satz

Folgende Theorien sind äquivalent:

(a) $\mathbf{S}^{\mathbf{1}}_{\mathbf{2}} + (\mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{i}}\text{-LIND})$

(b) $\mathbf{S}^{\mathbf{1}}_{\mathbf{2}} + (\mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{i}}\text{-PIND})$

(c) $\mathbf{S}^{\mathbf{1}}_{\mathbf{2}} + (\mathbf{\Pi}^{\mathbf{b}}_{\mathbf{i}}\text{-LIND})$

(d) $\mathbf{S}^{\mathbf{1}}_{\mathbf{2}} + (\mathbf{\Pi}^{\mathbf{b}}_{\mathbf{i}}\text{-PIND})$. □

Ein weiteres Axiom, als die bisher vorgestellten, ist noch von Interesse. Es ist ein spezielles Minimierungsaxiom:

(Ψ-LMIN) $\quad \exists x\, A(x) \to A(0) \vee \exists x \left(A(x) \wedge \forall y{\leq}\lfloor \tfrac{1}{2} x \rfloor \, (\neg A(y)) \right)$

für $A(a) \in \Psi$. Es gilt ([Buss 1986] §2.9 Theorem 24):

3.2 Satz

$$\mathbf{S}^{\mathbf{1}}_{\mathbf{2}} + (\mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{i}}\text{-LMIN}) \qquad \text{ist äquivalent zu} \qquad \mathbf{S}^{\mathbf{1}}_{\mathbf{2}} + (\mathbf{\Pi}^{\mathbf{b}}_{\mathbf{i}}\text{-PIND})\,.$$ □

Wir führen nun definierbare Funktionen und Prädikate ein. Sie spielen eine wichtige Rolle für Fragmente, da sie eine zulässige, d. h. konservative, sprachliche Erweiterung bilden.

3.3 Definition

Sei $\mathbb{F}$ ein Fragment der Beschränkten Arithmetik und $\mathbf{\Sigma}$ eine der Formelmengen $\mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{i}}$, $\mathbf{\Sigma}^{\mathbf{1,b}}_{\mathbf{i}}$ oder $\mathbf{\Sigma}^{\mathbf{1,w^\star}}_{\mathbf{i}}$. Dann sei $\mathbf{\Delta}$ die Bezeichnung $\mathbf{\Delta}^{\mathbf{b}}_{\mathbf{i}}$, $\mathbf{\Delta}^{\mathbf{1,b}}_{\mathbf{i}}$ bzw. $\mathbf{\Delta}^{\mathbf{1,w^\star}}_{\mathbf{i}}$.

(a) Sei $\exists y{\leq}t\, A(\vec{a}, y) \in \mathbf{\Sigma}$ mit $\mathsf{FV}(A) \subset \{\vec{a}, b\}$ und es gelte

$$\mathbb{F} \vdash \forall \vec{x}\, \exists y{\leq}t\, A(\vec{x}, y)$$

$$\mathbb{F} \vdash \forall \vec{x}\, \forall y\, \forall z \left(A(\vec{x}, y) \wedge A(\vec{x}, z) \to y = z \right).$$

Dann heißt die Funktion f mit $\mathbb{N} \models \forall \vec{x}\, A(\vec{x}, f(\vec{x}))$ $\mathbf{\Sigma}$-definierbar bezüglich $\mathbb{F}$.

(b) Sei A eine Formel, $B, \neg C \in \mathbf{\Sigma}$ und es gelte $\mathbb{F} \vdash A \leftrightarrow B$ und $\mathbb{F} \vdash A \leftrightarrow C$. Dann heißt A $\mathbf{\Delta}$ bezüglich $\mathbb{F}$.

(c) Sei A $\mathbf{\Delta}$ bezüglich $\mathbb{F}$, $\mathsf{FV}(A) \subset \{\vec{a}\}$. Dann heißt das Prädikat p mit $\mathbb{N} \models \forall \vec{x}\,(p(\vec{x}) \leftrightarrow A(\vec{x}))$ $\mathbf{\Delta}$-definierbar bezüglich $\mathbb{F}$.

Durch die Bedingung $\exists y{\leq}t\, A(\vec{a}, y) \in \mathbf{\Sigma_i^{1,w^\star}}$ folgt, daß es einen Term s mit $t \equiv |s|$ gibt. Also werden die $\mathbf{\Sigma_i^{1,w^\star}}$-definierbaren Funktionen schon durch Terme $|s|$ beschränkt.

Die $\mathbf{\Sigma_1^b}$-definierbaren Funktionen und $\mathbf{\Delta_1^b}$-definierbaren Prädikate spielen eine besondere Rolle bei den erststufigen Fragmenten $\mathbf{S_2^i}$ für $i{>}0$. Sie können in den Induktionen benutzt werden.
Analoges gilt für $\mathbf{\Sigma_1^{1,b}}$-definierbare Funktionen und $\mathbf{\Delta_1^{1,b}}$-definierbare Prädikate bezüglich $\mathbf{U_2^i}$. Auch sie können in den entsprechenden Induktionen benutzt werden.
Der Grund dafür liegt in folgendem Satz, der in [Buss 1986] §2.3 Theorem 2 und [Buss 1986] §9.5 Theorem 11 bewiesen ist.

3.4 Satz

Sei $\mathbb{F}$ ein Fragment der Beschränkten Arithmetik. Für

- $\mathbb{F} \subseteq \mathbf{S_2}$ seien $\mathbf{\Sigma_k} = \mathbf{\Sigma_k^b}$, $\mathbf{\Pi_k} = \mathbf{\Pi_k^b}$ und $\mathbf{\Delta_k} = \mathbf{\Delta_k^b}$.
- $\mathbb{F} \subseteq \mathbf{U_2}$ seien $\mathbf{\Sigma_k} = \mathbf{\Sigma_k^{1,b}}$, $\mathbf{\Pi_k} = \mathbf{\Pi_k^{1,b}}$ und $\mathbf{\Delta_k} = \mathbf{\Delta_k^{1,b}}$.

Seien $\vec{f}$ $\mathbf{\Sigma_1}$-definierbare Funktionen und $\vec{p}$ $\mathbf{\Delta_1}$-definierbare Prädikate bezüglich $\mathbb{F}$. $\mathbb{F}^*$ sei das Fragment $\mathbb{F}$ erweitert um $\vec{f}$ und $\vec{p}$ als neue Funktions-/Prädikatssymbole und deren definierenden Axiome.

Dann gilt für $i > 0$: ist $B \in \mathbf{\Sigma_i}(\vec{f}, \vec{p})$ oder $B \in \mathbf{\Pi_i}(\vec{f}, \vec{p})$, dann gibt es $B^* \in \mathbf{\Sigma_i}$ bzw. $B^* \in \mathbf{\Pi_i}$ mit $\mathbb{F}^* \vdash B \leftrightarrow B^*$. □

Aus diesem Satz erhalten wir folgende Konservativitätsaussagen ([Buss 1986] §2.3 Korollar 3 und [Buss 1986] §9.5 Korollar 12).

3.5 Korollar

Seien $f_1, \ldots, f_k$ $\mathbf{\Sigma_1^b}$-definierbare Funktionen und $p_1, \ldots, p_l$ $\mathbf{\Delta_1^b}$-definierbare Prädikate bezüglich $\mathbf{S_2^i}$, $i > 0$. $\mathbb{F}$ sei das Fragment $\mathbf{S_2^i}$ erweitert um $f_1, \ldots, f_k$, $p_1, \ldots, p_l$ als neue Funktions-/Prädikatssymbole, deren definierenden Axiome und alle ($\mathbf{\Sigma_i^b}(\vec{f}, \vec{p})$-PIND) Schlüsse.

Dann ist $\mathbb{F}$ eine konservative Erweiterung von $\mathbf{S_2^i}$. □

3.6 Korollar

Seien $f_1, \ldots, f_k$ $\mathbf{\Sigma_1^{1,b}}$-definierbare Funktionen und $p_1, \ldots, p_l$ $\mathbf{\Delta_1^{1,b}}$-definierbare Prädikate bezüglich $\mathbf{U_2^i}$, $i > 0$. $\mathbb{F}$ sei das Fragment $\mathbf{U_2^i}$ erweitert um $f_1, \ldots, f_k$, $p_1, \ldots, p_l$ als neue Funktions-/Prädikatssymbole, deren definierenden Axiome, alle ($\mathbf{\Sigma_i^{1,b}}(\vec{f}, \vec{p})$-PIND) Schlüsse.

Dann ist $\mathbb{F}$ eine konservative Erweiterung von $\mathbf{U_2^i}$. □

Damit sind wir in der Lage, die Hauptsätze der Beschränkten Arithmetik zu formulieren ([Buss 1986] §5.3 Korollar 7 und Theorem 9 bzw. [Buss 1986] §10.2 Theorem 4 und §10.5 Korollar 11).

3.7 Hauptsatz (erststufig)

Sei $i > 0$, f eine Funktion und p ein Prädikat, dann gilt:

$$\begin{array}{lcl} f \in \mathbf{\square_i^p} & \iff & f \text{ ist } \mathbf{\Sigma_i^b}\text{-definierbar in } \mathbf{S_2^i} \\ p \in \mathbf{\Delta_i^p} & \iff & p \text{ ist } \mathbf{\Delta_i^b}\text{-definierbar in } \mathbf{S_2^i}\,. \end{array}$$

□

3.8 Hauptsatz (zweitstufig)

Sei $i > 0$, f eine Funktion und p ein Prädikat, dann gilt:

$$\begin{array}{lcl} f \in \mathbf{PSPACE} & \iff & f \text{ ist } \mathbf{\Sigma_1^{1,b}}\text{-definierbar in } \mathbf{U_2^1} \\ p \in \mathbf{PSPACE} & \iff & p \text{ ist } \mathbf{\Delta_1^{1,b}}\text{-definierbar in } \mathbf{U_2^1}\,. \end{array}$$

□

Die in dieser Arbeit mit $\mathbf{\Sigma_i^{1,b}}$ bezeichneten Formelmengen und mit $\mathbf{U_2^i}$ bezeichneten Fragmente entsprechen $\mathbf{\tilde{\Sigma}_i^{1,b}}$ bzw. $\mathbf{\tilde{U}_2^i}$ in [Buss 1986]. Die hier verwendeten Bezeichnungen enthalten dort neben Mengenvariablen noch Funktionsvariablen. Dies ist aber zum einen eine konservative Erweiterung von $\mathbf{U_2^i}$ ([Buss 1986] §9.3 Satz 5), und zum anderen lassen sich die freien Funktionsvariablen eliminieren ([Buss 1986] §9.3 Lemma 6). Damit erhält man den Hauptsatz auch in der obigen Form.

3.9 Definition

Sei $A(a, b, \vec{c})$ eine Formel mit $\mathsf{FV}(A) \subset \{a, b, c_1, \ldots, c_k\}$.

(a) $f : \mathbb{N}^{k+1} \to \mathbb{N}$ ist durch *längenbeschränktes Zählen von A* definiert
$\iff$ für alle $m, \vec{n} \in \mathbb{N}$ gilt

$$\begin{array}{rcl} f(m, \vec{n}) & = & \#u{\leq}|m| A(u, m, \vec{n}) \\ & = & \text{die Anzahl aller } u \leq |m| \text{ mit } A(u, m, \vec{n}). \end{array}$$

(b) $f : \mathbb{N}^{k+1} \to \mathbb{N}$ ist durch *beschränktes Zählen von A* definiert
$\iff$ für alle $m, \vec{n} \in \mathbb{N}$ gilt

$$f(m, \vec{n}) = \#u{\leq}m A(u, m, \vec{n})$$

$$= \quad \text{die Anzahl aller } u \leq m \text{ mit } A(u, m, \vec{n}).$$

Mit [Buss 1986] §2.5 Theorem 7 und [Buss 1986] §10.2 Proposition 2 erhalten wir folgende Sätze:

3.10 Satz

Sei $A(a, b, \vec{c})$ aus $\mathbf{\Delta_1^b}$ bezüglich $\mathbf{S_2^1}$ und sei f durch längenbeschränktes Zählen von A definiert. Dann ist f $\mathbf{\Sigma_1^b}$-definierbar in $\mathbf{S_2^1}$. □

3.11 Satz

Sei $A(a, b, \vec{c})$ eine $\mathbf{\Sigma_0^{1,b}}$-Formel und sei f durch beschränktes Zählen von A definiert. Dann ist f $\mathbf{\Sigma_1^{1,b}}$-definierbar in $\mathbf{U_2^1}$. □

Wir definieren die Terme $\langle x_1, \ldots, x_n \rangle$ aus $\mathbf{L_{BA}}$ durch Rekursion nach n:

$$\begin{aligned} \langle x_1 \rangle &\quad :\equiv \quad x_1 * 0 \\ \langle x_{n+1}, \ldots, x_1 \rangle &\quad :\equiv \quad x_{n+1} * \langle x_n, \ldots, x_1 \rangle \,. \end{aligned}$$

Dann gibt es für jedes $n > 0$ Terme $\mathrm{SqBd}_n(a)$ in $\mathbf{L_{BA}}$, so daß

$$\mathbf{U_2^{1,w^\star}} \vdash \forall x_1 \leq |a| \ \ldots \forall x_n \leq |a| \, (\langle x_1, \ldots, x_n \rangle \leq |\mathrm{SqBd}_n(a)|) \,.$$

Dabei steht SqBd fr „Sequent Bound“ ([Buss 1986] §2.5). Außerdem gilt

$$\mathbf{U_2^{1,w^\star}} \vdash 0 < i \leq \underline{n} \rightarrow \beta(i, \langle x_1, \ldots, x_n \rangle) = x_i$$

und

$$\mathbf{U_2^{1,w^\star}} \vdash \beta(0, \langle x_1, \ldots, x_n \rangle) = \underline{n} \,,$$

was sich durch Induktion nach n einsehen läßt. Im Induktionsanfang erhalten wir für $n{=}1$

$$\beta(0, \langle x_1 \rangle) = \beta(0, x_1 * 0) = \mathrm{S}\beta(0, 0) = 1$$

$$\beta(1, \langle x_1 \rangle) = \beta(1, x_1 * 0) = x_1 \,.$$

Der Induktionsschritt von n nach $n + 1$ zeigt sich durch

$$\begin{aligned} \beta(0, \langle x_1, \ldots, x_{n+1} \rangle) &= \beta(0, x_1 * \langle x_2, \ldots, x_{n+1} \rangle) \\ &= \mathrm{S}\beta(0, \langle x_2, \ldots, x_{n+1} \rangle) \\ &\overset{I.V.}{=} \mathrm{S}n \end{aligned}$$

und für $1 < i \leq n+1$

$$\begin{aligned}\beta(i, \langle x_1, \ldots, x_{n+1}\rangle) &= \beta(i, x_1 * \langle x_2, \ldots, x_{n+1}\rangle) \\ &= \beta(i-1, \langle x_2, \ldots, x_{n+1}\rangle) \\ &\overset{I.V.}{=} x_i\,.\end{aligned}$$

Abschließend beobachten wir

$$\beta(1, \langle x_1, \ldots, x_{n+1}\rangle) = \beta(1, x_1 * \langle x_2, \ldots, x_{n+1}\rangle) = x_1\,.$$

In [Buss 1986] §4.5 wird erwähnt, daß es eine Majorantenfunktion σ auf den Termen gibt. Sind $t_1, \ldots, t_k$ Terme mit den freien Variablen $b_1, \ldots, b_l$, dann ist $\sigma[\vec{t}\,]$ ein Term mit denselben Variablen und es gilt für $1 \leq i \leq k$:

$$b_1 \leq c_1 \wedge \ldots \wedge b_l \leq c_l \rightarrow t_i(\vec{b}) \leq \sigma[\vec{t}\,](\vec{c})\,.$$

Es wird darüberhinaus noch gesagt, daß σ in Abhängigkeit von Fragmenten $\mathbb{F}$ gegeben ist, so daß in $\mathbb{F}$ die obige Aussage ohne Induktionsschlüsse bewiesen werden kann.
Für diese Arbeit genügt es aber, daß die Majoranteneigenschaft im Standardmodell gilt. Wir brauchen uns daher auch keine Gedanken hinsichtlich der Einfachheit und Konstuktivität von σ zu machen.

3.12 Lemma

Zu dem Term $t \in \mathbf{L}^{\mathbf{P}}_{\mathbf{BA}}$ mit den freien Variablen $b_1, \ldots, b_l$ sei $\sigma[t] \in \mathbf{L}^{\emptyset}_{\mathbf{BA}}$ ein Term mit denselben Variablen, so daß

$$b_1 \leq c_1 \wedge \ldots \wedge b_l \leq c_l \rightarrow t(\vec{b}) \leq \sigma[t](\vec{c})$$

gilt. □

Wir können $\sigma[t]$ aus dem Hauptsatz 3.7 erhalten, da t als Funktion in $\mathbf{P}$ $\mathbf{\Sigma^b_1}$-definierbar in $\mathbf{S^1_2}$ ist. Also gibt es einen Term $s \in \mathbf{L}^{\emptyset}_{\mathbf{BA}}$, so daß

$$\forall \vec{x}\left(t(\vec{x}) \leq s(\vec{x})\right)$$

gilt. Da s nur aus den Funktionen $0, \mathrm{S}, |.|, \lfloor \frac{1}{2}.\rfloor, +, \cdot, \#$ gebildet wird, ist s damit automatisch monoton. Wir setzen $\sigma[t] :\equiv s$ und erhalten so für $b_1 \leq c_1, \ldots, b_l \leq c_l$:

$$t(\vec{b}) \leq s(\vec{b}) \leq s(\vec{c}) = \sigma[t](\vec{c})\,.$$

Nun streben wir eine partielle Schnittelimination für die Tait-Kalküle der Beschränkten Arithmetik an. Dazu zeigen wir, daß wir uns auf Herleitungen beschränken können, deren Schnittformeln in ihrer Komplexität eingeschränkt sind.

4 Partielle Schnittelimination

In diesem Abschnitt geben wir für die Tait-Kalküle der Fragmente der Beschränkten Arithmetik, um sie besser analysieren zu können, Herleitungsprädikate mit zusätzlichen einschränkenden Größen an. Diese Größen sind die Herleitungslänge und der Schnittgrad. Beides sind obere Schranken, zum einen für die Tiefe des Herleitungsbaumes und zum anderen für die Komplexität der in der Herleitung auftretenden Schnitte. Mit Hilfe dieser Beschränkungsgrößen werden dann im Rest des Abschnitts verschiedene Eigenschaften der Kalküle bewiesen.

Die wesentliche Eigenschaft ist die Schnittelimination, die wir analog zum klassichen Gentzenschen Verfahren durchführen, wie z. B. in [Pohlers 1989] oder [Schwichtenberg 1977] dargestellt wird. Da wir i. allg. keine Chance haben, einen Schnitt mit der Hauptformel eines Induktionsschlusses oder eines Axioms zu eliminieren, lassen wir solche Schnitte ganz allgemein zu. Die Reduzierung der Schnitte bis auf eine gewisse Komplexität heißt partielle Schnittelimination.
Um Schnitte mit Hauptformeln aus den Induktionsschlüssen bzw. Axiomen zuzulassen, weisen wir diesen einen Schnittrang von Null zu. Dies ergibt sich, indem wir Ränge von Formeln über Formelklassen betrachten.
Sei Ψ eine Klasse von Formeln aus $\mathbf{L_{BA}}$, die alle atomaren Formeln von aus $\mathbf{L_{BA}}$ enthält.

4.1 Definition des *Ranges* $\Psi\text{-}\mathsf{rg}(F)$ einer Formel F aus $\mathbf{L_{BA}}$

Die Definition erfolgt durch Rekursion nach der Länge von F.

(a) Ist $F \in \Psi$, so sei $\Psi\text{-}\mathsf{rg}(F) := 0$.

(b) Ist $F \notin \Psi$ und

(1) $F \equiv G \circ H$ mit $\circ \in \{\wedge, \vee\}$, dann sei
$\Psi\text{-}\mathsf{rg}(F) := Max\{\Psi\text{-}\mathsf{rg}(G), \Psi\text{-}\mathsf{rg}(H)\} + 1$.

(2) $F \equiv \mathrm{Q}x\, G(x)$ oder $F \equiv \mathrm{Q}x{\leq}t\, G(x)$ mit $\mathrm{Q} \in \{\forall, \exists\}$, dann sei
$\Psi\text{-}\mathsf{rg}(F) := \Psi\text{-}\mathsf{rg}(G(a)) + 1$.

(3) $F \equiv \mathrm{Q}\phi\, G(\phi)$ mit $\mathrm{Q} \in \{\forall, \exists\}$, dann sei $\Psi\text{-}\mathsf{rg}(F) := \Psi\text{-}\mathsf{rg}(G(\alpha)) + 1$.

Die Wahl der Formelklasse Ψ, über die wir den Rang einer Formel definieren, hängt von der in dem Fragment vorliegenden Induktion ab. Ψ muß die Hauptformeln der Induktionen und deren Negationen umfassen. Für $\mathbf{S_2^i}$, $\mathbf{S_2^i}(\mathcal{A})$, $\mathbf{U_2^i}$, $\mathbf{U_2^{i,w^\star}}$ und $\mathbf{U_2^w}$ genügt es also sicherzustellen, daß Ψ die Menge $\mathbf{\Sigma_i^b \cup \Pi_i^b}$, $\mathbf{\Sigma_i^b}(\mathcal{A}) \cup \mathbf{\Pi_i^b}(\mathcal{A})$, $\mathbf{\Sigma_i^{1,b} \cup \Pi_i^{1,b}}$, $\mathbf{\Sigma_i^{1,w^\star} \cup \Pi_i^{1,w^\star}}$ bzw. $\mathbf{\Sigma^{1,w}}$ umfaßt.

Tatsächlich würde die Definition von Ψ als die zu dem Fragment passende, oben angegebene minimale Menge die schärfste Formulierung des partiellen Schnitteliminationssatzes ergeben, die sich ohne Mehraufwand zeigen ließe. I. allg. reicht es aber, die Schnittformeln der Herleitungen auf die Formelmengen $\mathbf{\Sigma^b}$, $\mathbf{\Sigma^b}(\mathcal{A})$, $\mathbf{\Sigma^{1,b}}$, $\mathbf{\Sigma^{1,w^\star}}$ bzw. $\mathbf{\Sigma^{1,w}}$ zu beschränken.

4.2 Definition

(a) $\mathbf{S^i_2}\text{-rg} \;:=\; \mathbf{S^i_2}(\mathcal{A})\text{-rg} \;:=\; \mathbf{\Sigma^b}(\mathcal{A})\text{-rg}$

(b) $\mathbf{U^i_2}\text{-rg} \;:=\; \mathbf{\Sigma^{1,b}}\text{-rg}$

(c) $\mathbf{U_2^{i,w^\star}}\text{-rg} \;:=\; \mathbf{\Sigma^{1,w^\star}}\text{-rg}$

(d) $\mathbf{U^w_2}\text{-rg} \;:=\; \mathbf{\Sigma^{1,w}}\text{-rg}$

Sei $\mathbb{F}$ eines der Fragmente $\mathbf{S^i_2}$, $\mathbf{S^i_2}(\mathcal{A})$, $\mathbf{U^i_2}$, $\mathbf{U_2^{i,w^\star}}$ oder $\mathbf{U^w_2}$.

4.3 Lemma

Seien F, F' aus $\mathbf{L_{BA}}$.

(i) $\mathbb{F}\text{-rg}(F) = \mathbb{F}\text{-rg}(\neg F)$

(ii) Geht F' aus F durch gebundene Umbenennung hervor, so gilt

$$\mathbb{F}\text{-rg}(F') = \mathbb{F}\text{-rg}(F).$$

(iii) $A(a) \in \mathbf{\Sigma_0^{1,b}} \implies \mathbf{U^i_2}\text{-rg}(F(\alpha)) = \mathbf{U^i_2}\text{-rg}(F(A(.)))$.

(iv) $A(a) \in \mathbf{\Sigma_0^{1,w^\star}} \implies \mathbf{U_2^{i,w^\star}}\text{-rg}(F(\alpha)) = \mathbf{U_2^{i,w^\star}}\text{-rg}(F(A(.)))$.

(v) $A(a) \in \mathbf{\Sigma^{1,w}} \implies \mathbf{U^w_2}\text{-rg}(F(\alpha)) = \mathbf{U^w_2}\text{-rg}(F(A(.)))$.

Beweis jeweils durch Induktion nach der Länge von F:

Sei Ψ die zu $\mathbb{F}$ gehörende Formelmenge. (i) bis (v) ergeben sich direkt aus der Definition von $\Psi\text{-rg}(F)$ und der Induktionsvoraussetzung unter Ausnutzung der Abgeschlossenheit von Ψ gegen gebundene Umbenennung bzw. Substitution von $\mathbf{\Sigma_0^{1,b}}$-, $\mathbf{\Sigma_0^{1,w^\star}}$- bzw. $\mathbf{\Sigma^{1,w}}$-Klassentermen. □

Sind $m, m_1, \ldots, m_k, k < \omega$, so wird im folgenden abkürzend $m > m_1, \ldots, m_k$ statt $m > Max\{m_1, \ldots, m_k\}$ geschrieben.

Wir definieren nun ein Herleitungsprädikat $\mathbb{F} \mid\!\!\frac{m}{r}\; \Gamma$ für endliche Formelmengen Γ. Dabei ist m eine obere Schranke für die Herleitungslänge und r eine echte obere Schranke für den Schnittgrad.

Dieser Begriff der Herleitbarkeit ist äquivalent zu dem Begriff mit lokal korrekten Herleitungsbäumen, an deren Blättern Axiome stehen.

4.4 Definition von $\mathbb{F} \mid\!\frac{m}{r}\ \Gamma$

(a) Ist Γ ein Axiom von $\mathbb{F}$, dann gelte $\mathbb{F} \mid\!\frac{m}{r}\ \Gamma$ für beliebige $m, r < \omega$.

(b) Ist $k \leq 1$, $\vdash \Xi_i$, $i \leq k$, $\Longrightarrow$ $\vdash \Gamma$ ein Schluß (S) ungleich (Schnitt) von $\mathbb{F}$ und gilt $\mathbb{F} \mid\!\frac{m_i}{r}\ \Xi_i$ für $i \leq k$, dann gelte $\mathbb{F} \mid\!\frac{m}{r}\ \Gamma$ für $m > m_1, \ldots, m_k$.

(c) (Schnitt): Gilt $\mathbb{F} \mid\!\frac{m_1}{r}\ \Gamma, F$ und $\mathbb{F} \mid\!\frac{m_2}{r}\ \Gamma, \neg F$ und $\mathbb{F}\text{-}\mathsf{rg}(F) < r$, dann gelte $\mathbb{F} \mid\!\frac{m}{r}\ \Gamma$ für $m > m_1, m_2$.

Wir schreiben $\mathbb{F} \mid\!\frac{}{r}\ \Gamma$ dafür, daß es ein $m < \omega$ mit $\mathbb{F} \mid\!\frac{m}{r}\ \Gamma$ gibt.
Die folgenden drei Aussagen sind rein technischer Natur. Sie geben uns das formale Rüstzeug, um die anschließenden Beweise einfacher zu formulieren.

4.5 Lemma

$$\mathbb{F} \mid\!\frac{m}{r}\ \Gamma \quad \Longrightarrow \quad \begin{array}{ll} \text{(i)} & \mathbb{F} \mid\!\frac{m}{r}\ \Gamma a(t) \text{ für jeden Term } t \text{ aus } \mathbf{L_{BA}} \\ \text{(ii)} & \mathbb{F} \mid\!\frac{m}{r}\ \Gamma \alpha(\beta) \text{ für jede freie Variable } \beta. \end{array}$$ □

Lemma 4.5 impliziert eine technische Vereinfachung für Beweise durch Herleitungsinduktion: Die Eigenvariablen in Schlüssen mit Variablenbedingung können immer außerhalb einer vorgegebenen endlichen Menge freier Variablen gewählt werden.

4.6 Tautologie- und Gleichheitslemma

(i) $\mathbb{F} \mid\!\frac{}{0}\ \neg A, A$

(ii) $\mathbb{F} \mid\!\frac{}{0}\ a \neq b, \neg A(a), A(b)$

Beweis durch Induktion nach der Länge von A:
Dabei benutzt der Indukionsanfang, also der Fall, daß A eine Primformel ist, in (i) ein logisches Axiom und in (ii) ein Gleichheitsaxiom. □

4.7 Lemma

Sei Γ', A' eine gebundene Umbenennung von Γ, A, dann gilt:

(i) $\mathbb{F} \mid\!\frac{m}{r}\ \Gamma \implies \mathbb{F} \mid\!\frac{m}{r}\ \Gamma'$

(ii) Für $G(\alpha) \in \mathbf{L_{BA}}$ mit $\mathsf{BV}(G) \cap \mathsf{BV}(A) = \emptyset = \mathsf{BV}(G) \cap \mathsf{BV}(A')$ gilt $\mathbb{F} \mid\!\frac{m}{r}\ \Gamma, G(A(.)) \implies \mathbb{F} \mid\!\frac{m}{r}\ \Gamma, G(A'(.))$.

Beweis:
Der erste Teil läßt sich durch Induktion nach m beweisen. Teil (ii) ergibt sich aus der Beobachtung, daß unter den gegebenen Voraussetzungen $G(A'(.))$ eine gebundene Umbenennung von $G(A(.))$ ist. □

4.8 Strukturschluß

$$\mathbb{F} \mid\!\!\frac{m}{r} \Gamma \quad \text{und} \quad m \leq n < \omega\,,\ r \leq s < \omega\,,\ \Gamma \subset \Lambda \text{ endlich} \quad \Longrightarrow \quad \mathbb{F} \mid\!\!\frac{n}{s} \Lambda$$

Beweis durch Induktion nach m:

Die Bemerkung im Anschluß an Lemma 4.5 zeigt, daß sich die Eigenvariablen von Schlüssen mit Variablenbedingung immer außerhalb von $\mathsf{FV}(\Lambda)$ wählen lassen. Darum folgt die Behauptung aus der Induktionsvoraussetzung durch Anwenden des gleichen Schlusses. □

Führt man einen Beweis durch Herleitungsinduktion, so läßt sich in der Mengenschreibweise, im Gegensatz zur Sequenzenschreibweise, der Konklusion eines Schlusses i. allg. nicht mehr die genaue Gestalt der Prämissen ansehen.
Hier liefert der Strukturschluß eine Vereinfachung in der Betrachtung möglicher Prämissen. Es genügt, den Fall zu betrachten, daß die Hauptformel schon in der Prämisse vorhanden ist, denn sonst fügt man sie per Strukturschluß hinzu. Dies ändert nicht die Herleitungslänge der Prämisse, man kann also immer noch die Induktionsvoraussetzung anwenden.

Wir bereiten nun den partiellen Schnitteliminationssatz vor. Wollen wir den Schnittrang einer Herleitung von $\mathbb{F}$ erniedrigen, so müssen wir unter anderem auch Schnitte mit der Hauptformel eines Komprehensionsschlusses reduzieren. Wir erhalten in solch einer Situation zwei Herleitungen

$$\mathbb{F} \mid\!\!\frac{}{r} \Gamma, F(A(.)) \quad \text{und} \quad \mathbb{F} \mid\!\!\frac{}{r} \Gamma, \neg F(\alpha)$$

mit $\alpha \notin \mathsf{FV}(\Gamma)$ und $\mathbb{F}\text{-}\mathsf{rg}(\exists\phi\, F(\phi)) = r$. Nun möchten wir gern in der zweiten Herleitung α durch $\{u : A(u)\}$ ersetzen und anschließend schneiden:

$$(\text{Schnitt})\ \frac{\Gamma, F(A(.)) \qquad \Gamma, \neg F(A(.))}{\Gamma}$$

Mit Lemma 4.3 gilt $\mathbb{F}\text{-}\mathsf{rg}(F(A(.))) < \mathbb{F}\text{-}\mathsf{rg}(\exists\phi\, F(\phi)) = r$, also ist dieser Schnitt einfacher als der ursprüngliche. Wir müssen noch sicherstellen, daß durch die Ersetzung der Schnittrang der zweiten Herleitung nicht wächst. Dies wird im Einsetzungslemma 4.10 geschehen.
Doch vorher tragen wir Eigenschaften der Einsetzung von Klassentermen in Formeln zusammen.

4.9 Lemma

Seien A, B, F Formeln, deren gebundenen Variablen paarweise verschieden sind.

(i) Sei $A(a) \in \mathbf{\Sigma_0^{1,b}}$.

$$F \in \mathbf{\Sigma_i^{1,b}} \implies F_\alpha(A(.)) \in \mathbf{\Sigma_i^{1,b}}$$

$$F \in \mathbf{\Pi_i^{1,b}} \implies F_\alpha(A(.)) \in \mathbf{\Pi_i^{1,b}}$$

(ii) Sei $A(a) \in \mathbf{\Sigma_0^{1,w^\star}}$.

$$F \in \mathbf{\Sigma_i^{1,w^\star}} \implies F_\alpha(A(.)) \in \mathbf{\Sigma_i^{1,w^\star}}$$

$$F \in \mathbf{\Pi_i^{1,w^\star}} \implies F_\alpha(A(.)) \in \mathbf{\Pi_i^{1,w^\star}}$$

(iii) $\Big(F_b(t)\Big)_\alpha(A(.)) \equiv \Big(F_\alpha(A(.))\Big)_b(t)$ falls $b \notin \mathsf{FV}(A)$.

(iv) $\Big(\mathrm{Q}\phi\, F(\phi)\Big)_\alpha(A(.)) \equiv \mathrm{Q}\phi \Big(F(\beta)_\alpha(A(.))\Big)_\beta(\phi)$ falls β neu ist.

(v) $\Big(F_\beta(\{u : B_b(u)\})\Big)_\alpha(A(.)) \equiv \Big(F_\alpha(A(.))\Big)_\beta(\{u : (B_\alpha(A(.)))_b(u)\})$
falls β neu für A und B ist.

Beweis:

(i) Sei $F' :\equiv F_\alpha(A(.))$. Durch Induktion nach der Länge von F wird gezeigt:

$$\forall i: \quad \begin{array}{ll} (1)\ F \in \mathbf{\Sigma_i^{1,b}} & \implies F' \in \mathbf{\Sigma_i^{1,b}} \\ (2)\ F \in \mathbf{\Pi_i^{1,b}} & \implies F' \in \mathbf{\Pi_i^{1,b}}. \end{array}$$

Dabei betrachten wir nur den Fall (1) $F \in \mathbf{\Sigma_i^{1,b}}$, der andere Fall (2) $F \in \mathbf{\Pi_i^{1,b}}$ wird dual bewiesen.

(a) $F \in \mathbf{\Sigma_i^{1,b}}$ sei eine Primformel.
Für $\alpha \notin \mathsf{FV}(F)$ ist $F' \equiv F$. Anderenfalls muß $F \equiv t \in \alpha$ oder $F \equiv t \notin \alpha$ sein. Also hat F' die Gestalt $F' \equiv A(t)$ bzw. $F' \equiv \neg A(t)$. Nun ist $A(a) \in \mathbf{\Sigma_0^{1,b}}$ und somit $F' \in \mathbf{\Sigma_0^{1,b}} \subset \mathbf{\Sigma_i^{1,b}}$.

(b) $F \equiv G \circ H \in \mathbf{\Sigma_i^{1,b}}$ mit $\circ \in \{\wedge, \vee\}$. Dann muß $G, H \in \mathbf{\Sigma_i^{1,b}}$ sein. Die Induktionsvoraussetzung liefert uns hieraus $G', H' \in \mathbf{\Sigma_i^{1,b}}$, also

$$F' \equiv G' \circ H' \in \mathbf{\Sigma_i^{1,b}}.$$

(c) $F \equiv \mathrm{Q}x{\le}t\, G(x) \in \mathbf{\Sigma_i^{1,b}}$ mit $\mathrm{Q} \in \{\forall, \exists\}$. Für eine neue Variable b gilt dann $G(b) \in \mathbf{\Sigma_i^{1,b}}$. Also produziert die Induktionsvoraussetzung $G'(b) \in \mathbf{\Sigma_i^{1,b}}$, mithin

$$F' \equiv \mathrm{Q}x{\le}t\, G'(x) \in \mathbf{\Sigma_i^{1,b}}.$$

(d) $F \equiv \mathrm{Q}x\, G(x) \in \mathbf{\Sigma_i^{1,b}}$ ist nicht möglich.

(e) $F \equiv \exists\phi\, G(\phi) \in \mathbf{\Sigma_i^{1,b}}$. Dann ist $G(\beta) \in \mathbf{\Sigma_i^{1,b}}$ für eine neue Variable β und $i > 0$. Aus der Induktionsvoraussetzung erhalten wir $G'(\beta) \in \mathbf{\Sigma_i^{1,b}}$ und somit

$$F' \equiv \exists\phi\, G'(\phi) \in \mathbf{\Sigma_i^{1,b}}.$$

(f) $F \equiv \forall\phi\, G(\phi) \in \mathbf{\Sigma_i^{1,b}}$. Nach der Definition von $\mathbf{\Sigma_i^{1,b}}$ muß $F \in \mathbf{\Pi_{i-1}^{1,b}}$ und $i > 1$ gelten, da $F \notin \mathbf{\Sigma_1^{1,b}}$ ist. Dann ist $G(\beta) \in \mathbf{\Pi_{i-1}^{1,b}}$ für eine neue Variable β und die Induktionsvoraussetzung zeigt $G'(\beta) \in \mathbf{\Pi_{i-1}^{1,b}}$, mithin

$$F' \equiv \forall\phi\, G'(\phi) \in \mathbf{\Pi_{i-1}^{1,b}} \subset \mathbf{\Sigma_i^{1,b}}.$$

(ii) Das Argument ist hier analog zu (i). In den Fällen (e) und (f) müssen wir zusätzlich für $F \equiv Q\phi\, G(\phi) \in \mathbf{\Sigma_i^{1,w^\star}/\Pi_i^{1,w^\star}}$ beachten, daß F die Gestalt $Q\phi\, H(\phi^{|t|})$ für eine Formel $H \in \mathbf{\Sigma_i^{1,w^\star}/\Pi_i^{1,w^\star}}$ hat, deren Länge dann auch kleiner als $\mathsf{L}(F)$ ist.

(iii) – (v) wird jeweils durch Induktion nach der Länge von F bewiesen. □

4.10 Einsetzungslemma

(i) Sei $A(a) \in \mathbf{\Sigma_0^{1,b}}$ mit $\mathsf{BV}(\Gamma) \cap \mathsf{BV}(A(a)) = \emptyset$, dann gilt

$$\mathbf{U_2^i} \vdash_r^m \Gamma \implies \mathbf{U_2^i} \vdash_r \Gamma\alpha(A(.)) .$$

(ii) Sei $A(a) \in \mathbf{\Sigma^{1,w}}$ mit $\mathsf{BV}(\Gamma) \cap \mathsf{BV}(A(a)) = \emptyset$, dann gilt

$$\mathbf{U_2^w} \vdash_r^m \Gamma \implies \mathbf{U_2^w} \vdash_r \Gamma\alpha(A(.)) .$$

Beweis in beiden Fällen durch Induktion nach m:
Sei $\Gamma' := \Gamma\alpha(A(.))$, entsprechend F'.

(i) Ist Γ ein logisches Axiom, so zeigt das Tautologielemma 4.6 (i) $\mathbf{U_2^i} \vdash_r \Gamma'$.

Falls $t \neq s, t \notin \alpha, s \in \alpha$ in Γ sind, folgt $\mathbf{U_2^i} \vdash_r \Gamma'$ durch zweimalige Termersetzung 4.5 (i) angewandt auf das Gleichheitslemma 4.6 (ii): $\mathbf{U_2^i} \vdash_0 t \neq s$, $\neg A(t), A(s)$.

Die übrigen Möglichkeiten für Γ, Axiom zu sein, beinhalten nur Formelmengen mit Hauptformeln, die α nicht enthalten. Damit hat Γ' dieselbe axiomatische Hauptformel wie Γ. Also gilt $\mathbf{U_2^i} \vdash_r \Gamma'$.

Liegt kein Axiom vor, so werden bezüglich des letzten Schlusses (S) folgende Fälle unterschieden:

> Ist (S) aus ($\wedge$), ($\vee$), ($\forall$), ($\exists$), ($\forall\leq$), ($\exists\leq$), dann erhalten wir die Behauptung direkt aus der Induktionsvoraussetzung mit demgleichen Schluß (S). Schwierigkeiten mit den obigen Variablebedingungen treten nicht auf, da unter Berücksichtigung der Bemerkung an Lemma 4.5 die Eigenvariablen in ($\forall$) und ($\forall\leq$) passend gewählt werden können.

(Schnitt) Der letzte Schluß hatte die Gestalt

$$\mathbf{U_2^i} \mid\!\!\frac{m_1}{r} \Gamma, F\,,\ \mathbf{U_2^i} \mid\!\!\frac{m_2}{r} \Gamma, \neg F \implies \mathbf{U_2^i} \mid\!\!\frac{m}{r} \Gamma$$

mit $m_1, m_2 < m$ und $\mathbf{U_2^i}\text{-}\mathsf{rg}(F) < r$.
Ohne Einschränkung sei $\mathsf{BV}(\Gamma, F) \cap \mathsf{BV}(A) = \emptyset$. Die Induktionsvoraussetzung liefert uns $\mathbf{U_2^i} \vdash_r \Gamma', F'$ und $\mathbf{U_2^i} \vdash_r \Gamma', \neg F'$. Nun erhalten wir aus Lemma 4.3 (iii), $\mathbf{U_2^i}\text{-}\mathsf{rg}(F') = \mathbf{U_2^i}\text{-}\mathsf{rg}(F) < r$, mit einem (Schnitt)

$$\mathbf{U_2^i} \vdash_r \Gamma'\,.$$

($\forall^2$) Als letzter Schluß liegt

$$\mathbf{U_2^i} \mid\!\!\frac{m_1}{r} \Gamma, \forall\phi\, F(\phi), F(\beta) \implies \mathbf{U_2^i} \mid\!\!\frac{m}{r} \Gamma, \forall\phi\, F(\phi)$$

mit $m_1 < m$ und $\beta \notin \mathsf{FV}(\Gamma, \forall\phi\, F(\phi), A) \cup \{\alpha\}$ wegen der Bemerkung zu Lemma 4.5 vor. Dann liefert uns die Induktionsvoraussetzung

$$\mathbf{U_2^i} \vdash_r \Gamma', (\forall\phi\, F(\phi))', (F(\beta))_\alpha\,(A(.))\ .$$

Lemma 4.9 (iv) zeigt

$$(\forall\phi\, F(\phi))' \ \equiv\ \forall\phi\ ((F(\beta))_\alpha\,(A(.)))_\beta\,(\phi)\ .$$

Also folgt mit ($\forall^2$) wegen $\beta \notin \mathsf{FV}(\Gamma', (\forall\phi\, F(\phi))')$

$$\mathbf{U_2^i} \vdash_r \Gamma', (\forall\phi\, F(\phi))'\ .$$

($\exists^2$) Da $F(\alpha)$ sich als $F(\{u : u{\in}\alpha\})$ schreiben läßt, können wir diesen Schluß als ($\mathbf{\Sigma_0^{1,b}}$-CA) auffassen.

($\mathbf{\Sigma_i^{1,b}}$-PIND) Hier folgt die Behauptung aus der Induktionsvoraussetzung unter Berücksichtigung von Lemma 4.9 (i), (iii).

($\mathbf{\Sigma_0^{1,b}}$-CA) Es gibt $B \in \mathbf{\Sigma_0^{1,b}}$ und $m_1 < m$ mit

$$\mathbf{U_2^i} \mid\!\!\frac{m_1}{r} \Gamma, \exists\phi\, F(\phi), F(B(.)) \implies \mathbf{U_2^i} \mid\!\!\frac{m}{r} \Gamma, \exists\phi\, F(\phi)\,.$$

Ohne Einschränkung gelte $\mathsf{BV}(B) \cap \mathsf{BV}(A) = \emptyset$. Seien β, b neue Variablen, dann ergibt folgende Definition

$$G :\equiv F(\beta)\,,\ C :\equiv B(b)$$

und die Induktionsvoraussetzung

$$\mathbf{U_2^i} \vdash_r \Gamma', (\exists\phi\, F(\phi))', \Big(G_\beta(C_b(.))\Big)'\ . \tag{1}$$

Lemma 4.9 (v) bezeugt

$$\Big(G_\beta(C_b(.))\Big)' \ \equiv\ G'_\beta(C'_b(.))\,.$$

Mit diesem und Lemma 4.9 (i) läßt sich ($\mathbf{\Sigma_0^{1,b}}$-CA) auf (1) anwenden:

$$\mathbf{U_2^i} \vdash_r \Gamma', (\exists\phi\, F(\phi))', \exists\phi\, G'_\beta(\phi)\,.$$

Lemma 4.9 (iv) liefert dann die Behauptung.

(ii) Dieser Punkt läuft analog zu (i) bis auf folgende Fälle:

($\mathbf{\Sigma^{1,w}}$-LIND) Hier folgt die Behauptung aus der Induktionsvoraussetzung unter Berücksichtigung von Lemma 4.9 (iii) und der Abgeschlossenheit von $\mathbf{\Sigma^{1,w}}$ gegen Substitution von $\mathbf{\Sigma^{1,w}}$-Klassentermen.

($\mathbf{\Sigma^{1,w}}$-CA) Mit $B \in \mathbf{\Sigma^{1,w}}$ und $m_1 < m$ liege folgender letzter Schluß vor:

$$\mathbf{U_2^w} \mid\!\!\frac{m_1}{r} \Gamma, \exists\phi\, F(\phi), F(B(.)) \implies \mathbf{U_2^w} \mid\!\!\frac{m}{r} \Gamma, \exists\phi\, F(\phi)\,.$$

Wie unter (i) folgt für $G :\equiv F(\beta)\,,\ C :\equiv B(b)$

$$\mathbf{U_2^w} \mid\!\!\frac{}{r} \Gamma', (\exists\phi\, F(\phi))'\,, G'_\beta(C'_b(.))\,.$$

Da $\mathbf{\Sigma^{1,w}}$ abgeschlossen ist unter Substitution, erhalten wir $C' \equiv B(b)' \in \mathbf{\Sigma^{1,w}}$ und daraus mit ($\mathbf{\Sigma^{1,w}}$-CA)

$$\mathbf{U_2^w} \mid\!\!\frac{}{} \Gamma', (\exists\phi\, F(\phi))'\,, \exists\phi\, G'_\beta(\phi)\,.$$

Wieder liefert Lemma 4.9 (iv) die Behauptung. □

In $\mathbf{U_2^{i,w^\star}}$ läßt sich ein Einsetzungslemma in der obigen Form nicht beweisen, da i. allg. die Menge $\{u \le |t| : A(u)\}$ so nicht beweisbar existent ist, sondern nur die Existenz von Mengen ϕ mit $\forall x{\le}|t|\,(x \in \phi \leftrightarrow A(x))$ gewährleistet wird. Hier müssen wir anders vorgehen.
Gehen wir davon aus, daß zwei Herleitungen

$$\mathbf{U_2^{i,w^\star}} \mid\!\!\frac{}{r} \Gamma, F(\{u \le |t| : A(u)\}) \quad \text{und} \quad \mathbf{U_2^{i,w^\star}} \mid\!\!\frac{}{r} \Gamma, \neg F(\alpha^{|t|})$$

mit $\alpha \notin \mathsf{FV}(\Gamma)$ und $\mathbf{U_2^{i,w^\star}}\text{-}\mathsf{rg}\big(\exists\phi\, F(\phi^{|t|})\big) = r$ gegeben sind, so setzen wir sie wie folgt zusammen, wobei für den ersten Schluß

$$\mathbf{U_2^{i,w^\star}}\text{-}\mathsf{rg}(F(\{u \le |t| : A(u)\})) < \mathbf{U_2^{i,w^\star}}\text{-}\mathsf{rg}(\exists\phi\, F(\phi)) = r$$

mit Lemma 4.3 ausgenutzt wird.

$$(\forall^2)\quad \frac{\underbrace{\Gamma, F(\{u \le |t| : A(u)\}) \qquad \Gamma, \neg F(\alpha^{|t|})}_{\Downarrow}}{\Gamma, \neg\exists\phi\,\forall x{\le}|t|\,(x \in \alpha^{|t|} \leftrightarrow A(x))}$$
$$\Gamma, \neg\exists\phi\,\forall x{\le}|t|\,(x \in \phi^{|t|} \leftrightarrow A(x))$$

Mit $A(a) \in \mathbf{\Sigma_0^{1,w^\star}}$ ist $\exists\phi\,\forall x{\le}|t|\,(x \in \phi^{|t|} \leftrightarrow A(x))$ eine $\mathbf{\Sigma_1^{1,w^\star}}$-Formel, also hat das Komprehensionsaxiom den Rang 0 und wir können damit schneiden.
Daß die benötigten Zwischenschritte auch schnittfrei herleitbar sind, zeigt das nächste Lemma.

4.11 Lemma

Sei $A(a) \in \mathbf{\Sigma_0^{1,w^\star}}$ und $G(\beta)$ eine beliebige Formel. Es gilt

(i) $\mathbf{U_2^{i,w^\star}} \mid\!\!\frac{}{0} \neg\forall x{\le}|t|\,(x \in \alpha^{|t|} \leftrightarrow A(x)), \neg G(\{u \le |t| : A(u)\}), G(\alpha^{|t|})\,.$

(ii) $\mathbf{U_2^{i,w^\star}} \mid\!\!\frac{}{0} \exists\phi\,\forall x{\le}|t|\,(x \in \phi^{|t|} \leftrightarrow A(x))\,.$

Beweis:

(i) Wir zeigen die Behauptung durch Induktion nach der Länge der Formel G. Ist $\beta \notin \mathsf{FV}(G)$, so liefert das Tautologielemma 4.6 (i) das Gewünschte.
Ist $G \equiv s{\in}\beta$, so ist $\neg G(\{u{\leq}|t| : A(u)\}) \equiv s{\not\leq}|t| \vee \neg A(s)$ und $G(\alpha^{|t|}) \equiv s \in \alpha^{|t|}$. Das Tautologielemma 4.6 (i) liefert uns schnittfreie Herleitungen von $\neg A(s), A(s)$ und von $s \notin \alpha^{|t|}, s \in \alpha^{|t|}$, mit denen wir dann die folgende schnittfreie Herleitung bilden:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\neg A(s), A(s) \qquad s \notin \alpha^{|t|}, s \in \alpha^{|t|}}{\neg A(s), A(s) \wedge s \notin \alpha^{|t|}, s \in \alpha^{|t|}}(\wedge)}{\neg A(s), \neg(s \in \alpha^{|t|} \leftrightarrow A(s)), s \in \alpha^{|t|}}(\vee)}{s \not\leq |t|, \neg A(s), \exists x{\leq}|t|\, \neg(x \in \alpha^{|t|} \leftrightarrow A(x)), s \in \alpha^{|t|}}(\exists{\leq})}{s \not\leq |t| \vee \neg A(s), \neg\forall x{\leq}|t|\, (x \in \alpha^{|t|} \leftrightarrow A(x)), s \in \alpha^{|t|}}\,2(\vee)$$

Ist $G \equiv s{\notin}\beta$, so gilt $\neg G(\{u{\leq}|t| : A(u)\}) \equiv s{\leq}|t| \wedge A(s)$ und $G(\alpha^{|t|}) \equiv s \notin \alpha^{|t|} \equiv s \not\leq |t| \vee s \notin \alpha$. Analog zu oben verwenden wir das Tautologielemma 4.6 (i), um die folgende schnittfreie Herleitung zu bilden:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\neg A(s), A(s) \qquad s \notin \alpha^{|t|}, s \in \alpha^{|t|}}{\neg A(s) \wedge s \in \alpha^{|t|}, A(s), s \notin \alpha^{|t|}}(\wedge)}{\neg(s \in \alpha^{|t|} \leftrightarrow A(s)), A(s), s \notin \alpha^{|t|}}(\vee) \qquad s \leq |t|, s \not\leq |t|}{\neg(s \in \alpha^{|t|} \leftrightarrow A(s)), s \leq |t| \wedge A(s), s \notin \alpha^{|t|}, s \not\leq |t|}(\wedge)}{\exists x{\leq}|t|\, \neg(x \in \alpha^{|t|} \leftrightarrow A(x)), s \leq |t| \wedge A(s), s \notin \alpha^{|t|}, s \not\leq |t|}(\exists{\leq})}{\neg\forall x{\leq}|t|\, (x \in \alpha^{|t|} \leftrightarrow A(x)), s \leq |t| \wedge A(s), s \notin \alpha^{|t|}}(\vee)$$

In den übrigen Fällen ergibt sich die Behauptung aus der Induktionsvoraussetzung und einem der Paare $(\wedge), 2\times(\vee)$, $(\exists{\leq}), (\forall{\leq})$, $(\exists), (\forall)$ oder $(\exists^2), (\forall^2)$.

(ii) Das Tautologielemma 4.6 (i) liefert uns eine schnittfreie Herleitung von $\neg A(a), A(a)$, die wir wie folgt schnittfrei verlängern:

$$\dfrac{\dfrac{\dfrac{\dfrac{\neg A(a), A(a)}{a \not\leq |t| \vee \neg A(a), A(a)}\,2(\vee)}{a \leq |t| \wedge A(a) \to A(a)}(\vee) \qquad \dfrac{\dfrac{\neg A(a), A(a) \qquad a \leq |t|, a \not\leq |t|}{\neg A(a), a \leq |t| \wedge A(a), a \not\leq |t|}(\wedge)}{a \not\leq |t|, A(a) \to a \leq |t| \wedge A(a)}\,2(\vee)}{a \not\leq |t|, a \leq |t| \wedge A(a) \leftrightarrow A(a)}(\wedge)$$

$$\dfrac{\dfrac{a \not\leq |t|, a \leq |t| \wedge A(a) \leftrightarrow A(a)}{\forall x{\leq}|t| \left(x \leq |t| \wedge A(x) \leftrightarrow A(x)\right)}(\forall{\leq})}{\exists\phi\, \forall x{\leq}|t| \left(\phi^{|t|} \leftrightarrow A(x)\right)}\,(\mathrm{w}\boldsymbol{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{0}}\text{-CA})$$

□

Sei $\mathbb{F}$ eines der Fragmente $\mathbf{S_2^i}$, $\mathbf{S_2^i}(\mathcal{A})$, $\mathbf{U_2^i}$, $\mathbf{U_2^{i,w^\star}}$ oder $\mathbf{U_2^w}$.

4.12 Inversionslemma

(i) $\mathbb{F} \vdash_r^m \Gamma, A_1 \wedge A_2 \implies \mathbb{F} \vdash_r^m \Gamma, A_i$ für $i = 1, 2$.

(ii) $\mathbb{F} \vdash_r^m \Gamma, \forall x\, F(x) \implies \mathbb{F} \vdash_r^m \Gamma, F(s)$ für s beliebig.

(iii) $\mathbb{F} \vdash_r^m \Gamma, \forall x{\leq}t\, F(x) \implies \mathbb{F} \vdash_r^m \Gamma, s \not\leq t, F(s)$ für s beliebig.

(iv) $\mathbb{F} \vdash_r^m \Gamma, \forall \phi\, F(\phi) \implies \mathbb{F} \vdash_r^m \Gamma, F(\alpha)$ für α beliebig.

Beweis durch Induktion nach m:

Unter Ausnutzung der Bemerkung zu Lemma 4.5 für (ii) und (iii) folgt die Behauptung elementar. □

4.13 Reduktionslemma

Sei F vom $\vee$-Typ mit $\mathbb{F}\text{-}\mathsf{rg}(F) = r > 0$, dann gilt:

$$\mathbb{F} \vdash_r^m \Gamma, F \;\&\; \mathbb{F} \vdash_r \Lambda, \neg F \implies \mathbb{F} \vdash_r \Gamma, \Lambda\,.$$

Beweis durch Induktion nach m:

Ist Γ, F ein Axiom, dann auch Γ, da jede Hauptformel eines Axioms den $\mathbb{F}$-Rang 0 hat und $r > 0$ ist.

Sei also Γ, F kein Axiom und (S) ein letzter Schluß. Es werden folgende Fälle unterschieden:

(i) F ist nicht Hauptformel dieses letzten Schlusses (S). Dann gibt es Formelmengen Ξ_i für $i < k$ mit

$$\mathbb{F} \vdash_1^{m_i} \Xi_i, F \text{ und } m_1, \ldots, m_k < m\,, \tag{1}$$

$$(\mathrm{S}) \quad \Xi_i\,,\ i \leq k\,, \implies \Gamma \quad \text{ist ein Schluß in } \mathbb{F},$$

und bei Berücksichtigung der Bemerkung nach Lemma 4.5 gilt überdies

$$(\mathrm{S}) \quad \Xi_i, \Lambda\,,\ i \leq k\,, \implies \Gamma, \Lambda \quad \text{ist ein Schluß in } \mathbb{F}. \tag{2}$$

Die Induktionsvoraussetzung angewandt auf (1) liefert $\mathbb{F} \vdash_r \Xi_i, \Lambda$ für $i \leq k$. Falls (S) = (Schnitt) ist, muß der $\mathbb{F}$-Rang der Schnittformel kleiner als r sein. Dann produziert (2) die Behauptung.

Nun sind noch die Fälle übrig, in denen F Hauptformel des letzten Schlusses ist. Da F vom $\vee$-Typ und $\mathbb{F}\text{-}\mathsf{rg}(F) > 0$ ist, kann (S) nur noch einer der Schlüsse ($\vee$), ($\exists$), ($\exists{\leq}$), ($\exists^2$), oder ($\mathbf{\Sigma_0^{1,b}}$-CA), ($\mathbf{\Sigma^{1,w}}$-CA) bzw. (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) sein.

(ii) Ist (S) aus ($\vee$), ($\exists$), ($\exists{\leq}$), ($\exists^2$), dann hat die Hauptformel F die Gestalt $A_1 \vee A_2\,,\ \exists x\, G(x)\,,\ \exists x{\leq}t\, G(x)$ bzw. $\exists \phi\, G(\phi)$, da für (S) = ($\exists{\leq}$) wegen $\mathbb{F}\text{-}\mathsf{rg}(F) > 0 = \mathbb{F}\text{-}\mathsf{rg}(s \leq t)$ die Hauptformel F nicht $s \leq t$ gewesen sein kann.

Sei H die Nebenformel des Schlusses, also hat H die Form A_{i_0} für ein $i_0 \in \{1,2\}$, $G(s)$ für einen Term s aus $\mathbf{L_{BA}}$ bzw. $G(\beta)$ für eine freie Variable β und es existiert ein $m_1 < m$ mit $\mathbb{F} \vdash\!\!\!\frac{m_1}{r} \Gamma, F, H$. Hieraus liefert die Induktionsvoraussetzung $\mathbb{F} \vdash\!\!\!_r \Gamma, \Lambda, G$. Mit 4.12 (i)-(iv) und einem Strukturschluß 4.8 folgt $\mathbb{F} \vdash\!\!\!_r \Gamma, \Lambda, \neg G$.
Nun ist $\mathbb{F}\text{-}\mathsf{rg}(G) < \mathbb{F}\text{-}\mathsf{rg}(F)$, also liefert ein (Schnitt) die Behauptung.

(iii) ($\mathbf{\Sigma^{1,b}_0}$-CA): F hat die Gestalt $\exists\phi\, G(\phi)$ und der letzte Schluß die Prämisse

$$\mathbf{U^i_2} \vdash\!\!\!\frac{m_1}{r} \Gamma, F, G(A(.))$$

mit $m_1 < m$ und $A(a) \in \mathbf{\Sigma^{1,b}_0}$. Die Induktionsvoraussetzung produziert

$$\mathbf{U^i_2} \vdash\!\!\!_r \Gamma, \Lambda, G(A(.)) \,. \tag{3}$$

Unter Berücksichtigung von Lemma 4.7 gelte ohne Einschränkung

$$\mathsf{BV}(A') \cap \mathsf{BV}(\Lambda, F) = \emptyset \,.$$

Mit dem Inversionslemma 4.12 (iv), dem Einsetzungslemma 4.10 (i) und einem Strukturschluß 4.8 erhalten wir aus der zweiten Voraussetzung

$$\mathbf{U^i_2} \vdash\!\!\!_r \Gamma, \Lambda, \neg G(A'(.)) \,. \tag{4}$$

Nun ist

$$\begin{array}{rcl} \mathbf{U^i_2}\text{-}\mathsf{rg}(G(A'(.))) & = & \mathbf{U^i_2}\text{-}\mathsf{rg}(G(A(.))) \\ & \overset{4.3\ (ii)}{=} & \mathbf{U^i_2}\text{-}\mathsf{rg}(G) \\ & < & \mathbf{U^i_2}\text{-}\mathsf{rg}(F) = r \,. \end{array}$$

Damit ergibt ein (Schnitt) von (3) und (4) die Behauptung.

(iv) (w$\mathbf{\Sigma^{1,w^\star}_0}$-CA): F hat die Gestalt $\exists\phi\, G(\phi^{|t|})$ und als Prämisse des letzten Schlusses liegt

$$\mathbf{U^{i,w^\star}_2} \vdash\!\!\!\frac{m_1}{r} \Gamma, F, G(\{u \le |t| : A(u)\})$$

mit $m_1 < m$ und $A(a) \in \mathbf{\Sigma^{1,w^\star}_0}$ vor.
Sei α eine neue Variable. Es ist $\mathbf{U^{i,w^\star}_2}\text{-}\mathsf{rg}\Big(G(\alpha^{|t|})\Big) < r$ und wie unter (iii) sehen wir $\mathbf{U^{i,w^\star}_2}\text{-}\mathsf{rg}(G(\{u \le |t| : A(u)\})) < r$. Mit Lemma 4.11 (i) gilt

$$\mathbf{U^{i,w^\star}_2} \vdash\!\!\!_0 \neg\forall x{\le}|t|\,(x \in \alpha^{|t|} \leftrightarrow A(x)), \neg G(\{u \le |t| : A(u)\}), G(\alpha^{|t|}) \,,$$

also liefert ein (Schnitt) mit der Induktionsvoraussetzung inklusive Strukturschluß 4.8

$$\mathbf{U^{i,w^\star}_2} \vdash\!\!\!_r \Gamma, \Lambda, G(\alpha^{|t|}), \neg\forall x{\le}|t|\,(x \in \alpha^{|t|} \leftrightarrow A(x)) \,.$$

Ein (Schnitt) mit dem Inversionslemma 4.12 (iv), angewandt auf die zweite Voraussetzung, zeigt

$$\mathbf{U_2^{i,w^\star}} \mathrel{|\!\frac{}{\,r\,}} \Gamma, \Lambda, \neg\forall x{\le}|t|\,(x \in \alpha^{|t|} \leftrightarrow A(x))\,,$$

also mit ($\forall^2$)

$$\mathbf{U_2^{i,w^\star}} \mathrel{|\!\frac{}{\,r\,}} \Gamma, \Lambda, \neg\exists\phi\,\forall x{\le}|t|\,(x \in \phi^{|t|} \leftrightarrow A(x))\,. \tag{5}$$

Da nach Lemma 4.11 (ii) (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) schnittfrei herleitbar ist, folgt mit einem Strukturschluß 4.8

$$\mathbf{U_2^{i,w^\star}} \mathrel{|\!\frac{}{\,r\,}} \Gamma, \Lambda, \exists\phi\,\forall x{\le}|t|\,(x \in \phi^{|t|} \leftrightarrow A(x))\,.$$

Nun ist

$$\mathbf{U_2^{i,w^\star}}\text{-}\mathsf{rg}\Big(\exists\phi\,\forall x{\le}|t|\,(x \in \phi^{|t|} \leftrightarrow A(x))\Big) = 0\,,$$

also liefert ein (Schnitt) mit (5) die Behauptung.

(v) ($\mathbf{\Sigma^{1,w}}$-CA): $F \;\equiv\; \exists\phi\, G(\phi)$ und der letzte Schluß hat die Prämisse

$$\mathbf{U_2^{w}} \mathrel{|\!\frac{m_1}{\,r\,}} \Gamma, F, G(A(.))$$

mit $m_1 < m$ und $A(a) \in \mathbf{\Sigma^{1,w}}$. Dann folgt die Behauptung wie unter (iii) mit dem einzigen Unterschied, daß hier Lemma 4.10 (ii) an Stelle von Lemma 4.10 (i) ausgenutzt wird. □

4.14 Eliminationssatz

$$\mathbb{F} \mathrel{|\!\frac{m}{\,r\,}} \Gamma \quad\Longrightarrow\quad \mathbb{F} \mathrel{|\!\frac{}{\,1\,}} \Gamma\,.$$

Beweis durch Hauptinduktion nach r und Nebeninduktion nach m:

Ist Γ ein Axiom, so ist nichts zu zeigen. Sei also Γ kein Axiom und (S) ein letzter Schluß. Ist (S) kein (Schnitt) vom Rang $r' > 0$, so folgt die Behauptung direkt aus der Nebeninduktionsvoraussetzung mit demgleichen Schluß (S). Also bleibt noch der Fall zu betrachten:

$$\text{(Schnitt)}\quad \mathbb{F} \mathrel{|\!\frac{m_1}{\,r\,}} \Gamma, F \quad\&\quad \mathbb{F} \mathrel{|\!\frac{m_2}{\,r\,}} \Gamma, \neg F \quad\Longrightarrow\quad \mathbb{F} \mathrel{|\!\frac{m}{\,r\,}} \Gamma$$

mit $m_1, m_2 < m$ und $0 < r' := \mathbb{F}\text{-}\mathsf{rg}(F) < r$. Nun liefert die Nebeninduktionsvoraussetzung

$$\mathbb{F} \mathrel{|\!\frac{}{\,1\,}} \Gamma, F \quad\&\quad \mathbb{F} \mathrel{|\!\frac{}{\,1\,}} \Gamma, \neg F\,.$$

Mit dem Reduktionslemma 4.13 folgt hieraus $\mathbb{F} \mathrel{|\!\frac{}{\,r'\,}} \Gamma$. Dann produziert die Hauptinduktionsvoraussetzung die Behauptung. □

Ist $\mathbb{F}$ eines der Fragmente $\mathbf{S_2^i}$, $\mathbf{S_2^i}(\mathcal{A})$, $\mathbf{U_2^i}$, $\mathbf{U_2^{i,w^\star}}$ oder $\mathbf{U_2^w}$, so erhalten wir für Formelmengen Γ aus $\mathbf{\Sigma^b}$, $\mathbf{\Sigma^b}(\mathcal{A})$, $\mathbf{\Sigma^{1,b}}$, $\mathbf{\Sigma^{1,w^\star}}$ bzw. $\mathbf{\Sigma^{1,w}}$ mit $\mathbb{F} \vdash \Gamma$ durch partielle Schnittelimination eine Herleitung von Γ in $\mathbb{F}$, in der alle auftretenden Formeln aus $\mathbf{\Sigma^b}$, $\mathbf{\Sigma^b}(\mathcal{A})$,

$\mathbf{\Sigma^{1,b}}$, $\mathbf{\Sigma^{1,w^\star}}$ bzw. $\mathbf{\Sigma^{1,w}}$ sind. Diese schwache Teilformeleigenschaft ist für die meisten Fragestellungen in der Berschränkten Arithmetik ausreichend, so auch für den weiteren Verlauf dieser Arbeit. Im nun folgenden mittleren Teil dieser Arbeit nutzen wir diese Teilformeleigenschaft aus, um mit Übersetzungen von $\mathbf{\Sigma^b}$ in $\mathbf{\Sigma^{1,w^\star}}$ und von $\mathbf{\Sigma^{1,w^\star}}$ in $\mathbf{\Sigma^b}$ durch Herleitungsinduktionen den erststufigen Hauptsatz der Beschränkten Arithmetik von $\mathbf{S_2^i}$ auf $\mathbf{U_2^{i,w^\star}}$ zu übertragen.

Teil B

Der Hauptsatz der Beschränkten Arithmetik für $\mathbf{U}_{\mathbf{2}}^{\mathbf{i,w^\star}}$

5 Beobachtungen in $\mathbf{U}_2^{\mathbf{i},\mathbf{w}^\star}$

Zu Beginn dieses Abschnitts übertragen wir die Ergebnisse aus Abschnitt 3 für $\mathbf{S}_2^{\mathbf{i}}$ auf $\mathbf{U}_2^{\mathbf{i},\mathbf{w}^\star}$. Darüberhinaus beschäftigen wir uns mit Komprehensionen sowohl im zweitstufigen als auch im erststufigen Bereich. Als wichtigstes Ergebnis erhalten wir, daß $\mathbf{U}_2^{\mathbf{i},\mathbf{w}^\star}$ für $i>0$ eine über (w$\mathbf{\Sigma}_0^{\mathbf{1},\mathbf{w}^\star}$-CA) hinausgehende Komprehension beweist, nämlich (w$\mathbf{\Sigma}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}$-CA). Im erststufigen Bereich ist die Komprehension von der Einschränkung der erststufigen Quantoren in $\mathbf{\Sigma}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}$ auf scharf beschränkte, also logarithmische, Anfangsstücke abhängig. Wie wir später noch sehen werden, hat dies zur Folge, daß eine Formulierung wie etwa

$$\exists x\, \forall y{\leq}|t|\, (y \in \alpha \leftrightarrow \mathrm{Bit}(y,x)=1)$$

nicht in $\mathbf{U}_2^{\mathbf{i},\mathbf{w}^\star}$ gilt, da der Existenzquantor nicht scharf beschränkt werden kann. Diesem gesamten Teil B liegt [Takeuti 1991] zugrunde.

Wir können hier die zu übertragenen Äquivalenzen aus Abschnitt 3 schon über $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star}$ beweisen, da in $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star}$ alle für die Beweise benötigten Funktionen aus $\mathbf{P}$ a priori vorhanden sind. Dagegen wurden sie in $\mathbf{S}_2^{\mathbf{i}}$ durch ein aufwendiges Bootstrapping-Verfahren definiert, bei dem man die gewünschten Eigenschaften beweisen muß. Das wesentliche Beweismittel dabei ist ($\mathbf{\Sigma}_\mathbf{1}^\mathbf{b}$-PIND).
Zuerst betrachten wir die verschiedenen P- und L-Induktionen über $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star}$. Für $\mathbf{S}_2^{\mathbf{1}}$ sind ($\mathbf{\Sigma}_\mathbf{i}^\mathbf{b}$-LIND), ($\mathbf{\Pi}_\mathbf{i}^\mathbf{b}$-LIND), ($\mathbf{\Sigma}_\mathbf{i}^\mathbf{b}$-PIND) und ($\mathbf{\Pi}_\mathbf{i}^\mathbf{b}$-PIND) äquivalent. Hier zeigen wir die Äquivalenz von

(a) $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star} + (\mathbf{\Sigma}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}\text{-LIND})$

(b) $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star} + (\mathbf{\Sigma}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}\text{-PIND})$

(c) $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star} + (\mathbf{\Pi}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}\text{-LIND})$

(d) $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star} + (\mathbf{\Pi}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}\text{-PIND})$.

5.1 Lemma

(i) $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star} + (\mathbf{\Sigma}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}\text{-LIND})$ beweist $(\mathbf{\Pi}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}\text{-LIND})$

(ii) $\mathbf{U}_2^{\mathbf{0},\mathbf{w}^\star} + (\mathbf{\Pi}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}\text{-LIND})$ beweist $(\mathbf{\Sigma}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}\text{-LIND})$.

Beweis:

Für (i) sei $A(a) \in \mathbf{\Pi}_\mathbf{i}^{\mathbf{1},\mathbf{w}^\star}$ mit $a \notin \mathsf{FV}(A(0))$ und t ein Term aus $\mathbf{L_{BA}}$. Da Induktionsregel und -axiom äquivalent sind, genügt es,

$$\mathbf{U}_2^{\mathbf{i},\mathbf{w}^\star} \vdash \neg A(0), \neg\forall x\, (A(x) \to A(\mathrm{S}x)), A(|t|)$$

zu beweisen. Wir führen den Beweis informal in $\mathbf{U_2^{i,w^\star}}$. Gelte

$$\neg A(|t|) \tag{1}$$

und

$$\forall x\,(\neg A(\mathrm{S}x) \to \neg A(x))\,. \tag{2}$$

Dann ist $\neg A(0)$ zu zeigen. Dazu sei

$$B(b) \mathrel{:\equiv} \neg A(|t| \dot{-} b)$$

für eine neue Variable b, dann ist $B(b) \in \mathbf{\Sigma_i^{1,w^\star}}$ und aus (1) folgt

$$B(0)\,. \tag{3}$$

Aus (2) erhalten wir

$$\forall x\,(B(x) \to B(\mathrm{S}x))\,, \tag{4}$$

denn gelte $B(x)$ für ein beliebiges x, also

$$\neg A(|t| \dot{-} x)\,. \tag{5}$$

Ist $|t| \dot{-} x = |t| \dot{-} \mathrm{S}x$, so zeigt (5) $\neg A(|t| \dot{-} \mathrm{S}x)$. Sei also $|t| \dot{-} x \neq |t| \dot{-} \mathrm{S}x$, dann zeigen die Axiome $\mathrm{S}(|t| \dot{-} \mathrm{S}x) = |t| \dot{-} x$, also folgt $\neg A(\mathrm{S}(|t| \dot{-} \mathrm{S}x))$ mit (5). Hieraus liefert nun die Voraussetzung (2) $\neg A(|t| \dot{-} \mathrm{S}x)$. In jedem Fall haben wir $B(\mathrm{S}x)$ gezeigt, womit (4) bewiesen ist.

Aus (3) und (4) folgt mit ($\mathbf{\Sigma_i^{1,w^\star}}$-LIND) $B(|t|)$, mithin $\neg A(0)$.

Der gleiche Beweis mit $A(a) \in \mathbf{\Sigma_i^{1,w^\star}}$ und Anwendung von ($\mathbf{\Pi_i^{1,w^\star}}$-LIND) zeigt auch (ii). □

5.2 Lemma

(i) $\mathbf{U_2^{0,w^\star}} + (\mathbf{\Sigma_i^{1,w^\star}}\text{-LIND})$ beweist $(\mathbf{\Sigma_i^{1,w^\star}}\text{-PIND})$

(ii) $\mathbf{U_2^{0,w^\star}} + (\mathbf{\Pi_i^{1,w^\star}}\text{-LIND})$ beweist $(\mathbf{\Pi_i^{1,w^\star}}\text{-PIND})$.

Beweis:

Für (i) sei $A(a) \in \mathbf{\Sigma_i^{1,w^\star}}$ mit $a \notin \mathsf{FV}(A(0))$ und t ein Term aus $\mathbf{L_{BA}}$. Wie in 5.1 genügt es, das äquivalente Induktionsaxiom herzuleiten:

$$\mathbf{U_2^{i,w^\star}} \vdash \neg A(0), \neg\forall x\,(A(\lfloor \tfrac{1}{2}x \rfloor) \to A(x)), A(t)\,.$$

Wir argumentieren wieder informal in $\mathbf{U_2^{i,w^\star}}$. Gelte also

$$A(0) \tag{1}$$

und

$$\forall x\,(A(\lfloor \tfrac{1}{2}x \rfloor) \to A(x))\,, \tag{2}$$

dann ist $A(t)$ zu zeigen. Sei b eine neue Variable. Für $B(b) \mathrel{:\equiv} A(\mathrm{MSP}(t, |t| \dot{-} b))$ folgt aus (1)

$$B(0)\,, \tag{3}$$

denn die Axiome liefern $\mathrm{MSP}(t, |t| \dot{-} 0) = 0$. Um

$$\forall x\,(B(x) \to B(\mathrm{S}x)) \tag{4}$$

zu zeigen, nehmen wir $B(x)$ für ein beliebiges x an, also

$$A(\mathrm{MSP}(t, |t| \dot{-} x))\,. \tag{5}$$

Ist $x < |t|$, so folgt aus den Axiomen

$$\mathrm{MSP}(t, |t| \dot{-} x) = \lfloor \tfrac{1}{2}\mathrm{MSP}(t, |t| \dot{-} \mathrm{S}x)\rfloor\,,$$

also mit (5) $A(\lfloor \frac{1}{2}\mathrm{MSP}(t, |t| \dot{-} \mathrm{S}x)\rfloor)$. Voraussetzung (2) darauf angewendet produziert $A(\mathrm{MSP}(t, |t| \dot{-} \mathrm{S}x))$, mithin $B(\mathrm{S}x)$. Im anderen Fall ist $x \geq |t|$, also $|t| \dot{-} x = 0 = |t| \dot{-} \mathrm{S}x$. Damit zeigt (5) $A(\lfloor \frac{1}{2}\mathrm{MSP}(t, |t| \dot{-} \mathrm{S}x)\rfloor)$, mithin $B(\mathrm{S}x)$. Insgesamt ist (4) gezeigt.

Aus (3) und (4) folgt mit ($\mathbf{\Sigma^{1,w^\star}_i}$-LIND) $B(|t|)$, also

$$A(\mathrm{MSP}(t, |t| \dot{-} |t|))\,.$$

Kombinieren wir dies mit $\mathrm{MSP}(t, |t| \dot{-} |t|) = t$, was wir aus den Axiomen extrahieren, so ergibt das

$$A(t)\,.$$

Der gleiche Beweis mit $A(a) \in \mathbf{\Pi^{1,w^\star}_i}$ und Anwendung von ($\mathbf{\Pi^{1,w^\star}_i}$-LIND) zeigt auch (ii). □

Die fehlenden Implikationen der behaupteten Äquivalenzen adaptieren wir aus [Buss 1986]:

5.3 Lemma

(i) $\mathbf{U^{0,w^\star}_2}$ + ($\mathbf{\Sigma^{1,w^\star}_i}$-PIND) zeigt ($\mathbf{\Sigma^{1,w^\star}_i}$-LIND)

(ii) $\mathbf{U^{0,w^\star}_2}$ + ($\mathbf{\Pi^{1,w^\star}_i}$-PIND) beweist ($\mathbf{\Pi^{1,w^\star}_i}$-LIND).

Beweis:

Für (i) sei $A(a) \in \mathbf{\Sigma^{1,w^\star}_i}$ mit $a \notin \mathsf{FV}(A(0))$ und t ein Term aus $\mathbf{L_{BA}}$. Wir zeigen wieder das äquivalente Axiom:

$$\mathbf{U^{i,w^\star}_2} \vdash \neg A(0), \neg\forall x\,(A(x) \to A(\mathrm{S}x)), A(|t|)\,.$$

Dazu sei $B(a) \equiv A(|a|)$. Es gilt

$$\mathbf{U^{i,w^\star}_2} \vdash \neg A(0), B(0)$$

und

$$\mathbf{U^{i,w^\star}_2} \vdash \neg\forall x\,(A(x) \to A(\mathrm{S}x)), \forall x\,(B(\lfloor \tfrac{1}{2}x\rfloor) \to B(x))\,.$$

Nun ist $B(a) \in \mathbf{\Sigma^{1,w^\star}_i}$, also folgt mit ($\mathbf{\Sigma^{1,w^\star}_i}$-PIND)

$$\mathbf{U^{i,w^\star}_2} \vdash \neg A(0), \neg\forall x\,(A(x) \to A(\mathrm{S}x)), B(t)\,,$$

was zu zeigen war.

Der gleiche Beweis mit $A(a) \in \mathbf{\Pi_i^{1,w^\star}}$ und Anwendung von ($\mathbf{\Pi_i^{1,w^\star}}$-PIND) zeigt auch (ii). □

5.4 Korollar

Wir haben nun die Äquivalenz folgender Theorien gezeigt:

(a) $\mathbf{U_2^{0,w^\star}} + (\mathbf{\Sigma_i^{1,w^\star}}\text{-LIND})$

(b) $\mathbf{U_2^{0,w^\star}} + (\mathbf{\Sigma_i^{1,w^\star}}\text{-PIND})$

(c) $\mathbf{U_2^{0,w^\star}} + (\mathbf{\Pi_i^{1,w^\star}}\text{-LIND})$

(d) $\mathbf{U_2^{0,w^\star}} + (\mathbf{\Pi_i^{1,w^\star}}\text{-PIND})$. □

Als nächsten Punkt beschäftigen wir uns mit logarithmischer Minimierung. Mit Satz 3.2 wissen wir schon, daß $\mathbf{S_2^1} + (\mathbf{\Sigma_i^b}\text{-LMIN})$ äquivalent zu $\mathbf{S_2^1} + (\mathbf{\Pi_i^b}\text{-PIND})$ ist. Wir haben eine analoge Aussage für $\mathbf{U_2^{i,w^\star}}$:

$$\mathbf{U_2^{0,w^\star}} + (\mathbf{\Sigma_i^{1,w^\star}}\text{-LMIN}) \qquad \text{ist äquivalent zu} \qquad \mathbf{U_2^{0,w^\star}} + (\mathbf{\Pi_i^{1,w^\star}}\text{-LIND})\,.$$

Dabei betrachten wir hier eine etwas andere Form des (Ψ-LMIN)-Axioms als in Abschnitt 3. Die dort verwendete Gestalt wird den Besonderheiten von $\mathbf{U_2^{i,w^\star}}$ nicht gerecht, da erststufige, beschränkte Quantoren auftreten, die nicht scharf beschränkt sind.

$$(\mathbf{\Sigma_i^{1,w^\star}}\text{-LMIN}) \quad \exists x{\leq}|b|\, A(x) \to \exists x{\leq}|b|\, \Big(A(x) \wedge \forall y{\leq}|b|\, (y < x \to \neg A(y))\Big)$$

für $A(a) \in \mathbf{\Sigma_i^{1,w^\star}}$ mit $a \notin \mathsf{FV}\,(A(0))$.

5.5 Lemma

$\mathbf{U_2^{0,w^\star}} + (\mathbf{\Sigma_i^{1,w^\star}}\text{-LMIN})$ beweist ($\mathbf{\Pi_i^{1,w^\star}}$-LIND).

Beweis:

Wir nehmen an, es gelte

$$A(0) \quad \text{und} \quad \neg A(|t|)$$

für $A(a) \in \mathbf{\Pi_i^{1,w^\star}}$. Dann existiert mit ($\mathbf{\Sigma_i^{1,w^\star}}$-LMIN) minimales $x \leq |t|$ mit $\neg A(x)$. Wegen $A(0)$ muß $x > 0$ sein, also folgt aus der Minimalität von x $A(x \dot{-} 1)$. Mithin erhalten wir $\exists x\,(A(x) \wedge \neg A(\mathrm{S}x))$. Damit haben wir

$$\neg\forall x\,(A(x) \to A(\mathrm{S}x))$$

gezeigt, insgesamt also ($\mathbf{\Pi_i^{1,w^\star}}$-LIND). □

Die andere Richtung der oben behaupteten Äquivalenz liefert das folgende Lemma.

5.6 Lemma

$\mathbf{U_2^{i,w^\star}}$ beweist ($\mathbf{\Sigma_i^{1,w^\star}}$-LMIN).

Beweis:

Sei $A(a) \in \mathbf{\Sigma_i^{1,w^\star}}$ und $a \notin \mathsf{FV}(A(0))$. Der Beweis erfolgt in $\mathbf{U_2^{i,w^\star}}$.

Gelte $\neg\exists x{\leq}|b|\,(A(x) \wedge \forall y{<}x\,\neg A(y))$, also

$$\forall x{\leq}|b|\,(\neg A(x) \vee \exists y{<}x\,A(y))\,, \tag{1}$$

dann ist $\forall x{\leq}|b|\,\neg A(x)$ zu zeigen.

Dazu sei $B(c) :\equiv \forall y{\leq}|b|\,(y \leq c \rightarrow \neg A(y)) \in \mathbf{\Pi_i^{1,w^\star}}$ für eine neue Variable c. Aus (1) folgt für $x = 0$ $\neg A(0)$ und somit

$$B(0)\,. \tag{2}$$

Um

$$\forall z\,(B(z) \rightarrow B(\mathrm{S}z)) \tag{3}$$

zu erhalten, nehmen wir ein beliebiges z mit B(z), also

$$\forall y{\leq}|b|\,(y \leq z \rightarrow \neg A(y))\,, \tag{4}$$

und schließen auf $B(\mathrm{S}z) \equiv \forall y{\leq}|b|\,(y \leq \mathrm{S}z \rightarrow \neg A(y))$. Nach der Voraussetzung (4) gilt für $y \leq |b|$ und $y \leq z$ schon $\neg A(y)$. Bleibt noch der Fall $y \leq |b| \wedge y \leq \mathrm{S}z$ und $y \not\leq z$ zu betrachten. Die Axiome stellen $y = \mathrm{S}z \leftrightarrow (y \not\leq z \wedge y \leq \mathrm{S}z)$ und $w < \mathrm{S}z \leftrightarrow w \leq z$ sicher, also erhalten wir mit (1)

$$\neg A(\mathrm{S}z) \vee \exists w{\leq}z\,A(w))\,. \tag{5}$$

Die Voraussetzung (4) zeigt $\forall w{\leq}z\,\neg A(w)$, daher ist in (5) das zweite Disjunktionsglied nicht erfüllt, also gilt $\neg A(\mathrm{S}z)$, d. h. $\neg A(y)$. Damit haben wir den Induktionsschritt (3) gezeigt.

Nun schließen wir mit ($\mathbf{\Pi_i^{1,w^\star}}$-LIND) aus (2) und (3) auf $B(|b|) \equiv \forall y{\leq}|b|\,(y{\leq}|b| \rightarrow \neg A(y))$, also auf

$$\forall x{\leq}|b|\,\neg A(x)\,. \qquad \square$$

Nun kommen wir zu Funktionen f, die durch längenbeschränktes Zählen aus einer Formel $A(a,b,c)$ definiert werden:

$$f(a,b) = \#u{\leq}|a|A(a,b,u)\,.$$

In $\mathbf{S_2^1}$ sind solche f für $A(a,b,c) \in \mathbf{\Delta_1^b}$ bezüglich $\mathbf{S_2^1}$ $\mathbf{\Sigma_1^b}$-definierbar in $\mathbf{S_2^1}$. Entsprechend gilt für $A(a,b,c) \in \mathbf{\Delta_1^{1,w^\star}}$ bezüglich $\mathbf{U_2^{1,w^\star}}$, daß f $\mathbf{\Sigma_1^{1,w^\star}}$-definierbar über $\mathbf{U_2^{1,w^\star}}$ ist.

5.7 Satz

Sei $A(a,b,c)$ aus $\mathbf{\Delta_1^{1,w^\star}}$ bezüglich $\mathbf{U_2^{1,w^\star}}$, $\mathsf{FV}(A) \subset \{a,b,c\}$ und sei f definiert durch längenbeschränktes Zählen nach A, also

$$f \coloneqq \lambda ab.\#u{\leq}|a|A(a,b,u)\,.$$

Dann ist f $\mathbf{\Sigma_1^{1,w^\star}}$-definierbar in $\mathbf{U_2^{1,w^\star}}$.

Beweis:

Sei d eine neue Variable. Wir definieren eine $\mathbf{\Sigma_1^{1,w^\star}}$-Formel $B(\alpha,d,a,b)$, die folgendes beschreibt:

$$\forall x{\leq}d\left(\alpha(x)=\#u{\leq}xA(a,b,u)\right).$$

Wir müssen also beschreiben, daß α eingeschränkt auf $\{0,\dots,d\}$ eine Funktion mit $\forall x{\leq}d\,(\alpha(x)\leq \mathrm{S}x)$ ist:

$$\forall x{\leq}|a|\,(x\leq d\to\exists y{\leq}\mathrm{S}|a|\,(\langle x,y\rangle\in\alpha\wedge y\leq \mathrm{S}x)) \tag{1}$$

$$\forall x{\leq}|a|\,\forall y{\leq}\mathrm{S}|a|\,\forall z{\leq}\mathrm{S}|a|\,(\langle x,y\rangle\in\alpha\wedge\langle x,z\rangle\in\alpha\to y=z)\,, \tag{2}$$

daß $\alpha(0)=\begin{cases}0 & : \neg A(a,b,0)\\ 1 & : A(a,b,0)\end{cases}$ gilt:

$$(\langle 0,0\rangle\in\alpha\vee\langle 0,1\rangle\in\alpha)\wedge(\langle 0,1\rangle\in\alpha\leftrightarrow A(a,b,0))\,, \tag{3}$$

und daß für $\alpha(x)=y$ dann $\alpha(\mathrm{S}x)=\begin{cases}y & : \neg A(a,b,\mathrm{S}x)\\ \mathrm{S}y & : A(a,b,\mathrm{S}x)\end{cases}$ ist:

$$\begin{array}{l}\forall x{\leq}|a|\,\forall y{\leq}|a|\,(x<|a|\wedge x<d\wedge\langle x,y\rangle\in\alpha\\ \to((\langle \mathrm{S}x,y\rangle\in\alpha\vee\langle \mathrm{S}x,\mathrm{S}y\rangle\in\alpha)\wedge(\langle \mathrm{S}x,\mathrm{S}y\rangle\in\alpha\leftrightarrow A(a,b,\mathrm{S}x))))\,.\end{array} \tag{4}$$

Die Konjunktion der Formeln (1) bis (4) ergibt $B(\alpha,d,a,b)$. Da A aus $\mathbf{\Delta_1^{1,w^\star}}$ bezüglich $\mathbf{U_2^{1,w^\star}}$ ist, ist ohne Einschränkung $B\in\mathbf{\Sigma_1^{1,w^\star}}$. Sei $t:\equiv \mathrm{SqBd}_2(2a+1)$, dann gilt

$$\forall x{\leq}\mathrm{S}a\,\forall y{\leq}\mathrm{S}a\,(\langle x,y\rangle\leq|t|)\,.$$

Wir zeigen nun $\mathbf{U_2^{i,w^\star}}\vdash\exists\phi\,B(\phi^{|t|},|a|,a,b)$ durch ($\mathbf{\Sigma_1^{1,w^\star}}$-LIND) nach d in $\exists\phi\,B(\phi^{|t|},d,a,b)$. Es gilt:

(i) $\mathbf{U_2^{1,w^\star}}\vdash\exists\phi\,B(\phi^{|t|},0,a,b)$

(ii) $\mathbf{U_2^{1,w^\star}}\vdash\neg\exists\phi\,B(\phi^{|t|},d,a,b),\exists\phi\,B(\phi^{|t|},\mathrm{S}d,a,b)$.

Denn (i) ergibt sich mit zweimal (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) aus

$$\mathbf{U_2^{1,w^\star}}\vdash B(\{\langle 0,0\rangle\},0,a,b),B(\{\langle 0,1\rangle\},0,a,b)$$

und (ii) erhalten wir durch zweimal (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) und ($\forall^2$) aus

$$\mathbf{U_2^{1,w^\star}}\vdash\neg B(\alpha^{|t|},d,a,b),B(V_1,\mathrm{S}d,a,b),B(V_2,\mathrm{S}d,a,b)$$

mit

$$V_1=\{u\leq|t|:(\beta(1,u)\leq d\wedge u\in\alpha^{|t|})\vee\exists y{\leq}|a|\,(\langle d,y\rangle\in\alpha^{|t|}\wedge\langle \mathrm{S}d,y\rangle=u)\}$$

und

$$V_2=\{u\leq|t|:(\beta(1,u)\leq d\wedge u\in\alpha^{|t|})\vee\exists y{\leq}|a|\,(\langle d,y\rangle\in\alpha^{|t|}\wedge\langle \mathrm{S}d,\mathrm{S}y\rangle=u)\}$$

Nun ist $\exists\phi\,B(\phi^{|t|},d,a,b)\in\mathbf{\Sigma_1^{1,w^\star}}$, also zeigt ($\mathbf{\Sigma_1^{1,w^\star}}$-LIND) mit (ii) und (Schnitt) mit (i)

$$\mathbf{U_2^{1,w^\star}}\vdash\exists\phi\,B(\phi^{|t|},|a|,a,b)\,.$$

Sei $C(a,b,e)$ die $\mathbf{\Sigma_1^{1,w^\star}}$-Formel

$$\exists\phi\,(B(\phi^{|t|},|a|,a,b)\wedge e\leq|a|+1\wedge\langle|a|,e\rangle\in\phi^{|t|})\,.$$

Damit zeigt die Definition von $B(\alpha,d,a,b)$

$$\mathbf{U_2^{1,w^\star}}\;\vdash\forall x\,\forall y\,\exists z{\leq}\mathrm{S}|x|\,C(x,y,z)$$

$$\mathbf{U_2^{1,w^\star}}\;\vdash\forall x\,\forall y\,\forall z_1\,\forall z_2\,(C(x,y,z_1)\wedge C(x,y,z_2)\to z_1=z_2)\,.$$

Des weiteren gilt $\mathbb{N}\models\forall x\,\forall y\,C(x,y,\mathrm{f}(x,y))$, denn wir erhalten für $\alpha\subset\mathbb{N}$ mit $\mathbb{N}\models B(\alpha^{|t|},|a|,a,b)$ durch Induktion nach d

$$\mathbb{N}\models\forall x{\leq}d\,\forall y{\leq}\mathrm{S}|a|\,\Big(\langle x,y\rangle\in\alpha^{|t|}\leftrightarrow y=\#u{\leq}xA(a,b,u)\Big)$$

für $d\leq|a|$. Mithin

$$\begin{array}{lll} C(a,b,e) & \Longleftrightarrow & \langle|a|,e\rangle\in\alpha^{|t|}\wedge e\leq|a|+1\\ & \Longleftrightarrow & e=\#u{\leq}|a|A(a,b,u)=\mathrm{f}(a,b)\,.\end{array}$$

Also läßt sich f $\mathbf{\Sigma_1^{1,w^\star}}$-definieren bezüglich $\mathbf{U_2^{1,w^\star}}$. □

Bemerkung

Die Aussage von Satz 5.7 läßt sich auch auf Formeln $A(\alpha,a,b,c)$ aus $\mathbf{\Delta_1^{1,w^\star}}$ bezüglich $\mathbf{U_2^{1,w^\star}}$ mit freien Mengenvariablen relativieren. Man erhält dann nur noch eine Quasifunktion F mit

$$F(\alpha,a,b)=\#u{\leq}|a|A(\alpha,a,b,u)\,,$$

die durch eine $\mathbf{\Sigma_1^{1,w^\star}}$-Formel $C(\alpha,a,b,e)$ definiert wird.

$$\mathbb{N}\models\forall\phi\,\forall x\,\forall y\,\Big(C(\phi,x,y,\#u{\leq}|x|A(\phi,x,y,u))\Big)$$

Für C zeigt $\mathbf{U_2^{i,w^\star}}$ die Funktionseigenschaft:

$$\mathbf{U_2^{1,w^\star}}\;\vdash\forall\phi\,\forall x\,\forall y\,\exists z{\leq}\mathrm{S}|x|\,C(\phi,x,y,z)$$

$$\mathbf{U_2^{1,w^\star}}\;\vdash\forall\phi\,\forall x\,\forall y\,\forall z_1\,\forall z_2\,(C(\phi,x,y,z_1)\wedge C(\phi,x,y,z_2)\to z_1=z_2)$$

Diese Bemerkung geht in den Beweis von (w$\mathbf{\Sigma_i^{1,w^\star}}$-CA) in $\mathbf{U_2^{i,w^\star}}$ in der Form ein, daß durch längenbeschränktes Zählen die Menge $\alpha^{|t|} \subset \{u \leq |t| : A(u)\}$ maximert wird. Dann gilt auch die andere Inklusion und somit ist die Existenz eines α mit $\alpha^{|t|} = \{u \leq |t| : A(u)\}$ gezeigt.

5.8 Satz

$\mathbf{U_2^{i,w^\star}}$ beweist (w$\mathbf{\Sigma_i^{1,w^\star}}$-CA).

Beweis:

Sei $A(a) \in \mathbf{\Sigma_i^{1,w^\star}}$, t ein Term aus $\mathbf{L_{BA}}$, b, c neue Variablen und

$$B(b) \mathrel{:\equiv} \exists\phi \left(\#u{\leq}|t|(u \in \phi^{|t|}) = b \wedge \forall x{\leq}|t| \, (x \in \phi^{|t|} \to A(x))\right).$$

Die Bemerkung zu Satz 5.7 zeigt, daß $\#u{\leq}|t|(u \in \phi^{|t|}) = b$ durch eine $\mathbf{\Sigma_1^{1,w^\star}}$-Formel beschrieben werden kann. Also ist $B(b) \in \mathbf{\Sigma_i^{1,w^\star}}$. Um mit ($\mathbf{\Sigma_i^{1,w^\star}}$-LMIN) ein maximales b mit $B(b)$ zu bestimmen, sei $C(b) \mathrel{:\equiv} B(|t| + 2 \dot{-} b)$. Aus den Axiomen folgt $\mathbf{U_2^{i,w^\star}} \vdash |4t + 2| = |t| + 2$, also erhalten wir

$$\mathbf{U_2^{i,w^\star}} \vdash C(|4t + 2|)$$

mit (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA), da $\#u{\leq}|t|(u \in \emptyset) = 0 \wedge \forall x{\leq}|t| \, (x \in \emptyset \to A(x))$ erfüllt ist.

Mit ($\mathbf{\Sigma_i^{1,w^\star}}$-LMIN), Lemma 5.6, erhalten wir

$$\mathbf{U_2^{i,w^\star}} \vdash \exists y{\leq}|4t + 2| \, (C(y) \wedge \forall z{\leq}|4t + 2| \, (z < y \to \neg C(z))).$$

Nun argumentieren wir in $\mathbf{U_2^{i,w^\star}}$:

Sei $y \leq |t| + 2$ mit

$$B(|t| + 2 \dot{-} y) \tag{1}$$

und

$$\forall z{<}y \, \neg B(|t| + 2 \dot{-} z), \tag{2}$$

dann gibt es für $k \coloneqq |t| + 2 \dot{-} y$ ein ϕ mit

$$\#u{\leq}|t|(u \in \phi^{|t|}) = k \quad \& \quad \forall x{\leq}|t| \, (x \in \phi^{|t|} \to A(x)). \tag{3}$$

Da immer $\#u{\leq}|t|(\ldots) \leq |t| + 1$ ist, muß $k \leq |t| + 1$ und damit $y > 0$ sein. Also liefert (2)

$$\neg B(k + 1). \tag{4}$$

Um $\forall x{\leq}|t| \, (A(x) \to x \in \phi^{|t|})$ einzusehen, nehmen wir an, daß ein $x \leq |t|$ mit $A(x)$ und $x \notin \phi^{|t|}$ existiert. Mit (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) existiert eine Menge ψ, für die $\psi^{|t|} = \phi^{|t|} \cup \{x\}$ gilt. Dann erhalten wir

$$\forall x{\leq}|t| \, (x \in \psi^{|t|} \to A(x)). \tag{5}$$

Durch ($\mathbf{\Sigma_1^{1,w^\star}}$-LIND) nach d läßt sich

$$\#u{\leq}d(u \in \psi^{|t|}) = \begin{cases} \#u{\leq}d(u \in \phi^{|t|}) & : \quad d < x \\ \#u{\leq}d(u \in \phi^{|t|}) + 1 & : \quad x \leq d \leq |t| \end{cases}$$

zeigen, was für $d = |t|$

$$\#u{\leq}|t|(u \in \psi^{|t|}) = k + 1$$

liefert. Dies ergibt mit (5) $B(k+1)$ im Widerspruch zu (4).

Es zeigt sich $\forall x{\leq}|t|\,(A(x) \to x \in \phi^{|t|})$ und somit $\forall x{\leq}|t|\,(A(x) \leftrightarrow x \in \phi^{|t|})$, also gilt die Behauptung. □

Um den erststufigen und zweitstufigen Bereich von $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ noch weiter zu charakterisieren, untersuchen wir, welche Form von Komprehension sich im erststufigen Bereich simulieren läßt. Wir haben unter anderem folgende Möglichkeiten, die Komprehension zu übertragen:

(i) $\exists x\,\forall y{<}a\,(y \in \alpha \leftrightarrow \mathrm{Bit}(y,x) = 1)$

(ii) $\exists x\,\forall y{<}|a|\,(y \in \alpha \leftrightarrow \mathrm{Bit}(y,x) = 1)$

(iii) $\exists x\,\forall y{<}\Big|\,|a|\,\Big|\,(y \in \alpha \leftrightarrow \mathrm{Bit}(y,x) = 1)$.

Die erste Möglichkeit erscheint wenig erfolgversprechend, da x in der Größenordnung 2^a gewählt werden muß und die Exponentiation keine beweisbar totale Funktion in der beschränkten Arithmetik ist. Bei der zweiten Variante muß x in der Größenordnung a gewählt werden, der Existenzquantor läßt sich daher nicht scharf beschränken. Dies ist aber für $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ eine ungünstige Situation, da polynomiale Quantoren nur über die zweite Stufe in $\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}$ realisiert werden. In der Tat werden wir im dritten Teil dieser Arbeit sehen, daß diese Formel in keinem Fragment $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ beweisbar ist. Die dritte Variante sucht x im Bereich von $|a|$. Dies scheint die richtige Komplexität für $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ zu sein.
Die unten gewählt Grenze für x läßt sich wie folgt berechnen. Für $a = 0$ ist

$$\sum_{i<\left|\,|0|\,\right|} (i)_\alpha \cdot 2^i = 0 = 2 \cdot |a| \dot{-} 1\,.$$

Ist $2^b \leq |a| < 2^{b+1}$, so gilt $\Big|\,|a|\,\Big| = b+1$, mithin

$$\sum_{i<\left|\,|a|\,\right|} (i)_\alpha \cdot 2^i \leq 2^{\left||a|\right|} \dot{-} 1 = 2^{b+1} \dot{-} 1 = 2 \cdot 2^b \dot{-} 1 \leq 2 \cdot |a| \dot{-} 1\,.$$

Nun ist $|2\#a| = \mathrm{S}(|2| \cdot |a|) = 2 \cdot |a| + 1$.

5.9 Satz

$$\mathbf{U_2^{0,w^\star}} \vdash \exists x{\leq}|2\#a|\,\forall y{<}\Big|\,|a|\,\Big|\,\Big(y \in \alpha \leftrightarrow \mathrm{Bit}(y,x)=1\Big)$$

Beweis:

Im weiteren argumentieren wir in $\mathbf{U_2^{0,w^\star}}$. Wir betrachten folgende $\mathbf{\Sigma_0^{1,w^\star}}$-Formel:

$$\begin{aligned} B(b) \quad :\equiv \quad & \exists x{\leq}|2\#b|\,\Big(|x| \leq \Big|\,|b|\,\Big| \wedge \forall y{<}\Big|\,|b|\,\Big|\,\Big(y < \Big|\,|a|\,\Big| \rightarrow \\ & ((\Big|\,|a|\,\Big| \dot{-} \Big|\,|b|\,\Big|) + y \in \alpha \leftrightarrow \mathrm{Bit}(y,x)=1)\Big)\Big)\,. \end{aligned}$$

Es gilt $B(a) \rightarrow \exists x{\leq}|2\#a|\,\forall y{<}\Big|\,|a|\,\Big|\,(y \in \alpha \leftrightarrow \mathrm{Bit}(y,x)=1)$. Darum zeigen wir durch ($\mathbf{\Sigma_0^{1,w^\star}}$-PIND) nach a $B(a)$.

Da mit $|0|=0$ auch $\Big|\,|0|\,\Big|=0$ ist, gilt

$$|0| \leq \Big|\,|0|\,\Big| \wedge \forall y{<}\Big|\,|0|\,\Big|\,(\ldots)\,.$$

Also ergibt sich der Induktionsanfang

$$B(0)\,. \tag{1}$$

Für den Induktionsschritt ist

$$\forall z\,(B(\lfloor \tfrac{1}{2}z \rfloor) \rightarrow B(z)) \tag{2}$$

zu zeigen, was für $z{=}0$ trivial ist. Darum nehmen wir an, es gelte $z{>}0$ und $B(\lfloor \frac{1}{2}z \rfloor)$. Dann existiert $x \leq |2\#\lfloor \frac{1}{2}z \rfloor|$ mit $|x| \leq \Big|\,|\lfloor \frac{1}{2}z \rfloor|\,\Big|$ und

$$\begin{aligned} & \forall y{<}\Big|\,|\lfloor \tfrac{1}{2}z \rfloor|\,\Big|\,(y < \Big|\,|a|\,\Big| \rightarrow \\ & ((\Big|\,|a|\,\Big| \dot{-} \Big|\,|\lfloor \tfrac{1}{2}z \rfloor|\,\Big|) + y \in \alpha \leftrightarrow \mathrm{Bit}(y,x)=1))\,. \end{aligned} \tag{3}$$

Ist $\Big|\,|z|\,\Big| = \Big|\,|\lfloor \frac{1}{2}z \rfloor|\,\Big|$, so ist nichts zu zeigen, da $x \leq |2\#\lfloor \frac{1}{2}z \rfloor| \leq |2\#z|$ gilt.

Sei also $\Big|\,|z|\,\Big| > \Big|\,|\lfloor \frac{1}{2}z \rfloor|\,\Big|$. Dann ist

$$\Big|\,|z|\,\Big| = \mathrm{S}\Big|\,|\lfloor \tfrac{1}{2}z \rfloor|\,\Big|\,, \tag{4}$$

da $|z| = \mathrm{S}|\lfloor \frac{1}{2}z \rfloor|$ und somit $\Big|\,|z|\,\Big| = \Big|\mathrm{S}|\lfloor \frac{1}{2}z \rfloor|\,\Big| \leq \mathrm{S}\Big|\,|\lfloor \frac{1}{2}z \rfloor|\,\Big|$.

Für $\Big|\,|z|\,\Big| > \Big|\,|a|\,\Big|$ gilt mit (4) $\Big|\,|\lfloor \frac{1}{2}z \rfloor|\,\Big| \geq \Big|\,|a|\,\Big|$, also folgt

$$\Big|\,|a|\,\Big| \dot{-} \Big|\,|\lfloor \tfrac{1}{2}z \rfloor|\,\Big| = 0 = \Big|\,|a|\,\Big| \dot{-} \Big|\,|z|\,\Big|$$

und aus $y < \Big|\,|a|\,\Big|$ schon $y < \Big|\,|\lfloor \frac{1}{2}z \rfloor|\,\Big|$; somit liefert uns (3)

$$\forall y{<}\Big|\,|z|\,\Big|\,(y < \Big|\,|a|\,\Big| \rightarrow ((\Big|\,|a|\,\Big| \dot{-} \Big|\,|z|\,\Big|) + y \in \alpha \leftrightarrow \mathrm{Bit}(y,x)=1))\,.$$

Mithin $B(z)$, da wieder $x \leq |2\#\lfloor \frac{1}{2}z \rfloor| \leq |2\#z|$ gilt.

Ist $\Big|\,|z|\,\Big| \leq \Big|\,|a|\,\Big|$, dann folgt mit (4) $\Big|\,|\lfloor \frac{1}{2}z \rfloor|\,\Big| < \Big|\,|a|\,\Big|$, also

$$\Big|\,|a|\,\Big| \dot{-} \Big|\,|\lfloor \tfrac{1}{2}z \rfloor|\,\Big| = \mathrm{S}(\Big|\,|a|\,\Big| \dot{-} \mathrm{S}\Big|\,|\lfloor \tfrac{1}{2}z \rfloor|\,\Big|) = \mathrm{S}(\Big|\,|a|\,\Big| \dot{-} \Big|\,|z|\,\Big|)\,.$$

Nun zeigt (3)

$$\forall y{<}\big|\,|\lfloor\tfrac{1}{2}z\rfloor|\,\big|\,(y<\big||a|\big|\rightarrow((\big||a|\big|\dot{-}\big||z|\big|)+\mathrm{S}y\in\alpha\leftrightarrow\mathrm{Bit}(y,x)=1))\,.$$

Dies impliziert für $\tilde{x}=2\cdot x$ und $\tilde{x}=2\cdot x+1$, da $\mathrm{Bit}(y,x)=\mathrm{Bit}(\mathrm{S}y,\tilde{x})$,

$$\forall y{<}\big||z|\big|\,(0<y<\big||a|\big|\rightarrow((\big||a|\big|\dot{-}\big||z|\big|)+y\in\alpha\leftrightarrow\mathrm{Bit}(y,\tilde{x})=1))\,. \tag{5}$$

Für $y=0$ unterscheiden wir zwei Fälle. Ist $\big||a|\big|\dot{-}\big||z|\big|\in\alpha$, dann gilt wegen (5) und $\mathrm{Bit}(0,2\cdot x+1)=1$

$$\forall y{<}\big||z|\big|\,(y<\big||a|\big|\rightarrow((\big||a|\big|\dot{-}\big||z|\big|)+y\in\alpha\leftrightarrow\mathrm{Bit}(y,2\cdot x+1)=1))\,. \tag{6}$$

Wir beobachten

$$|2\cdot x+1|=|x|+1\leq\big|\,|\lfloor\tfrac{1}{2}z\rfloor|\,\big|+1=\big||z|\big| \tag{7}$$

und

$$\big||2\#z|\big|=\big|\mathrm{S}(2\cdot|z|)\big|=\big||z|\big|+1\,,$$

woraus

$$2\cdot x+1<|2\#z| \tag{8}$$

folgt. Also liefern (6), (7) und (8) $B(z)$.

Im anderen Fall ist $\big||a|\big|\dot{-}\big||z|\big|\notin\alpha$, also gilt wegen $\mathrm{Bit}(0,2\cdot x)\neq 1$ und (5)

$$\forall y{<}\big||z|\big|\,(y<\big||a|\big|\rightarrow((\big||a|\big|\dot{-}\big||z|\big|)+y\in\alpha\leftrightarrow\mathrm{Bit}(y,2\cdot x)=1))\,. \tag{9}$$

Mit (7) und (8) folgt

$$|2\cdot x|\leq|2\cdot x+1|\leq\big||z|\big|$$

und

$$2\cdot x<2\cdot x+1<|2\#z|\,.$$

Dies zusammen mit (9) ergibt auch hier $B(z)$. Mithin ist (2) gezeigt.

(1) und (2) liefern mit ($\mathbf{\Sigma_0^{1,w^\star}}$-PIND)

$$B(a)\,,$$

was zu zeigen war. □

Die letzten Aussagen drehen sich um definierbare Funktionen und Prädikate, die ja ganz allgemein eine definitorische Erweiterung bilden. Aus der Gültigkeit von (w$\mathbf{\Sigma_i^{1,w^\star}}$-CA) in $\mathbf{U_2^{i,w^\star}}$ ergibt sich eine verschärfte Konservativitätsaussage für die Hinzunahme von $\mathbf{\Sigma_1^{1,w^\star}}$-definierbaren Funktionen $\vec{f}$ und $\mathbf{\Delta_1^{1,w^\star}}$-definierbaren Prädikaten $\vec{p}$ bezüglich $\mathbf{U_2^{1,w^\star}}$:

$\mathbf{U_2^{0,w^\star}}$ + ($\mathbf{\Sigma_i^{1,w^\star}}(\vec{f},\vec{p})$-LIND) + (w$\mathbf{\Sigma_0^{1,w^\star}}(\vec{f},\vec{p})$-CA)+ definierende Axiome für $\vec{f}$ und $\vec{p}$ ist konservativ über $\mathbf{U_2^{i,w^\star}}$ für $i>0$.

Die Verschärfung besteht hier in der uneingeschränkten Verwendung der definierbaren Funktions- und Prädikatszeichen auch in den Komprehensionsaxiomen.
Der nächste Satz kann durch die gleiche Begründung wie Satz 3.4 bewiesen werden.

5.10 Satz

Seien $f_1, \ldots, f_k$ $\mathbf{\Sigma_1^{1,w^\star}}$-definierbare Funktionen und $p_1, \ldots, p_l$ $\mathbf{\Delta_1^{1,w^\star}}$-definierbare Prädikate bezüglich $\mathbf{U_2^{i,w^\star}}$, $i > 0$. $\mathbb{F}$ sei das Fragment $\mathbf{U_2^{i,w^\star}}$ erweitert um $\vec{f}$ und $\vec{p}$ als neue Funktions-/Prädikatssymbole und deren definierenden Axiome.

Damit gilt für $k > 0$: ist $B \in \mathbf{\Sigma_k^{1,w^\star}}(\vec{f}, \vec{p})$ oder $B \in \mathbf{\Pi_k^{1,w^\star}}(\vec{f}, \vec{p})$, dann gibt es $B^* \in \mathbf{\Sigma_k^{1,w^\star}}$ bzw. $B^* \in \mathbf{\Pi_k^{1,w^\star}}$ mit $\mathbb{F} \vdash B \leftrightarrow B^*$. □

Da (w$\mathbf{\Sigma_i^{1,w^\star}}$-CA) in $\mathbf{U_2^{i,w^\star}}$ beweisbar ist, erhalten wir folgendes verschärftes Konservativitätsresultat.

5.11 Korollar

Seien $f_1, \ldots, f_k$ $\mathbf{\Sigma_1^{1,w^\star}}$-definierbare Funktionen und $p_1, \ldots, p_l$ $\mathbf{\Delta_1^{1,w^\star}}$-definierbare Prädikate bezüglich $\mathbf{U_2^{i,w^\star}}$, $i > 0$. $\mathbb{F}$ sei das Fragment $\mathbf{U_2^{i,w^\star}}$ erweitert um $f_1, \ldots, f_k$, $p_1, \ldots, p_l$ als neue Funktions-/Prädikatssymbole, deren definierenden Axiome, alle ($\mathbf{\Sigma_i^{1,w^\star}}(\vec{f}, \vec{p})$-LIND) und (w$\mathbf{\Sigma_i^{1,w^\star}}(\vec{f}, \vec{p})$-CR) Schlüsse.

Dann ist $\mathbb{F}$ eine konservative Erweiterung von $\mathbf{U_2^{i,w^\star}}$. □

Durch die Gültigkeit von (w$\mathbf{\Sigma_1^{1,w^\star}}$-CA) in $\mathbf{U_2^{i,w^\star}}$ für $i > 0$ erhalten $\mathbf{\Delta_1^{1,w^\star}}$-Prädikate eine besondere Bedeutung, was auch schon aus dem letzten Korollar ersichtlich ist. Wir zeigen, daß freie Mengenvariablen in einer $\mathbf{U_2^{1,w^\star}}$-Herleitung durch $\mathbf{\Delta_1^{1,w^\star}}$-Klassenterme substituiert werden können, was wegen der auf scharf beschränkte Klassenterme eingeschränkten Komprehension nicht unproblematisch ist.

6 $\mathbf{\Delta_1^{1,w^\star}}$-Klassenterme

Substituiert man für $i>0$ in eine $\mathbf{\Sigma_i^{1,w^\star}}$-Formel $F(\alpha)$ einen Klassenterm $\{u : A(u)\}$ der Komplexität $\mathbf{\Delta_1^{1,w^\star}}$ bezüglich $\mathbf{U_2^{1,w^\star}}$, so ist $F(A(.))$ i. allg. keine $\mathbf{\Sigma_i^{1,w^\star}}$-Formel mehr. Nun existieren aber zu A Formeln $B, \neg C \in \mathbf{\Sigma_i^{1,w^\star}}$ mit $\mathbf{U_2^{1,w^\star}} \vdash A \leftrightarrow B$ und $\mathbf{U_2^{1,w^\star}} \vdash A \leftrightarrow C$. Wird α in $F(\alpha)$ asymmetrisch durch $B(.)$ bzw. $C(.)$ ersetzt, so erhalten wir eine Formel $G \in \mathbf{\Sigma_i^{1,w^\star}}$ mit $\mathbf{U_2^{1,w^\star}} \vdash F(A(.)) \leftrightarrow G$. Daher sind die substituierten Induktions- und Komprehensionsschlüsse, die ursprünglich an die Formelmenge $\mathbf{\Sigma_i^{1,w^\star}}$ gebunden sind, in $\mathbf{U_2^{i,w^\star}}$ beweisbar, da (w$\mathbf{\Sigma_1^{1,w^\star}}$-CA) in $\mathbf{U_2^{i,w^\star}}$ gilt.
Diese Substitutionseigenschaft zu erarbeiten ist das Hauptanliegen dieses Abschnitts.

Zuerst vergrößern wir die Formelmengen $\mathbf{\Sigma^{1,w^\star}}$ und $\mathbf{\Pi^{1,w^\star}}$ vermöge der Äquivalenzrelation auf den Formeln, die durch $\mathbf{U_2^{1,w^\star}} \vdash A \leftrightarrow B$ gegeben ist.

6.1 Definition

Sei $\mathbb{F}$ ein Fragment der Beschränkten Arithmetik und Ψ eine Formelmenge, so sei $\Psi^{\mathbb{F}}$ definiert durch

$$F \in \Psi^{\mathbb{F}} :\Longleftrightarrow \text{ es gibt } G \in \Psi \text{ mit } \mathbb{F} \vdash F \leftrightarrow G\,.$$

Speziell sei

$$\begin{aligned}
\mathbf{\Sigma_i}^{\mathbf{U_2^{1,w^\star}}} &:= \left(\mathbf{\Sigma_i^{1,w^\star}}\right)^{\mathbf{U_2^{1,w^\star}}} \cap \mathbf{\Sigma^{1,w^\star}} \\
\mathbf{\Pi_i}^{\mathbf{U_2^{1,w^\star}}} &:= \left(\mathbf{\Pi_i^{1,w^\star}}\right)^{\mathbf{U_2^{1,w^\star}}} \cap \mathbf{\Sigma^{1,w^\star}} \\
\mathbf{\Delta_i}^{\mathbf{U_2^{1,w^\star}}} &:= \mathbf{\Sigma_i}^{\mathbf{U_2^{1,w^\star}}} \cap \mathbf{\Pi_i}^{\mathbf{U_2^{1,w^\star}}}\,.
\end{aligned}$$

6.2 Lemma

Für $i>0$ beweist $\mathbf{U_2^{i,w^\star}}$ ($\mathbf{\Sigma_i}^{\mathbf{U_2^{1,w^\star}}}$-LIND) und (w$\mathbf{\Sigma_i}^{\mathbf{U_2^{1,w^\star}}}$-CA).

Beweis:

Sei $A(a) \in \mathbf{\Sigma_i}^{\mathbf{U_2^{1,w^\star}}}$, d. h. es gibt $B(a) \in \mathbf{\Sigma_i^{1,w^\star}}$ mit

$$\mathbf{U_2^{i,w^\star}} \vdash \forall x\,(A(x) \leftrightarrow B(x))\,. \tag{1}$$

Um das Induktionsaxiom zu beweisen, betrachten wir ($\mathbf{\Sigma_i^{1,w^\star}}$-LIND) für B:

$$\mathbf{U_2^{i,w^\star}} \vdash \neg B(0), \neg\forall x\,(B(x) \to B(\mathrm{S}x)), B(|t|)\,.$$

Mit (1) folgt aus diesem

$$\mathbf{U_2^{i,w^\star}} \vdash \neg A(0), \neg\forall x\,(A(x) \to A(\mathrm{S}x)), A(|t|)\,,$$

also ($\mathbf{\Sigma_i^{U_2^1,w^\star}}$-LIND).

Entsprechendes gilt für die Komprehension. Wir wissen nach Satz 5.8, daß $\mathbf{U_2^{i,w^\star}}$ (w$\mathbf{\Sigma_i^{1,w^\star}}$-CA) beweist, also gilt

$$\mathbf{U_2^{i,w^\star}} \vdash \exists\phi\,\forall x{\leq}|t|\,\Big(x \in \phi^{|t|} \leftrightarrow B(x)\Big)\,.$$

Mit (1) folgt wieder

$$\mathbf{U_2^{i,w^\star}} \vdash \exists\phi\,\forall x{\leq}|t|\,\Big(x \in \phi^{|t|} \leftrightarrow A(x)\Big)\,,$$

mithin (w$\mathbf{\Sigma_i^{U_2^1,w^\star}}$-CA). □

Nach diesen einführenden Betrachtungen wollen wir jetzt zeigen, daß für $k{>}0$ die Formelmengen $\mathbf{\Sigma_k^{U_2^1,w^\star}}$, $\mathbf{\Pi_k^{U_2^1,w^\star}}$ und $\mathbf{\Delta_k^{U_2^1,w^\star}}$ abgeschlossen sind unter Substitution von $\mathbf{\Delta_1^{U_2^1,w^\star}}$-Klassentermen. Dazu sei $A(a) \in \mathbf{\Delta_1^{U_2^1,w^\star}}$, $F \in \mathbf{\Sigma_k^{U_2^1,w^\star}}$, dann gibt es $G \in \mathbf{\Sigma_k^{1,w^\star}}$ mit $\mathbf{U_2^{1,w^\star}} \vdash F \leftrightarrow G$. Nun möchten wir folgern, daß auch $\mathbf{U_2^{1,w^\star}} \vdash F_\alpha(A(.)) \leftrightarrow G_\alpha(A(.))$ und $G_\alpha(A(.)) \in \mathbf{\Sigma_k^{U_2^1,w^\star}}$ gilt. Also müssen wir zuerst folgende Zwischenschritte zeigen:

(i) $G \in \mathbf{\Sigma_k^{1,w^\star}}\big(\mathbf{\Pi_k^{1,w^\star}}\big)$ und $A(a) \in \mathbf{\Delta_1^{U_2^1,w^\star}} \implies G_\alpha(A(.)) \in \mathbf{\Sigma_k^{U_2^1,w^\star}}\big(\mathbf{\Pi_k^{U_2^1,w^\star}}\big)$

(ii) $\Gamma \subset \mathbf{\Sigma^{1,w^\star}}$, $A(a) \in \mathbf{\Delta_1^{U_2^1,w^\star}}$ und $\mathbf{U_2^{i,w^\star}} \vdash \Gamma \implies \mathbf{U_2^{i,w^\star}} \vdash \Gamma_\alpha(A(.))\,.$

Um zu zeigen, daß in dem Beweis der Ersetzung (ii) ($\mathbf{\Sigma_i^{1,w^\star}}$-LIND) in ($\mathbf{\Sigma_i^{U_2^1,w^\star}}$-LIND) und (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) in (w$\mathbf{\Sigma_1^{U_2^1,w^\star}}$-CA) übergeht, benötigen wir den Teil (i). Darum ist die Reihenfolge der Teilschritte zwingend.

6.3 Definition

Eine Formelmenge Ψ heißt *abgeschlossen unter*

(a) $\wedge, \vee$, wenn mit $A, B \in \Psi$ auch $A \wedge B$ bzw. $A \vee B \in \Psi$ sind.

(b) $\forall x{\leq}|t|\,, \exists x{\leq}|t|\,$, wenn für beliebige Terme t und Variablen a, x mit $A(a) \in \Psi$ auch $\forall x{\leq}|t|\,A(x)$ bzw. $\exists x{\leq}|t|\,A(x) \in \Psi$ sind.

(c) $\forall\phi^{|t|}\,, \exists\phi^{|t|}\,$, wenn für beliebige Terme t und Variablen α, ϕ mit $A(\alpha) \in \Psi$ auch $\forall\phi\,A(\phi^{|t|})$ bzw. $\exists\phi\,A(\phi^{|t|}) \in \Psi$ sind.

(d) $\neg$, wenn mit $A \in \Psi$ auch $\neg A \in \Psi$ ist.

6.4 Lemma

(i) $\mathbf{\Sigma_i^{U_2^1,w^\star}} \subset \mathbf{\Delta_{i+1}^{U_2^1,w^\star}}$ und $\mathbf{\Pi_i^{U_2^1,w^\star}} \subset \mathbf{\Delta_{i+1}^{U_2^1,w^\star}}$.

(ii) $\mathbf{\Sigma_i^{U_2^1,w^\star}}$, $\mathbf{\Pi_i^{U_2^1,w^\star}}$ und $\mathbf{\Delta_i^{U_2^1,w^\star}}$ sind abgeschlossen unter $\wedge, \vee, \forall x{\leq}|t|$ und $\exists x{\leq}|t|$.

(iii) Für $i{>}0$ ist $\mathbf{\Sigma_i^{U_2^1,w^\star}}$ abgeschlossen unter $\exists \phi^{|t|}$ und $\mathbf{\Pi_i^{U_2^1,w^\star}}$ abgeschlossen unter $\forall \phi^{|t|}$.

(iv) $\mathbf{\Delta_i^{U_2^1,w^\star}}$ ist abgeschlossen unter $\neg$.

Beweis:

(i) Da $\mathbf{\Sigma_i^{1,w^\star}} \cup \mathbf{\Pi_i^{1,w^\star}} \subset \mathbf{\Sigma_{i+1}^{1,w^\star}} \cap \mathbf{\Pi_{i+1}^{1,w^\star}}$, folgt $\mathbf{\Sigma_i^{U_2^1,w^\star}} \subset \mathbf{\Delta_{i+1}^{U_2^1,w^\star}}$ und $\mathbf{\Pi_i^{U_2^1,w^\star}} \subset \mathbf{\Delta_{i+1}^{U_2^1,w^\star}}$ sofort aus der Definition von $\mathbf{\Sigma_i^{U_2^1,w^\star}}$, $\mathbf{\Pi_i^{U_2^1,w^\star}}$ und $\mathbf{\Delta_{i+1}^{U_2^1,w^\star}}$.

(ii) Nach Definiton sind $\mathbf{\Sigma_i^{1,w^\star}}$ und $\mathbf{\Pi_i^{1,w^\star}}$ abgeschlossen unter $\wedge, \vee, \forall x{\leq}|t|, \exists x{\leq}|t|$. Daraus ergibt sich der Abschluß von $\mathbf{\Sigma_i^{U_2^1,w^\star}}$, $\mathbf{\Pi_i^{U_2^1,w^\star}}$ und $\mathbf{\Delta_i^{U_2^1,w^\star}}$ unter $\wedge, \vee$, $\forall x{\leq}|t|, \exists x{\leq}|t|$.

(iii) Entsprechend zu (ii) folgt die Behauptung aus der Abgeschlossenheit von $\mathbf{\Sigma_i^{1,w^\star}}$ unter $\exists \phi^{|t|}$ und der Abgeschlossenheit von $\mathbf{\Pi_i^{1,w^\star}}$ unter $\forall \phi^{|t|}$ für $i > 0$.

(iv) Hier folgt die Behauptung aus dem Dualitätsprinzip für $\mathbf{\Sigma_i^{1,w^\star}}$ und $\mathbf{\Pi_i^{1,w^\star}}$:

$$A \in \mathbf{\Sigma_i^{1,w^\star}} \iff \neg A \in \mathbf{\Pi_i^{1,w^\star}}$$ □

6.5 Lemma

Sei $A(a) \in \mathbf{\Delta_1^{U_2^1,w^\star}}$, dann gilt für beliebige Formeln F:

$$\forall k > 0: \quad \begin{array}{ll} \text{(i)} & F \in \mathbf{\Sigma_k^{1,w^\star}} \implies F_\alpha(A(.)) \in \mathbf{\Sigma_k^{U_2^1,w^\star}}, \\ \text{(ii)} & F \in \mathbf{\Pi_k^{1,w^\star}} \implies F_\alpha(A(.)) \in \mathbf{\Pi_k^{U_2^1,w^\star}}. \end{array} \tag{1}$$

Beweis:

Wir zeigen (1) durch Induktion nach der Länge von F. Als Induktionsvoraussetzung haben wir dann (1) für alle Formeln G mit $\mathsf{L}(G) < \mathsf{L}(F)$. Dabei betrachten wir nur (i), (ii) läßt sich dual beweisen. Sei also $k > 0$ und $F \in \mathbf{\Sigma_k^{1,w^\star}}$.

(a) Ist F eine Primformel, so ist $F_\alpha(A(.)) \in \mathbf{\Delta_1^{U_2^1,w^\star}} \subset \mathbf{\Sigma_k^{U_2^1,w^\star}}$.

(b) Ist $F \equiv G \circ H$, $F \equiv \mathrm{Q}x{\leq}|t|\, G(x)$ für $\circ \in \{\wedge, \vee\}$, $\mathrm{Q} \in \{\forall, \exists\}$ oder $F \equiv \exists \phi\, G(\phi)$, so folgt die Behauptung aus der Induktionsvoraussetzung und der Abgeschlossenheit von $\mathbf{\Sigma_k^{U_2^1,w^\star}}$ unter $\wedge, \vee, \forall x{\leq}|t|, \exists x{\leq}|t|$ und $\exists \phi^{|t|}$.

(c) Ist $F \equiv \forall \phi\, G(\phi)$, dann muß $F \in \mathbf{\Pi_{k-1}^{1,w^\star}}$ und $k > 1$ sein, da $F \notin \mathbf{\Sigma_1^{1,w^\star}}$ ist. Außerdem gibt es eine Formel $H \in \mathbf{\Pi_{k-1}^{1,w^\star}}$ und einen Term t mit $F \equiv \forall \phi\, H(\phi^{|t|})$.

Aus der Induktionsvoraussetzung erhalten wir $H(\beta)_\alpha(A(.)) \in \mathbf{\Pi}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{k-1}}$ und wegen der Abgeschlossenheit von $\mathbf{\Pi}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{k-1}}$ unter $\forall\phi^{|t|}$ auch

$$F_\alpha(A(.)) \equiv \forall\phi\left(H(\beta)_\alpha(A(.))_\beta(\phi^{|t|})\right) \in \mathbf{\Pi}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{k-1}} .$$

Wegen $\mathbf{\Pi}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{k-1}} \subset \mathbf{\Delta}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{k}} \subset \mathbf{\Sigma}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{k}}$ folgt die Behauptung. □

Im folgenden sei $i>0$. Das letzte Lemma hat uns gezeigt, daß für $A \in \mathbf{\Delta}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{1}}$ die ersetzte Formel $F_\alpha(A(.))$ in der entsprechenden Formelmenge $\mathbf{\Sigma}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{i}}/\mathbf{\Pi}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{i}}$ wie F liegt. Damit haben wir gute Karten, um die Ersetzung von $\mathbf{\Delta}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{1}}$-Klassentermen bezüglich $\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}}$ zu beweisen. Denn nun haben wir sichergestellt, daß aus einer Hauptformel von ($\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{i}}$-LIND) eine $\mathbf{\Sigma}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{i}}$-Formel und aus einer Hauptformel von (w$\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{0}}$-CA) eine $\mathbf{\Sigma}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{1}}$-Formel wird. (w$\mathbf{\Sigma}^{\mathbf{U}^{\mathbf{1}},\mathbf{w}^\star}_{\mathbf{2}\,\mathbf{1}}$-CA) ist aber in $\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}}$ beweisbar.
Doch vorher müssen wir uns noch mit dem technischen Detail der Vertauschung der Reihenfolge von Klassentermsubstitutionen beschäftigen.

6.6 Lemma

Seien $A(a), B(a)$ Formeln mit $\beta \notin \mathsf{FV}(A)$ und $\alpha \not\equiv \beta$. Weiter sei F eine Formel, und es gelte

$$\mathsf{BV}(F) \cap \mathsf{BV}(B) = \emptyset \quad \text{und} \quad \mathsf{BV}\left(F_\beta(B(.))\right) \cap \mathsf{BV}(A) = \emptyset . \tag{1}$$

Dann gilt:

$$\left(F_\beta(B(.))\right)_\alpha(A(.)) \equiv \left(F_\alpha(A(.))\right)_\beta(\{u : B(u)_\alpha(A(.))\}) .$$

Die Ersetzungen sind alle wegen (1) wohldefiniert.

Beweis durch Induktion nach der Länge von F:

Ist F eine Primformel, so werden folgende Fälle unterschieden:

(i) $\beta \notin \mathsf{FV}(F)$, (a)

dann gilt mit (1)

$\beta \notin \mathsf{FV}(F_\alpha(A(.))$, (b)

mithin

$$\begin{aligned} &\left(F_\beta(B(.))\right)_\alpha(A(.)) \\ &\overset{(a)}{\equiv} \quad F_\alpha(A(.)) \\ &\overset{(b)}{\equiv} \quad \left(F_\alpha(A(.))\right)_\beta(\{u : B(u)_\alpha(A(.))\}) . \end{aligned}$$

(ii) $F \equiv t \in \beta$ für ein t, dann ist

$$\left((t \in \beta)_\beta(B(.))\right)_\alpha(A(.))$$

$$\stackrel{(c)}{\equiv} \quad (B(t))\alpha(A(.))$$
$$\stackrel{(d)}{\equiv} \quad \Big((t \in \beta)\alpha(A(.))\Big)_\beta(\{u : B(u)\alpha(A(.))\})$$

mit (c): Definition der Ersetzung, (d): $\alpha \not\equiv \beta$.

(iii) $F \equiv t \notin \beta$ für ein t, dann ist

$$\Big((t \notin \beta)_\beta(B(.))\Big)_\alpha(A(.))$$
$$\stackrel{(e)}{\equiv} \quad (\neg B(t))\alpha(A(.))$$
$$\stackrel{(f)}{\equiv} \quad \Big((t \notin \beta)\alpha(A(.))\Big)_\beta(\{u : B(u)\alpha(A(.))\})$$

mit (e): Definition der Ersetzung, (f): $\alpha \not\equiv \beta$.

Wenn F keine Primformel ist, dann folgt die Behauptung direkt aus der Induktionsvoraussetzung und der Definition der Ersetzung. □

Bei der Ersetzung freier Mengenvariablen durch Klassenterme in $\mathbf{U}_\mathbf{2}^{\mathbf{i},\mathbf{w}^\star}$-Herleitungen von $\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}$-Formelmengen geht wesentlich die partielle Schnittelimination ein, damit alle Formeln in der Herleitung aus $\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}$ sind. Dies ist wichtig, damit jede in der Herleitung auftretende zweitstufige Existenzformel die Gestalt $\exists\phi\, F(\phi^{|t|})$ für eine Formel $F(\beta)$ und einen Term t hat. Denn dann geht ein $(\exists^2)$-Schluß in der Herleitung in einen (w$\mathbf{\Sigma}_\mathbf{1}^{\mathbf{1},\mathbf{w}^\star}$-CA)-Schluß über.

$$\frac{\Gamma, F(\alpha^{|t|})}{\Gamma, \exists\phi\, F(\phi^{|t|})} \quad \rightsquigarrow \quad \frac{\Gamma\alpha(A(.)), F_{\alpha,\,\beta}(A(.), \{u \le |t| : A(u)\})}{\Gamma\alpha(A(.)), (\exists\phi\, F(\phi^{|t|}))\alpha(A(.))}$$

6.7 Satz

Sei $i > 0$ und $A(a) \in \mathbf{\Delta}_\mathbf{1}^{\mathbf{U}_\mathbf{2}^{\mathbf{1},\mathbf{w}^\star}}$, dann gilt für $\Gamma \subset \mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}$ mit $\mathsf{BV}(A) \cap \mathsf{BV}(\Gamma) = \emptyset$:

$$\mathbf{U}_\mathbf{2}^{\mathbf{i},\mathbf{w}^\star} \vdash \Gamma \implies \mathbf{U}_\mathbf{2}^{\mathbf{i},\mathbf{w}^\star} \vdash \Gamma\alpha(A(.)).$$

Beweis:

Aus dem Eliminationssatz 4.14 folgt $\mathbf{U}_\mathbf{2}^{\mathbf{i},\mathbf{w}^\star} \vdash_1^m \Gamma$ für ein $m < \omega$. Wir zeigen nun die Behauptung durch Induktion nach m.

Ist Γ ein logisches Axiom, dann ergibt sich aus dem Tautologielemma 4.6 (i) $\mathbf{U}_\mathbf{2}^{\mathbf{i},\mathbf{w}^\star} \vdash \Gamma\alpha(A(.))$.

Falls $t \neq s$, $t \notin \alpha$, $s \in \alpha \in \Gamma$ ist, folgt $\mathbf{U}_\mathbf{2}^{\mathbf{i},\mathbf{w}^\star} \vdash \Gamma\alpha(A(.))$ aus dem Gleichheitslemma 4.6 (ii).

Ansonsten enthält die Hauptformel α nicht als freie Variable. Darum hat $\Gamma\alpha(A(.))$ dieselbe axiomatische Hauptformel wie Γ, und es gilt $\mathbf{U}_\mathbf{2}^{\mathbf{i},\mathbf{w}^\star} \vdash \Gamma\alpha(A(.))$.

Bleiben noch folgende Fälle zu untersuchen:

War der letzte Schluß ($\wedge$), ($\vee$), ($\forall\leq$) oder ($\exists\leq$), so folgt die Behauptung direkt aus der Induktionsvoraussetzung mit demselben Schluß unter Berücksichtigung der Bemerkung an Lemma 4.5.

(Schnitt) Als letzter Schluß lag vor

$$\mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m_1}{1} \Gamma, F \text{ und } \mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m_2}{1} \Gamma, \neg F \implies \mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m}{1} \Gamma$$

mit $m_1, m_2 < m$ und $\mathbf{U_2^{i,w^\star}}\text{-}\mathsf{rg}(F) = 0$. Also ist $\Gamma, F \subset \mathbf{\Sigma^{1,w^\star}}$. Wir können mit Lemma 4.5 ohne Einschränkung annehmen, daß $\mathsf{BV}(A) \cap \mathsf{BV}(F) = \emptyset$ ist, dann liefert die Induktionsvoraussetzung

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma\alpha(A(.)), F\alpha(A(.)) \qquad \text{und}$$

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma\alpha(A(.)), (\neg F)\alpha(A(.)) .$$

Nun ist $(\neg F)\alpha(A(.)) \equiv \neg F\alpha(A(.))$, also folgt mit einem (Schnitt)

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma\alpha(A(.)) .$$

($\forall^2$) Der letzte Schluß hatte die Gestalt

$$\mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m'}{1} \Gamma, \forall\phi\, F(\phi), F(\beta) \implies \mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m}{1} \Gamma, \forall\phi\, F(\phi)$$

mit $\beta \notin \mathsf{FV}(\Gamma, \forall\phi\, F(\phi), A) \cup \{\alpha\}$ und $m' < m$. Dann folgt aus der Induktionsvoraussetzung mit $\Gamma, \forall\phi\, F(\phi), F(\beta) \subset \mathbf{\Sigma^{1,w^\star}}$

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma\alpha(A(.)), (\forall\phi\, F(\phi))\alpha(A(.)), F(\beta)\alpha(A(.)) .$$

Mit ($\forall^2$) folgt wegen $\beta \notin \mathsf{FV}(\Gamma\alpha(A(.)), (\forall\phi\, F(\phi))\alpha(A(.)))$

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma\alpha(A(.)), (\forall\phi\, F(\phi))\alpha(A(.)) .$$

($\exists^2$) Dieser Schluß läßt sich als (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) auffassen, da $\Gamma \subset \mathbf{\Sigma^{1,w^\star}}$ ist:

$$\mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m'}{1} \Gamma, \exists\phi\, F(\phi), F(\beta) \implies \mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m}{1} \Gamma, \exists\phi\, F(\phi)$$

mit $m' < m$. Da $\exists\phi\, F(\phi) \in \mathbf{\Sigma^{1,w^\star}}$ ist, gibt es einen Term t und eine Formel G mit

$$F(\beta) \equiv G(\beta^{|t|}) .$$

Also läßt sich der obige Schluß schreiben als

$$\mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m'}{1} \Gamma, \exists\phi\, G(\phi^{|t|}), G(\{u \leq |t| : u \in \beta\})$$
$$\implies \mathbf{U_2^{i,w^\star}} \mid\!\!\frac{m}{1} \Gamma, \exists\phi\, G(\phi^{|t|}) ,$$

was als eine Anwendung von (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) gelesen werden kann.

($\mathrm{w}\mathbf{\Sigma}_{\mathbf{0}}^{\mathbf{1},\mathbf{w}^\star}$-CA) Für ein $B(b) \in \mathbf{\Sigma}_{\mathbf{0}}^{\mathbf{1},\mathbf{w}^\star}$ und $m' < m$ gilt

$$\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \mid\!\!\frac{m'}{1} \Gamma, \exists\phi\, F(\phi^{|t|}), F(\{u \leq |t| : B(u)\}) \quad \Longrightarrow \quad \mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \mid\!\!\frac{m}{1} \Gamma, \exists\phi\, F(\phi^{|t|})\,.$$

Ohne Einschränkung gelte $\mathsf{BV}(B) \cap \mathsf{BV}(A) = \emptyset$ und $b \notin \mathsf{FV}(A)$. Sei β eine neue Variable, dann folgt aus der Induktionsvoraussetzung

$$\begin{aligned}\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \vdash\ & \Gamma\alpha(A(.)), (\exists\phi\, F(\phi^{|t|}))\alpha(A(.)), \\ & (F_\beta(\{u \leq |t| : B(u)\}))\alpha(A(.))\,.\end{aligned} \tag{1}$$

Da nun nach Lemma 6.6

$$\begin{aligned}&\Big(F(\{u \leq |t| : B(u)\})\Big)_\alpha(A(.)) \\ &\quad\equiv \quad \Big(F(\beta)\alpha(A(.))\Big)_\beta\Big(\{u \leq |t| : B(u)\alpha(A(.))\}\Big)\,,\end{aligned}$$

nach Lemma 6.5 (i) $B(b)\alpha(A(.)) \in \mathbf{\Sigma}_{\mathbf{1}}^{\mathbf{U}_{\mathbf{2}}^{\mathbf{1}},\mathbf{w}^\star}$ und nach Lemma 6.2 ($\mathrm{w}\mathbf{\Sigma}_{\mathbf{1}}^{\mathbf{U}_{\mathbf{2}}^{\mathbf{1}},\mathbf{w}^\star}$-CA) in $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ gilt, folgt aus (1)

$$\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \vdash \Gamma\alpha(A(.)), (\exists\phi\, F(\phi^{|t|}))\alpha(A(.)), \exists\phi\, \Big(F(\beta)\alpha(A(.))\Big)_\beta(\phi^{|t|})\,. \tag{2}$$

Mit Lemma 6.6 folgt

$$\begin{aligned}\exists\phi\, \Big(F(\beta)\alpha(A(.))\Big)_\beta(\phi^{|t|}) \quad &\equiv \quad \exists\phi\, \Big(F(\beta^{|t|})\alpha(A(.))\Big)_\beta(\phi) \\ &\equiv \quad (\exists\phi\, F(\phi^{|t|}))\alpha(A(.))\,,\end{aligned}$$

also zeigt (2) die Behauptung.

($\mathbf{\Sigma}_{\mathbf{i}}^{\mathbf{1},\mathbf{w}^\star}$-LIND) Für ein $F(b) \in \mathbf{\Sigma}_{\mathbf{i}}^{\mathbf{1},\mathbf{w}^\star}$ und $m' < m$ mit $b \notin \mathsf{FV}(\Gamma, F(0))$ gilt

$$\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \mid\!\!\frac{m'}{1} \Gamma, \neg F(b), F(\mathrm{S}b) \implies \mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \mid\!\!\frac{m}{1} \Gamma, \neg F(0), F(|t|)\,.$$

Nach der Bemerkung an Lemma 4.5 sei ohne Einschränkung $b \notin \mathsf{FV}(A)$. Dann liefert die Induktionsvoraussetzung

$$\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \vdash \Gamma\alpha(A(.)), \neg F\alpha(A(.))(b), F\alpha(A(.))(\mathrm{S}b)\,.$$

Nun ergibt ($\mathbf{\Sigma}_{\mathbf{i}}^{\mathbf{U}_{\mathbf{2}}^{\mathbf{1}},\mathbf{w}^\star}$-LIND) wegen $b \notin \mathsf{FV}(\Gamma\alpha(A(.)), F\alpha(A(.))(0))$

$$\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \vdash \Gamma\alpha(A(.)), \neg F\alpha(A(.))(0), F\alpha(A(.))(|t|)\,,$$

woraus die Behauptung folgt. □

6.8 Satz

Für $k > 0$ sind die Formelmengen $\mathbf{\Sigma_k^{U_2^1,w^\star}}$, $\mathbf{\Pi_k^{U_2^1,w^\star}}$ und $\mathbf{\Delta_k^{U_2^1,w^\star}}$ abgeschlossen unter Substitution von $\mathbf{\Delta_1^{U_2^1,w^\star}}$ Klassentermen.

Beweis:

Sei $A \in \mathbf{\Delta_1^{U_2^1,w^\star}}$. Für $F \in \mathbf{\Sigma_k^{U_2^1,w^\star}}$ gibt es eine Formel $G \in \mathbf{\Sigma_k^{1,w^\star}}$ mit

$$\mathbf{U_2^{i,w^\star}} \vdash F \leftrightarrow G\,.$$

Da $F \in \mathbf{\Sigma^{1,w^\star}}$ ist, ist auch $F \leftrightarrow G \in \mathbf{\Sigma^{1,w^\star}}$, also zeigt der Einsetzungssatz 6.7

$$\mathbf{U_2^{i,w^\star}} \vdash F_\alpha(A(.)) \leftrightarrow G_\alpha(A(.))\,.$$

Mit $G_\alpha(A(.)) \in \mathbf{\Sigma_k^{U_2^1,w^\star}}$ nach Lemma 6.5 (ii) ist dann auch $F_\alpha(A(.)) \in \mathbf{\Sigma_k^{U_2^1,w^\star}}$.

Dual zeigt man die Behauptung für $\mathbf{\Pi_k^{U_2^1,w^\star}}$.

Da $\mathbf{\Delta_k^{U_2^1,w^\star}} = \mathbf{\Sigma_k^{U_2^1,w^\star}} \cap \mathbf{\Pi_k^{U_2^1,w^\star}}$ ist, folgt aus den ersten beiden Resultaten auch die Behauptung für $F \in \mathbf{\Delta_k^{U_2^1,w^\star}}$. □

Nun beginnen wir mit der Übersetzung von $\mathbf{\Sigma^b}$ in $\mathbf{\Sigma^{1,w^\star}}$. Terme werden in $\mathbf{\Delta_1^{U_2^1,w^\star}}$-Klassenterme und darauf aufbauend $\mathbf{\Sigma_k^b}$-Formeln in $\mathbf{\Sigma_k^{U_2^1,w^\star}}$-Formeln übersetzt.

7 Interpretation von $\mathbf{\Sigma^b}$ in $\mathbf{\Sigma^{1,w^\star}}$

Zwecks Charakterisierung von $\mathbf{\Delta_i^p}$ in $\mathbf{U_2^{i,w^\star}}$ durch den erststufigen Hauptsatz der Beschränkten Arithmetik 3.7 wird eine natürliche Interpretation ^{w} der Terme und Formeln von $\mathbf{S_2^i}$ in $\mathbf{U_2^{i,w^\star}}$ gesucht, so daß für $\Gamma \subset \mathbf{\Sigma^b}$ und $i > 0$

$$\mathbf{S_2^i} \vdash \Gamma \implies \mathbf{U_2^{i,w^\star}} \vdash \Gamma^w$$

gilt. Als Vorlage dient uns dabei [Takeuti 1988] Seite 88 ff. und [Takeuti 1991].

Da die Induktionen immer auf gewisse Formelmengen eingeschränkt sind, muß die Interpretation diese respektieren. Das heißt, wir müssen $\mathbf{\Sigma_i^b}$-Formeln in $\mathbf{\Sigma_i^{U_2^{1,w^\star}}}$-Formeln überführen: ein beschränkter, nicht scharf beschränkter Quantor $Qx{\leq}t$ muß durch einen zweitstufigen Quantor $Q\phi^{|t|}$ über scharf beschränkte Anfangsstücke von Mengen, im weiteren *scharfe Anfangsstücke* genannt, ersetzt werden. Aus technischen Gründen betrachten wir folgende Zuordnung von Variablentupeln auf scharfe Anfangsstücke

$$(a, \alpha) \longmapsto \alpha^{<|a|} := \{u < |a| : u \in \alpha\}\,,$$

denn dann gilt im Standardmodell der Arithmetik $(\mathbb{N}, \mathcal{P}(\mathbb{N}), \ldots)$ für beliebiges α

$$\alpha^{<|0|} = \emptyset\,.$$

Diese Interpretation hat zur Folge, daß wir in $\mathbf{U_2^{i,w^\star}}$ Quasiterme und Quasiformeln entwickeln müssen, die statt auf Individuenvariablen auf scharfen Anfangsstücken leben. Wir geben $\mathbf{\Sigma_0^{1,w^\star}}$-Formeln an, die die Prädikatszeichen $=$, $\neq$, $\leq$ und $\not\leq$ repräsentieren. Für die Funktionszeichen f aus 0, S, $\lfloor\frac{1}{2}.\rfloor$, $|.|$, $+$, $\cdot$ und $\#$ entwickeln wir $\mathbf{\Delta_1^{U_2^{1,w^\star}}}$-Formeln F_f und Beschränkungsterme T_f, so daß mit $U_f :\equiv \{u : F_f(u)\}$ das scharfe Anfangsstück $U_f^{<|T_f|}$ die Funktion f repräsentiert. Bezogen auf das Standardmodell der Arithmetik $(\mathbb{N}, \mathcal{P}(\mathbb{N}), \ldots)$ geben wir Heuristiken an, die auch gleichzeitig als Begründung für die Korrektheit der gewählten Interpretation, Satz 7.4, dienen: sei $A \in \mathbf{\Sigma^b}$ mit $\mathsf{FV}(A) \subset \{a_1, \ldots, a_k\}$, dann gilt mit $U(a) :\equiv \{u : \mathrm{Bit}(u, a) = 1\}$

$$(\mathbb{N}, \mathcal{P}(\mathbb{N}), \ldots) \models A \leftrightarrow A^w_{\alpha_1, \ldots, \alpha_k}(U(a_1), \ldots, U(a_k))\,.$$

Fassen wir $\alpha^{<|a|}$ als eine Binärdarstellung der Zahl

$$\sum_{i<|a|} (i)_\alpha \cdot 2^i =_{\mathrm{bin}} (|a|-1)_\alpha \ldots (0)_\alpha \quad \text{mit} \quad (i)_\alpha = \begin{cases} 0 & : \quad i \notin \alpha \\ 1 & : \quad i \in \alpha \end{cases}$$

auf, dann läßt sich die Korrektheit einer Funktionsinterpretation auch so formulieren:

$$f(\ldots, \alpha_i^{<|a_i|}, \ldots) = \{u : F_f(\vec{a}, \vec{\alpha}, u)\}^{<|T_f(\vec{a})|}\,.$$

Wir bezeichnen mit $\mathrm{v}\big(\alpha^{<|a|}\big)$, dem *Volumen des scharfen Anfangsstücks*, das kleinste Element, das größer ist als alle Elemente aus $\alpha^{<|a|}$. Mit $v := \mathrm{v}\big(\alpha^{<|a|}\big)$ erhalten wir

$$v \le |a| \quad \text{und} \quad \alpha^{<|a|} = \alpha^{<v}\,.$$

Diese Definition wird uns helfen, die richtige Wahl der Schranken für die Anfangsstücke der Funktionsinterpretationen zu treffen.

Wir fangen mit der Interpretation der Primformeln an. Mit der Betrachtung als Binärdarstellung einer Zahl ist $\alpha^{<|a|} = \beta^{<|b|}$ äquivalent dazu, daß $\alpha^{<|a|}$ und $\beta^{<|b|}$ Bit-Weise übereinstimmen, also äquivalent zur extensionalen Mengengleichheit von $\alpha^{<|a|}$ und $\beta^{<|b|}$. Für „$<$“ beobachten wir

$$\begin{aligned}
&\alpha^{<|a|} < \beta^{<|b|}\\
&\quad\iff\quad (|a|-1)\alpha \ldots (0)\alpha < (|b|-1)_\beta \ldots (0)_\beta\\
&\quad\iff\quad (|a|-1)_{\alpha^{<|a|}} \le (|b|-1)_{\beta^{<|b|}}, \ldots, (x+1)_{\alpha^{<|a|}} \le (x+1)_{\beta^{<|b|}}\,,\\
&\qquad\quad 0 = (x)_{\alpha^{<|a|}} < (x)_{\beta^{<|b|}} = 1 \quad \text{für ein} \quad x < |b|\,.
\end{aligned}$$

Dies führt zu folgenden Definitionen:

7.1 Definition

$$\begin{aligned}
\alpha^{<|a|} = \beta^{<|b|} \;&:\equiv\; \forall x{<}|a|\,(x \in \alpha^{<|a|} \to x \in \beta^{<|b|}) \wedge\\
&\qquad \forall x{<}|b|\,(x \in \beta^{<|b|} \to x \in \alpha^{<|a|})\\
\alpha^{<|a|} < \beta^{<|b|} \;&:\equiv\; \exists x{<}|b|\,(x \in \beta^{<|b|} \wedge x \notin \alpha^{<|a|} \wedge\\
&\qquad\qquad \forall y{<}|a|\,(x < y \wedge y \in \alpha^{<|a|} \to y \in \beta^{<|b|}))\\
\alpha^{<|a|} \le \beta^{<|b|} \;&:\equiv\; \alpha^{<|a|} = \beta^{<|b|} \vee \alpha^{<|a|} < \beta^{<|b|}
\end{aligned}$$

Nun entwickeln wir in $\mathbf{U_2^{1,w^\star}}$ auf den scharfen Anfangsstücken die Funktionen aus $\mathbf{S_2^i}$, wobei wir die oben beschriebene Korrektheitsbedingung respektieren.

0: Hier setzen wir

$$\begin{aligned}
T_0 \;&:\equiv\; 0\\
F_0(c) \;&:\equiv\; c \neq c\,.
\end{aligned}$$

S: Sei $w \le |a|$ und z als Wort über dem Alphabet $\{0,1\}$ so bestimmt, daß $(w)_{\alpha^{<|a|}} = 0$ und

$$\alpha^{<|a|} = (|a|-1)\alpha \ldots (0)\alpha = (|a|-1)\alpha \ldots (w)_{\alpha^{<|a|}} 1 \ldots 1 = z(w)_{\alpha^{<|a|}} 1 \ldots 1$$

gilt, dann ist

$$\mathrm{S}(\alpha^{<|a|}) = z10\ldots0$$

und somit

$$\mathrm{v}\Big(\mathrm{S}(\alpha^{<|a|})\Big) \leq \mathrm{v}\Big(\alpha^{<|a|}\Big) + 1 \leq |a| + 1\,.$$

Also definieren wir

$$\begin{array}{rcl} T_{\mathrm{S}}(a) & :\equiv & 2\cdot a + 1 \\ F_{\mathrm{S}}(a,\alpha,c) & :\equiv & \exists w{\leq}|a|\,\Big(w \notin \alpha^{<|a|} \wedge \forall v{\leq}|a|\,(v < w \rightarrow v \in \alpha^{<|a|}) \wedge \\ & & \qquad (c = w \vee (c > w \wedge c \in \alpha^{<|a|}))\Big) \end{array}$$

$\lfloor\frac{1}{2}.\rfloor$: Es ist

$$\lfloor\tfrac{1}{2}\alpha^{<|a|}\rfloor = (|a|-1)_\alpha \ldots (1)_\alpha\,,$$

also

$$\mathrm{v}\Big(\lfloor\tfrac{1}{2}\alpha^{<|a|}\rfloor\Big) \leq \mathrm{v}\Big(\alpha^{<|a|}\Big) \dot{-} 1 \leq |a| \dot{-} 1\,.$$

Dies führt zu

$$\begin{array}{rcl} T_{\lfloor\frac{1}{2}.\rfloor}(a) & :\equiv & \lfloor\frac{1}{2}a\rfloor \\ F_{\lfloor\frac{1}{2}.\rfloor}(a,\alpha,c) & :\equiv & \mathrm{S}c \in \alpha^{<|a|} \end{array}$$

$|.|$: Wir wählen $w \leq |a|$ mit

$$\alpha^{<|a|} = (w-1)_\alpha \ldots (0)_\alpha \quad \text{und} \quad [(w-1)_\alpha = 1 \text{ oder } w = 0]\,.$$

Dann ist

$$|\alpha^{<|a|}| = w$$

also gilt

$$\mathrm{v}\Big(|\alpha^{<|a|}|\Big) = |w| \leq \Big||a|\Big|\,.$$

Wir definieren

$$\begin{array}{rcl} T_{|.|}(a) & :\equiv & |a| \\ F_{|.|}(a,\alpha,c) & :\equiv & \exists w{\leq}|a|\,(\mathrm{Bit}(c,w) = 1 \wedge (w = 0 \vee w \dot{-} 1 \in \alpha^{<|a|}) \wedge \\ & & \qquad \forall v{<}|a|\,(w \leq v \rightarrow v \notin \alpha^{<|a|})) \end{array}$$

#: Wieder wählen wir $v_1 \leq |a|$ und $v_2 \leq |b|$ mit

$$\alpha^{<|a|} = (v_1 - 1)\alpha \ldots (0)\alpha \quad \text{und} \quad [(v_1 - 1)\alpha = 1 \text{ oder } v_1 = 0]$$

und

$$\beta^{<|b|} = (v_2 - 1)_\beta \ldots (0)_\beta \quad \text{und} \quad [(v_2 - 1)_\beta = 1 \text{ oder } v_2 = 0] .$$

Dann ist

$$\alpha^{<|a|} \# \beta^{<|b|} = \{v_1 \cdot v_2\}$$

und somit

$$\mathrm{v}\Big(\alpha^{<|a|} \# \beta^{<|b|}\Big) = v_1 \cdot v_2 + 1 \leq |a| \cdot |b| + 1 = |a \# b| .$$

Also definieren wir

$$\begin{aligned} T_\#(a,b) &\equiv a \# b \\ F_\#(a,b,\alpha,\beta,c) &\equiv \exists v_1 \leq |a| \, \exists v_2 \leq |b| \, (c = v_1 \cdot v_2 \wedge \\ &\qquad (v_1 = 0 \vee v_1 \dot{-} 1 \in \alpha^{<|a|}) \wedge \forall w < |a| \, (v_1 \leq w \to w \notin \alpha^{<|a|}) \wedge \\ &\qquad (v_2 = 0 \vee v_2 \dot{-} 1 \in \beta^{<|b|}) \wedge \forall w < |b| \, (v_2 \leq w \to w \notin \beta^{<|b|})) \end{aligned}$$

+: Es gilt

$$u \in \alpha^{<|a|} + \beta^{<|b|}$$

genau dann, wenn

(i) $(u)_{\alpha^{<|a|}} \neq (u)_{\beta^{<|b|}}$ und kein Übertrag trat auf, d. h. $u = 0$ oder

$$\exists v < u \quad [v = 0 \text{ oder } (v \dot{-} 1)_{\alpha^{<|a|}} = (v \dot{-} 1)_{\beta^{<|b|}} = 0] \quad \text{und}$$

$$\forall w < u \, [v \leq w \to (w)_{\alpha^{<|a|}} = 0 \text{ oder } (w)_{\beta^{<|b|}} = 0] .$$

In beiden Fällen ist

$$u < \mathrm{Max}(|a|, |b|) \leq |2 \cdot (a + b)| .$$

(ii) $(u)_{\alpha^{<|a|}} = (u)_{\beta^{<|b|}}$ und ein Übertrag trat auf, also

$$\exists v < u \quad (v)_{\alpha^{<|a|}} = (v)_{\beta^{<|b|}} = 1 \quad \text{und}$$

$$\forall w < u \, [v \leq w \to (w)_{\alpha^{<|a|}} = 1 \text{ oder } (w)_{\beta^{<|b|}} = 1] .$$

Hier muß $w < \mathrm{Max}(|a|, |b|) \leq |a + b|$ sein, also gilt

$$u \leq |a + b| < |2 \cdot (a + b)| ,$$

da $a + b > 0$ ist.

Damit ergeben sich folgende Definitionen:

$$
\begin{aligned}
T_+(a,b) \;&\mathrel{:\equiv}\; 2\cdot(a+b)\\
F_+(a,b,\alpha,\beta,c) \;&\mathrel{:\equiv}\\
&\Big[(c\in\alpha^{<|a|}\leftrightarrow c\notin\beta^{<|b|})\wedge(c=0\vee(c>0\wedge\\
&\quad\exists v{\le}|T_+(a,b)|\,(v<c\wedge(v=0\vee(v\dot{-}1\notin\alpha^{<|a|}\wedge v\dot{-}1\notin\beta^{<|b|}))\wedge\\
&\quad\forall w{\le}|T_+(a,b)|\,(v\le w\wedge w<c\to w\notin\alpha^{<|a|}\vee w\notin\beta^{<|b|})))\Big]\vee\\
&\Big[c>0\wedge(c\in\alpha^{<|a|}\leftrightarrow c\in\beta^{<|b|})\wedge\\
&\quad\exists v{<}|a|\,(v\in\alpha^{<|a|}\wedge v\in\beta^{<|b|}\wedge v<c\wedge\\
&\quad\forall w{\le}|T_+(a,b)|\,(v<w\wedge w<c\to w\in\alpha^{<|a|}\vee w\in\beta^{<|b|}))\Big]
\end{aligned}
$$

Wir wollen noch begründen, daß für $u>0$ nur die Fälle „Übertrag“ bzw. „kein Übertrag“ nach u bei $\alpha^{<|a|}+\beta^{<|b|}$ auftreten können. Dazu gelte nicht, daß

kein Übertrag nach u bei $\alpha^{<|a|}+\beta^{<|b|}$

auftritt, d. h.

$$
\begin{aligned}
&\forall x{<}u\,[(x=0\vee(x\dot{-}1)_{\alpha^{<|a|}}=(x\dot{-}1)_{\beta^{<|b|}}=0)\\
&\quad\to\;\exists v{<}u\,(x\le v\wedge(v)_{\alpha^{<|a|}}=(v)_{\beta^{<|b|}}=1)]\,.
\end{aligned}
$$

Insbesondere zeigt $x=0$

$$\exists v{<}u\,((v)_{\alpha^{<|a|}}=(v)_{\beta^{<|b|}}=1)\,.$$

Mit ($\mathbf{\Sigma_0^{1,w^\star}}$-LMIN) gibt es dann ein maximales v mit $v<u$ und $(v)_{\alpha^{<|a|}}=(v)_{\beta^{<|b|}}=1$, dann gilt

$$\forall w{<}u\,(v\le w\to(w)_{\alpha^{<|a|}}=1\vee(w)_{\beta^{<|b|}}=1)\,.$$

Mithin tritt

ein Übertrag nach u bei $\alpha^{<|a|}+\beta^{<|b|}$

auf.

Bisher sind die beschreibenden Formeln der Abstrakte aus $\mathbf{\Sigma_0^{1,w^\star}}$, also insbesondere aus $\mathbf{\Delta_1^{U_2^1,w^\star}}$.

In [Takeuti 1991] wird die Multiplikation durch „shifting and carry-save adding“ berechnet. Diese Methode ist in [Savage 1976] als geradliniger Algorithmus, d. h. als Algorithmus

ohne Schleifen, vorgestellt, der bei Implementierung logische Elemente in der Größenordnung n^2 benötigt, deren Anordnungstiefe im optimalen Fall größenordnungsmäßig $\log n$ beträgt. Dabei werden zwei Zahlen der Länge n in Binärdarstellung multipliziert.
Dieses Verfahren ist zwar bezüglich dieser Komplexitäten einfach, aber für die Interpretation der Multiplikation zu unhandlich. Die daraus abgeleitete Definition ist nicht symmetrisch in den Argumenten. Zudem erweist sich die Berechnung der „carry-save“ Addition als ziemlich kompliziert. Deshalb wählen wir hier einen anderen Zugang.
Sei $|t|$ die Länge der Binärdarstellung von $\alpha^{<|a|} \cdot \beta^{<|b|}$. Wir werden t später genau angeben. Wir beobachten

$$\begin{aligned}
&\alpha^{<|a|} \cdot \beta^{<|b|} \\
&= (\sum_{i<|a|} (i)\alpha \cdot 2^i) \cdot (\sum_{j<|b|} (j)_\beta \cdot 2^j) \\
&= \sum_{i,j} (i)_{\alpha^{<|a|}} \cdot (j)_{\beta^{<|b|}} \cdot 2^{i+j} \\
&= \sum_{i} (\sum_{j=0}^{i} (j)_{\alpha^{<|a|}} \cdot (i \dot{-} j)_{\beta^{<|b|}}) \cdot 2^i \\
&= \sum_{x<|t|} d_x \cdot 2^x
\end{aligned}$$

mit

$$d_x := \#z{\leq}|a|(z \leq x \wedge z \in \alpha^{<|a|} \wedge x \dot{-} z \in \beta^{<|b|}) \,. \tag{1}$$

Dies ist i. allg. noch keine Binärdarstellung, da $d_x > 1$ möglich ist. Um nun zu einer Binärdarstellung $b_{|t|}, \ldots, b_0$ von $\alpha^{<|a|} \cdot \beta^{<|b|}$ zu gelangen, nutzen wir sukzessive

$$d \cdot 2^x = \lfloor \tfrac{1}{2} d \rfloor \cdot 2^{x+1} + \mathrm{mod}_2(d) \cdot 2^x$$

aus, wobei sich $\mathrm{mod}_2(d)$ als Abkürzung für $\mathrm{Bit}(0, d)$ auffassen läßt. Wir gehen dabei wie in Tabelle 2 dargestellt vor.

Stufe			Berechnungsfeld					
0	$\ldots$		d_x	$\ldots$			d_1	d_0
1	$\ldots$		d_x	$\ldots$		d_2	d'_1	b_0
2	$\ldots$		d_x	$\ldots$		d'_2	b_1	b_0
			$\vdots$					
$x-1$	$\ldots$		d_x	d'_{x-1}	b_{x-2}	$\ldots$		b_0
x	$\ldots$	d_{x+1}	d'_x	b_{x-1}	b_{x-2}	$\ldots$		b_0
			$\vdots$					
$\lvert t\rvert$	$\ldots$		b_x	$\ldots$			b_1	b_0

Tabelle 2: Berechnung der Binärdarstellung

Wir bilden also

$$\begin{aligned} d'_0 &:= d_0 \\ d'_{x+1} &:= \lfloor \tfrac{1}{2} d'_x \rfloor + d_{x+1} \\ b_x &:= \mathrm{mod}_2(d'_x) \end{aligned}$$

Um nun die Länge der Binärdarstellung $|t|$ zu bestimmen, stellen wir fest:

(i) $d_x \leq |a|$

(ii) $d_{(|b| \dot{-} 1)+k} \leq |a| \dot{-} k$

(iii) $d'_x \leq 2|a|$

(iv) $d'_{(|b| \dot{-} 1)+k} \leq 2 \cdot (|a| + 1 \dot{-} k) \dot{-} 1$.

Wir begründen dies:

(i) Es gilt $d_x \leq \#z{\leq}|a|(z \in \alpha^{<|a|}) \leq |a|$.

(ii) Für $x := (|b| \dot{-} 1) + k$ gilt

$$\begin{aligned} d_x &\leq \#z{\leq}|a|(z \in \alpha^{<|a|} \wedge x \dot{-} z \in \beta^{<|b|}) \\ &\leq \#z{\leq}|a|((|b| \dot{-} 1) + k \dot{-} z < |b| \wedge z < |a|) \\ &\leq \#\{k, \ldots, |a| - 1\} \\ &= |a| \dot{-} k \,. \end{aligned}$$

(iii) Es gilt $d'_0 = d_0 \overset{(i)}{\leq} |a| \leq 2|a|$ und durch Induktion folgt $d'_{x+1} = \lfloor \tfrac{1}{2} d'_x \rfloor + d_{x+1} \leq |a| + |a| = 2|a|$.

(iv) Sei $x := (|b| \dot{-} 1) + k$. Für $k = 0$ ist $d'_x \leq 2|a| < 2 \cdot (|a| + 1 \dot{-} 0) \dot{-} 1$. Ist $k > 0$, so gilt mit Induktion

$$\begin{aligned} d'_{x+1} &= \lfloor \tfrac{1}{2} d'_x \rfloor + d_{x+1} \\ &\leq \lfloor \tfrac{1}{2} (2 \cdot (|a| + 1 \dot{-} k) \dot{-} 1) \rfloor + (|a| \dot{-} (k+1)) \\ &\leq \lfloor \tfrac{1}{2} (2 \cdot (|a| \dot{-} k) + 1) \rfloor + (|a| + 1 \dot{-} (k+1)) \dot{-} 1 \\ &= (|a| \dot{-} k) + (|a| + 1 \dot{-} (k+1)) \dot{-} 1 \\ &= 2 \cdot (|a| + 1 \dot{-} (k+1)) \dot{-} 1 \,. \end{aligned}$$

Also gilt $d'_{|a|+|b|+k} = 0$ für $k \geq 0$, denn ist $|b| = 0$, dann gilt $d_x = 0$ für alle x , also auch $d'_x = 0$ für alle x . Für $|b| > 0$ erhalten wir

$$d'_{|a|+|b|+k} = d'_{(|b| \dot{-} 1)+(|a|+1+k)} \overset{(iv)}{\leq} 2 \cdot (|a| + 1 \dot{-} (|a| + 1 + k)) \dot{-} 1 = 0 \,.$$

Das motiviert

$$T. \;:\equiv\; 2 \cdot (\mathrm{S}a) \cdot (\mathrm{S}b)\,,$$

denn dann ist $|T.| = \mathrm{S}|(\mathrm{S}a) \cdot (\mathrm{S}b)| \geq |a| + |\mathrm{S}b| \geq |a| + |b|$. Abkürzend sei weiterhin $t :\equiv T.$.
$G(i, a, b, \alpha, \beta, \gamma)$ sei die $\mathbf{\Sigma_1^{1,w^\star}}$-Formel, die obiges Vorgehen beschreibt.

$$\begin{aligned}
&G(i,a,b,\alpha,\beta,\gamma) \;:\equiv\\
&\quad [i = 0 \wedge \forall x{\leq}|t|\,\forall y{\leq}|t|\,(\langle 0,x,y\rangle \in \gamma \leftrightarrow\\
&\qquad \#z{\leq}|a|(z \leq x \wedge z \in \alpha^{<|a|} \wedge x \dot{-} z \in \beta^{<|b|}) = y)] \vee\\
&\quad [i > 0 \wedge \forall x{\leq}|t|\,\forall y{\leq}|t|\,(\langle i,x,y\rangle \in \gamma \leftrightarrow\\
&\qquad i \leq |t| \wedge \exists z_1{\leq}|a|\,\exists z_2{\leq}|a|\,(\langle 0,i,z_1\rangle \in \gamma \wedge \langle i \dot{-} 1, i \dot{-} 1, z_2\rangle \in \gamma \wedge\\
&\qquad (x = i \dot{-} 1 \to y = \mathrm{mod}_2(z_2)) \wedge (x = i \to y = z_1 + \lfloor \tfrac{1}{2} z_2 \rfloor) \wedge\\
&\qquad (x < i \dot{-} 1 \to \langle i \dot{-} 1, x, y\rangle \in \gamma) \wedge (x > i \to \langle 0,x,y\rangle \in \gamma)))]
\end{aligned}$$

Für $\tilde{t} :\equiv \mathrm{SqBd}_3(t)$ gilt dann

– $\mathbf{U_2^{1,w^\star}} \vdash \exists\chi\,\forall i{\leq}|t|\,G(i, \chi^{|\tilde{t}|})$

– $\mathbf{U_2^{1,w^\star}} \vdash \neg\forall i{\leq}|t|\,G(i, \gamma_1^{|\tilde{t}|}), \neg\forall i{\leq}|t|\,G(i, \gamma_2^{|\tilde{t}|}),$
$\forall i{\leq}|t|\,\forall x{\leq}|t|\,\forall y{\leq}|t|\,(\langle i,x,y\rangle \in \gamma_1^{|\tilde{t}|} \leftrightarrow \langle i,x,y\rangle \in \gamma_2^{|\tilde{t}|})\,.$

Zur Begründung der Existenzaussage sei

$$H(d) \;:\equiv\; \exists\chi\,\forall i{\leq}|t|\,(i \leq d \to G(i, \chi^{|\tilde{t}|}))\,,$$

dann zeigen wir $H(|t|)$ durch ($\mathbf{\Sigma_1^{1,w^\star}}$-LIND) nach d.
Für $d = 0$ existiert mit (w$\mathbf{\Sigma_1^{1,w^\star}}$-CA) eine Menge χ mit

$$\begin{aligned}
&\forall x{\leq}|t|\,\forall y{\leq}|t|\,\Big(\langle 0,x,y\rangle \in \chi^{|\tilde{t}|} \leftrightarrow\\
&\qquad\qquad y = \#z{\leq}|a|(z \leq x \wedge z \in \alpha^{<|a|} \wedge x \dot{-} z \in \beta^{<|b|})\Big)\,,
\end{aligned}$$

da durch längenbeschränktes Zählen definierte Funktionen in $\mathbf{U_2^{1,w^\star}}$ $\mathbf{\Sigma_1^{1,w^\star}}$-definierbar sind (Lemma 5.7). Dann gilt $G(0, \chi^{|\tilde{t}|})$.
Um $\forall z\,(H(z) \to H(\mathrm{S}z))$ zu zeigen, sei z beliebig mit $H(z)$, also gibt es χ_0 mit

$$\forall i{\leq}|t|\,(i \leq z \to G(i, \chi_0^{|\tilde{t}|}))\,. \tag{2}$$

Ist $z \geq |t|$, so gilt auch

$$\forall i{\leq}|t|\,(i \leq \mathrm{S}z \to G(i, \chi_0^{|\tilde{t}|}))\,.$$

Sei also $z < |t|$, dann definieren wir mit ($\mathrm{w}\mathbf{\Sigma}_{\mathbf{0}}^{\mathbf{1},\mathbf{w}^\star}$-CA) eine Menge χ_1 durch

$$\begin{aligned}\forall i{\leq}\mathrm{S}z\,\forall x{\leq}|t|\,\forall y{\leq}|t|\,\Big(\langle i,x,y\rangle \in \chi_1^{|\tilde{t}|} \leftrightarrow [\,& i \leq z \wedge \langle i,x,y\rangle \in \chi_0^{|\tilde{t}|}] \vee \\ & [i = \mathrm{S}z \wedge i \leq |t| \wedge \exists z_1{\leq}|a|\,\exists z_2{\leq}|a|\,(\langle 0,i,z_1\rangle \in \chi_0^{|\tilde{t}|} \wedge \langle i \dot{-} 1, i \dot{-} 1, z_2\rangle \in \chi_0^{|\tilde{t}|} \wedge \\ & (x = i \dot{-} 1 \to y = \mathrm{mod}_2(z_2)) \wedge (x = i \to y = z_1 + \lfloor \tfrac{1}{2} z_2 \rfloor) \wedge \\ & (x < i \dot{-} 1 \to \langle i \dot{-} 1, x, y\rangle \in \chi_0^{|\tilde{t}|}) \wedge (x > i \to \langle 0,x,y\rangle \in \chi_0^{|\tilde{t}|}))]\Big)\,.\end{aligned}$$

Damit gilt

$$\forall i{\leq}|t|\,(i \leq \mathrm{S}z \to G(i, \chi_1^{|\tilde{t}|}))\,,$$

also erhalten wir $H(\mathrm{S}z)$ und somit den Induktionsschritt.

Für die Eindeutigkeit gelte

$$\forall i{\leq}|t|\,G(i,\gamma_1^{|\tilde{t}|}) \quad \text{und} \quad \forall i{\leq}|t|\,G(i,\gamma_2^{|\tilde{t}|})\,.$$

Dann zeigen wir für

$$H(d) \;:\equiv\; \forall i{\leq}|t|\,(i \leq d \to \forall x{\leq}|t|\,\forall y{\leq}|t|\,(\langle i,x,y\rangle \in \gamma_1^{|\tilde{t}|} \leftrightarrow \langle i,x,y\rangle \in \gamma_2^{|\tilde{t}|}))$$

durch ($\mathbf{\Sigma}_{\mathbf{1}}^{\mathbf{1},\mathbf{w}^\star}$-LIND) nach d $H(|t|)$.
Der Induktionsanfang folgt aus der Eindeutigkeit der Funktion $\#z{\leq}|a|(\ldots)$, der Induktionsschritt aus der Induktionsvoraussetzung und der Eindeutigkeit von $\mathrm{mod}_2(.)$ und $\lfloor \frac{1}{2}.\rfloor$.

Damit definieren wir nun

$$F.(a,b,\alpha,\beta,c) \;:\equiv\; \exists\chi\,(\forall i{\leq}|t|\,G(i,\chi^{|\tilde{t}|}) \wedge c \leq |t| \wedge \langle |t|,c,1\rangle \in \chi^{|\tilde{t}|})\,.$$

Dann gilt

$$\mathbf{U}_{\mathbf{2}}^{\mathbf{1},\mathbf{w}^\star} \;\vdash F.(a,b,\alpha,\beta,c) \leftrightarrow \forall\chi\,(\forall i{\leq}|t|\,G(i,\chi^{|\tilde{t}|}) \to c \leq |t| \wedge \langle |t|,c,1\rangle \in \chi^{|\tilde{t}|})\,,$$

also ist $F. \in \mathbf{\Delta}_{\mathbf{1}}^{\mathbf{U}_{\mathbf{2}}^{\mathbf{1},\mathbf{w}^\star}}$.

Mit Hilfe der Funktionsinterpretationen sind wir nun in der Lage, Terme T_t und Formeln F_t anzugeben, so daß $\{u : F_t(u)\}^{<|T_t|}$ den Term t repräsentiert.

7.2 Definition der Terminterpretationen

Für Terme t aus $\mathbf{L}^{\emptyset}_{\mathbf{BA}}$ definieren wir Terme T_t und $\mathbf{\Delta}^{\mathbf{U}^{\mathbf{1}}_{\mathbf{2}},\mathbf{w}^\star}_{\mathbf{1}}$-Formeln F_t durch Rekursion nach dem Aufbau von t:

(a) $t \equiv 0$ ist schon definiert.

(b) $t \equiv a_i$, dann sei $T_{a_i} :\equiv a_i$ und $F_{a_i} :\equiv b \in \alpha_i$.

(c) $t \equiv \mathrm{f}s$ für $\mathrm{f} \in \{\mathrm{S}, \lfloor \frac{1}{2} \rfloor, ||\}$, dann sei $T_t :\equiv T_{\mathrm{f}}(T_s)$ und $F_t :\equiv F_{\mathrm{f}}(T_s, F_s(.))$.

(d) $t \equiv \mathrm{f}s_1s_2$ für $\mathrm{f} \in \{+, \#, \cdot\}$, dann sei $T_t :\equiv T_{\mathrm{f}}(T_{s_1}, T_{s_2})$ und $F_t :\equiv F_{\mathrm{f}}(T_{s_1}, T_{s_2}, F_{s_1}(.), F_{s_2}(.))$.

Da nach Satz 6.7 die $\mathbf{\Delta}^{\mathbf{U}^{\mathbf{1}}_{\mathbf{2}},\mathbf{w}^\star}_{\mathbf{1}}$-Formeln abgeschlossen unter Substitutuion von $\mathbf{\Delta}^{\mathbf{U}^{\mathbf{1}}_{\mathbf{2}},\mathbf{w}^\star}_{\mathbf{1}}$-Klassentermen sind, ist F_t immer eine $\mathbf{\Delta}^{\mathbf{U}^{\mathbf{1}}_{\mathbf{2}},\mathbf{w}^\star}_{\mathbf{1}}$-Formel.

Wir schreiben U_t für den Klassentem $\{u : F_t(u)\}$ und $U(a)$ für $\{u : \mathrm{Bit}(u, a) = 1\}$. Unter Berücksichtigung der Identifikation der scharfen Anfangsstücke mit Zahlen ergibt sich für $U(a)^{<|a|}$ die Zahl

$$\sum_{i<|a|} (i)_{U(a)} \cdot 2^i = \sum_{i<|a|} \mathrm{Bit}(i, a) \cdot 2^i = a\,.$$

Also liefern die Heuristiken unter Beachtung von

$$f(\ldots, \alpha_i^{<|a_i|}, \ldots) = \{u : F_f(\vec{a}, \vec{\alpha}, u)\}^{<|T_f(\vec{a})|}$$

den Zusammenhang

$$U(t) = U(t)^{<|t|} = U_t^{<|T_t|}\alpha_1, \ldots, \alpha_{\mathrm{k}}(U(a_1), \ldots, U(a_k))$$

für Terme t mit $\mathsf{FV}(t) \subset \{a_1, \ldots, a_{\mathrm{k}}\}$ durch Induktion nach dem Aufbau von t.
Nun definieren wir die Interpretation einer Formeln aus $\mathbf{\Sigma^b}$.

7.3 Definition der Interpretation $w : \mathbf{\Sigma^b} \longrightarrow \mathbf{\Sigma^{1,w^\star}}$

durch Rekursion nach der Länge der Formel $A \in \mathbf{\Sigma^b}$:

(a) $A \equiv (\neg)t_1 = t_2$ oder $A \equiv (\neg)t_1 \leq t_2$, dann sei

$$A^w :\equiv (\neg)U_{t_1}^{<|T_{t_1}|} = U_{t_2}^{<|T_{t_2}|}$$

beziehungsweise

$$A^w :\equiv (\neg)U_{t_1}^{<|T_{t_1}|} \leq U_{t_2}^{<|T_{t_2}|}\,.$$

(b) $A \equiv B \circ C$ mit $\circ \in \{\wedge, \vee\}$, dann sei

$$A^w :\equiv B^w \circ C^w .$$

(c) $A \equiv \forall x{\leq}|t|\, B(x)$ oder $A \equiv \exists x{\leq}|t|\, B(x)$ und a eine neue Variable, so sei

$$A^w :\equiv \forall x{\leq}|2\#T_t|\, \Big(\Big(a \leq |t| \to B(a)\Big)^w_{a,\,\alpha}\Big(T_{|t|}, U(x)\Big)\Big)$$

beziehungsweise

$$A^w :\equiv \exists x{\leq}|2\#T_t|\, \Big(\Big(a \leq |t| \wedge B(a)\Big)^w_{a,\,\alpha}\Big(T_{|t|}, U(x)\Big)\Big) .$$

(d) $A \equiv \forall x{\leq}t\, B(x)$ oder $A \equiv \exists x{\leq}t\, B(x)$, t habe nicht die Gestalt $|s|$ für einen Term s und a sei eine neue Variable. Wir definieren

$$A^w :\equiv \forall \phi\, \Big(\Big(a \leq t \to B(a)\Big)^w_{a,\,\alpha}\Big(T_t, \phi^{|T_t|}\Big)\Big)$$

beziehungsweise

$$A^w :\equiv \exists \phi\, \Big(\Big(a \leq t \wedge B(a)\Big)^w_{a,\,\alpha}\Big(T_t, \phi^{|T_t|}\Big)\Big) .$$

Die Punkte (c) und (d) sind wohldefiniert, da genau genommen nur die Voraussetzung für $B(a)$ benötigt wird:

$$(a \leq |t| \to B(a))^w \equiv (a \not\leq |t|)^w \vee (B(a))^w .$$

Wir begründen abschließend, daß sich die Interpretation ^{w} im Standardmodell der Arithmetik korrekt verhält. Es werden somit durch $\mathbf{\Sigma^b_i}$-Formeln und deren Interpretation im Prinzip die gleichen Prädikate beschrieben.

7.4 Satz Korrektheit der Interpretation ^{w}

Sei $A \in \mathbf{\Sigma^b}$ mit $\mathsf{FV}(A) \subset \{a_1, \ldots, a_k\}$, dann gilt mit $U(a) :\equiv \{u : \mathrm{Bit}(u, a) = 1\}$

$$(\mathbb{N}, \mathcal{P}(\mathbb{N}), \ldots) \models A \leftrightarrow A^w_{\alpha_1, \ldots, \alpha_k}(U(a_1), \ldots, U(a_k)) .$$

Beweis erfolgt durch Induktion nach der Länge von A:

Ist A eine Primformel, so haben wir mit den obigen Heuristiken schon die Behauptung begründet. Für $A \equiv B \circ C$ mit $\circ \in \{\wedge, \vee\}$ folgt die Behauptung direkt aus der Induktionsvoraussetzung.

Ist $A \equiv \forall x{\leq}t\, B(x)$, so gilt nach der Induktionsvoraussetzung

$$B(a) \leftrightarrow C(a, U(a)) \tag{1}$$

für $C(a, \alpha) :\equiv (B(a))^w_{\alpha_1, \ldots, \alpha_k}(U(a_1), \ldots, U(a_k))$. Wir beobachten

$$\alpha^{<|a|} = \beta^{<|b|} \wedge C(a, \alpha) \to C(b, \beta) \tag{2}$$

und mit der Anmerkung an die Definition der Terminterpretationen

$$U_t^{<|T_t|}{}\alpha_1, \ldots, \alpha_k(U(a_1), \ldots, U(a_k)) = U(t) . \tag{3}$$

Nun fügen wir alle Teile zusammen, um

$$\forall x{\leq}t\, B(x) \leftrightarrow \forall\phi\left((\phi^{|T_t|})^{<|T_t|} \leq U(t) \rightarrow C(T_t, \phi^{|T_t|})\right) \tag{4}$$

zu zeigen.

„$\rightarrow$“ Sei $\phi \subset \mathbb{N}$ beliebig mit $\phi^{<|T_t|} \leq U(t)$, dann sei x die mit $\phi^{<|T_t|}$ assoziierte Zahl, also gilt

$$U(x) = \phi^{<|T_t|} \leq U(t)\,,$$

mithin $x \leq t$. Nun zeigen (1) und (2) wegen $U(x) = U(x)^{<|x|}$ und $\phi^{<|T_t|} = (\phi^{|T_t|})^{<|T_t|}$

$$B(x) \overset{(1)}{\leftrightarrow} C(x, U(x)) \overset{(2)}{\leftrightarrow} C(T_t, \phi^{|T_t|})\,.$$

Mit $x \leq t$ folgt aus der Voraussetzung $B(x)$, mithin

$$C(T_t, \phi^{|T_t|})\,.$$

„$\leftarrow$“ Ist $x \leq t$, dann sei $\phi = U(x)$. Mit $t \leq T_t$ gilt

$$\phi^{<|T_t|} = U(x)^{<|T_t|} = U(x) \leq U(t)\,.$$

Wieder zeigen (1) und (2)

$$C(T_t, \phi^{|T_t|}) \leftrightarrow B(x)\,.$$

Mit $\phi^{<|T_t|} {\leq} U(t)$ folgt diesmal aus der Voraussetzung $C(T_t, \phi^{|T_t|})$, mithin $B(x)$.

Damit ist (4) gezeigt.

Nun gilt für $t \equiv |s|$

$$\forall\phi\, C(T_t, \phi^{|T_t|}) \leftrightarrow \forall x{\leq}|2\#T_s|\, C(T_t, U(x))\,,$$

da mit $T_t \equiv T_{|.|}(T_s) \equiv |T_s|$ schon

$$\sum_{i<|T_t|} (i)_\phi \cdot 2^i \leq 2^{|T_t|} \dot{-} 1 \leq 2 \cdot |T_s| \dot{-} 1 < 2 \cdot |T_s| + 1 = |2\#T_s|$$

gilt. Mithin ist $A \leftrightarrow A^w_{\alpha_1,\ldots,\alpha_k}(U(a_1),\ldots,U(a_k))$ gezeigt.

Der Fall $A \equiv \exists x{\leq}t\, B(x)$ ergibt sich aus dem gerade Gezeigten durch Negation. □

Nachdem wir die Korrektheit der Interpretation ^{w} im Standardmodell begründet haben, zeigen wir im nächsten Abschnitt, daß diese Übersetzung eine Einbettung von $\mathbf{S^i_2}$ in $\mathbf{U^{i,w^\star}_2}$ liefert:

$$\Gamma \subset \mathbf{\Sigma^b} \text{ und } \mathbf{S^i_2} \vdash \Gamma \implies \mathbf{U^{i,w^\star}_2} \vdash \Gamma^w\,.$$

8 Einbettung von $\mathbf{S_2^i}$ in $\mathbf{U_2^{i,w^\star}}$

Wir zeigen für beliebige $\Gamma \subset \mathbf{\Sigma^b}$

$$\mathbf{S_2^i} \vdash \Gamma \implies \mathbf{U_2^{i,w^\star}} \vdash \Gamma^w .$$

Dabei ist der arbeitsintensivste Teil das Nachrechnen der übersetzten BASIC($\emptyset$)-Axiome in $\mathbf{U_2^{i,w^\star}}$. Hier kommt uns die im Vergleich zu [Buss 1986] veränderte Definition von BASIC($\emptyset$) gelegen, da die aufwendig nachzurechnenden Axiome für die Multiplikation auf ein Minimum reduziert sind.

Zur Abkürzung und Vereinfachung der Schreibweisen treffen wir folgende Definitionen:

$$\begin{aligned} \alpha^{<|a|} \setminus \beta^{<|b|} &:= \{u : u \in \alpha^{<|a|} \wedge u \notin \beta^{<|b|}\} \\ \alpha^{<|a|} \subset \beta^{<|b|} &:\equiv \forall x{<}|a| \, (x \in \alpha^{<|a|} \to x \in \beta^{<|b|}) . \end{aligned}$$

Sei

$$\max\left(\alpha^{<|a|}\right) = c \;:\equiv\; (c \in \alpha^{<|a|} \vee c = 0) \wedge \forall x{<}|a| \, (c < x \to x \notin \alpha^{<|a|}) .$$

In $\mathbf{U_2^{1,w^\star}}$ gilt ($\mathbf{\Sigma_0^{1,w^\star}}$-LMIN), also sind

$$\max\left(\alpha^{<|a|}\right)$$

und auch

$$\max\left(\alpha^{<|a|} \setminus \beta^{<|b|}\right)$$

in $\mathbf{U_2^{1,w^\star}}$ beweisbar existent. Damit schreiben sich in $\mathbf{U_2^{1,w^\star}}$

$$\alpha^{<|a|} = \beta^{<|b|} \;\leftrightarrow\; \alpha^{<|a|} \subset \beta^{<|b|} \wedge \beta^{<|b|} \subset \alpha^{<|a|}$$

und

$$\alpha^{<|a|} < \beta^{<|b|} \;\leftrightarrow\; \exists x{\leq}|b| \left(x \in \beta^{<|b|} \setminus \alpha^{<|a|} \wedge x \geq \max\left(\alpha^{<|a|} \setminus \beta^{<|b|}\right)\right) .$$

Wir beobachten

$$\alpha^{<|a|} \subset \beta^{<|b|} \;\to\; \alpha^{<|a|} \leq \beta^{<|b|} ,$$

$$x \in \alpha^{<|a|} \setminus \beta^{<|b|} \;\to\; x \leq \max\left(\alpha^{<|a|} \setminus \beta^{<|b|}\right)$$

und

$$\begin{aligned} &\forall x{<}|b| \left(x \in \beta^{<|b|} \setminus \alpha^{<|a|} \to x < \max\left(\alpha^{<|a|} \setminus \beta^{<|b|}\right)\right) \\ &\quad\to\; \max\left(\beta^{<|b|} \setminus \alpha^{<|a|}\right) < \max\left(\alpha^{<|a|} \setminus \beta^{<|b|}\right) . \end{aligned}$$

Wir beginnen mit dem Nachrechnen der übersetzten BASIC($\emptyset$)-Axiome, indem wir zuerst die Definition von $<$ und $\leq$ überprüfen, und insbesondere deren Linearität und Transitivität nachweisen.

8.1 Lemma

(i) $\mathbf{U_2^{0,w^\star}} \vdash \alpha^{<|a|} \leq \beta^{<|b|}, \beta^{<|b|} < \alpha^{<|a|}$

(ii) $\mathbf{U_2^{0,w^\star}} \vdash \neg\alpha^{<|a|} \leq \beta^{<|b|}, \neg\beta^{<|b|} < \alpha^{<|a|}$

(iii) $\mathbf{U_2^{0,w^\star}} \vdash \neg\alpha^{<|a|} \leq \beta^{<|b|}, \neg\beta^{<|b|} \leq \gamma^{<|c|}, \alpha^{<|a|} \leq \gamma^{<|c|}$

Beweis in $\mathbf{U_2^{0,w^\star}}$:

(i) Gelte $\neg\alpha^{<|a|} \leq \beta^{<|b|}$, also $\alpha^{<|a|} \neq \beta^{<|b|}$ und $\alpha^{<|a|} \not< \beta^{<|b|}$.
Ist $\beta^{<|b|}\backslash\alpha^{<|a|} = \emptyset$, so erhalten wir $\alpha^{<|a|}\backslash\beta^{<|b|} \neq \emptyset$ aus $\alpha^{<|a|} \neq \beta^{<|b|}$, also gilt $x \geq \max\left(\beta^{<|b|}\backslash\alpha^{<|a|}\right)$ für beliebige $x \in \alpha^{<|a|}\backslash\beta^{<|b|}$. Mithin $\alpha^{<|a|} < \beta^{<|b|}$.
Ist $\beta^{<|b|}\backslash\alpha^{<|a|} \neq \emptyset$, dann ist $x < \max\left(\alpha^{<|a|}\backslash\beta^{<|b|}\right)$ für jedes $x \in \beta^{<|b|}\backslash\alpha^{<|a|}$, also gibt es $y \in \alpha^{<|a|}\backslash\beta^{<|b|}$ mit $y \geq \max\left(\beta^{<|b|}\backslash\alpha^{<|a|}\right)$. Und wieder ist $\alpha^{<|a|} < \beta^{<|b|}$.

(ii) Gelte $\beta^{<|b|} < \alpha^{<|a|}$, also gibt es $x \in \alpha^{<|a|}\backslash\beta^{<|b|}$ mit $x \geq \max\left(\beta^{<|b|}\backslash\alpha^{<|a|}\right)$. Somit ist $\alpha^{<|a|}\backslash\beta^{<|b|} \neq \emptyset$, also $\alpha^{<|a|} \neq \beta^{<|b|}$. Des weiteren gilt $y < x \leq \max\left(\alpha^{<|a|}\backslash\beta^{<|b|}\right)$ für $y \in \beta^{<|b|}\backslash\alpha^{<|a|}$, also $\alpha^{<|a|} \not< \beta^{<|b|}$.

(iii) Gelte $\alpha^{<|a|} \leq \beta^{<|b|}$ und $\beta^{<|b|} \leq \gamma^{<|c|}$, dann ist zu zeigen $\alpha^{<|a|} \leq \gamma^{<|c|}$. Dabei ist der interessante Fall, daß $\alpha^{<|a|} < \beta^{<|b|}$ und $\beta^{<|b|} < \gamma^{<|c|}$ ist.
Also nehmen wir an, daß x und y existieren mit

$$x \in \beta^{<|b|}\backslash\alpha^{<|a|} \quad (1) \qquad \text{und} \qquad x \geq \max\left(\alpha^{<|a|}\backslash\beta^{<|b|}\right) \quad (2)$$

und

$$y \in \gamma^{<|c|}\backslash\beta^{<|b|} \quad (3) \qquad \text{und} \qquad y \geq \max\left(\beta^{<|b|}\backslash\gamma^{<|c|}\right). \quad (4)$$

Wir halten fest, daß $x \neq y$ ist, da $x \in \beta^{<|b|}$, aber $y \notin \beta^{<|b|}$ ist.
Für $d \in \alpha^{<|a|}\backslash\gamma^{<|c|}$ gibt es zwei Fälle.
(a) Ist $d \in \beta^{<|b|}$, so folgt $d \in \beta^{<|b|}\backslash\gamma^{<|c|}$ und wegen (4) $d < y$.
(b) Im anderen Fall ist $d \notin \beta^{<|b|}$, also $d \in \alpha^{<|a|}\backslash\beta^{<|b|}$ und mit (2) folgt $d < x$.
Insgesamt ist also $\max(x,y) > \max\left(\alpha^{<|a|}\backslash\gamma^{<|c|}\right)$, darum genügt zum Beweis von $\alpha^{<|a|} < \gamma^{<|c|}$

$$\max(x,y) \in \gamma^{<|c|}\backslash\alpha^{<|a|}$$

zu zeigen. Wir unterscheiden folgende Möglichkeiten:
(a) Ist $y \in \alpha^{<|a|}$, dann zeigt (3) $y \in \alpha^{<|a|}\backslash\beta^{<|b|}$ und mit (2) $y < x$. Nach (4) muß $x \notin \beta^{<|b|}\backslash\gamma^{<|c|}$ gelten, was aber wegen $x \in \beta^{<|b|}$ nur für $x \in \gamma^{<|c|}$ möglich ist. Insgesamt erhalten wir

$$\max(x,y) = x \in \gamma^{<|c|}\backslash\alpha^{<|a|}.$$

(b) Sind $y \notin \alpha^{<|a|}$ und $x \in \gamma^{<|c|}$, dann sind mit (1) und (3) $x, y \in \gamma^{<|c|} \backslash \alpha^{<|a|}$, in jedem Fall also
$$\max(x, y) \in \gamma^{<|c|} \backslash \alpha^{<|a|}.$$
(c) Sind $y \notin \alpha^{<|a|}$ und $x \notin \gamma^{<|c|}$, so erhalten wir mit (3) und (1) $y \in \gamma^{<|c|} \backslash \alpha^{<|a|}$ und $x \in \beta^{<|b|} \backslash \gamma^{<|c|}$. Aus letzterem folgt mit (4) $y > x$. Mithin
$$\max(x, y) = y \in \gamma^{<|c|} \backslash \alpha^{<|a|}.$$ □

Wir bestimmen $0^{<|0|}, 1^{<|1|}, 2^{<|2|}$ zu

$$0^{<|0|} = \{u : u \neq u\},$$

$$1^{<|1|} = \mathrm{S}(0^{<|0|}) = \{u : u = 0\},$$

$$2^{<|2|} = \mathrm{S}(1^{<|1|}) = \{u : u = 1\}.$$

Wenn der Kontext es zuläßt, schreiben wir kurz $0, 1, 2$ für $0^{<|0|}, 1^{<|1|}$ bzw. $2^{<|2|}$. Wir rechnen nun die übersetzten BASIC($\emptyset$)-Axiome von Seite 26 nach.

(a) $(0 \leq a)^w$

Es gilt $0 \subset \alpha^{<|a|}$, also folgt $0 \leq \alpha^{<|a|}$.

(b) $(b \leq a \vee a \leq b)^w$

(c) $(a \leq b \wedge b \leq a \to a = b)^w$

(d) $(a \leq b \wedge b \leq c \to a \leq c)^w$

Die letzten drei Punkte folgen aus 8.1 (i), (ii) und (iii). Als nächstes beschäftigen wir uns mit der Nachfolgerfunktion.

(e) $(b \leq a \leftrightarrow b < \mathrm{S}a)^w$

Da $|a| \notin \alpha^{<|a|}$, gibt es mit ($\mathbf{\Sigma_0^1, w^*}$-LMIN) ein minimales $w \leq |a|$ mit $w \notin \alpha^{<|a|}$. Aus der Minimalität folgt

$$\forall v \leq |a| \, (v < w \to v \in \alpha^{<|a|}), \tag{1}$$

also gilt

$$\mathrm{S}(\alpha^{<|a|}) = \{u : u = w \vee (u > w \wedge u \in \alpha^{<|a|})\} \,. \tag{2}$$

Für $(b \leq a \to b < \mathrm{S}a)^w$ zeigen wir zuerst

$$\alpha^{<|a|} < \mathrm{S}(\alpha^{<|a|}) \,.$$

Nach Definition von w und von $\mathrm{S}(\alpha^{<|a|})$ (2) gilt

$$w \in \mathrm{S}(\alpha^{<|a|}) \backslash \alpha^{<|a|} \,. \tag{3}$$

Wir beobachten für $v < |a|$ mit $w < v \wedge v \in \alpha^{<|a|}$ wegen (2) $v \in \mathrm{S}(\alpha^{<|a|})$. Also erhalten wir

$$w \geq \max\left(\alpha^{<|a|} \backslash \mathrm{S}(\alpha^{<|a|})\right) \,,$$

was mit (3) $\alpha^{<|a|} < \mathrm{S}(\alpha^{<|a|})$ ergibt, mithin $\neg\mathrm{S}(\alpha^{<|a|}) \leq \alpha^{<|a|}$.
Ist nun $\beta^{<|b|} \leq \alpha^{<|a|}$, so folgt aus der Transitivität von $\leq$ $\neg\mathrm{S}(\alpha^{<|a|}) \leq \beta^{<|b|}$, also

$$\beta^{<|b|} < \mathrm{S}(\alpha^{<|a|}) \,.$$

Die andere Implikation $(b < \mathrm{S}a \to b \leq a)^w$ zeigen wir durch Kontraposition. Gelte $\alpha^{<|a|} < \beta^{<|b|}$, d. h. es gibt $x \leq |b|$ mit

$$x \in \beta^{<|b|} \backslash \alpha^{<|a|} \quad \text{und} \quad x \geq \max\left(\alpha^{<|a|} \backslash \beta^{<|b|}\right) =: y \,. \tag{4}$$

Wir haben folgende Situation vorliegen:

$$\begin{array}{rccccc} & & & w & & \\ \mathrm{S}(\alpha^{<|a|}): & \underbrace{\ldots}_{=} & 1 & 0 & \ldots & 0 \\ \alpha^{<|a|}: & \overbrace{\ldots}^{=} & 0 & 1 & \ldots & 1 \end{array}$$

$$\begin{array}{rccccc} & & & x \geq w & & y \\ \alpha^{<|a|}: & \ldots & 0 & & \ldots & \Big| \\ \beta^{<|b|}: & \ldots & 1 & & \ldots & \Big| \end{array}$$

Da für $v < w$ mit (1) schon $v \in \alpha^{<|a|}$, aber $x \notin \alpha^{<|a|}$ gilt, muß $w \leq x$ sein. Ist $w = x$, dann folgt $\mathrm{S}(\alpha^{<|a|}) \subset \beta^{<|b|}$, denn sei $v \in \mathrm{S}(\alpha^{<|a|})$. Dann impliziert (2) $v \geq w$. Für $v = w$ ist mit (4) $v \in \beta^{<|b|}$. Im anderen Fall ist $v > w$, also folgern wir mit (4) $v \notin \alpha^{<|a|} \backslash \beta^{<|b|}$. Zusammen mit (2) $v \in \alpha^{<|a|}$ ergibt das

$$v \in \beta^{<|b|} \,.$$

Mithin gilt $\mathrm{S}(\alpha^{<|a|}) \leq \beta^{<|b|}$.

Schließlich bleibt noch der Fall $w < x$ zu betrachten. Hier gilt für alle $v \leq |a|$ mit $v \geq x$ wegen (2)

$$v \in \alpha^{<|a|} \leftrightarrow v \in \mathrm{S}(\alpha^{<|a|}) \,.$$

Damit erhalten wir aus (4)

$$x \in \beta^{<|b|} \backslash \mathrm{S}(\alpha^{<|a|}) \quad \text{und} \quad x \geq \max\left(\mathrm{S}(\alpha^{<|a|}) \backslash \beta^{<|b|}\right) \,.$$

Mithin $\mathrm{S}(\alpha^{<|a|}) < \beta^{<|b|}$.

In den Axiomen spielt die Funktion $(a \mapsto 2 \cdot a)$ eine besondere Rolle, weshalb wir sie getrennt von der Multiplikation betrachten. Wir berechnen $2 \cdot \alpha^{<|a|}$:

Behauptung

$2 \cdot \alpha^{<|a|} = \{u : u > 0 \wedge u \dot{-} 1 \in \alpha^{<|a|}\}$

Beweis:

Sei $t :\equiv T.(2, a) \equiv 2 \cdot (\mathrm{S2}) \cdot (\mathrm{S}a)$ und $\tilde{t} :\equiv \mathrm{SqBd}_3(t)$. Es gilt

$$\#z{\leq}|2|(z \leq x \wedge z \in 2 \wedge x \dot{-} z \in \alpha^{<|a|}) = \begin{cases} 1 & : \quad x \dot{-} 1 \in \alpha^{<|a|} \wedge x \geq 1 \\ 0 & : \quad \text{sonst} \end{cases}$$

Darum definieren wir mit (w$\mathbf{\Sigma}_{\mathbf{0}}^{\mathbf{1},\mathbf{w}^\star}$-CA) ein γ derart, daß

$$\begin{aligned} \gamma^{|\tilde{t}|} \quad = \quad & \{\langle i, x, y\rangle \leq |\tilde{t}| : (x = 0 \wedge y = 0) \vee \\ & (x \dot{-} 1 \notin \alpha^{<|a|} \wedge y = 0) \vee (x > 0 \wedge x \dot{-} 1 \in \alpha^{<|a|} \wedge y = 1)\} \end{aligned}$$

ist. Nach Konstruktion gilt für G wie in Abschnitt 7 definiert

$$\forall i{\leq}|t|\, G(i, 2, a, 2^{<|2|}, \alpha^{<|a|}, \gamma^{|\tilde{t}|}) \,,$$

also ist

$$\begin{aligned} 2 \cdot \alpha^{<|a|} \quad &= \quad \{u : u \leq |t| \wedge \langle |t|, u, 1\rangle \in \gamma^{|\tilde{t}|}\} \\ &= \quad \{u : u > 0 \wedge u \dot{-} 1 \in \alpha^{<|a|}\} \,. \end{aligned}$$

□

(f) $\qquad (a < b \to \mathrm{S}(2 \cdot a) < 2 \cdot b)^w$

Gelte $\alpha^{<|a|} < \beta^{<|b|}$, dann gibt es $x \leq |b|$ mit

$$x \in \beta^{<|b|} \backslash \alpha^{<|a|} \quad \text{und} \quad x \geq \max\left(\alpha^{<|a|} \backslash \beta^{<|b|}\right) =: y \,.$$

Dann gilt

$$\mathrm{S}x \in (2 \cdot \beta^{<|b|}) \backslash (\mathrm{S}(2 \cdot \alpha^{<|a|}))$$

und

$$\mathrm{S}x \geq \max\left((\mathrm{S}(2 \cdot \alpha^{<|a|}))\backslash(2 \cdot \beta^{<|b|})\right) ,$$

also $\mathrm{S}(2 \cdot \alpha^{<|a|}) < 2 \cdot \beta^{<|b|}$.

(g) $(a = \lfloor \frac{1}{2} b \rfloor \leftrightarrow (2 \cdot a = b \vee \mathrm{S}(2 \cdot a) = b))^w$

Es sind

$$\lfloor \tfrac{1}{2} \beta^{<|b|} \rfloor = \{u : \mathrm{S}u \in \beta^{<|b|}\}$$

und

$$2 \cdot \alpha^{<|a|} = \{u : u > 0 \wedge u \dot{-} 1 \in \alpha^{<|a|}\} .$$

Damit gilt

$$\mathrm{S}(2 \cdot \alpha^{<|a|}) = \{u : u \dot{-} 1 \in \alpha^{<|a|} \vee u = 0\} .$$

Ist $2 \cdot \alpha^{<|a|} = \beta^{<|b|}$ oder $\mathrm{S}(2 \cdot \alpha^{<|a|}) = \beta^{<|b|}$, so folgt

$$\lfloor \tfrac{1}{2} \beta^{<|b|} \rfloor = \{u : \mathrm{S}u \in \beta^{<|b|}\} = \{u : (\mathrm{S}u) \dot{-} 1 \in \alpha^{<|a|}\} = \alpha^{<|a|} .$$

Umgekehrt sei $\alpha^{<|a|} = \lfloor \frac{1}{2} \beta^{<|b|} \rfloor$. Ist $0 \notin \beta^{<|b|}$, so gilt

$$\begin{aligned} 2 \cdot \alpha^{<|a|} &= \{u : u > 0 \wedge u \dot{-} 1 \in \alpha^{<|a|}\} \\ &= \{u : u > 0 \wedge \mathrm{S}(u \dot{-} 1) \in \beta^{<|b|}\} \\ &= \{u : u > 0 \wedge u \in \beta^{<|b|}\} \\ &= \beta^{<|b|} . \end{aligned}$$

Für $0 \in \beta^{<|b|}$ haben wir

$$\begin{aligned} \mathrm{S}(2 \cdot \alpha^{<|a|}) &= \{u : u = 0 \vee u \dot{-} 1 \in \alpha^{<|a|}\} \\ &= \{u : u = 0 \vee \mathrm{S}(u \dot{-} 1) \in \beta^{<|b|}\} \\ &= \{u : u = 0 \vee u \in \beta^{<|b|}\} \\ &= \beta^{<|b|} . \end{aligned}$$

(h) $(|0| = 0)^w$

Wir berechnen

$$|0^{<|0|}| = \{u : \mathrm{Bit}(u, 0) = 1\}^{<\left||0|\right|} = 0^{<|0|} .$$

Es gilt $0 = 0 \vee 0 \dot{-} 1 \in \alpha^{<|a|}$, also existiert mit ($\mathbf{\Sigma_0^{1,w^\star}}$-LMIN) ein maximales $w_a \leq |a|$ mit $w_a = 0 \vee w_a \dot{-} 1 \in \alpha^{<|a|}$. Aus der Maximalität folgt

$$\forall v{\leq}|a|\,(w_a \leq v \to v \notin \alpha^{<|a|})\,,$$

also ist

$$\alpha^{<|a|} = (w_a - 1)_\alpha \ldots (0)_\alpha\,.$$

Analog gibt es maximale $w_b \leq |b|$ und $w_c \leq |c|$ mit

$$w_b = 0 \vee w_b \dot{-} 1 \in \beta^{<|b|} \quad \text{und} \quad w_c = 0 \vee w_c \dot{-} 1 \in \gamma^{<|c|}$$

derart, daß

$$\forall v{\leq}|b|\,(w_b \leq v \to v \notin \beta^{<|b|}) \quad \text{und} \quad \forall v{\leq}|c|\,(w_c \leq v \to v \notin \gamma^{<|c|})$$

gilt.

(i) $\qquad (a \neq 0 \to |a| = \mathrm{S}(|\lfloor \tfrac{1}{2} a \rfloor|))^w$

Wir berechnen

$$|\alpha^{<|a|}| = \{u : \mathrm{Bit}(u, w_a) = 1\}^{<\left||a|\right|}\,.$$

Sei $\alpha^{<|a|} \neq 0$, dann muß $w_a \neq 0$ und somit $w_a \dot{-} 1 \in \alpha^{<|a|}$ gelten. Für $w_a = 1$ folgt die Behauptung durch Nachrechnen. Ist $w_a > 1$, dann gilt

$$\begin{aligned} \lfloor \tfrac{1}{2} \alpha^{<|a|} \rfloor &= \{u : \mathrm{S}u \in \alpha^{<|a|}\}^{<\left|\lfloor \frac{1}{2} a \rfloor\right|} \\ &= \{u : (u < w_a \dot{-} 2 \wedge \mathrm{S}u \in \alpha^{<|a|}) \vee u = w_a \dot{-} 2\}\,. \end{aligned}$$

Also ist für $\overline{w_a} := w_a \dot{-} 1$

$$\overline{w_a} \dot{-} 1 \in \lfloor \tfrac{1}{2} \alpha^{<|a|} \rfloor$$

und

$$\forall v{\leq}|\lfloor \tfrac{1}{2} a \rfloor|\,(\overline{w_a} \leq v \to v \notin \lfloor \tfrac{1}{2} \alpha^{<|a|} \rfloor)\,.$$

Mithin

$$|\lfloor \tfrac{1}{2} \alpha^{<|a|} \rfloor| = \{u : \mathrm{Bit}(u, \overline{w_a}) = 1\}^{<\left||\lfloor \frac{1}{2} a \rfloor|\right|}\,.$$

Es ist $\overline{w_a} < |a|$, also gilt $\mathrm{Bit}(\left||\lfloor \tfrac{1}{2} a \rfloor|\right|, \overline{w_a}) = 0$. Mit ($\mathbf{\Sigma_0^{1,w^\star}}$-LMIN) existiert ein minimales $v \leq \left||\lfloor \tfrac{1}{2} a \rfloor|\right|$ mit $\mathrm{Bit}(v, \overline{w_a}) = 0$, dann gilt

$$\forall z{\leq}\left||\lfloor \tfrac{1}{2} a \rfloor|\right|\,(z < v \to \mathrm{Bit}(z, \overline{w_a}) = 1)\,.$$

Damit erhalten wir

$$\begin{aligned}&\mathrm{S}(\{u : \mathrm{Bit}(u, \overline{w_a}) = 1\}^{<\left|\lfloor\frac{1}{2}a\rfloor\right|})\\ &= \{u : u = v \vee (u > v \wedge u < \left|\lfloor\tfrac{1}{2}a\rfloor\right| \wedge \mathrm{Bit}(u, \overline{w_a}) = 1)\}\\ &= \{u : u \leq \left|\lfloor\tfrac{1}{2}a\rfloor\right| \wedge \mathrm{Bit}(u, \mathrm{S}\overline{w_a}) = 1\}\,.\end{aligned}$$

Da $\mathrm{S}\overline{w_a} = w_a \leq |a|$ ist, gilt $\mathrm{Bit}(\left||a|\right|, \mathrm{S}\overline{w_a}) = 0$, mithin

$$\mathrm{S}(\lfloor\tfrac{1}{2}\alpha^{<|a|}\rfloor) = \{u : \mathrm{Bit}(u, \mathrm{S}\overline{w_a}) = 1\}^{<\left||a|\right|} = |\alpha^{<|a|}|\,.$$

(j) $\quad (a \leq b \to |a| \leq |b|)^w$

Ist $(a \leq b)^w$, dann folgt $w_a \leq w_b$. Wir benutzen wieder die Abkürzung $U(x) :\!= \{u : \mathrm{Bit}(u, x) = 1\}$, um $U(w_a)^{<\left||a|\right|} \leq U(w_b)^{<\left||b|\right|}$ zu zeigen. Dann ist $(|a| \leq |b|)^w$ bewiesen.

Für die obige Behauptung nehmen wir $U(w_a)^{<\left||a|\right|} > U(w_b)^{<\left||b|\right|}$ an und führen diese Annahme zum Widerspruch. Es ist $|w_a| \leq |w_b| \leq \left||b|\right|$, also gibt es mit ($\mathbf{\Sigma_0^{1,w^\star}}$-LMIN) ein maximales $x \leq |w_b|$ derart, daß

$$x \in U(w_a)^{<\left||a|\right|} \backslash U(w_b)^{<\left||b|\right|} \quad \text{und} \quad x \geq \max\left(U(w_b)^{<\left||b|\right|} \backslash U(w_a)^{<\left||a|\right|}\right)$$

erfüllt ist. Dann gilt für $x < y \leq |w_b|$

$$y \in U(w_a)^{<\left||a|\right|} \leftrightarrow y \in U(w_b)^{<\left||b|\right|}\,.$$

Insgesamt haben wir $\mathrm{Bit}(x, w_a){=}1$, $\mathrm{Bit}(x, w_b){=}0$ und $\forall y{\leq}|w_b|\,(y{>}x \to \mathrm{Bit}(y, w_a){=}\mathrm{Bit}(y, w_b))$. Dann erhalten wir

$$w_b < w_a$$

im Widerspruch zur Voraussetzung $w_a \leq w_b$.

(k) $\quad (0\#a = 1)^w$

Wir beobachten

$$0\#\alpha^{<|a|} = \{0 \cdot w_a\} = \{0\} = 1^{<|1|}\,.$$

(l) $(a \neq 0 \to 1\#a = 2 \cdot (1\#\lfloor \frac{1}{2}a \rfloor))^w$

Sei $(a \neq 0)^w$, dann ist $w_a > 0$. Mit

$$\lfloor \tfrac{1}{2}\alpha^{<|a|} \rfloor = \{u : \mathrm{S}u \in \alpha^{<|a|}\}$$

ist $w_a \dot{-} 1$ maximal mit

$$w_a \dot{-} 1 = 0 \vee (w_a \dot{-} 1) \dot{-} 1 \in \lfloor \tfrac{1}{2}\alpha^{<|a|} \rfloor ,$$

also gilt

$$1\#\lfloor \tfrac{1}{2}\alpha^{<|a|} \rfloor = \{1 \cdot (w_a \dot{-} 1)\} = \{w_a \dot{-} 1\} .$$

Mithin

$$\begin{aligned} 2 \cdot (1\#\lfloor \tfrac{1}{2}\alpha^{<|a|} \rfloor) &= \{u : u > 0 \wedge (u \dot{-} 1) \in (1\#\lfloor \tfrac{1}{2}\alpha^{<|a|} \rfloor)\} = \{w_a\} \\ &= 1\#\alpha^{<|a|} . \end{aligned}$$

(m) $(a \neq 0 \to a\#b = (\lfloor \frac{1}{2}a \rfloor \#b) \cdot (1\#b))^w$

Sei $(a \neq 0)^w$, dann ist $w_a > 0$. Wir berechnen

$$\lfloor \tfrac{1}{2}\alpha^{<|a|} \rfloor \#\beta^{<|b|} = \{(w_a \dot{-} 1) \cdot w_b\}$$

und

$$1\#\beta^{<|b|} = \{w_b\} .$$

Es gilt

$$\begin{aligned} &\#z{\leq}\Big||b|\Big|(z \leq x \wedge z \in \{w_b\} \wedge x \dot{-} z \in \{(w_a \dot{-} 1) \cdot w_b\}) \\ &= \begin{cases} 1 & x = (w_a \dot{-} 1) \cdot w_b + w_b \overset{w_a > 0}{=} w_a \cdot w_b \\ 0 & \text{sonst} \end{cases} \end{aligned}$$

also folgt

$$(\lfloor \tfrac{1}{2}\alpha^{<|a|} \rfloor \#\beta^{<|b|}) \cdot (1\#\beta^{<|b|}) = \{w_a \cdot w_b\} = \alpha^{<|a|}\#\beta^{<|b|} .$$

(n) $(a\#b = b\#a)^w$

Es gilt

$$\alpha^{<|a|}\#\beta^{<|b|} = \{w_a \cdot w_b\} = \beta^{<|b|}\#\alpha^{<|a|} .$$

(o) $(|a| = |b| \to a\#c = b\#c)^w$

Gelte $(|a| = |b|)^w$, dann ist $\mathrm{Bit}(i, w_a) = \mathrm{Bit}(i, w_b)$ für alle $i < \max(|w_a|, |w_b|)$ und somit $w_a = w_b$, mithin

$$\alpha^{<|a|}\#\gamma^{<|c|} = \{w_a \cdot w_c\} = \{w_b \cdot w_c\} = \beta^{<|b|} \cdot \gamma^{<|c|}\,.$$

(p) $(a + 0 = a)^w$

Wir beobachten $\forall w{\leq}|T_+(a,0)|\,(w \notin 0^{<|0|})$. Also gilt

$$\alpha^{<|a|} + 0 = \{u : u \in \alpha^{<|a|} \leftrightarrow u \notin 0^{<|0|}\} = \alpha^{<|a|}\,.$$

(q) $(a + \mathrm{S}b = \mathrm{S}(a + b))^w$

Sei $t :\equiv T_+(a,b)$. ($\mathbf{\Sigma_0^1}^{,\mathbf{w^\star}}$-LMIN) liefert nun minimale $w_b \leq |b|$ und $w \leq |t|$ mit $w_b \notin \beta^{<|b|}$ und $w \notin \alpha^{<|a|} + \beta^{<|b|}$, dann sind

$$\mathrm{S}(\beta^{<|b|}) = \{u : u = w_b \vee (u > w_b \wedge u \in \beta^{<|b|})\}$$

und

$$\mathrm{S}(\alpha^{<|a|} + \beta^{<|b|}) = \{u : u = w \vee (u > w \wedge u \in \alpha^{<|a|} + \beta^{<|b|})\}\,.$$

In den Tabellen bezeichne „=“ die Bit-weise Übereinstimmung und „xor“ die Bit-weise Nicht-Übereinstimmung der angegebenen Bereiche.

			w_b	
$\beta^{<|b|}$	:	$\overbrace{\ldots}^{\equiv}$	0	$1\ldots1$
$\mathrm{S}(\beta^{<|b|})$	:	$\underbrace{\ldots}_{\equiv}$	1	$0\ldots0$

Tabelle 3: Die Binärdarstellung des Nachfolgers von $\beta^{<|b|}$

Also gilt für $u \leq |t|$ (Tabelle 3)

$$\begin{aligned} u \leq w_b &: \; u \in \beta^{<|b|} \leftrightarrow u \notin \mathrm{S}(\beta^{<|b|}) \\ u > w_b &: \; u \in \beta^{<|b|} \leftrightarrow u \in \mathrm{S}(\beta^{<|b|}) \end{aligned}$$

$$\begin{array}{rcl} & & \overset{w}{} \\ \alpha^{<|a|}+\beta^{<|b|} & : & \overbrace{\ldots}^{\equiv} \; 0 \quad 1\ldots 1 \\ \mathrm{S}(\alpha^{<|a|}+\beta^{<|b|}) & : & \ldots \quad 1 \quad 0\ldots 0 \end{array}$$

Tabelle 4: Die Binärdarstellung des Nachfolgers von $\alpha^{<|a|}+\beta^{<|b|}$

und (Tabelle 4)

$$\begin{array}{rcl} u \le w & : & u \in \alpha^{<|a|}+\beta^{<|b|} \leftrightarrow u \notin \mathrm{S}(\alpha^{<|a|}+\beta^{<|b|}) \\ u > w & : & u \in \alpha^{<|a|}+\beta^{<|b|} \leftrightarrow u \in \mathrm{S}(\alpha^{<|a|}+\beta^{<|b|})\,. \end{array}$$

Außerdem beobachten wir:

tritt kein Übertrag nach u bei $\alpha^{<|a|}+\beta^{<|b|}$ auf, so gilt
$u \in \alpha^{<|a|}+\beta^{<|b|} \iff \left(u \in \alpha^{<|a|} \leftrightarrow u \notin \beta^{<|b|}\right)$

und

tritt ein Übertrag nach u bei $\alpha^{<|a|}+\beta^{<|b|}$ auf, so gilt
$u \in \alpha^{<|a|}+\beta^{<|b|} \iff \left(u \in \alpha^{<|a|} \leftrightarrow u \in \beta^{<|b|}\right)$

(i) Ist $u = 0$, so gilt

$$\begin{array}{l} 0 \in \alpha^{<|a|}+\mathrm{S}(\beta^{<|b|}) \\ \quad \iff \quad \left(0 \in \alpha^{<|a|} \leftrightarrow 0 \notin \mathrm{S}(\beta^{<|b|})\right) \\ \quad \iff \quad \left(0 \in \alpha^{<|a|} \leftrightarrow 0 \in \beta^{<|b|}\right) \\ \quad \iff \quad 0 \notin \alpha^{<|a|}+\beta^{<|b|} \\ \quad \iff \quad 0 \in \mathrm{S}(\alpha^{<|a|}+\beta^{<|b|})\,. \end{array}$$

(ii) Sei $u > 0$ und es trete

kein Übertrag nach u bei $\alpha^{<|a|}+\beta^{<|b|}$ (1)

auf, d. h.

$$\begin{array}{l} \exists v{<}u\,[(v = 0 \vee (v \dot{-} 1)_{\alpha^{<|a|}} = (v \dot{-} 1)_{\beta^{<|b|}} = 0) \\ \quad \wedge \quad \forall x{<}u\,(v \le x \to (x)_{\alpha^{<|a|}} = 0 \vee (x)_{\beta^{<|b|}} = 0)]\,. \end{array} \tag{2}$$

Mit ($\mathbf{\Sigma_0^{1,w^\star}}$-LMIN) wählen wir v maximal in (2).

(A) Ist $v > 0$, dann gilt $(v \dot{-} 1)_{\beta^{<|b|}} = 0$ laut Definition von v, also ist nach Definiton von w_b $v \dot{-} 1 \ge w_b$.
Ist $v \dot{-} 1 = w_b$, so gilt $\forall x{<}u\,((x)_{\alpha^{<|a|}} = 0 \vee (x)_{\mathrm{S}(\beta^{<|b|})} = 0)$ (Tabelle 5). Ist $v \dot{-} 1 > w_b$, so gilt $\forall x{<}u\,(v{<}x \to (x)_{\alpha^{<|a|}} = 0 \vee (x)_{\mathrm{S}(\beta^{<|b|})} = 0)$ (Tabelle 6).

$$
\begin{array}{rcccccc}
 & & & u & & w_b & \\
\beta^{<|b|} & : & \ldots & \overbrace{\ldots}^{\text{xor}} & 0 & 1\ldots1 & \\
\alpha^{<|a|} & : & \ldots & \overbrace{\ldots}^{\text{xor}} & 0 & \ldots & \\
\mathrm{S}(\beta^{<|b|}) & : & \ldots & \overbrace{\ldots}^{\text{xor}} & 1 & 0\ldots0 &
\end{array}
$$

Tabelle 5: $u > v > 0$ und $v - 1 = w_b$

$$
\begin{array}{rcccccccc}
 & & & u & & v \dot{-} 1 & & w_b & \\
\beta^{<|b|} & : & \ldots & \overbrace{\ldots}^{\text{xor}} & 0 & \ldots & 0 & 1\ldots1 & \\
\alpha^{<|a|} & : & \ldots & \overbrace{\ldots}^{\text{xor}} & 0 & \ldots & & \ldots & \\
\mathrm{S}(\beta^{<|b|}) & : & \ldots & \overbrace{\ldots}^{\text{xor}} & 0 & \ldots & 1 & 0\ldots0 &
\end{array}
$$

Tabelle 6: $u > v > 0$ und $v - 1 > w_b$

Mithin tritt

$$\text{kein Übertrag nach } u \text{ bei } \quad \alpha^{<|a|} + \mathrm{S}(\beta^{<|b|}) \tag{3}$$

auf und es ist $w \leq w_b$. Also gilt

$$u > v > w_b \geq w\,.$$

Damit berechnen wir

$$
\begin{array}{ll}
u \in \alpha^{<|a|} + \mathrm{S}(\beta^{<|b|}) & \\
\overset{(3)}{\Longleftrightarrow} & \Big(u \in \alpha^{<|a|} \leftrightarrow u \notin \mathrm{S}(\beta^{<|b|})\Big) \\
\overset{u>w_b}{\Longleftrightarrow} & \Big(u \in \alpha^{<|a|} \leftrightarrow u \notin \beta^{<|b|}\Big) \\
\overset{(1)}{\Longleftrightarrow} & u \in \alpha^{<|a|} + \beta^{<|b|} \\
\overset{u>w}{\Longleftrightarrow} & u \in \mathrm{S}(\alpha^{<|a|} + \beta^{<|b|})
\end{array}
$$

(B) Ist $v = 0$, dann ist

$$u \leq w\,,$$

da aus der Maximalität von v in (2) schon $\forall x{<}u\,((x)_{\alpha^{<|a|}} \neq (x)_{\beta^{<|b|}})$ folgt.

Damit gilt

$$
\begin{array}{ll}
u \in \mathrm{S}(\alpha^{<|a|} + \beta^{<|b|}) & \\
\overset{u\leq w}{\Longleftrightarrow} & u \notin \alpha^{<|a|} + \beta^{<|b|} \\
\overset{(1)}{\Longleftrightarrow} & \Big(u \in \alpha^{<|a|} \leftrightarrow u \in \beta^{<|b|}\Big) \\
\Longleftrightarrow & \begin{array}{ll} u \leq w_b & : \Big(u \in \alpha^{<|a|} \leftrightarrow u \notin \mathrm{S}(\beta^{<|b|})\Big) \\ u > w_b & : \Big(u \in \alpha^{<|a|} \leftrightarrow u \in \mathrm{S}(\beta^{<|b|})\Big) \end{array} \\
\Longleftrightarrow & u \in \alpha^{<|a|} + \mathrm{S}(\beta^{<|b|})
\end{array}
$$

Um die letzte Äquivalenz zu erhalten, müssen wir zeigen:

$u \leq w_b \iff$ es tritt kein Übertrag nach u bei $\alpha^{<|a|} + \mathrm{S}(\beta^{<|b|})$ auf.

			w_b	
$\beta^{<|b|}$	:	$\ldots$	0	$1 \ldots 1$
			u	
$\alpha^{<|a|}$	:	$\ldots$		$0 \ldots 0$
$\mathrm{S}(\beta^{<|b|})$	:	$\ldots$	1	$0 \ldots 0$

Tabelle 7: $u > v = 0$ und $u \leq w_b$

			u	w_b	
$\beta^{<|b|}$	:	$\ldots$	$\underbrace{\ldots}_{\text{xor}}$	0	$1 \ldots 1$
$\alpha^{<|a|}$	:	$\ldots$	$\overbrace{\ldots}^{\text{xor}}$	1	$0 \ldots 0$
$\mathrm{S}(\beta^{<|b|})$	:	$\ldots$	$\overbrace{\ldots}^{\text{xor}}$	1	$0 \ldots 0$

Tabelle 8: $u > v = 0$ und $u > w_b$

Sei $u \leq w_b$ (Tabelle 7). Mithin tritt
kein Übertrag nach u bei $\alpha^{<|a|} + \mathrm{S}(\beta^{<|b|})$
auf. Im anderen Fall sei $u > w_b$ (Tabelle 8). Mithin tritt
ein Übertrag nach u bei $\alpha^{<|a|} + \mathrm{S}(\beta^{<|b|})$
auf.

(iii) Sei $u > 0$ und trete

$$\text{ein Übertrag nach } u \text{ bei } \alpha^{<|a|} + \beta^{<|b|} \tag{4}$$

auf, d. h.

$$\begin{aligned} &\exists v{<}u\,[(v)_{\alpha^{<|a|}} = (v)_{\beta^{<|b|}} = 1 \\ &\quad \wedge \ \forall x{<}u\,(v \leq x \to (x)_{\alpha^{<|a|}} = 1 \vee (x)_{\beta^{<|b|}} = 1)]\,. \end{aligned} \tag{5}$$

Mit ($\mathbf{\Sigma_0^{1,w^\star}}$-LMIN) wählen wir v maximal in (5). Es ist $w \leq v$, denn für $z \leq v$ minimal mit $(z)_{\alpha^{<|a|}} = (z)_{\beta^{<|b|}} = 1$ gilt $w \leq z \leq v$. Mithin

$u > w$.

Wir erhalten

$$\begin{aligned} & u \in \mathrm{S}(\alpha^{<|a|} + \beta^{<|b|}) \\ \overset{u>w}{\Longleftrightarrow} \quad & u \in \alpha^{<|a|} + \beta^{<|b|} \\ \overset{(4)}{\Longleftrightarrow} \quad & \left(u \in \alpha^{<|a|} \leftrightarrow u \in \beta^{<|b|}\right) . \end{aligned}$$

Wie oben müssen wir nun noch zeigen:

$$u \leq w_b \iff \text{es tritt kein Übertrag nach } u \text{ bei } \alpha^{<|a|} + \mathrm{S}(\beta^{<|b|}) \text{ auf.}$$

		u	v		w_b	
$\beta^{<\lvert b\rvert}$	$\ldots$	$\overbrace{\ldots}^{\text{xor}}$	1	$\ldots$	0	$1\ldots1$
$\alpha^{<\lvert a\rvert}$	$\ldots$	$\underbrace{\ldots}_{\text{xor}}$	1	$\ldots$		$\ldots$
$\mathrm{S}(\beta^{<\lvert b\rvert})$	$\ldots$	$\overbrace{\ldots}^{\text{xor}}$	1	$\ldots$	1	$0\ldots0$

Tabelle 9: $u > v > w_b$

(A) Ist $v > w_b$, dann gilt $u > v > w_b$ (Tabelle 9). Dann tritt ein Übertrag nach u bei $\alpha^{<|a|} + \mathrm{S}(\beta^{<|b|})$ auf.

			w_b		v	
$\beta^{<\lvert b\rvert}$	:	$\ldots$	0	$1\ldots1$	1	$1\ldots1$
			u			
$\alpha^{<\lvert a\rvert}$	:	$\ldots$	$0\ldots0$		1	$\ldots$
$\mathrm{S}(\beta^{<\lvert b\rvert})$	:	$\ldots$	1	$0\ldots0$	0	$0\ldots0$

Tabelle 10: $w_b \geq u > v$

			u	w_b		v	
$\beta^{<\lvert b\rvert}$	:	$\ldots$	$\overbrace{\ldots}^{\text{xor}}$	0	$1\ldots1$	1	$1\ldots1$
$\alpha^{<\lvert a\rvert}$	:	$\ldots$	$\underbrace{\ldots}_{\text{xor}}$	1	$0\ldots0$	1	$0\ldots0$
$\mathrm{S}(\beta^{<\lvert b\rvert})$	:	$\ldots$	$\overbrace{\ldots}^{\text{xor}}$	1	$0\ldots0$	0	$0\ldots0$

Tabelle 11: $u > w_b > v$

(B) Sei $v < w_b$. Ist $u \leq w_b$ (Tabelle 10), so tritt
kein Übertrag nach u bei $\alpha^{<|a|} + \mathrm{S}(\beta^{<|b|})$
auf. Im anderen Fall ist $u > w_b$ (Tabelle 11). Mithin tritt
ein Übertrag nach u bei $\alpha^{<|a|} + \mathrm{S}(\beta^{<|b|})$
auf.

(r) $(a + b = b + a)^w$

Die Definition von + ist symmetrisch in $\alpha^{<|a|}$ und $\beta^{<|b|}$, es gilt

$$F_+(a, b, \alpha, \beta, c) \leftrightarrow F_+(b, a, \beta, \alpha, c) \quad \text{und} \quad T_+(a, b) = T_+(b, a) .$$

Bevor wir uns den weiteren Additionsaxiomen zuwenden, beweisen wir ein spezielles Distributivgesetz:

$$\begin{aligned}
& u \in \left(2 \cdot (\alpha^{<|a|} + \beta^{<|b|})\right) \\
\iff \quad & u > 0 \wedge u \dot{-} 1 \in \alpha^{<|a|} + \beta^{<|b|} \\
\iff \quad & u > 0 \wedge F_+(a, b, \alpha, \beta, u \dot{-} 1) \\
\iff \quad & F_+(2 \cdot a + 1, 2 \cdot b + 1, 2 \cdot \alpha^{<|a|}, 2 \cdot \beta^{<|b|}, u) \\
\iff \quad & u \in \left((2 \cdot \alpha^{<|a|}) + (2 \cdot \beta^{<|b|})\right)
\end{aligned}$$

Zudem definieren wir

$$\mathrm{MSP}(\alpha^{<|a|}, d) := \{u : u + d \in \alpha^{<|a|}\}^{<|a|} .$$

(s) $((a+b)+c=a+(b+c))^w$

Wir können dies durch ($\mathbf{\Sigma_0^{1,w^\star}}$-LIND) für $d=|a+b+c|,\ldots,0$ in

$$\begin{aligned}&\Big(\mathrm{MSP}(\alpha^{<|a|},d)+\mathrm{MSP}(\beta^{<|b|},d)\Big)+\mathrm{MSP}(\gamma^{<|c|},d)\\ &\quad=\ \mathrm{MSP}(\alpha^{<|a|},d)+\Big(\mathrm{MSP}(\beta^{<|b|},d)+\mathrm{MSP}(\gamma^{<|c|},d)\Big)\end{aligned}$$

zeigen. Dabei benutzen wir im Induktionsschritt obiges spezielles Distributivgesetz sowie die bewiesenen Axiome (q) und (r) aus. Für $d=0$ ergibt sich die Behauptung.

(t) $(b<c\to a+b<a+c)^w$

Sei $\beta^{<|b|}<\gamma^{<|c|}$, dann gilt für $x=\max\left(\gamma^{<|c|}\backslash\beta^{<|b|}\right)$

$$x\in\gamma^{<|c|}\backslash\beta^{<|b|}\quad\text{ und }\quad x\geq\max\left(\beta^{<|b|}\backslash\gamma^{<|c|}\right).$$

Wir zeigen nun durch ($\mathbf{\Sigma_0^{1,w^\star}}$-LIND) nach d

$$\begin{aligned}&\mathrm{MSP}(\alpha^{<|a|},x\dot{-}d)+\mathrm{MSP}(\beta^{<|b|},x\dot{-}d)\\ &\quad<\ \mathrm{MSP}(\alpha^{<|a|},x\dot{-}d)+\mathrm{MSP}(\gamma^{<|c|},x\dot{-}d)\end{aligned}\tag{1}$$

Sei $d=0$. Es folgt $\mathrm{MSP}(\beta^{<|b|},\mathrm{S}x)=\mathrm{MSP}(\gamma^{<|c|},\mathrm{S}x)$ aus der Maximalität von x, also gilt

$$\mathrm{S}(\mathrm{MSP}(\beta^{<|b|},x))=\mathrm{MSP}(\gamma^{<|c|},x)\,.$$

Dann zeigen die schon bewiesenen Axiome (e) und (q)

$$\begin{aligned}&\mathrm{MSP}(\alpha^{<|a|},x)+\mathrm{MSP}(\beta^{<|b|},x)\\ &\quad<\ \mathrm{S}(\mathrm{MSP}(\alpha^{<|a|},x)+\mathrm{MSP}(\beta^{<|b|},x))\\ &\quad=\ \mathrm{MSP}(\alpha^{<|a|},x)+\mathrm{S}(\mathrm{MSP}(\beta^{<|b|},x))\\ &\quad=\ \mathrm{MSP}(\alpha^{<|a|},x)+\mathrm{MSP}(\gamma^{<|c|},x)\,.\end{aligned}$$

Für den Induktionsschritt haben wir die Induktionsvoraussetzung im Falle $d<x$

$$\lfloor\tfrac{1}{2}\bar{\alpha}\rfloor+\lfloor\tfrac{1}{2}\bar{\beta}\rfloor<\lfloor\tfrac{1}{2}\bar{\alpha}\rfloor+\lfloor\tfrac{1}{2}\bar{\gamma}\rfloor$$

mit $\bar{\alpha}:=\mathrm{MSP}(\alpha^{<|a|},x\dot{-}\mathrm{S}d)$ etc. Nun zeigt (f)

$$\mathrm{S}\left(2\cdot(\lfloor\tfrac{1}{2}\bar{\alpha}\rfloor+\lfloor\tfrac{1}{2}\bar{\beta}\rfloor)\right)<2\cdot(\lfloor\tfrac{1}{2}\bar{\alpha}\rfloor+\lfloor\tfrac{1}{2}\bar{\gamma}\rfloor)\,,$$

also folgt aus dem oben gezeigten speziellen Distributivgesetz

$$\begin{aligned} 2 \cdot \lfloor \tfrac{1}{2}\bar{\alpha} \rfloor + 2 \cdot \lfloor \tfrac{1}{2}\bar{\beta} \rfloor &< 2 \cdot \lfloor \tfrac{1}{2}\bar{\alpha} \rfloor + \mathrm{S}(2 \cdot \lfloor \tfrac{1}{2}\bar{\beta} \rfloor) \\ &< 2 \cdot \lfloor \tfrac{1}{2}\bar{\alpha} \rfloor + 2 \cdot \lfloor \tfrac{1}{2}\bar{\gamma} \rfloor \\ &< 2 \cdot \lfloor \tfrac{1}{2}\bar{\alpha} \rfloor + \mathrm{S}(2 \cdot \lfloor \tfrac{1}{2}\bar{\gamma} \rfloor) \,. \end{aligned}$$

Mithin ist

$$2 \cdot \lfloor \tfrac{1}{2}\bar{\alpha} \rfloor + \bar{\beta} < 2 \cdot \lfloor \tfrac{1}{2}\bar{\alpha} \rfloor + \bar{\gamma} \,. \tag{2}$$

Ganz allgemein erhalten wir mit (e)

$$\begin{aligned} (u < v)^w \implies \neg(v \leq u)^w \overset{(e)}{\implies} \neg(v < \mathrm{S}u)^w \implies (\mathrm{S}u \leq v)^w \\ \overset{(e)}{\implies} (\mathrm{S}u < \mathrm{S}v)^w \,. \end{aligned}$$

Auf (2) angewendet ergibt das

$$\mathrm{S}(2 \cdot \lfloor \tfrac{1}{2}\bar{\alpha} \rfloor) + \bar{\beta} < \mathrm{S}(2 \cdot \lfloor \tfrac{1}{2}\bar{\alpha} \rfloor) + \bar{\gamma} \,.$$

In jedem Fall haben wir

$$\bar{\alpha} + \bar{\beta} < \bar{\alpha} + \bar{\gamma}$$

gezeigt.
Durch Induktion folgt (1) für $d = |c|$, also erhalten wir wegen $x \dot{-} |c| = 0$

$$\alpha^{<|a|} + \beta^{<|b|} < \alpha^{<|a|} + \gamma^{<|c|} \,.$$

(u) $(a \cdot 0 = 0)^w$

Sei $t :\equiv T(a, 0)$. Es ist

$$\#z{\leq}|a|(z \leq x \wedge z \in \alpha^{<|a|} \wedge x \dot{-} z \in 0^{<|0|}) = 0$$

für beliebiges x. Also gilt für die Menge ϕ, die

$$\forall i{\leq}|t| \, \forall x{\leq}|t| \, \forall y{\leq}|t| \, (\langle i, x, y \rangle \in \phi \leftrightarrow y = 0)$$

erfüllt und mit (w$\mathbf{\Sigma}_{\mathbf{0}}^{\mathbf{1},\mathbf{w}^\star}$-CA) existiert,

$$\forall i{\leq}|t| \, G(i, a, 0, \alpha, \emptyset, \phi) \,.$$

Mithin ist

$$\alpha^{<|a|} \cdot 0 = \{u < |t| : \langle |t|, u, 1 \rangle \in \phi\} = \{u < |t| : u \neq u\} = 0^{<|0|} \,.$$

(v) $(a \cdot (\mathrm{S}b) = (a \cdot b) + a)^w$

Die Schwierigkeit bei diesem Beweis liegt in der Verknüpfung der scharfen Anfangsstücke mit den Berechnungsfeldern der Multiplikation. Die Idee dabei ist, die Addition auf der ersten Zeile der Berechnungsfelder zu definieren:

$$\sum_{i<|t|} d_i \cdot 2^i + \sum_{i<|t|} e_i \cdot 2^i = \sum_{i<|t|} (d_i + e_i) \cdot 2^i \,,$$

um anschließend dann wie bei der Multiplikation eine Binärdarstellung zu berechnen. Die eigentliche Aufgabe ist zu zeigen, daß diese Berechnung der Addition beweisbar zum richtigen Ergebnis führt.

Zu diesem Zwecke führen wir einige Notationen ein. Sei $t(a) :\equiv T.(a,a) \equiv 2 \cdot (\mathrm{S}a) \cdot (\mathrm{S}a)$ und $\tilde{t}(a) :\equiv \mathrm{SqBd}_3(t(a))$, dann ist $|t(a)| \geq 2 \cdot |a|$. Ein *a-Berechnungsfeld* ist eine Menge γ von Tripeln, für die

$$\begin{aligned} &\forall x{\leq}|t(a)|\, \exists! y{\leq}|t(a)|\, (\langle 0,x,y\rangle \in \gamma) \\ &\quad \wedge \quad \forall x{\leq}|t(a)|\, \forall y{\leq}|t(a)|\, (\langle 0,x,y\rangle \in \gamma \rightarrow \\ &\qquad y \leq |a| \wedge (x \geq |a| \dot{-} 1 \rightarrow y \leq 2 \cdot |a| \dot{-} (\mathrm{S}x))) \end{aligned} \tag{1}$$

und

$$\forall i{\leq}|t(a)|\, (i > 0 \rightarrow G(i,a,a,\gamma)) \tag{2}$$

gilt. Dabei ist G die Formel, die das Berechnungsfeld der Multiplikation beschreibt. Der für $i > 0$ relevante Teil von G ist eine $\mathbf{\Sigma_0^{1,w^\star}}$-Formel. Also ist die Eigenschaft, ein a-Berechnungsfeld zu sein, durch eine $\mathbf{\Sigma_0^{1,w^\star}}$-Formel gegeben. Analog zum Existenz- und Eindeutigkeitsbeweis der Multiplikationsberechnung können wir auch hier durch ($\mathbf{\Sigma_1^{1,w^\star}}$-LIND) und (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) zeigen, daß sich jede Menge mit (1) auf den Tripeln eindeutig zu einem a-Berechnungsfeld fortsetzen läßt.

Nun garantiert (2), daß

$$\forall i{\leq}|t(a)|\, (\langle i, |t(a)|, 0\rangle \in \gamma)$$

und

$$\forall x{\leq}|t(a)|\, \forall y{\leq}|t(a)|\, (\langle |t(a)|, x, y\rangle \in \gamma \rightarrow y \leq 1)$$

gilt. Sei $\mathrm{be}(a,\gamma)$, das Ergebnis des Berechnungsfeldes γ, mit (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) definiert durch

$$\mathrm{be}(a,\gamma) :\equiv \{u : \langle |t(a)|, u, 1\rangle \in \gamma\}^{<|t(a)|} \,,$$

dann ist dies eine Binärdarstellung der Ausgangszeile von γ.

Auf den Berechnungsfeldern sei $+^*$ die Addition, d. h. sind γ_0 und γ_1 a-Berechnungsfelder und δ ein $t(a)$-Berechnungsfeld, dann gilt $\gamma_0 +^* \gamma_1 = \delta$ genau dann, wenn

$$\begin{aligned} &\forall x{\leq}|t(a)|\,\forall y_0{\leq}|a|\,\forall y_1{\leq}|a|\,(\langle 0,x,y_0\rangle \in \gamma_0 \wedge \langle 0,x,y_1\rangle \in \gamma_1 \\ &\qquad \rightarrow \langle 0,x,y_0+y_1\rangle \in \delta) \\ &\wedge \quad \forall x{\leq}|t(t(a))|\,(x > |t(a)| \rightarrow \langle 0,x,0\rangle \in \delta)\,. \end{aligned} \tag{3}$$

Dies ist wiederum eine $\mathbf{\Sigma_0^{1,w^\star}}$-Beschreibung.

Zu a-Berechnungsfeldern γ_0 und γ_1 gibt es mit (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) ein δ mit (3) und der Eigenschaft (1) eines $t(a)$-Berechnungsfeldes. Dies δ läßt sich in eindeutiger Weise zu einem $t(a)$-Berechnungsfeld fortsetzen.

Wir wollen nun zuerst folgende Homomorphieeigenschaft zeigen:

$$\mathrm{be}(t(a), \gamma_0 +^* \gamma_1) = \mathrm{be}(a,\gamma_0) + \mathrm{be}(a,\gamma_1)\,. \tag{4}$$

Dazu verallgemeinern wir $+^*$ auf scharfe Anfangsstücke, indem wir von $\alpha^{<|a|}$ zum kanonischen a-Berechnungsfeld

$$\{\langle i,x,y\rangle \leq |\tilde{t}(a)| : y \leq 1 \wedge (y=1 \leftrightarrow x \in \alpha^{<|a|})\}$$

übergehen, dessen Existenz wieder durch (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) gesichert ist.

Ist γ ein a-Berechnungsfeld, dann gibt es ein (2a+1)-Berechnungsfeld δ mit $\gamma +^* \alpha^{<|a|} = \delta$. Für jedes solche δ gilt

$$\mathrm{be}(2a+1,\delta) = \mathrm{be}(a,\gamma) + \alpha^{<|a|}\,. \tag{5}$$

Beweis:

Sei $\overline{\gamma}^{<|t(a)|} = \mathrm{be}(a,\gamma)$. Durch ($\mathbf{\Sigma_0^{1,w^\star}}$-LIND) zeigen wir für $0 < i \leq |t(a)|$:

$$\begin{aligned} &\forall x{\leq}|t(2a+1)|\,\forall y{\leq}|t(2a+1)|\,\Big[\langle i,x,y\rangle \in \delta \leftrightarrow \\ &\qquad [(\text{ bei } \overline{\gamma}^{<|t(a)|} + \alpha^{<|a|} \text{ tritt} \\ &\qquad\quad \text{kein Übertrag auf die Stelle } x \text{ auf oder } x=0\ ) \\ &\qquad \wedge (x<i \rightarrow y \leq 1 \wedge (y=1 \leftrightarrow (x \notin \alpha^{<|a|} \leftrightarrow x \in \overline{\gamma}^{<|t(a)|}))) \\ &\qquad \wedge (x=i \rightarrow \exists z{\leq}|t(a)|\,(\langle i,i,z\rangle \in \gamma \\ &\qquad\quad \wedge z \leq y \wedge y \leq z+1 \wedge (y=z \leftrightarrow i \notin \alpha^{<|a|})))] \\ &\quad \vee \quad [(\text{ bei } \overline{\gamma}^{<|t(a)|} + \alpha^{<|a|} \text{ tritt ein Übertrag auf die Stelle } x \text{ auf }) \\ &\qquad \wedge (x<i \rightarrow y \leq 1 \wedge (y=1 \leftrightarrow (x \in \alpha^{<|a|} \leftrightarrow x \in \overline{\gamma}^{<|t(a)|}))) \\ &\qquad \wedge (x=i \rightarrow \exists z{\leq}|t(a)|\,(\langle i,i,z\rangle \in \gamma \\ &\qquad\quad \wedge z+1 \leq y \wedge y \leq z+2 \wedge (y=z+1 \leftrightarrow i \notin \alpha^{<|a|})))]\Big] \end{aligned}$$

Dann gilt

$$\begin{aligned}
&\mathrm{be}(2a+1,\delta)\\
&= \{u : \langle |t(2a+1)|, u, 1\rangle \in \delta\}^{<|t(2a+1)|}\\
&= \{u < |t(2a+1)| : [(\text{ bei } \ \overline{\gamma}^{<|t(a)|} + \alpha^{<|a|} \ \text{ tritt}\\
&\qquad\qquad \text{kein Übertrag auf die Stelle } u \text{ auf oder } u = 0\ )\\
&\qquad\quad \wedge (u \notin \alpha^{<|a|} \leftrightarrow u \in \overline{\gamma}^{<|t(a)|})]\\
&\qquad \vee [(\text{ bei } \ \overline{\gamma}^{<|t(a)|} + \alpha^{<|a|} \ \text{ tritt ein Übertrag auf die Stelle } u \text{ auf }\ )\\
&\qquad\quad \wedge (u \in \alpha^{<|a|} \leftrightarrow u \in \overline{\gamma}^{<|t(a)|})]\}\\
&= \overline{\gamma}^{<|t(a)|} + \alpha^{<|a|}\,.
\end{aligned}$$

□

Seien γ, δ a-Berechnungsfelder. Wir zeigen nun durch ($\mathbf{\Sigma_1^{1,w^\star}}$-LIND) nach b

$$\begin{aligned}
&\exists\phi\,\exists\psi\,\Big[\quad \phi^{<|\tilde{t}(a)|} \text{ ist } a\text{-Berechnungsfeld}\\
&\quad\wedge\quad \psi^{<|\tilde{t}(t(a))|} \text{ ist } t(a)\text{-Berechnungsfeld}\\
&\quad\wedge\quad \forall x{\leq}|t(a)|\,\forall y{\leq}|t(a)|\,(\langle 0,x,y\rangle \in \phi^{<|\tilde{t}(a)|} \leftrightarrow\\
&\qquad (y \leq b \wedge \langle 0,x,y\rangle \in \delta) \vee (y = b \wedge \exists z{\leq}|t(a)|\,(\langle 0,x,z\rangle \in \delta \wedge z > b)))\\
&\quad\wedge\quad \psi^{<|\tilde{t}(t(a))|} = \gamma +^* \phi^{<|\tilde{t}(a)|}\\
&\quad\wedge\quad \mathrm{be}(t(a), \psi^{<|\tilde{t}(t(a))|}) = \mathrm{be}(a,\gamma) + \mathrm{be}(a, \phi^{<|\tilde{t}(a)|})\Big]\,,
\end{aligned} \tag{6}$$

für $b = |t(a)|$, dann gilt

$$\begin{aligned}
\phi = \delta \quad &\Longrightarrow \quad \psi = \gamma +^* \delta\\
&\Longrightarrow \quad \mathrm{be}(t(a), \gamma +^* \delta) = \mathrm{be}(a,\gamma) + \mathrm{be}(a,\delta)\,,
\end{aligned}$$

also die gewünschte Homomorphieeigenschaft (4).

Beweis:

Für $b = 0$ sei $\phi = 0$ und $\psi = \gamma$, dann gilt

$$\psi = \gamma +^* \phi$$

und

$$\begin{aligned}
\mathrm{be}(t(a),\psi) &= \mathrm{be}(t(a),\gamma) = \mathrm{be}(a,\gamma) = \mathrm{be}(a,\gamma) + 0\\
&= \mathrm{be}(a,\gamma) + \mathrm{be}(a,\phi)\,.
\end{aligned}$$

Im Induktionsschritt gelte (6) für b, also gibt es Mengen ϕ_0, ψ_0 mit den gewünschten Eigenschaften. Wir definieren a- bzw. $t(a)$-Berechnungsfelder ϕ_1 und ψ_1 durch

$$\begin{aligned}
\langle 0,x,y\rangle \in \phi_1 \quad \leftrightarrow \quad &(y \leq \mathrm{S}b \wedge \langle 0,x,y\rangle \in \delta) \vee\\
&(y = \mathrm{S}b \wedge \exists z{\leq}|t(a)|\,(\langle 0,x,z\rangle \in \delta \wedge z > \mathrm{S}b))
\end{aligned}$$

und

$$\psi_1 = \gamma +^* \phi_1\,.$$

Mit (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) sei

$$\alpha^{<|t(a)|} = \{u : \exists y{\leq}|t(a)|\,(y > \mathrm{S}b \wedge \langle 0, u, y\rangle \in \delta)\}\,.$$

Dann gilt

$$\phi_1 = \phi_0 +^* \alpha^{<|t(a)|}$$

und somit

$$\begin{aligned}\psi_1 &= \gamma +^* \phi_1 = \gamma +^* (\phi_0 +^* \alpha^{<|t(a)|}) = (\gamma +^* \phi_0) +^* \alpha^{<|t(a)|}\\ &= \psi_0 +^* \alpha^{<|t(a)|}\,.\end{aligned}$$

Also gilt mit obigem (5)

$$\begin{aligned}\mathrm{be}(t(a), \psi_1) &\overset{(5)}{=} \mathrm{be}(t(a), \psi_0) + \alpha^{<|t(a)|}\\ &= (\mathrm{be}(a, \gamma) + \mathrm{be}(a, \phi_0)) + \alpha^{<|t(a)|}\\ &= \mathrm{be}(a, \gamma) + (\mathrm{be}(a, \phi_0) + \alpha^{<|t(a)|})\\ &\overset{(5)}{=} \mathrm{be}(a, \gamma) + \mathrm{be}(2a+1, \phi_0 +^* \alpha^{<|t(a)|})\\ &= \mathrm{be}(a, \gamma) + \mathrm{be}(a, \phi_1)\,.\end{aligned}$$

Dabei geht bei dem zweiten „=“ die Induktionsvoraussetzung ein. □

Um jetzt die Rekursionsgleichung zu zeigen, berechnen wir zuerst $\mathrm{S}(\beta^{<|b|})$: Mit ($\mathbf{\Sigma_0^{1,w^\star}}$-LMIN) existiert wegen $|b| \notin \beta^{<|b|}$ ein minimales $w \leq |b|$ mit $w \notin \beta^{<|b|}$. Es gilt also

$$\forall v{\leq}|b|\,(v < w \to v \in \beta^{<|b|})\,.$$

Dann ist

$$\mathrm{S}(\beta^{<|b|}) = \{u : (u > w \wedge u \in \beta^{<|b|}) \vee u = w\}\,.$$

Sei $c := 2{\cdot}\max(a, b){+}1$, dann gibt es c-Berechnungsfelder γ_0 und γ_1, die $\alpha^{<|a|}\cdot\beta^{<|b|}$ und $\alpha^{<|a|}\cdot\mathrm{S}(\beta^{<|b|})$ beschreiben:

$$\begin{aligned}&\langle 0, x, y\rangle \in \gamma_0 \iff\\ y &= \#z{\leq}|b|(z \leq x \wedge z \in \beta^{<|b|} \wedge x \dot{-} z \in \alpha^{<|a|})\\ &= \#z{\leq}|b|(z \leq x \wedge z > w \wedge z \in \beta^{<|b|} \wedge x \dot{-} z \in \alpha^{<|a|})\\ &\quad +\#z{\leq}|b|(z \leq x \wedge z < w \wedge x \dot{-} z \in \alpha^{<|a|})\\ &\langle 0, x, y\rangle \in \gamma_1 \iff\\ y &= \#z{\leq}|2b+1|(z \leq x \wedge z \in \mathrm{S}(\beta^{<|b|}) \wedge x \dot{-} z \in \alpha^{<|a|})\\ &= \#z{\leq}|2b+1|(z \leq x \wedge z > w \wedge z \in \mathrm{S}(\beta^{<|b|}) \wedge x \dot{-} z \in \alpha^{<|a|})\\ &\quad +(x \dot{-} w)_{\alpha^{<|a|}} \cdot 1_{w\leq x}\\ &= \#z{\leq}|b|(z \leq x \wedge z > w \wedge z \in \beta^{<|b|} \wedge x \dot{-} z \in \alpha^{<|a|})\\ &\quad +(x \dot{-} w)_{\alpha^{<|a|}} \cdot 1_{w\leq x}\,.\end{aligned}$$

Wir zeigen nun

$$\mathrm{be}(c,\gamma_1) = \mathrm{be}(c,\gamma_0 +^* \alpha^{<|a|}) \,. \tag{7}$$

Dazu beweisen wir durch ($\mathbf{\Sigma_1^{1,w^*}}$-LIND) nach l

$$\begin{aligned}
&\exists\phi\,\exists\psi\,\Big[\quad \phi^{<|\tilde{t}(c)|} \text{ und } \psi^{<|\tilde{t}(c)|} \text{ sind } c\text{-Berechnungsfelder}\\
&\quad\wedge\quad \phi^{<|\tilde{t}(c)|} = \gamma_0 +^* \alpha^{<|a|}\\
&\quad\wedge\quad \forall x{\leq}|t(c)|\,\forall y{\leq}|t(c)|\,(\langle 0,x,y\rangle \in \psi^{<|\tilde{t}(c)|} \leftrightarrow\\
&\qquad\quad y = \#z{\leq}|b|(z\leq x \wedge z > w \wedge z\in\beta^{<|b|} \wedge x \dot{-} z \in \alpha^{<|a|})\\
&\qquad\quad +\#z{\leq}|b|(z\leq x \wedge z < w \wedge z \geq l \wedge x \dot{-} z \in \alpha^{<|a|})\\
&\qquad\quad +(x \dot{-} l)_{\alpha^{<|a|}} \cdot 1_{l\leq x})\\
&\quad\wedge\quad \mathrm{be}(c,\psi^{<|\tilde{t}(c)|}) = \mathrm{be}(c,\phi^{<|\tilde{t}(c)|})\Big]\,,
\end{aligned} \tag{8}$$

für $l = w \leq |b|$.

Beweis:

Ist $l = 0$, so erfüllt $\psi = \phi = \gamma_0 +^* \alpha^{<|a|}$ die Formel (8). Im Induktionsschritt gelte nach Induktionsvoraussetzung (7) für l. Es gibt also c-Berechnungsfelder ϕ und ψ_0 mit

$$\phi = \gamma_0 +^* \alpha^{<|a|}$$

und

$$\mathrm{be}(c,\phi) = \mathrm{be}(c,\psi_0)\,. \tag{9}$$

Sei μ ein c-Berechnungsfeld mit

$$\begin{aligned}
&\langle 0,x,y\rangle \in \mu \leftrightarrow\\
y \;&=\; \#z{\leq}|b|(z\leq x \wedge z > w \wedge z\in\beta^{<|b|} \wedge x \dot{-} z \in \alpha^{<|a|})\\
&\quad + \#z{\leq}|b|(z\leq x \wedge z < w \wedge z \geq \mathrm{S}l \wedge x \dot{-} z \in \alpha^{<|a|})\,,
\end{aligned}$$

dann gilt

$$\begin{aligned}
\psi_0 \;&=\; (\mu +^* 2^l \cdot \alpha^{<|a|}) +^* 2^l \cdot \alpha^{<|a|}\\
&=\; \mu +^* (2^l \cdot \alpha^{<|a|} +^* 2^l \cdot \alpha^{<|a|})\,.
\end{aligned} \tag{10}$$

Sei ψ_1 ein c-Berechnungsfeld mit

$$\psi_1 = \mu +^* 2^{l+1} \cdot \alpha^{<|a|}\,. \tag{11}$$

Wir erhalten

$$\begin{aligned}
\mathrm{be}(c,\phi) &\overset{(9)}{=} \mathrm{be}(c,\psi_0)\\
&\overset{(10)}{=} \mathrm{be}(c,\mu +^* (2^l\cdot\alpha^{<|a|} +^* 2^l\cdot\alpha^{<|a|}))\\
&= \mathrm{be}(c,\mu) + \mathrm{be}(c, 2^l\cdot\alpha^{<|a|} +^* 2^l\cdot\alpha^{<|a|})\\
&= \mathrm{be}(c,\mu) + (\mathrm{be}(c, 2^l\cdot\alpha^{<|a|}) + \mathrm{be}(c, 2^l\cdot\alpha^{<|a|}))\\
&= \mathrm{be}(c,\mu) + (2^l\cdot\alpha^{<|a|} + 2^l\cdot\alpha^{<|a|})\\
&= \mathrm{be}(c,\mu) + 2^{l+1}\cdot\alpha^{<|a|}\\
&= \mathrm{be}(c,\mu) + \mathrm{be}(c, 2^{l+1}\cdot\alpha^{<|a|})\\
&= \mathrm{be}(c,\mu +^* 2^{l+1}\cdot\alpha^{<|a|})\\
&\overset{(11)}{=} \mathrm{be}(c,\psi_1)\,,
\end{aligned}$$

wobei wir in der fünften und siebten Zeile $l+1+|a| \le |b|+|a| < |c|$ beachten. □

Mithin ist gezeigt:

$$\begin{aligned}
\alpha^{<|a|}\cdot\beta^{<|b|} + \alpha^{<|a|} &= \mathrm{be}(c,\gamma_0) + \mathrm{be}(c,\alpha^{<|a|})\\
&\overset{(4)}{=} \mathrm{be}(c,\gamma_0 +^* \alpha^{<|a|})\\
&\overset{(7)}{=} \mathrm{be}(c,\gamma_1)\\
&= \alpha^{<|a|}\cdot \mathrm{S}(\beta^{<|b|})\,.
\end{aligned}$$

(w) $(a\cdot b = b\cdot a)^w$

Dies folgt sofort aus der Definition der Multiplikation, die wegen

$$\begin{aligned}
&\#z{\le}|a|(z\le x \wedge z\in\alpha^{<|a|} \wedge x\dot{-}z\in\beta^{<|b|})\\
&\quad= \#z{\le}|b|(z\le x \wedge z\in\beta^{<|b|} \wedge x\dot{-}z\in\alpha^{<|a|})
\end{aligned}$$

symmetrisch in $\alpha^{<|a|}$ und $\beta^{<|b|}$ ist.

(x) $((a\cdot b)\cdot 2 = a\cdot(b\cdot 2))^w$

Wie bei der Definition der Multiplikation gezeigt gibt es ϕ und ψ, die $\alpha^{<|a|}\cdot\beta^{<|b|}$ und $\alpha^{<|a|}\cdot\left(\beta^{<|b|}\cdot 2\right)$ beschreiben. Dabei ist $\beta^{<|b|}\cdot 2 = \{u : u>0 \wedge u\dot{-}1\in\beta^{<|b|}\}$. Durch ($\mathbf{\Sigma_0^{1,w^\star}}$-LIND) nach i läßt sich

$$\begin{aligned}
\forall x{\le}|t|\,\forall y{\le}|t|\,[\langle i,x,y\rangle\in\phi \;\leftrightarrow\; &(i=0\wedge\langle 0,\mathrm{S}x,y\rangle\in\psi)\\
&\vee (i>0\wedge\langle \mathrm{S}i,\mathrm{S}x,y\rangle\in\psi)]
\end{aligned}$$

für $i=|t|$ mit $t :\equiv T.(a,b)$ zeigen.

Nun ist

$$\begin{aligned} T.(a, 2\cdot b+1) &\equiv 2\cdot(\mathrm{S}a)\cdot(\mathrm{S}(2\cdot b+1)) \\ &= 2\cdot(\mathrm{S}a)\cdot(2\cdot(\mathrm{S}b)) \;=\; 2\cdot(2\cdot(\mathrm{S}a)\cdot(\mathrm{S}b)) \\ &= 2\cdot t\,, \end{aligned}$$

und da $t>0$ ist, folgt $|T.(a, 2\cdot b+1)| = \mathrm{S}|t| = |2\cdot t+1|$.

Wir beobachten $\langle i,0,0\rangle \in \psi$ für $i \leq \mathrm{S}|t|$. Also gilt für $x \leq \mathrm{S}|t|$

$$\begin{aligned} x \in \left(\alpha^{<|a|}\cdot\beta^{<|b|}\right)\cdot 2 &\leftrightarrow x>0 \wedge x \dot{-} 1 \in \alpha^{<|a|}\cdot\beta^{<|b|} \\ &\leftrightarrow x>0 \wedge \langle |t|, x\dot{-}1, 1\rangle \in \phi \\ &\leftrightarrow x>0 \wedge \langle \mathrm{S}|t|, \mathrm{S}(x\dot{-}1), 1\rangle \in \psi \\ &\leftrightarrow \langle |2\cdot t+1|, x, 1\rangle \in \psi \\ &\leftrightarrow x \in \alpha^{<|a|}\cdot\left(\beta^{<|b|}\cdot 2\right)\,. \end{aligned}$$

Wir fassen unser bisheriges Mühen in Lemma 8.2 zusammen.

8.2 Lemma

Für $A \in \textsc{Basic}(\emptyset)$ gilt $\mathbf{U_2^{1,w^\star}} \vdash A^w$. □

Für die Einbettung von $\mathbf{S_2^i}$ in $\mathbf{U_2^{i,w^\star}}$ treffen wir noch einige technische Vorbereitungen.

8.3 Lemma

Es gilt:

(i) $\neg(A^w) \equiv (\neg A^w)$

(ii) Für $i>0$ gilt

$$A \in \mathbf{\Sigma_i^b} \implies A^w \in \mathbf{\Sigma_i^{U_2^{1,w^\star}}}$$

$$A \in \mathbf{\Pi_i^b} \implies A^w \in \mathbf{\Pi_i^{U_2^{1,w^\star}}}\,.$$

(iii) $\mathbf{U_2^{i,w^\star}} \vdash \neg U^{<|s|} = V^{<|t|}, \neg(A(a))^w_{a,\,\alpha}(s,U), (A(a))^w_{a,\,\alpha}(t,V)$
für beliebige Terme s,t und Klassenterme U,V .

(iv) $(A(t))^w \equiv (A(a))^w_{a,\,\alpha}(T_t, U_t)$.

Beweis:
durch Induktion nach der Länge von A . □

8.4 Satz

Sei $A(a) \in \mathbf{\Sigma^b}$, $B(a,\alpha) :\equiv (A(a))^w$, dann gilt

(i) $\mathbf{U_2^{0,w^\star}} \vdash \neg\forall\phi\, B(T_{|t|}, \phi^{|T_{|t|}|}), \forall x{<}|2\#T_t|\, B(T_{|t|}, U(x))$.

(ii) $\mathbf{U_2^{0,w^\star}} \vdash \neg\exists\phi\, B(T_{|t|}, \phi^{|T_{|t|}|}), \exists x{<}|2\#T_t|\, B(T_{|t|}, U(x))$.

Beweis:

Sei b eine neue Variable. Aus Lemma 8.3 (iii) erhalten wir

$$\mathbf{U_2^{0,w^\star}} \vdash \neg\alpha^{<|T_{|t|}|} = U(b)^{<|T_{|t|}|}, \neg B(T_{|t|}, \alpha^{|T_{|t|}|}), B(T_{|t|}, U(b)) .$$

Nun zeigt die Definition von $\alpha^{<|a|} = \beta^{<|b|}$

$$\mathbf{U_2^{0,w^\star}} \vdash \alpha^{<|T_{|t|}|} = U(b)^{<|T_{|t|}|}, \neg\forall y{<}|T_{|t|}|\, (y \in \alpha^{|T_{|t|}|} \leftrightarrow \mathrm{Bit}(y,b) = 1) .$$

Insgesamt ergibt das

$$\begin{aligned} \mathbf{U_2^{0,w^\star}} \vdash\ & \neg\forall y{<}|T_{|t|}|\, (y \in \alpha^{|T_{|t|}|} \leftrightarrow \mathrm{Bit}(y,b) = 1), \\ & \neg B(T_{|t|}, \alpha^{|T_{|t|}|}), B(T_{|t|}, U(b)) . \end{aligned} \tag{1}$$

(i) (1) führt mit $(\exists^2)$ und $(\forall^2)$ auf

$$\begin{aligned} \mathbf{U_2^{0,w^\star}} \vdash\ & \forall\phi\, \neg\forall y{<}|T_{|t|}|\, (y \in \phi^{|T_{|t|}|} \leftrightarrow \mathrm{Bit}(y,b) = 1), \\ & \exists\phi\, \neg B(T_{|t|}, \phi^{|T_{|t|}|}), B(T_{|t|}, U(b)) . \end{aligned} \tag{2}$$

Es gilt

$$\mathbf{U_2^{0,w^\star}} \vdash \forall y{<}|T_{|t|}|\, (y \le |T_{|t|}| \wedge \mathrm{Bit}(y,b) = 1 \leftrightarrow \mathrm{Bit}(y,b) = 1) .$$

Dann ergibt (w$\mathbf{\Sigma_0^{1,w^\star}}$-CA) :

$$\mathbf{U_2^{0,w^\star}} \vdash \exists\phi\, \forall y{<}|T_{|t|}|\, (y \in \phi^{|T_{|t|}|} \leftrightarrow \mathrm{Bit}(y,b) = 1) .$$

(Schnitt) mit (2) und $(\forall{\le})$ liefern die Behauptung.

(ii) Hier führt (1) mit $(\exists{\le})$ und $(\forall{\le})$ auf

$$\begin{aligned} \mathbf{U_2^{0,w^\star}} \vdash\ & \forall x{\le}|2\#T_t|\, \neg\forall y{<}|T_{|t|}|\, (y \in \alpha^{|T_{|t|}|} \leftrightarrow \mathrm{Bit}(y,x) = 1), \\ & \neg B(T_{|t|}, \alpha^{|T_{|t|}|}), \exists x{\le}|2\#T_t|\, B(T_{|t|}, U(x)) . \end{aligned} \tag{3}$$

Nun zeigt Satz 5.9 für $a = T_t$ unter Ausnutzung von $\big||T_t|\big| \equiv |T_{||}|(T_t) \equiv |T_{|t|}|$

$$\mathbf{U_2^{0,w^\star}} \vdash \exists x{\le}|2\#T_t|\, \forall y{<}|T_{|t|}|\, (y \in \alpha^{|T_{|t|}|} \leftrightarrow \mathrm{Bit}(y,x) = 1) .$$

Ein (Schnitt) mit (3) und $(\forall^2)$ liefert das Gewünschte. □

8.5 Einbettungssatz von $\mathbf{S_2^i}$ in $\mathbf{U_2^{i,w^\star}}$

Sei $i > 0$, $\Gamma \subset \mathbf{\Sigma^b}$ und $\mathbf{S_2^i} \vdash \Gamma$, dann gilt $\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w$.

Beweis:

Mit dem Eliminationssatz 4.14 folgt aus der Voraussetzung $\mathbf{S_2^i} \mid\!\!\frac{m}{1} \Gamma$ für ein $m < \omega$. Nun zeigen wir durch Induktion nach m die Behauptung.

(i) Liegt ein logisches Axiom vor, so folgt mit Lemma 8.3 (i), $(\neg A)^w \equiv \neg A^w$, die Behauptung. Die Definition von $=^w$ als extensionale Mengengleichheit liefert sofort die Reflexivität, Symmetrie und Transitivität von $=^w$. Da die übersetzten Funktionen und Prädikate auf den Mengenextensionen definiert sind, erhalten wir somit alle Gleichheitsaxiome.

(ii) Die Substitutionsinstanzen der Axiome aus $\textsc{Basic}(\emptyset)$ ergeben sich aus den nachgerechneten Axiomen (Lemma 8.2) durch Substitution von $\mathbf{\Delta_1^{U_2^1,w^\star}}$-Klassentermen (Satz 6.7) der Gestalt $U_t = \{u : F_t(u)\}$.

(iii) War der letzte Schluß $(\wedge)$ oder $(\vee)$, so folgt die Behauptung direkt aus der Induktionsvoraussetzung. Fast genau so einfach ist (Schnitt). Hier wird neben der Induktionsvoraussetzung noch Lemma 8.3 (i), $\neg(A^w) \equiv (\neg A)^w$, benötigt.

$(\forall\leq)$ Ohne Einschränkung habe der Schluß die Voraussetzung

$$\mathbf{S_2^i} \mid\!\!\frac{}{1} \Gamma, a \not\leq t, A(a)$$

mit $a \notin \mathsf{FV}(\Gamma, \forall x{\leq}t\, A(x))$. Die Induktionsvoraussetzung liefert daraus

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, (a \not\leq t)^w, (A(a))^w,$$

mithin

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, (a \leq t \to A(a))^w.$$

Da $a \notin \mathsf{FV}(\Gamma)$, sind $a, \alpha \notin \mathsf{FV}(\Gamma^w)$. Außerdem folgt $\Gamma^w \subset \mathbf{\Sigma^{1,w^\star}}$ aus $\Gamma \subset \mathbf{\Sigma^b}$. Dann erhalten wir durch Termersetzung 4.5 (i) und Klassentermersetzung 6.7, da $\alpha^{|T_t|}$ ein $\mathbf{\Sigma_0^{1,w^\star}}$-Klassenterm ist,

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, (a \leq t \to A(a))^w_{a,\,\alpha}(T_t, \alpha^{|T_t|})$$

und mit einem $(\forall^2)$

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, \forall\phi\, (a \leq t \to A(a))^w_{a,\,\alpha}(T_t, \phi^{|T_t|}).$$

Ist $t \equiv |s|$ für einen Term s, so folgt aus Lemma 8.4 (i) mit einem (Schnitt)

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, (\forall x{\leq}t\, A(x))^w$$

wegen

$$\forall x{\leq}|2\#T_s|\, (a \leq |s| \to A(a))^w_{a,\,\alpha}(T_{|s|}, \alpha^{|T_{|s|}|}) \equiv (\forall x{\leq}t\, A(x))^w.$$

Sonst gilt die Behauptung, da in diesem Fall

$$\forall\phi\, (a \leq t \to A(a))^w_{a,\,\alpha}(T_t, \phi^{|T_t|}) \equiv (\forall x{\leq}t\, A(x))^w.$$

($\exists\leq$) Der letzte Schluß hatte die Gestalt

$$\mathbf{S}^{\mathbf{i}}_{\mathbf{2}} \vdash_1 \Gamma, A(t) \implies \mathbf{S}^{\mathbf{i}}_{\mathbf{2}} \vdash_1 \Gamma, t \not\leq s, \exists x{\leq}s\, A(x)\,.$$

Dann liefert die Induktionsvoraussetzung

$$\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \vdash \Gamma^w, (A(t))^w\,. \tag{1}$$

Wir zeigen nun

$$\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \vdash \Gamma^w, (t \not\leq s)^w, \exists\phi\left([a \leq s \wedge A(a)]^w_{a,\,\alpha}(T_s, \phi^{|T_s|})\right), \tag{2}$$

indem wir informal in $\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}}$ argumentieren.
Gelte $\neg\bigvee\Gamma^w$ und $\neg(t \not\leq s)^w$, d. h.

$$U_t^{<|T_t|} \leq U_s^{<|T_s|}\,, \tag{3}$$

dann folgt einerseits aus (1)

$$(A(t))^w\,. \tag{4}$$

Andererseits gilt

$$\left(U_t^{<|T_t|}\right)^{<|T_s|} = U_t^{<|T_t|}\,, \tag{5}$$

da aus $U_t^{<|T_t|}{\leq}U_s^{<|T_s|}$ für $x{\in}U_t^{<|T_t|}$ schon $x{<}|T_s|$ folgt, also die Einschränkung von $U_t^{<|T_t|}$ auf $\left(U_t^{<|T_t|}\right)^{<|T_s|}$ in Wirklichkeit keine ist.
Also folgt mit (5) aus den Gleichheitsaxiomen^w 8.3 (iii) angewandt auf (3)

$$\left(U_t^{<|T_t|}\right)^{<|T_s|} \leq U_s^{<|T_s|}$$

und aus $(A(t))^w \equiv (A(a))^w_{a,\,\alpha}(T_t, U_t)$ 8.3 (iv) und den Gleichheitsaxiomen^w 8.3 (iii) angewandt auf (4)

$$(A(a))^w_{a,\,\alpha}(T_s, U_t^{<|T_t|})\,,$$

mithin

$$(a \leq s \wedge A(a))^w_{a,\,\alpha}(T_s, U_t^{<|T_t|})\,.$$

Analog zu (5) sehen wir

$$\left(U_t^{<|T_t|}\right)^{|T_s|} = U_t^{<|T_t|}\,,$$

also folgt wieder aus den Gleichheitsaxiomen^w 8.3 (iii)

$$(a \leq s \wedge A(a))^w_{a,\,\alpha}\left(T_s, \left(U_t^{<|T_t|}\right)^{|T_s|}\right)\,.$$

Mit (w$\mathbf{\Sigma}^{\mathbf{U}^{\mathbf{1}}_{\mathbf{2}},\mathbf{w}^\star}_{\mathbf{1}}$-CA), die nach Lemma 6.2 in $\mathbf{U}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{2}}$ herleitbar ist, folgt nun

$$\exists\phi\left([a \leq s \wedge A(a)]^w_{a,\,\alpha}(T_s, \phi^{|T_s|})\right),$$

also (2).

Ist nicht $s \equiv |\tilde{s}|$ für einen Term $\tilde{s}$, so sind wir an dieser Stelle fertig. In dem anderen Fall, wo $s \equiv |\tilde{s}|$ für einen Term $\tilde{s}$ ist, zeigt Lemma 8.4 (ii)

$$\begin{aligned}\mathbf{U_2^{0,w^\star}} \vdash\ & \neg\exists\phi\,(A(a))^w_{a,\,\alpha}(T_{|\tilde{s}|}, \phi^{|T_{|\tilde{s}|}|}),\\ & \exists x{\leq}|2\#T_{\tilde{s}}|\,\Big([a \leq |\tilde{s}| \wedge A(a)]^w_{a,\,\alpha}(T_{|\tilde{s}|}, U(x))\Big)\,.\end{aligned}$$

Ein (Schnitt) mit (2) liefert nun

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, (t \not\leq s)^w, (\exists x{\leq}|\tilde{s}|\, A(x))^w\,.$$

($\mathbf{\Sigma_i^b}$-PIND) Als letzter Schluß liegt vor

$$\mathbf{S_2^i} \mid\!\!\!\frac{}{}_1\ \Gamma, \neg A(\lfloor\tfrac{1}{2}b\rfloor), A(b) \implies \mathbf{S_2^i} \mid\!\!\!\frac{}{}_1\ \Gamma, \neg A(0), A(t)$$

mit $b \notin \mathsf{FV}(\Gamma, A(0))$ und $A(a) \in \mathbf{\Sigma_i^b}$. Die Induktionsvoraussetzung zeigt hier mit Lemma 8.3

$$\begin{aligned}\mathbf{U_2^{i,w^\star}} \vdash\ & \Gamma^w, \neg(A(a))^w_{a,\,\alpha}(\lfloor\tfrac{1}{2}b\rfloor, \{u : \mathrm{S}u < |b| \wedge \mathrm{S}u \in \beta\}),\\ & (A(a))^w_{a,\,\alpha}(b, \{u < |b| : u \in \beta\})\,.\end{aligned}$$

Da die Äquivalenz $(\mathrm{S}u < |b| \leftrightarrow u < |\lfloor\tfrac{1}{2}b\rfloor|)$ in $\mathbf{U_2^{i,w^\star}}$ gilt, erhalten wir

$$\begin{aligned}\mathbf{U_2^{i,w^\star}} \vdash\ & \Gamma^w, \neg(A(a))^w_{a,\,\alpha}(\lfloor\tfrac{1}{2}b\rfloor, \{u < |\lfloor\tfrac{1}{2}b\rfloor| : \mathrm{S}u \in \beta\}),\\ & (A(a))^w_{a,\,\alpha}(b, \{u < |b| : u \in \beta\})\,.\end{aligned}$$

Nun wird β durch den $\mathbf{\Delta_1^{U_2^1,w^\star}}$-Klassenterm

$$\{u : |T_t| \dot{-} (|b| \dot{-} u) \in U_t\}$$

ersetzt. Die Herleitbarkeit der entstehenden Formelmenge garantiert Satz 6.7.

$$\begin{aligned}\mathbf{U_2^{i,w^\star}} \vdash\ & \Gamma^w, (A(a))^w_{a,\,\alpha}(b, \{u < |b| : |T_t| \dot{-} (|b| \dot{-} u) \in U_t\}),\\ & \neg(A(a))^w_{a,\,\alpha}(\lfloor\tfrac{1}{2}b\rfloor, \{u < |\lfloor\tfrac{1}{2}b\rfloor| : |T_t| \dot{-} (|b| \dot{-} \mathrm{S}u) \in U_t\})\,.\end{aligned}$$

Da $A(a) \in \mathbf{\Sigma_i^b}$ ist, folgt mit Lemma 8.3 (ii) $(A(a))^w \in \mathbf{\Sigma_i^{U_2^1,w^\star}}$ und, weil U_t aus $\mathbf{\Delta_1^{U_2^1,w^\star}}$ ist, mit Satz 6.8

$$B(b) \mathrel{:\equiv} (A(a))^w_{a,\,\alpha}(b, \{u < |b| : |T_t| \dot{-} (|b| \dot{-} u) \in U_t\}) \in \mathbf{\Sigma_i^{U_2^1,w^\star}}\,.$$

Wir beobachten in $\mathbf{U_2^{i,w^\star}}$

$$\begin{aligned} b > 0 \ &\to\ |b| = \mathrm{S}|\lfloor\tfrac{1}{2}b\rfloor|\\ &\to\ |b| \dot{-} \mathrm{S}u = \mathrm{S}|\lfloor\tfrac{1}{2}b\rfloor| \dot{-} \mathrm{S}u = |\lfloor\tfrac{1}{2}b\rfloor| \dot{-} u\\ b = 0 \ &\to\ |b| \dot{-} \mathrm{S}u = 0 = |\lfloor\tfrac{1}{2}b\rfloor| \dot{-} u\,,\end{aligned}$$

mithin gilt

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, \neg B(\lfloor\tfrac{1}{2}b\rfloor), B(b)\,.$$

Außerdem ist $b \notin \mathsf{FV}(\Gamma^w, B(0))$, also zeigt ($\mathbf{\Sigma_i^{U_2^1,w^\star}}$-PIND)

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, \neg B(0), B(T_t)\,,$$

mithin

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, \neg(A(a))^w_{a,\,\alpha}(0, U_0), (A(a))^w_{a,\,\alpha}(T_t, U_t^{<|T_t|})\,.$$

Das Gleichheitsaxiom^w Lemma 8.3 (iii) im Zusammenhang mit

$$\left(U_t^{<|T_t|}\right)^{<|T_t|} = U_t^{<|T_t|}$$

liefert hieraus

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, \neg(A(a))^w_{a,\,\alpha}(0, U_0), (A(a))^w_{a,\,\alpha}(T_t, U_t)\,.$$

Lemma 8.3 (iv) und (i) produzieren nun

$$\mathbf{U_2^{i,w^\star}} \vdash \Gamma^w, (\neg A(0))^w, (A(t))^w\,. \qquad \square$$

Mit diesem Einbettungssatz läßt sich zeigen, daß die $\mathbf{\Delta_i^P}$-Prädikate, die nach dem Hauptsatz 3.7 $\mathbf{\Delta_i^b}$-definierbar in $\mathbf{S_2^i}$ sind, in $\mathbf{U_2^{i,w^\star}}$ durch $\mathbf{\Delta_i^{1,w^\star}}$-Formeln beschrieben werden. Die Umkehrung dieser Aussage streben wir als nächstes an, um so den Hauptsatz auch für $\mathbf{U_2^{i,w^\star}}$ zu bekommen.

9 Charakterisierung der Polynomialen Hierarchie in $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$

Nachdem wir im letzten Abschnitt gezeigt haben, daß die in $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}$ herleitbaren $\mathbf{\Sigma}^{\mathbf{b}}$-Formeln in „äquivalenter Form“ in $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ beweisbar sind, zeigen wir hier quasi die Umkehrung. Die in $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ herleitbaren $\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}$-Formeln sind in „äquivalenter Form“ in $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A})$ herleitbar. Mit diesem und dem Hauptsatz 3.7 zeigen wir, daß die $\mathbf{\Delta}_{\mathbf{i}}^{\mathbf{p}}$-Prädikate genau diejenigen sind, die durch $\mathbf{\Delta}_{\mathbf{i}}^{\mathbf{1},\mathbf{w}^\star}$-Formeln bezüglich $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ beschrieben werden.

Die Einbettung von $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ in $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A})$ gestaltet sich weitaus einfacher als die in den letzten beiden Abschnitten bewiesene, da wir bei der Übersetzung der zweiten Stufe in die erste nicht die sprachlichen Probleme wie vorher haben. Wir übersetzen

$$\mathrm{Q}\phi\, B(\phi^{|t|}) \quad \text{durch} \quad \mathrm{Q}x{\leq}(4\cdot t+1)\, B(U(x)^{|t|})\,,$$

wobei wie üblich $U(a)$ der Klassenterm $\{u : \mathrm{Bit}(u,a)=1\}$ ist. Die Grenze $4\cdot t+1$ ist richtig gewählt, denn für $t=0$ erhalten wir

$$\sum_{i\leq|0|}(i)_\phi\cdot 2^i \leq 1 = 4\cdot 0+1\,,$$

und für $t>0$ folgt $2^s\leq t<2^{s+1}$ mit $s=|t|-1$, mithin gilt

$$\sum_{i\leq|t|}(i)_\phi\cdot 2^i \leq 2^{|t|+1}-1 = 2^{s+2}-1 = 4\cdot 2^s-1 \leq 4\cdot t-1<4\cdot t+1\,.$$

Da die zu den Funktionszeichen aus $\mathcal{F}^{\mathrm{w}}$ gehörenden Funktionen $\mathbf{\Sigma}_{\mathbf{1}}^{\mathbf{b}}$-definierbar bezüglich $\mathbf{S}_{\mathbf{2}}^{\mathbf{1}}$ sind, können wir nach Korollar 3.5 ohne Einschränkung davon ausgehen, daß sie in $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}$ enthalten sind.

Ein wesentlicher Punkt bei der Durchführung der Einbettung ist, eine erststufige Komprehension in $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A})$ einzusehen.

9.1 Satz

Sei $A(a)$ aus $\mathbf{\Delta}_{\mathbf{1}}^{\mathbf{b}}(\mathcal{A},\mathcal{F}^{\mathrm{w}})$ bezüglich $\mathbf{S}_{\mathbf{2}}^{\mathbf{1}}(\mathcal{A})$, dann gilt

$$\mathbf{S}_{\mathbf{2}}^{\mathbf{1}}(\mathcal{A}) \vdash \exists x{\leq}(4\cdot t+1)\,\forall z{\leq}|t|\,(A(z)\leftrightarrow \mathrm{Bit}(z,x)=1)\,.$$

Beweis:

Sei $B(a) :\equiv \exists x{\leq}((4\cdot a\dot{-}2)+1)\,\forall z{\leq}|a|\,\Big[A(|t|\dot{-}(|a|\dot{-}z))\leftrightarrow \mathrm{Bit}(z,x)=1\Big]\,.$

Wir argumentieren in $\mathbf{S}_{\mathbf{2}}^{\mathbf{1}}(\mathcal{A})$, um $\mathbf{S}_{\mathbf{2}}^{\mathbf{1}}(\mathcal{A})\vdash B(t)$ zu zeigen. Mit der Voraussetzung $A\in\mathbf{\Delta}_{\mathbf{1}}^{\mathbf{b}}(\mathcal{A},\mathcal{F}^{\mathrm{w}})$ bezüglich $\mathbf{S}_{\mathbf{2}}^{\mathbf{1}}(\mathcal{A})$ ist die Formel B aus $\mathbf{\Sigma}_{\mathbf{1}}^{\mathbf{b}}(\mathcal{A},\mathcal{F}^{\mathrm{w}})$. Wir zeigen durch ($\mathbf{\Sigma}_{\mathbf{1}}^{\mathbf{b}}(\mathcal{A},\mathcal{F}^{\mathrm{w}})$-PIND) nach a $B(t)$.

Gilt $A(|t|)$, so sei $x = 1$, ansonsten $x = 0$. In beiden Fällen erhalten wir

$$\forall z{\leq}|0|\left[A(|t|) \leftrightarrow \mathrm{Bit}(z,0) = 1\right],$$

da $\mathrm{Bit}(0,0) = 0$ und $\mathrm{Bit}(0,1) = 1$ ist. Mithin $B(0)$, also ist der Induktionsanfang gezeigt.

Für den Induktionsschritt nehmen wir für beliebiges a

$$B(\lfloor\tfrac{1}{2}a\rfloor) \tag{1}$$

an. Für $a = 0$ folgt daraus schon $B(a)$, also sei $a \neq 0$. Dann gibt es wegen (1) $x \leq (4 \cdot \lfloor\frac{1}{2}a\rfloor \dot{-} 2) + 1$ mit

$$\forall z{\leq}|\lfloor\tfrac{1}{2}a\rfloor|\left[A(|t| \dot{-} (|\lfloor\tfrac{1}{2}a\rfloor| \dot{-} z)) \leftrightarrow \mathrm{Bit}(z,x) = 1\right]. \tag{2}$$

Gilt $A(|t| \dot{-} |a|)$, so sei $\tilde{x} = 2 \cdot x + 1$, sonst $\tilde{x} = 2 \cdot x$. Beide Mal erhalten wir

$$A(|t| \dot{-} |a|) \leftrightarrow \mathrm{Bit}(0,\tilde{x}), \tag{3}$$

da $\mathrm{Bit}(0, 2 \cdot x) = 0$ und $\mathrm{Bit}(0, 2 \cdot x + 1) = 1$ ist.

Wir zeigen nun

$$\forall z{\leq}|a|\left[A(|t| \dot{-} (|a| \dot{-} z)) \leftrightarrow \mathrm{Bit}(z,\tilde{x}) = 1\right]$$

Ist $z = 0$, so gilt mit (3)

$$A(|t| \dot{-} (|a| \dot{-} 0)) \leftrightarrow A(|t| \dot{-} |a|) \leftrightarrow \mathrm{Bit}(0,\tilde{x}) = 1.$$

Für $0{<}z{\leq}|a|$ sei $\tilde{z} := z \dot{-} 1$, so daß $z{=}\mathrm{S}\tilde{z}$ gilt. Nun wird $|a|{=}\mathrm{S}|\lfloor\frac{1}{2}a\rfloor|$ von $a{>}0$ impliziert, mithin ist $\tilde{z} \leq |\lfloor\frac{1}{2}a\rfloor|$. Wir beobachten $\mathrm{Bit}(\mathrm{S}\tilde{z},\tilde{x}) = \mathrm{Bit}(\tilde{z},x)$, also gilt

$$\begin{aligned}
A(|t| \dot{-} (|a| \dot{-} z)) &\leftrightarrow A(|t| \dot{-} (\mathrm{S}(|\lfloor\tfrac{1}{2}a\rfloor|) \dot{-} \mathrm{S}\tilde{z})) \\
&\leftrightarrow A(|t| \dot{-} (|\lfloor\tfrac{1}{2}a\rfloor| \dot{-} \tilde{z})) \\
&\overset{(2)}{\leftrightarrow} \mathrm{Bit}(\tilde{z},x) = 1 \\
&\leftrightarrow \mathrm{Bit}(\mathrm{S}\tilde{z},\tilde{x}) = 1 \\
&\leftrightarrow \mathrm{Bit}(z,\tilde{x}) = 1.
\end{aligned}$$

Nun bleibt noch zu zeigen, daß $\tilde{x} \leq (4 \cdot a \dot{-} 2) + 1$ ist. Nach Voraussetzung ist $x \leq (4 \cdot \lfloor\frac{1}{2}a\rfloor \dot{-} 2) + 1$, also gilt

$$\begin{aligned}
a = 1: &\quad 2 \cdot x \leq 2 \cdot x + 1 \leq 2 \cdot ((4 \cdot 0 \dot{-} 2) + 1) + 1 = (4 \cdot 1 \dot{-} 2) + 1 \\
a > 1: &\quad 2 \cdot x \leq 2 \cdot x + 1 \leq 2 \cdot ((4 \cdot \lfloor\tfrac{1}{2}a\rfloor \dot{-} 2) + 1) + 1 \\
&\quad \leq 2 \cdot ((2 \cdot a \dot{-} 2) + 1) + 1 = (4 \cdot a \dot{-} 2) + 1.
\end{aligned}$$

Mithin erhalten wir $B(a)$, was den Induktionsschritt vollendet.

Durch P-Induktion folgt nun $B(t)$, also die Behauptung. □

9.2 Definition der Übersetzung $\circ : \mathbf{\Sigma^{1,w^\star}} \longrightarrow \mathbf{\Sigma^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$

durch Induktion nach der Länge der Formel A.

(a) Ist A atomar, so sei $A^\circ :\equiv A$.

(b) Ist $A \equiv B \circ C$ mit $\circ \in \{\wedge, \vee\}$, dann definieren wir $A^\circ :\equiv B^\circ \circ C^\circ$.

(c) Hat A die Gestalt $\mathrm{Q}x_k{\leq}|t|\, B(x_k)$ mit $\mathrm{Q} \in \{\forall, \exists\}$ und ist a eine neue Variable, dann sei

$$A^\circ :\equiv \mathrm{Q}x_{2k}{\leq}|t|\, (B(a))^\circ_a(x_{2k}) .$$

(d) Ist $A \equiv \mathrm{Q}\phi_k\, B(\phi_k^{|t|})$ mit $\mathrm{Q} \in \{\forall, \exists\}$ und ist α eine neue Variable, dann sei

$$A^\circ :\equiv \mathrm{Q}x_{2k+1}{\leq}(4 \cdot t + 1)\, (B(\alpha))^\circ_\alpha(\{u \leq |t| : \mathrm{Bit}(u, x_{2k+1}) = 1\}) .$$

Für $\Gamma = \{A_1, \ldots, A_n\}$ sei $\Gamma^\circ = \{A_1^\circ, \ldots, A_n^\circ\}$.

9.3 Lemma

Es gilt

(i) $\neg A^\circ \equiv (\neg A)^\circ$

(ii) Sei $i \geq 0$:

$$A \in \mathbf{\Sigma_i^{1,w^\star}} \quad \Longrightarrow \quad A^\circ \in \mathbf{\Sigma_i^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$$
$$A \in \mathbf{\Pi_i^{1,w^\star}} \quad \Longrightarrow \quad A^\circ \in \mathbf{\Pi_i^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$$

(iii) $A \in \mathbf{\Sigma_0^{1,w^\star}} \implies A^\circ \equiv A$

(iv) $(A(t))^\circ \equiv (A(a))^\circ_a(t)$

(v) $(A(\{u : B(u)\}))^\circ \equiv (A(\alpha))^\circ_\alpha(\{u : B^\circ(u)\})$

Punkt (iv) erlaubt uns einfach $A^\circ(a)$ zu schreiben.

Beweis:

durch Induktion nach der Länge von A. □

Bevor wir uns dem Einbettungssatz zuwenden, müssen wir eine Einsetzung von $\mathbf{\Sigma_0^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$-Klassentermen in eine $\mathbf{\Sigma^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$ Formelmenge Γ für $\mathbf{S_2^i}(\mathcal{A})$ beweisen. Da in $\mathbf{S_2^i}(\mathcal{A})$ keine Komprehensionsregel zur Verfügung steht, ist hier ganz wesentlich, daß keine Formel aus Γ einen zweitstufigen Quantor enthält, daß also $\Gamma \subset \mathbf{\Sigma^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$ gilt. Später in der Anwendung im Einbettungssatz betrachten wir Formelmengen aus $\mathbf{\Sigma^{1,w^\star}}$. Deren Übersetzung ist dann eine $\mathbf{\Sigma^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$-Formelmenge. Also spielt die Einschränkung keine Rolle.

9.4 Lemma

Ist $A(a) \in \mathbf{\Sigma^b_0}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$ und $\Gamma \subset \mathbf{\Sigma^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$ mit $\mathsf{BV}(\Gamma) \cap \mathsf{BV}(A) = \emptyset$, dann gilt

$$\mathbf{S^i_2}(\mathcal{A}) \vdash \Gamma \implies \mathbf{S^i_2}(\mathcal{A}) \vdash \Gamma\alpha(A(.)) .$$

Beweis:

Zuerst beobachten wir analog zu 4.9 (i), daß für beliebige Formeln F

$$\forall i \quad \begin{array}{ll} \text{(i)} & F \in \mathbf{\Sigma^b_i}(\mathcal{A}, \mathcal{F}^{\mathrm{w}}) \implies F\alpha(A(.)) \in \mathbf{\Sigma^b_i}(\mathcal{A}, \mathcal{F}^{\mathrm{w}}) \\ \text{(ii)} & F \in \mathbf{\Pi^b_i}(\mathcal{A}, \mathcal{F}^{\mathrm{w}}) \implies F\alpha(A(.)) \in \mathbf{\Pi^b_i}(\mathcal{A}, \mathcal{F}^{\mathrm{w}}) \end{array}$$

gilt. Der Schnitteliminationssatz 4.14 zeigt

$$\mathbf{S^i_2}(\mathcal{A}) \mid\!\!\!\frac{}{}_1 \Gamma .$$

Nun können wir analog zu 4.10 (i) durch Herleitungsinduktion die Behauptung zeigen, da in dieser Konstellation nie $(\forall^2)$ oder $(\exists^2)$ angewandt wurde (die Hauptformel des Schlusses wäre sonst nicht mehr in $\mathbf{\Sigma^b}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$). □

Da die Übersetzung $^\circ$ nur für Formeln aus $\mathbf{\Sigma^{1,w^\star}}$ Sinn macht, können wir den Einbettungssatz auch nur für $\Gamma \subset \mathbf{\Sigma^{1,w^\star}}$ beweisen.

9.5 Einbettungssatz von $\mathbf{U^{i,w^\star}_2}$ in $\mathbf{S^i_2}(\mathcal{A})$

Sei $i > 0$, $\Gamma \subset \mathbf{\Sigma^{1,w^\star}}$ und $\mathbf{U^{i,w^\star}_2} \vdash \Gamma$, dann gilt $\mathbf{S^i_2}(\mathcal{A}) \vdash \Gamma^\circ$.

Beweis:

Mit dem Eliminationssatz 4.14 erhalten wir $\mathbf{U^{i,w^\star}_2} \mid\!\!\!\frac{m}{}_1 \Gamma$ für ein $m < \omega$. Nun zeigen wir durch Induktion nach m $\mathbf{S^i_2}(\mathcal{A}) \vdash \Gamma^\circ$.

(i) Die Axiome von $\mathbf{U^{i,w^\star}_2}$ sind in $\mathbf{S^1_2}(\mathcal{A})$ beweisbar.

(ii) War der letzte Schluß einer von $(\wedge)$, $(\vee)$, $(\forall\leq)$, $(\exists\leq)$, so folgt die Behauptung direkt aus der Induktionsvoraussetzung. Liegt ein (Schnitt) vor, so liefert die Induktionsvoraussetzung mit $\neg A^\circ \equiv (\neg A)^\circ$ das Gewünschte. Die Induktionsvoraussetzung ist in diesem Fall anwendbar, da durch den Schnittgrad von 1 garantiert ist, daß die Schnittformel auch aus $\mathbf{\Sigma^{1,w^\star}}$ ist.

$(\forall^2)$ Da $\Gamma \subset \mathbf{\Sigma^{1,w^\star}}$ vorausgesetzt ist, liege ohne Einschränkung folgender Schluß vor:

$$\mathbf{U^{i,w^\star}_2} \mid\!\!\!\frac{}{}_1 \Gamma, F(\alpha^{|t|}) \implies \mathbf{U^{i,w^\star}_2} \mid\!\!\!\frac{}{}_1 \Gamma, \forall\phi\, F(\phi^{|t|})$$

mit $\alpha \notin \mathsf{FV}\left(\Gamma, \forall\phi\, F(\phi^{|t|})\right)$.

Dann liefert die Induktionsvoraussetzung mit Lemma 9.3 (v)

$$\mathbf{S^i_2}(\mathcal{A}) \vdash \Gamma^\circ, (F(\alpha))^\circ_\alpha(\alpha^{|t|}) .$$

Nun ersetzen wir α durch den Klassenterm $\{u : \mathrm{Bit}(u, a) = 1\}$ für eine neue Variable a, die Herleitbarkeit zeigt Lemma 9.4.

$$\mathbf{S^i_2}(\mathcal{A}) \vdash \Gamma^\circ, (F(\alpha))^\circ_\alpha(\{u \leq |t| : \mathrm{Bit}(u, a) = 1\}) .$$

Mithin

$$\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A}) \vdash \Gamma^\circ, \forall x{\leq}(4\cdot t+1)\,(F(\alpha))^\circ_\alpha(\{u \leq |t| : \mathrm{Bit}(u,x)=1\})\,.$$

($\exists^2$) Da nach Voraussetzung $\Gamma \subset \mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}$ ist, habe der letzte Schluß die Gestalt

$$\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \mid\!\!\!\frac{}{}_1\ \Gamma, F(\alpha^{|t|}) \implies \mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \mid\!\!\!\frac{}{}_1\ \Gamma, \exists\phi\, F(\phi^{|t|})\,.$$

Wir schreiben $F(\alpha^{|t|}) \equiv F(\{u \leq |t| : u \in \alpha\})$ und fassen somit, da $(a \in \alpha) \in \mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{0}}$ ist, diesen Schluß als (w$\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{0}}$-CA) auf.

($\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{i}}$-LIND) Hier liegt für $a \notin \mathsf{FV}(\Gamma, A(0))$, $A(a) \in \mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{i}}$ der folgende Schluß vor

$$\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \mid\!\!\!\frac{}{}_1\ \Gamma, \neg A(a), A(\mathrm{S}a) \implies \mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \mid\!\!\!\frac{}{}_1\ \Gamma, \neg A(0), A(|t|)\,.$$

Daraus liefert die Induktionsvoraussetzung mit Lemma 9.3

$$\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A}) \vdash \Gamma^\circ, \neg A^\circ(a), A^\circ(\mathrm{S}a)\,.$$

Weiterhin beobachten wir mit Lemma 9.3

$$a \notin \mathsf{FV}(\Gamma, A^\circ(0)) \quad \text{und} \quad A^\circ(a) \in \mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{i}}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})\,.$$

Also beweist ($\mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{i}}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$-LIND)

$$\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A}) \vdash \Gamma^\circ, \neg A^\circ(0), A^\circ(|t|)\,.$$

(w$\mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{0}}$-CA) Der interessanteste Fall sieht wie folgt aus:

$$\mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \mid\!\!\!\frac{}{}_1\ \Gamma, F(\{u \leq |t| : A(u)\}) \implies \mathbf{U}^{\mathbf{i},\mathbf{w}^\star}_{\mathbf{2}} \mid\!\!\!\frac{}{}_1\ \Gamma, \exists\phi\, F(\phi^{|t|})$$

mit $A \in \mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{0}}$. Mit der Induktionsvoraussetzung schließen wir hieraus

$$\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A}) \vdash \Gamma^\circ, (F(\{u \leq |t| : A(u)\}))^\circ$$

und mit Lemma 9.3 (v) und (iii)

$$\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A}) \vdash \Gamma^\circ, F^\circ(\{u \leq |t| : A(u)\})\,. \tag{1}$$

Wir beobachten für eine neue Variable b

$$\begin{aligned}\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A}) \vdash\ & \neg\forall z{\leq}|t|\,(A(z) \leftrightarrow \mathrm{Bit}(z,b)=1),\\ & \neg F^\circ(\{u \leq |t| : A(u)\}), F^\circ(\{u \leq |t| : \mathrm{Bit}(u,b)=1\})\,,\end{aligned}$$

woraus mit (1) und ($\exists{\leq}$), ($\forall{\leq}$) folgt:

$$\begin{aligned}\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}(\mathcal{A}) \vdash\ & \Gamma^\circ, \exists x{\leq}(4\cdot t+1)\, F^\circ(\{u \leq |t| : \mathrm{Bit}(u,x)=1\}),\\ & \forall x{\leq}(4\cdot t+1)\,\neg\forall z{\leq}|t|\,(A(z) \leftrightarrow \mathrm{Bit}(z,x)=1)\,.\end{aligned}$$

Da aus $A \in \mathbf{\Sigma}^{\mathbf{1},\mathbf{w}^\star}_{\mathbf{0}} = \mathbf{\Sigma}^{\mathbf{b}}_{\mathbf{0}}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$ offensichtlich $A \in \mathbf{\Delta}^{\mathbf{b}}_{\mathbf{1}}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$ bezüglich $\mathbf{S}^{\mathbf{1}}_{\mathbf{2}}(\mathcal{A})$ folgt, liefert ein (Schnitt) mit Satz 9.1 das Gewünschte. □

Wir möchten nun mit Hilfe der beiden Einbettungssätze 8.5 und 9.5 via der Bussschen Charakterisierung der Polynomialen Hierarchie 3.7 eine für $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ erlangen. Dazu müssen wir noch zeigen, daß die $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A})$-Herleitungen von $\mathbf{\Sigma}^{\mathbf{b}}$-Formeln schon in $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}$-Herleitungen umgewandelt werden können. Dies ist möglich, da in solchen Herleitungen zweitstufige Variablen ausschließlich als Parametervariablen auftreten und diese sich durch $\emptyset$ ersetzen lassen.

9.6 Lemma

Für $\Gamma \subset \mathbf{\Sigma}^{\mathbf{b}}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$, dessen freie Mengenvariablen unter $\alpha_1, \ldots, \alpha_k$ auftreten, gilt

$$\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A}) \vdash \Gamma \implies \mathbf{S}_{\mathbf{2}}^{\mathbf{i}} \vdash \Gamma_{\vec{\alpha}}(\vec{\emptyset}) .$$

Beweis:

Der Eliminationssatz 4.14 zeigt $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A}) \left|\frac{m}{1}\right. \Gamma$ für ein $m < \omega$. Wir zeigen durch Induktion nach m die Behauptung.

Zu jeder Formel F sei $F' :\equiv F_{\vec{\alpha}}(\vec{\emptyset})$, wobei die freien Mengenvariablen von F unter $\alpha_1, \ldots, \alpha_k$ auftreten sollen.

(i) Liegt ein Axiom vor, welches α nicht enthält, so ist nichts zu zeigen, da alle Axiome von $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A})$, die keine Mengenvariablen enthalten, schon Axiome von $\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}$ sind. In den anderen Fällen folgt die Behauptung schon aus dem Gleichheitsaxiom $t = t$.

(ii) War der letzte Schluß kein (Schnitt), so folgt die Behauptung direkt aus der Induktionsvoraussetzung.

(iii) Der letzte Schluß war ein (Schnitt):

$$\mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A}) \left|\frac{m_1}{1}\right. \Gamma, F \quad \text{und} \quad \mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A}) \left|\frac{m_2}{1}\right. \Gamma, F \implies \mathbf{S}_{\mathbf{2}}^{\mathbf{i}}(\mathcal{A}) \left|\frac{m}{1}\right. \Gamma$$

mit $m_1, m_2 < m$. Da der Schnittgrad 1 ist, muß $\mathbf{\Sigma}^{\mathbf{b}}\text{-}\mathsf{rg}(F) = 0$ sein, also auch $F \in \mathbf{\Sigma}^{\mathbf{b}}(\mathcal{A}, \mathcal{F}^{\mathrm{w}})$. Die Induktionsvoraussetzung produziert

$$\mathbf{S}_{\mathbf{2}}^{\mathbf{i}} \vdash \Gamma', F' \quad \text{und} \quad \mathbf{S}_{\mathbf{2}}^{\mathbf{i}} \vdash \Gamma', \neg F'$$

und ein (Schnitt) liefert

$$\mathbf{S}_{\mathbf{2}}^{\mathbf{i}} \vdash \Gamma' .$$

□

9.7 Hauptsatz für $\mathbf{U_2^{i,w^\star}}$

Ist $i > 0$, so gilt folgende Äquivalenz:

$$\mathrm{A} \in \mathbf{\Delta_i^p} \iff \mathrm{A} \text{ ist in } \mathbf{\Delta_i^{1,w^\star}} \text{ bezüglich } \mathbf{U_2^{i,w^\star}} .$$

Beweis:

Der Beweis benutzt den aus [Buss 1986] übernommenen Hauptsatz 3.7:

$$\mathrm{A} \in \mathbf{\Delta_i^p} \quad \text{genau dann, wenn} \quad \mathrm{A} \text{ in } \mathbf{\Delta_i^b} \text{ bezüglich } \mathbf{S_2^i} \text{ ist.} \tag{1}$$

„$\Longrightarrow$“ Ist $\mathrm{A} \in \mathbf{\Delta_i^p}$, dann existieren wegen (1) $B, \neg C \in \mathbf{\Sigma_i^b}$ mit $\mathsf{FV}(B,C) \subset \{a_1, \ldots, a_\mathrm{k}\}$,

$$\mathbf{S_2^i} \vdash B \leftrightarrow C \tag{2}$$

und $\mathrm{A}(\vec{n}) \iff B(\vec{n}) \iff C(\vec{n})$ für alle $\vec{n} \in \mathbb{N}^k$. Sei

$$F(\vec{a}) :\equiv B^w_{\alpha_1, \ldots, \alpha_\mathrm{k}}(U(a_1), \ldots, U(a_\mathrm{k})) \in \mathbf{\Sigma_i^{1,w^\star}} ,$$

$$G(\vec{a}) :\equiv C^w_{\alpha_1, \ldots, \alpha_\mathrm{k}}(U(a_1), \ldots, U(a_\mathrm{k})) \in \mathbf{\Pi_i^{1,w^\star}} ,$$

dann gilt für alle $\vec{n} \in \mathbb{N}^k$ mit dem Korrektheitssatz 7.4 der Übersetzung ^{w}

$$F(\vec{n}) \overset{7.4}{\iff} B(\vec{n}) \iff \mathrm{A}(\vec{n}) \iff C(\vec{n}) \overset{7.4}{\iff} G(\vec{n}) .$$

Mit dem Eliminationssatz 4.14 folgt aus (2) $\mathbf{S_2^i} \mid\!\!\!\frac{}{1} B \leftrightarrow C$. Darauf angewendet zeigt Satz 8.5 $\mathbf{U_2^{i,w^\star}} \vdash (B \leftrightarrow C)^w$, also folgt mit dem Einsetzungssatz 6.7

$$\mathbf{U_2^{i,w^\star}} \vdash F \leftrightarrow G .$$

Mithin ist A in $\mathbf{\Delta_i^{1,w^\star}}$ bezüglich $\mathbf{U_2^{i,w^\star}}$.

„$\Longleftarrow$“ Ist A in $\mathbf{\Delta_i^{1,w^\star}}$ bezüglich $\mathbf{U_2^{i,w^\star}}$, dann gibt es $F, \neg G \in \mathbf{\Sigma_i^{1,w^\star}}$ mit $\mathsf{FV}(F,G) \subset \{a_1, \ldots, a_\mathrm{k}\}$,

$$\mathbf{U_2^{i,w^\star}} \vdash F \leftrightarrow G \tag{3}$$

und $\mathrm{A}(\vec{n}) \iff F(\vec{n}) \iff G(\vec{n})$ für alle $\vec{n} \in \mathbb{N}^k$.

Wieder folgt mit dem Eliminationssatz 4.14 $\mathbf{U_2^{i,w^\star}} \mid\!\!\!\frac{}{1} F \leftrightarrow G$ und daraus mit Satz 9.5 $\mathbf{S_2^i}(\mathcal{A}) \vdash (F \leftrightarrow G)^\circ$. Nun sind $F^\circ, \neg G^\circ \in \mathbf{\Sigma_i^b}$, da F und G keine Mengenvariablen enthalten, also erhalten wir unter Ausnutzung des vorherigen Lemmas

$$\mathbf{S_2^i} \vdash F^\circ \leftrightarrow G^\circ .$$

Nach Konstruktion gilt

$$F^\circ(\vec{n}) \iff F(\vec{n}) \iff \mathrm{A}(\vec{n}) \iff G(\vec{n}) \iff G^\circ(\vec{n})$$

für alle $\vec{n} \in \mathbb{N}^k$, also ist A in $\mathbf{\Delta_i^b}$ bezüglich $\mathbf{S_2^i}$. Mit (1) erhalten wir $\mathrm{A} \in \mathbf{\Delta_i^p}$. □

Mit diesem Hauptsatz ist das Ziel des zweiten Teils erreicht. Die Funktionen der Polynomialen Hierarchie lassen sich auf diesem Weg nicht in $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ definieren, denn wir erhalten mit dem Hauptsatz 3.7 und dem Einbettungssatz 8.5 aus $f \in \mathbf{\Box}_{\mathbf{i}}^{\mathbf{p}}$ die Existenz einer Formel $A \in \mathbf{\Sigma}_{\mathbf{i}}^{\mathbf{1},\mathbf{w}^\star}$ und eines Terms t mit

$$\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star} \vdash \forall \vec{x}\, \exists \Psi\, A(\vec{x}, \Psi^{|t|}) \qquad \text{und} \qquad f(\vec{x}) = y \iff A(\vec{x}, U(y)^{|t|})\,,$$

wobei wieder $U(y) \equiv \{u : \mathrm{Bit}(u, y) = 1\}$ ist. Um nun auf $\forall \vec{x}\, \exists y{\leq}(4 \cdot t + 1)\, A(\vec{x}, U(y))$ schließen zu können, müßten wir eine Komprehension in der Form

$$\exists y{\leq}4 \cdot t + 1\, \forall z{\leq}|t| \left(\mathrm{Bit}(z, y) = 1 \leftrightarrow z \in \alpha^{|t|}\right)$$

in $\mathbf{U}_{\mathbf{2}}^{\mathbf{i},\mathbf{w}^\star}$ beweisen, was sich aber in Abschnitt 14 als unmöglich herausstellen wird.

Teil C

Eine Methode zum Beweis von Unbeweisbarkeiten in U_2^w

10 Ein halbformales System für die Beschränkte Arithmetik

Zu Anfang dieses Abschnitts definieren wir ein halbformales System und beweisen einen Schnitteliminationssatz dafür. Danach zeigen wir, daß auf Grund der besonderen Struktur der $\mathbf{\Sigma^{1,b}}$-Formeln (sie enthalten nur beschränkte erststufige Quantoren) einer Formel F unter ihnen, die ohne freie Individuenvariablen ist, ein endlicher Abschnitt $\{0,\ldots,t_F\}$ von $\mathbb{N}$ zugeordnet werden kann, der die Gültigkeit von F im Standardmodell entscheidet:

$$\mathbb{N} \models F \iff \{0,\ldots,t_F\} \models F\,.$$

Dadurch lassen sich in solchen Formeln F Teilformeln der Gestalt $Q\phi\, G(\phi)$ mit $Q \in \{\forall, \exists\}$ durch *endliche* Konjunktionen bzw. Disjunktionen

$$\overline{Q}\{G(M) : M \subset \{0,\ldots,t_F\}\}$$

ersetzen, wobei $\overline{\forall} \equiv \bigwedge$ und $\overline{\exists} \equiv \bigvee$ ist. Daher können wir zu solchen $\mathbf{\Sigma^{1,b}}$-Formeln äquivalente $\mathbf{\Sigma_0^{1,b}}$-Formeln konstruieren und auf diesem Wege mit der ($\mathbf{\Sigma_0^{1,b}}$-CA)-Regel die ($\mathbf{\Sigma^{1,b}}$-CA)-Regel beweisen.
Insgesamt läßt sich sowohl $\mathbf{U_2^w}$ mit seiner ($\mathbf{\Sigma^{1,b}}$-CA)-Regel in das halbformale System einbetten als auch nur unter Verwendung prädikativer Methoden die vollständige Schnittelimination für das halbformale System beweisen.
Die hier verwendeten Methoden im Umgang mit halbformalen Systemen werden in ähnlicher Form in [Pohlers 1989] vorgestellt. Die Definition der Ordinalzahlen sowie hier verwendete elementare Eigenschaften lese man z. B. in [Pohlers 1989] nach.

P ist die in Abschnitt 1 definierte Menge aller Funktionen, die durch eine Turingmaschine in polynomialer Zeit berechnet werden. Mit dem Hauptsatz 3.7 sind sie $\mathbf{\Sigma_1^b}$-definierbar in $\mathbf{S_2^1}$, mithin $\mathbf{\Sigma_0^{1,b}}$-definierbar in $\mathbf{U_2^0}$. Wir gehen ab jetzt für den Rest der Arbeit davon aus, daß $\mathbf{\Sigma_i^{1,b}}$ über $\mathbf{L_{BA}^P}$ gebildet ist, also ehemals $\mathbf{\Sigma_i^{1,b}}(\mathbf{P})$ entspricht.
Das halbformale System verwendet die ($\mathbf{\Sigma_0^{1,b}}$-CA)-Regel, also Komprehensionen von Formeln ohne zweitstufige Quantoren. Um nun hier mit dem klassischen Gentzenschen Schnitteliminationsverfahren zu einem Ergebnis zu kommen, benötigen wir eine geschickte Rangdefinition, die Formeln $Q\phi\, F(\phi)$ einen größeren Rang zuweist als $F(A(.))$ für beliebige $\mathbf{\Sigma_0^{1,b}}$-Formeln $A(a)$. Aus diesem Grund lassen wir den Rang von F beim ersten zweitstufigen Quantor auf ω springen, in den übrigen Fällen zählen wir die Tiefe der induktiven Definition von F.

10.1 Definition des Rangs $\mathsf{b\text{-}rg} : \mathbf{\Sigma^{1,b}} \longrightarrow \omega * 2$

(a) Ist F eine Primformel, so sei $\mathsf{b\text{-}rg}(F) := 0$.

(b) Ist $F \equiv G \circ H$ mit $\circ \in \{\wedge, \vee\}$, dann sei
$\mathsf{b\text{-}rg}(F) := \mathrm{Max}(\mathsf{b\text{-}rg}(G), \mathsf{b\text{-}rg}(H)) + 1$.

(c) Ist $F \equiv \mathrm{Q}x{\leq}t\, G(x)$ mit $\mathrm{Q} \in \{\forall, \exists\}$, dann sei $\mathsf{b\text{-}rg}(F) := \mathsf{b\text{-}rg}(G(a)) + 1$.

(d) Ist $F \equiv \mathrm{Q}\phi\, G(\phi)$ mit $\mathrm{Q} \in \{\forall, \exists\}$, dann sei
$\mathsf{b\text{-}rg}(F) := \mathrm{Max}(\omega, \mathsf{b\text{-}rg}(G(\alpha)) + 1)$.

Durch die geschickte Verwendung von ω in der obigen Rangdefinition erreichen wir die Abgeschlossenheit des Rangs oberhalb von ω gegen Substitution von $\mathbf{\Sigma_0^{1,b}}$-Klassentermen.

10.2 Lemma

Sei $A(a) \in \mathbf{\Sigma_0^{1,b}}$ mit einziger freien Individuenvariablen a und $F(\alpha) \in \mathbf{\Sigma^{1,b}}$, dann gilt für alle $\rho \geq \omega$

$$\mathsf{b\text{-}rg}(F) < \rho \implies \mathsf{b\text{-}rg}(F(A(.))) < \rho\,.$$

Beweis:

Wir zeigen die Behauptung simultan für beliebiges $\rho \geq \omega$ durch Induktion nach der Länge von F. Sei $F' :\equiv F(A(.))$.

(i) F ist eine Primformel. Da der Rang erststufiger Formeln kleiner als ω ist, erhalten wir $\mathsf{b\text{-}rg}(F(\{u : A(u)\})) < \omega \leq \rho$.

(ii) Ist $F \equiv G \circ H$ mit $\circ \in \{\wedge, \vee\}$, dann ist $\mathsf{b\text{-}rg}(F) = \mathrm{Max}(\mathsf{b\text{-}rg}(G), \mathsf{b\text{-}rg}(H)) + 1$. Ist $\mathsf{b\text{-}rg}(F) < \omega$, so auch $\mathsf{b\text{-}rg}(G)$ und $\mathsf{b\text{-}rg}(H)$. Damit liefert die Induktionsvoraussetzung $\mathsf{b\text{-}rg}(G'), \mathsf{b\text{-}rg}(H') < \omega$, mithin

$$\mathsf{b\text{-}rg}(F') = \mathrm{Max}(\mathsf{b\text{-}rg}(G'), \mathsf{b\text{-}rg}(H')) + 1 < \omega \leq \rho\,.$$

Ist $\mathsf{b\text{-}rg}(F) \geq \omega$, dann folgt aus $\mathsf{b\text{-}rg}(G), \mathsf{b\text{-}rg}(H) < \mathsf{b\text{-}rg}(F)$ mit der Induktionsvoraussetzung $\mathsf{b\text{-}rg}(G'), \mathsf{b\text{-}rg}(H') < \mathsf{b\text{-}rg}(F)$, also

$$\mathsf{b\text{-}rg}(F') = \mathrm{Max}(\mathsf{b\text{-}rg}(G'), \mathsf{b\text{-}rg}(H')) + 1 < \mathsf{b\text{-}rg}(F) + 1 \leq \rho\,.$$

(iii) Ist $F \equiv \mathrm{Q}x{\leq}t\, G(x)$ mit $\mathrm{Q} \in \{\forall, \exists\}$, dann ist $\mathsf{b\text{-}rg}(F) = \mathsf{b\text{-}rg}(G(a)) + 1$. Wie unter (ii) folgt aus $\mathsf{b\text{-}rg}(F) < \omega$ schon $\mathsf{b\text{-}rg}(F') < \omega \leq \rho$ und aus $\mathsf{b\text{-}rg}(F) \geq \omega$ mit $\mathsf{b\text{-}rg}(G) < \mathsf{b\text{-}rg}(F)$ und der Induktionsvoraussetzung

$$\mathsf{b\text{-}rg}(F') = \mathsf{b\text{-}rg}(G') + 1 < \mathsf{b\text{-}rg}(F) + 1 \leq \rho\,.$$

(iv) Ist $F \equiv \mathrm{Q}\phi\, G(\phi)$ mit $\mathrm{Q} \in \{\forall, \exists\}$, dann ist $\rho > \omega$ wegen $\mathsf{b\text{-}rg}(F) = \mathrm{Max}(\omega, \mathsf{b\text{-}rg}(G(\alpha)) + 1) \geq \omega$. Ist $\mathsf{b\text{-}rg}(G') < \omega$, so gilt

$$\mathsf{b\text{-}rg}(F') = \mathrm{Max}(\omega, \mathsf{b\text{-}rg}(G') + 1) = \omega < \rho\,.$$

Im anderen Fall liefert die Induktionsvoraussetzung aus $\mathsf{b\text{-}rg}(G) < \mathsf{b\text{-}rg}(F)$

$$\mathsf{b\text{-}rg}(F') = \mathsf{b\text{-}rg}(G') + 1 < \mathsf{b\text{-}rg}(F) + 1 \leq \rho\,. \qquad \square$$

Im halbformalen System ist die Struktur der natürlichen Zahlen in den erststufigen Bereich hineindefiniert. Es werden daher nur Formelmengen ohne freie Individuenvariablen hergeleitet. Eine Induktionsregel ist dann überflüssig, jede einzelne Anwendung wird durch endlich viele Schnitte ersetzt.
Wir betrachten in dem halbformalen System nur $\mathbf{\Sigma^{1,b}}$-Formeln, daher verwenden wir auch nur beschränkte $(\forall)$-Schlüsse. Also existiert keine volle ω-Regel, die Herleitungsbäume sind immer nur endlich verzweigt, insbesondere auch bei der Einbettung der Induktionsregel aus dem formalen System. Dies hat zur Folge, daß wir hier im Gegensatz zur Schnittelimination für die Peano Arithmetik immer mit endlichen Herleitungslängen auskommen.
Die Menge M in der anschließenden Definition von $M \mid\!\!\frac{m}{\rho}\, \Gamma$ dient zur Kontrolle von zusätzlichen Regeln, die später bei den Anwendungen angegeben werden. Die hier vorgestellte Version des halbformalen Systems wird von M nicht beeinflußt. Die Größen m und ρ sind wie üblich obere Schranken für die Tiefe des Herleitungsbaumes sowie für die Ränge der in der Herleitung verwendeten Schnittformeln, wobei ρ eine echte obere Schranke ist. Für jede natürliche Zahl i sei $\underline{i}$ der Term $\underbrace{\mathrm{S}\ldots\mathrm{S}}_{i\text{-mal}}0$. Wir identifizieren in der Folge häufig i mit $\underline{i}$ sowie t mit $t^{\mathbf{N}}$. Es wird an den entsprechenden Stellen immer klar sein, ob die natürliche Zahl oder ihr repräsentierender Term bzw. der Term oder seine Auswertung gemeint sind.

10.3 Induktive Definition von $M \mid\!\!\frac{m}{\rho}\, \Gamma$

für $M \subset_{\text{fin}} \mathbb{N}$, $m < \omega$, $\rho < \omega \cdot 2$ und $\Gamma \subset \mathbf{\Sigma^{1,b}}$ ohne freie Individuenvariablen.

Axiome:

(a) Ist $(s^{\mathbf{N}}, t^{\mathbf{N}}) \in P^{\mathbf{N}}$ für $P \in \{=, \neq, \leq, \not\leq\}$, so gelte $M \mid\!\!\frac{m}{\rho}\, \Gamma, (Pst)$.

(b) Ist $s^{\mathbf{N}} = t^{\mathbf{N}}$, so gelte $M \mid\!\!\frac{m}{\rho}\, \Gamma, s \in \alpha, t \notin \alpha$.

Schlüsse:

$(\wedge)$ $M \mid\!\!\frac{m_i}{\rho}\, \Gamma, A_i$ für $i = 0$ und $i = 1$ $\implies$ $M \mid\!\!\frac{m}{\rho}\, \Gamma, A_0 \wedge A_1$

$(\vee)$ $M \mid\!\!\frac{m'}{\rho}\, \Gamma, A_i$ für $i = 0$ oder $i = 1$ $\implies$ $M \mid\!\!\frac{m}{\rho}\, \Gamma, A_1 \vee A_2$

$(\forall\leq)$ $M \mid\!\!\frac{m_i}{\rho}\, \Gamma, F(\underline{i})$ für alle $i \leq t^{\mathbf{N}}$ $\implies$ $M \mid\!\!\frac{m}{\rho}\, \Gamma, \forall x{\leq}t\, F(x)$

$(\exists\leq)$ $M \mid\!\!\frac{m'}{\rho}\, \Gamma, F(\underline{i})$ für ein $i \leq t^{\mathbf{N}}$ $\implies$ $M \mid\!\!\frac{m}{\rho}\, \Gamma, \exists x{\leq}t\, F(x)$

$(\forall^2)$ $M \mid\!\!\frac{m'}{\rho}\, \Gamma, F(\alpha)$ und $\alpha \notin \mathsf{FV}(\Gamma, \forall\phi\, F(\phi))$ $\implies$ $M \mid\!\!\frac{m}{\rho}\, \Gamma, \forall\phi\, F(\phi)$

$(\exists^2)$ $M \mid\!\!\frac{m'}{\rho}\, \Gamma, F(\alpha)$ $\implies$ $M \mid\!\!\frac{m}{\rho}\, \Gamma, \exists\phi\, F(\phi)$

$(\mathbf{\Sigma^{1,b}_0}\text{-CA})$ $M \mid\!\!\frac{m'}{\rho}\, \Gamma, F(A(.))$ mit $A(a) \in \mathbf{\Sigma^{1,b}_0}$ $\implies$ $M \mid\!\!\frac{m}{\rho}\, \Gamma, \exists\phi\, F(\phi)$

(Schnitt) $M \mid\!\!\frac{m_0}{\rho}\, \Gamma, F$, $M \mid\!\!\frac{m_1}{\rho}\, \Gamma, \neg F$ und $\mathsf{b\text{-}rg}(F) < \rho$ $\implies$ $M \mid\!\!\frac{m}{\rho}\, \Gamma$

für $m > m'$, $m > m_0, m_1$ bzw. $m > m_0, \ldots, m_{t^{\mathbb{N}}}$. Wie üblich schreiben wir

$$M \mid\!\!\frac{m}{\rho}\!\!- \Gamma \iff \text{es existiert ein } m < \omega \text{ mit } M \mid\!\!\frac{m}{\rho}\!\!- \Gamma$$

$$M \vdash \Gamma \iff \text{es existiert ein } \rho < \omega \cdot 2 \text{ mit } M \mid\!\!\frac{}{\rho}\!\!- \Gamma$$

$$\vdash \Gamma \iff \text{es existiert ein } M \subset_{\text{fin}} \mathbb{N} \text{ mit } M \vdash \Gamma$$

Die Begriffe Hauptformel eines Axioms oder einer Regel werden hier wie gehabt benutzt.

In dem halbformalen System läßt sich die Komprehension nicht als Axiom formulieren, da sprachlich keine unbeschränkten erststufigen Quantoren zugelassen sind.
Wir beobachten, daß Strukturschlüsse erlaubt sind sowie Terme durch gleichwertige ersetzt werden können. Die Beweise erfolgen jeweils durch Herleitungsinduktion.

10.4 Lemma

$M \mid\!\!\frac{m}{\rho}\!\!- \Gamma$ und $M \subset M'$, $\Gamma \subset \Gamma'$, $m \leq m'$, $\rho \leq \rho' \implies M' \mid\!\!\frac{m'}{\rho'}\!\!- \Gamma'$. □

10.5 Gleichheitslemma

Ist $s^{\mathbf{N}} = t^{\mathbf{N}}$ und gilt $M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, F(s)$, dann gilt auch $M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, F(t)$. □

Für das Einsetzungslemma nutzen wir die oben bewiesene Abgeschlossenheit der Rangdefinition unter Substitution von $\mathbf{\Sigma_0^{1,b}}$-Klassentermen oberhalb von ω aus.

10.6 Einsetzungslemma

Gilt $M \mid\!\!\frac{m}{\rho}\!\!- \Gamma$ für $\rho \geq \omega$ und ist $A(a) \in \mathbf{\Sigma_0^{1,b}}$ mit einziger freien Variablen a, so folgt $M \mid\!\!\frac{}{\rho}\!\!- \Gamma_\alpha(A(.))$.

Beweis durch Induktion nach m:
Dies geht analog zum Einsetzungslemma 4.10 (i) unter Ausnutzung von Lemma 10.2. □

10.7 Inversionslemma

(i) $M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, F$ und F ist eine unwahre Primformel $\implies M \mid\!\!\frac{m}{\rho}\!\!- \Gamma$.

(ii) $M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, A_0 \wedge A_1 \implies M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, A_i$ für $i = 0$ und $i = 1$.

(iii) $M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, \forall x{\leq}t\, F(x) \implies M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, F(s)$ für Terme s mit $s^{\mathbf{N}} \leq t^{\mathbf{N}}$.

(iv) $M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, \forall \phi\, F(\phi) \implies M \mid\!\!\frac{m}{\rho}\!\!- \Gamma, F(\alpha)$ für α beliebig.

Beweis durch Induktion nach m:
(i) Eine unwahre Primformel kann nie Hauptformel eines Axioms gewesen sein.

(ii) - (iv) Diese Punkte werden wie im Inversionslemma 4.12 bewiesen, wobei in (iii) noch das Gleichheitslemma 10.5 eingeht. □

Zur Erinnerung ist eine Formel F vom $\vee$-Typ, wenn sie eine negative Primformel oder von der Gestalt $(A \vee B)$, $(\exists x\, A_a(x))$, $(\exists x{\leq}t\, A_a(x))$ oder $(\exists \phi\, A_\alpha(\phi))$ ist.

10.8 Reduktionslemma

Ist F vom $\vee$-Typ mit $\mathsf{b\text{-}rg}(F) = \rho$, dann gilt

$$M \mid\!\!\frac{m}{\rho}\ \Gamma, F \quad \text{und} \quad M \mid\!\!\frac{}{\rho}\ \Lambda, \neg F \implies M \mid\!\!\frac{}{\rho}\ \Gamma, \Lambda\,.$$

Beweis durch Induktion nach m:

Ist Γ, F ein Axiom und F nicht die Hauptformel, so ist mit Γ auch Γ, Λ ein Axiom. Ist F eine Hauptformel des Axioms, so werden folgende Fälle unterschieden:

(i) F ist eine wahre Primformel, dann folgt mit dem Lemma 10.7 (i) $M \mid\!\!\frac{}{\rho}\ \Lambda$ und mit einem Strukturschluß 10.4 $M \mid\!\!\frac{}{\rho}\ \Gamma, \Lambda$.

(ii) Ist $F \equiv s \notin \alpha$, dann muß es ein t mit $s^{\mathbf{N}} = t^{\mathbf{N}}$ und $(t \in \alpha) \in \Gamma$ geben, da nur ein Axiom der Gestalt (b) vorliegen kann. Das Gleichheitslemma 10.5 zeigt $M \mid\!\!\frac{}{\rho}\ \Lambda, t \in \alpha$, und mit einem Strukturschluß 10.4 folgt $M \mid\!\!\frac{}{\rho}\ \Gamma, \Lambda$.

Sei also Γ, F kein Axiom und (S) ein letzter Schluß. War F nicht die Hauptformel von (S), so wenden wir die Induktionsvoraussetzung auf die Prämissen von (S) an und führen anschließend wieder (S) aus, analog zum Reduktionslemma 4.13.

Übrig bleiben die Fälle, in denen F Hauptformel von (S) und vom $\vee$-Typ ist.

($\vee$) Ist $F \equiv A \vee B$, dann folgt die Behauptung aus der Induktionsvoraussetzung durch einen (Schnitt) der Prämisse mit der Inversion der zweiten Voraussetzung 10.7 (ii).

($\exists{\leq}$) Ist $F \equiv \exists x{\leq}t\, G(x)$, dann hat die Prämisse von (S) für ein $m' < m$ und ein $s^{\mathbf{N}} \leq t^{\mathbf{N}}$ die Gestalt

$$M \mid\!\!\frac{m'}{\rho}\ \Gamma, \exists x{\leq}t\, G(x), G(s)\,.$$

Also liefert die Induktionsvoraussetzung

$$M \mid\!\!\frac{}{\rho}\ \Gamma, \Lambda, G(s)\,.$$

Hieraus folgt die Behauptung durch einen (Schnitt) mit der Inversion der zweiten Voraussetzung 10.7 (iii).

($\exists^2$) Dieser Schluß läßt sich als ($\mathbf{\Sigma^{1,b}_0}$-CA) auffassen.

($\mathbf{\Sigma^{1,b}_0}$-CA) Ist $F \equiv \exists \phi\, G(\phi)$, dann hat die Prämisse von (S) für ein $m' < m$ und $A(a) \in \mathbf{\Sigma^{1,b}_0}$ mit $A(0)$ erststufig geschlossen die Gestalt

$$M \mid\!\!\frac{m'}{\rho}\ \Gamma, \exists \phi\, G(\phi), G(A(.))\,.$$

Daraus liefert die Induktionsvoraussetzung

$$M \vdash_\rho \Gamma, \Lambda, G(A(.))\,. \tag{1}$$

Das Inversionslemma 10.7 (iv) zusammen mit dem Einsetzungslemma 10.6 und der Beobachtung $\rho = \mathsf{b\text{-}rg}(\exists\phi\, G(\phi)) \geq \omega$ produzieren

$$M \vdash_\rho \Gamma, \Lambda, \neg G(A(.))\,. \tag{2}$$

Aus $\mathsf{b\text{-}rg}(G(\alpha)) < \rho$ folgt mit Lemma 10.2 $\mathsf{b\text{-}rg}(G(A(.))) < \rho$ und darum durch einen Schnitt von (1) und (2)

$$M \vdash_\rho \Gamma, \Lambda\,. \qquad \square$$

Die später bei den Anwendungen hinzuzufügenden Axiome und Regeln haben allesamt die Eigenschaft, daß deren Hauptformeln die Gestalt $s \in \alpha$ für spezielle Terme s haben und somit nicht vom $\vee$-Typ sind. Da außerdem die neuen Axiome und Regeln so formuliert sein werden, daß das Gleichheitslemma 10.5 wieder gilt, läßt sich dann das Reduktionslemma wortwörtlich übernehmen.

Das auf den ersten Blick verblüffende an dem nachstehenden Eliminationssatz ist, daß die Herleitungslänge endlich bleibt, obwohl der Schnittrang größer als ω sein kann. Die Begründung dafür ist die, daß ein Herleitungsbaum aufgrund der ausschließlichen Verwendung der *beschränkten* ω-Regel an jedem Knoten nur endlich verzweigt und darum insgesamt nur endlich viele Knoten und damit auch Schnitte enthält. Insbesondere läßt sich bei einer solchen Herleitung mit Schnittrang ω ein maximaler *endlicher* Schnittrang ablesen, wohingegen bei endlichen Herleitungen mit unbeschränkter ω-Regel das Supremum aller Schnittränge ω sein kann.

10.9 Eliminationssatz

$$M \vdash^m_\rho \Gamma \implies M \vdash^n_0 \Gamma \text{ für ein } n < \omega\,.$$

Beweis durch Hauptinduktion nach ρ und Nebeninduktion nach m:

Ist Γ ein Axiom, so ist nichts zu zeigen. Sei also Γ kein Axiom und (S) ein letzter Schluß. Ist (S) kein (Schnitt), so folgt die Behauptung direkt aus der Nebeninduktionsvoraussetzung mit demselben Schluß (S). Bleibt also noch der Fall

$$\text{(Schnitt)} \qquad M \vdash^{m_0}_\rho \Gamma, F \quad \text{und} \quad M \vdash^{m_1}_\rho \Gamma, \neg F \implies M \vdash^m_\rho \Gamma$$

mit $m_0, m_1 < m$ und $\rho' := \mathsf{b\text{-}rg}(F) < \rho$. Nun liefert die Nebeninduktionsvoraussetzung

$$M \vdash_0 \Gamma, F \quad \text{und} \quad M \vdash_0 \Gamma, \neg F\,.$$

Hieraus folgt mit einem Strukturschluß 10.4 und dem Reduktionslemma 10.8

$$M \vdash_{\rho'} \Gamma\,.$$

Mit der Hauptinduktionsvoraussetzung folgt nun die Behauptung. $\square$

Wir zeigen nun, daß im halbformalen System ($\mathbf{\Sigma^{1,b}}$-CA) als Regel beweisbar ist. Die Idee dabei ist, die Tatsache, daß alle erststufigen Quantoren der Formeln in $\mathbf{\Sigma^{1,b}}$ beschränkt sind, in der Form auszunutzen, daß wir zu einer Formel $F \in \mathbf{\Sigma^{1,b}}$ einen Term t_F angeben, der den Abschnitt $\{0,\dots,t_F\}$ definiert, auf dem F lebt:

$$\mathbb{N} \models F \iff \{0,\dots,t_F\} \models F\,.$$

Dadurch erreichen wir eine Beschränkung der zweitstufigen Quantoren von außen; sie laufen also nicht mehr über die gesamte Potenzmenge $\mathcal{P}(\mathbb{N})$, sondern nur noch über die endliche Menge $\mathcal{P}(\{0,\dots,t_F\})$. Deshalb können sie im halbformalen System durch endliche Disjunktionen bzw. Konjunktionen ersetzt werden.
Wir benutzen die Funktion σ aus 3.12, die zu einem Term eine Majorante liefert.

10.10 Definition

Für $F \in \mathbf{\Sigma^{1,b}}$ mit $\mathsf{FV}(F) = \{\vec{b},\vec{\beta}\}$ und $m \in \mathbb{N}$ definieren wir Terme t_F und Beschränkungen F^m, so daß $\mathsf{FV}(t_F) = \{\vec{b}\}$ und $\mathsf{FV}(F^m) = \{\vec{b},\vec{\beta}\}$ ist.

(a) Ist $F \equiv (Pst)$ für $P \in \{=,\neq,\leq,\not\leq\}$, so sei $t_F :\equiv s+t$ und $F^m :\equiv F$.

(b) Ist $F \equiv s \in \beta$ oder $F \equiv s \notin \beta$, so sei $t_F :\equiv s$ und $F^m :\equiv F$.

(c) Für $F \equiv G \circ H$ mit $\circ \in \{\wedge,\vee\}$ sei $t_F :\equiv t_G + t_H$ und $F^m :\equiv G^m \circ H^m$.

(d) Für $F \equiv \mathrm{Q}x{\leq}s\,G(x)$ mit $\mathrm{Q} \in \{\forall,\exists\}$, sei $t_F :\equiv \sigma[t_{G(a)}]a(s)$ und $F^m :\equiv \mathrm{Q}x{\leq}s\,G^m(x)$.

(e) Ist $F \equiv \mathrm{Q}\phi\,G(\phi)$ mit $\mathrm{Q} \in \{\forall,\exists\}$, so sei $t_F :\equiv t_{G(\alpha)}$ und $F^m :\equiv \mathrm{Q}\phi\,G^m(\phi^m)$.

10.11 Lemma

Sei $F(\vec{b},\vec{\beta}) \in \mathbf{\Sigma^{1,b}}$ mit $\mathsf{FV}(F) \supset \{b_1,\dots,b_k,\beta_1,\dots,\beta_l\}$ ohne weitere freie Individuenvariablen. Dann gilt für $A_1(a),\dots,A_l(a) \in \mathbf{\Sigma^{1,b}}$, in denen höchstens die freie Individuenvariable a auftritt:

(i) $\forall \vec{n} \in \mathbb{N}^k\, \forall m \geq t_F(\vec{n}) \quad \vdash F^{\vec{}}_{\vec{b},\,\vec{\beta}}\big(\vec{n}, A_1(.),\dots,A_l(.)\big) \leftrightarrow$
$$F^{\vec{}}_{\vec{b},\,\vec{\beta}}\big(\vec{n}, \{u \leq m : A_1(u)\},\dots,\{u \leq m : A_l(u)\}\big)$$

(ii) $\forall \vec{n} \in \mathbb{N}^k\, \forall m \geq t_F(\vec{n}) \quad \vdash F^{\vec{}}_{\vec{b}}(\vec{n}) \leftrightarrow F^{m\,\vec{}}_{\vec{b}}(\vec{n})$.

Beweis durch Induktion nach der Länge von F:

Da $\neg F^m \equiv (\neg F)^m$ ist, genügt es, sich auf die Fälle, daß F vom $\vee$-Typ ist, zu beschränken, d. h., daß F eine negative Primformel ist oder eine der folgenden Gestalten hat: $G \vee H, \exists x{\leq}t\, G(x), \exists \phi\, G(\phi)$. Die anderen folgen dann durch Negation.

(i) Es ergeben sich alle Fälle bis auf die folgenden sofort aus der Induktionsvoraussetzung. Abkürzend schreiben wir

$$F' :\equiv F^{\vec{}}_{\vec{b},\,\vec{\beta}}\Big(\vec{n}, A_1(.), \ldots, A_l(.)\Big)$$

und

$$F'' :\equiv F^{\vec{}}_{\vec{b},\,\vec{\beta}}\Big(\vec{n}, \{u \leq m : A_1(u)\}, \ldots, \{u \leq m : A_l(u)\}\Big)\,.$$

(a) Sei F eine Primformel. Dann ist nur etwas zu zeigen, falls $\beta_i \in \mathsf{FV}(F)$ ist. Ohne Einschränkung sei $i{=}1$, also $F \equiv s{\notin}\beta_1$. Für $m{\geq}t_F(\vec{n}){=}s(\vec{n})$ gilt

$$\vdash s(\vec{n}) \leq m\,. \tag{1}$$

Es ist

$$F' \equiv \neg A_1(s(\vec{n}))$$

und

$$F'' \equiv s(\vec{n}) \not\leq m \vee \neg A_1(s(\vec{n}))\,.$$

Mit (1) gilt $\vdash F' \leftrightarrow F''$.

(b) Sei $F \equiv \exists x{\leq}s\, G(x)$. Hier ist $t_F \equiv \sigma[t_{G(a)}]a(s)$ und für $\vec{n} \in \mathbb{N}^k$

$$F' \equiv \exists x{\leq}s(\vec{n})\, G\Big(x, \vec{n}, A_1(.), \ldots, A_l(.)\Big)$$

$$F'' \equiv \exists x{\leq}s(\vec{n})\, G\Big(x, \vec{n}, \{u \leq m : A_1(u)\}, \ldots, \{u \leq m : A_l(u)\}\Big)\,.$$

Dann gilt nach Induktionsvoraussetzung

$$\forall l \in \mathbb{N}\, \forall m \geq t_{G(a)}(\vec{n}, l) \quad \vdash G\Big(l, \vec{n}, A_1(.), \ldots, A_l(.)\Big) \leftrightarrow G\Big(l, \vec{n}, \{u \leq m : A_1(u)\}, \ldots, \{u \leq m : A_l(u)\}\Big)\,.$$

Wir beobachten für $m \geq t_F(\vec{n})$

$$l \leq s(\vec{n}) \implies t_{G(a)}(\vec{n}, l) \leq \sigma[t_{G(a)}]^{\vec{}}_{\vec{b},\,a}(\vec{n}, s(\vec{n})) \leq m\,,$$

daher folgt aus der Induktionsvoraussetzung

$$l \leq s(\vec{n}) \implies \vdash G\Big(l, \vec{n}, A_1(.), \ldots, A_l(.)\Big) \leftrightarrow G\Big(l, \vec{n}, \{u \leq m : A_1(u)\}, \ldots, \{u \leq m : A_l(u)\}\Big)\,. \tag{2}$$

Also erhalten wir dann im halbformalen System

$$\begin{aligned} F' &\leftrightarrow \text{für ein } l \leq s(\vec{n}) \text{ gilt } G\Big(l, \vec{n}, A_1(.), \ldots, A_l(.)\Big) \\ &\overset{(2)}{\leftrightarrow} \text{für ein } l \leq s(\vec{n}) \text{ gilt } G\Big(l, \vec{n}, \{u \leq m : A_1(u)\}, \ldots, \{u \leq m : A_l(u)\}\Big) \\ &\leftrightarrow F''\,. \end{aligned}$$

(ii) Der einzige Fall, der nicht direkt aus der Induktionsvoraussetzung folgt, ist $F \equiv \exists\phi\, G(\phi)$. Dann ist $t_F \equiv t_{G(\alpha)}$ und

$$F^m \equiv \exists\phi\, G^m(\phi^m) \equiv \exists\phi\, G^m(\{u \leq m : u \in \phi\}) .$$

Mit der Induktionsvoraussetzung gilt für $m \geq t_F(\vec{n})$ im halbformalen System

$$G(\vec{n},\alpha) \leftrightarrow G^m(\vec{n},\alpha) \overset{(i)}{\leftrightarrow} G^m(\vec{n},\alpha^m) ,$$

also folgt

$$\vdash \exists\phi\, G(\vec{n},\phi) \leftrightarrow \exists\phi\, G^m(\vec{n},\phi^m) . \qquad \square$$

Den Vorteil, den wir durch diese Beschränkungen F^m für natürliche Zahlen m und Formeln $F \in \mathbf{\Sigma^{1,b}}$ erhalten, ist der, daß wir nun zu F^m äquivalente $\mathbf{\Sigma_0^{1,b}}$-Formeln konstruieren können.

10.12 Definition

Zu $\mathcal{M} \subset_{\text{fin}} \mathbb{N}$ sei $\overline{\mathcal{M}}$ folgender $\mathbf{\Sigma_0^{1,b}}$-Klassenterm

$$\overline{\mathcal{M}} := \{u : 0 \neq 0 \vee \bigvee_{i \in \mathcal{M}} (u = \underline{i})\} .$$

Zu $F \in \mathbf{\Sigma^{1,b}}$ definieren wir Formeln $\overline{F^m}$ für Primformeln als Identität und in den übrigen Fällen homomorph bis auf

$$F \equiv \forall\phi\, G(\phi) \implies \overline{F^m} :\equiv \bigwedge \left\{\overline{G^m}(\overline{\mathcal{M}}) : \mathcal{M} \subset \{0,\ldots,m\}\right\}$$
$$F \equiv \exists\phi\, G(\phi) \implies \overline{F^m} :\equiv \bigvee \left\{\overline{G^m}(\overline{\mathcal{M}}) : \mathcal{M} \subset \{0,\ldots,m\}\right\} .$$

10.13 Lemma

Ist $F \in \mathbf{\Sigma^{1,b}}$ und $m \in \mathbb{N}$, so gilt $\overline{F^m} \in \mathbf{\Sigma_0^{1,b}}$. $\square$

10.14 Satz

Für $F \in \mathbf{\Sigma^{1,b}}$ mit den freien Individuenvariablen $b_1,\ldots,b_k$ gilt

$$\forall \vec{n}, m \in \mathbb{N}^{k+1} \qquad \vdash F^m(\vec{n}) \leftrightarrow \overline{F^m}(\vec{n}) .$$

Beweis durch Induktion nach der Länge von F:

Da $\left(\neg\overline{F^m}\right) \equiv \overline{(\neg F)^m}$ ist, können wir uns auf F vom $\vee$-Typ beschränken, denn sonst erhalten wir die Behauptung durch Negation aus dem schon Gezeigten. Alle übriggebliebenen Fälle bis auf den nachstehenden folgen direkt aus der Induktionsvoraussetzung.

Ist $F \equiv \exists\phi\, G(\phi)$, so ist $F^m \equiv \exists\phi\, G^m(\phi^m)$. Um nun die Behauptung zu zeigen, seien $\vec{n}, m \in \mathbb{N}^{k+1}$. Die Induktionsvoraussetzung liefert

$$\vdash G^m(\beta,\vec{n}) \leftrightarrow \overline{G^m}(\beta,\vec{n}) . \qquad (1)$$

Im weiteren unterdrücken wir $\vec{n}$, um die Übersicht ein wenig zu erhöhen. Es bleiben zwei Richtungen zu zeigen.

„$\leftarrow$“ Für $\mathcal{M} \subset \{0,\ldots,m\}$ folgt aus (1) mit dem Einsetzungslemma 10.6, da $\overline{\mathcal{M}} \in \mathbf{\Sigma_0^{1,b}}$ ist,

$$\vdash \neg\overline{G^m}(\overline{\mathcal{M}}), G^m(\overline{\mathcal{M}})\,.$$

Nun gilt für alle i

$$\vdash i \in \overline{\mathcal{M}} \leftrightarrow i \leq m \wedge i \in \overline{\mathcal{M}}\,,$$

mithin erhalten wir

$$\vdash \neg\overline{G^m}(\overline{\mathcal{M}}), G^m(\{u \leq m : u \in \overline{\mathcal{M}}\})\,.$$

Die Anwendung von ($\mathbf{\Sigma_0^{1,b}}$-CA) als Regel liefert

$$\vdash \neg\overline{G^m}(\overline{\mathcal{M}}), \exists\phi\, G^m(\phi^m)$$

für alle $\mathcal{M} \subset \{0,\ldots,m\}$. Dann produzieren endlich viele ($\wedge$)-Anwendungen

$$\vdash \bigwedge\left\{\neg\overline{G^m}(\overline{\mathcal{M}}) : \mathcal{M} \subset \{0,\ldots,m\}\right\}, \exists\phi\, G^m(\phi^m)\,,$$

mithin $\vdash \overline{F^m}(\vec{n}) \rightarrow F^m(\vec{n})\,.$

„$\rightarrow$“ Sei $[\alpha = \mathcal{M}]^{<m}$ die Formel $\forall x{<}m\,(x \in \alpha \leftrightarrow x \in \overline{\mathcal{M}})$. Dann läßt sich analog zu 4.11 (i) für beliebige $\mathbf{\Sigma^{1,b}}$-Formeln $H(\beta)$ und $\mathcal{M} \subset \{0,\ldots,m\}$ durch Induktion nach der Länge von H

$$\vdash \neg[\alpha = \mathcal{M}]^{<m+1}, \neg H(\alpha^m), H(\overline{\mathcal{M}})$$

zeigen. Für $H(\beta) \equiv G^m(\beta)$ folgt hieraus mit einigen ($\vee$)-Schlüssen

$$\vdash \neg[\alpha = \mathcal{M}]^{<m+1}, \neg G^m(\alpha^m), \bigvee\left\{G^m(\overline{\mathcal{N}}) : \mathcal{N} \subset \{0,\ldots,m\}\right\}$$

für beliebige $\mathcal{M} \subset \{0,\ldots,m\}$. Es bleibt uns also noch

$$\vdash \left\{[\alpha = \mathcal{M}]^{<m+1} : \mathcal{M} \subset \{0,\ldots,m\}\right\} \tag{2}$$

zu zeigen, denn dann folgt aus Obigem mit endlich vielen Schnitten

$$\vdash \neg G^m(\alpha^m), \overline{F^m}\,.$$

Durch einen ($\forall^2$)-Schluß erhalten wir dann

$$\vdash \forall\phi\, \neg G^m(\alpha^m), \overline{F^m}\,,$$

mithin $\vdash F^m(\vec{n}) \rightarrow \overline{F^m}(\vec{n})\,.$

Wir beweisen (2) durch Induktion nach m. Vorher überlegen wir uns den für den Induktionsschritt benötigten Zusammenhang

$$\vdash \neg[\alpha = \mathcal{N}]^{<m}, [\alpha = \mathcal{N}]^{<m+1}, [\alpha = \mathcal{N} \cup \{m\}]^{<m+1} \tag{3}$$

für $\mathcal{N} \subset \{0, \ldots, m-1\}$. Wir erhalten dies aus dem Axiom $m \notin \alpha, m \in \alpha$ sowie aus den Tatsachen $m \notin \mathcal{N}$ und $m \in \mathcal{N} \cup \{m\}$, woraus $\vdash m \notin \overline{\mathcal{N}}$ und $\vdash m \in \overline{\mathcal{N} \cup \{m\}}$ folgt. Für $m = 0$ zeigt (3)

$$\vdash \neg[\alpha = \emptyset]^{<0}, [\alpha = \emptyset]^{<1}, [\alpha = \{0\}]^{<1}\,.$$

Da $\vdash [\alpha = \emptyset]^{<0}$ gilt, folgt der Induktionsanfang durch einen Schnitt. Im Induktionsschritt liefert die Induktionsvoraussetzung

$$\vdash \left\{[\alpha = \mathcal{M}]^{<m+1} : \mathcal{M} \subset \{0, \ldots, m\}\right\}.$$

Durch endlich viele Schnitte mit (3) für alle $\mathcal{N} \subset \{0, \ldots, m\}$ erhalten wir

$$\vdash \left\{[\alpha = \mathcal{M}]^{<m+2} : \mathcal{M} \subset \{0, \ldots, m\}\right\},$$
$$\left\{[\alpha = \mathcal{M} \cup \{m+1\}]^{<m+2} : \mathcal{M} \subset \{0, \ldots, m\}\right\},$$

oder umgeschrieben

$$\vdash \left\{[\alpha = \mathcal{M}]^{<m+2} : \mathcal{M} \subset \{0, \ldots, m+1\}\right\},$$

mithin die Behauptung (2). □

Der im letzten Beweis gezeigte Zusammenhang (2) läßt sich auch zur Begründung eines Vollständigkeitssatzes für das halbformale System heranziehen. Ist $F \in \mathbf{\Sigma^{1,b}}$ ohne freie Individuenvariablen, so gilt:

$$\begin{aligned} \vdash F \quad &\overset{!}{\Longleftrightarrow} \quad (\mathbb{N}, \mathcal{P}(\mathbb{N})) \models F \\ &\overset{10.11}{\Longleftrightarrow} \quad (\{0, \ldots, t_F\}, \mathcal{P}(\{0, \ldots, t_F\})) \models F\,. \end{aligned}$$

„$\Longrightarrow$“ Diese Richtung ist der Korrektheitssatz.

„$\Longleftarrow$“ Aus $(\mathbb{N}, \mathcal{P}(\mathbb{N})) \models F$ folgt $(\{0, \ldots, t_F\}, \mathcal{P}(\{0, \ldots, t_F\})) \models F$ mit der zweiten Äquivalenz. Die Menge $\mathcal{P}(\{0, \ldots, t_F\})$ ist endlich, mithin abzählbar, also kann man hier die Methode der Quasideduktionsbäume anwenden (siehe [Pohlers 1989] §5). Dabei wird ein ausgezeichneter Redex $\forall\phi\, G(\phi)$ durch die Formeln $G(\overline{\mathcal{M}})$ für alle $\mathcal{M} \in \mathcal{P}(\{0, \ldots, t_F\})$ ersetzt. Beim Beweis des syntaktischen Hauptlemmas geht dann (2) ein, um von

$$\bigwedge \left\{G(\overline{\mathcal{M}}) : \mathcal{M} \in \mathcal{P}(\{0, \ldots, t_F\})\right\}$$

auf $\forall\phi\, G(\phi)$ zu schließen.

Bis hierhin können wir noch alles in ähnlicher Form in formalen Systemen der Beschränkten Arithmetik beweisen. Die entscheidenden Schritte zum Beweis der großen Komprehensionsregel ($\mathbf{\Sigma^{1,b}}$-CA) ist, für $F(A(.)) \in \mathbf{\Sigma^{1,b}}$ eine natürliche Zahl m zu finden, so daß

$$\vdash F(A(.)) \leftrightarrow F(A^m(.))$$

gilt. Dies ist in halbformalen Systemen möglich, da nur Formelmengen, die keine freien Individuenvariablen enthalten, hergeleitet werden. Also ist dieser Schritt in einem formalen System nur dann durchführbar, wenn der Klassenterm und die Formeln, in denen er auftritt, keine freien Individuenvariablen enthalten.

10.15 Satz

Das halbformale System beweist ($\mathbf{\Sigma^{1,b}}$-CA). Genauer gilt für $F(\alpha), A(a) \in \mathbf{\Sigma^{1,b}}$ mit $F(A(.))$ ohne freie Individuenvariablen

$$\vdash \neg F(A(.)), \exists \phi\, F(\phi)\,.$$

Beweis:

Sei $m = \sigma[t_A]_a(t_F)$. Mit Lemma 10.11 (ii) gilt

$$\forall n \in \mathbb{N}\, \forall l \geq t_A(n) \quad \vdash A(n) \leftrightarrow A^l(n)\,.$$

Für $n \leq t_F$ zeigt Lemma 3.12 $t_A(n) \leq \sigma[t_A]_a(t_F) = m$, also folgt

$$\forall n \leq t_F \quad \vdash A(n) \leftrightarrow A^m(n)$$

und mit Satz 10.14

$$\forall n \leq t_F \quad \vdash A(n) \leftrightarrow \overline{A^m}(n)\,.$$

Durch Induktion nach der Länge von F erhalten wir daraus

$$\vdash \neg F\Big(\{u \leq t_F : A(u)\}\Big), F\Big(\{u \leq t_F : \overline{A^m}(u)\}\Big)\,.$$

Hierauf zweimal Lemma 10.11 (i) angewandt liefert

$$\vdash \neg F(A(.)), F(\overline{A^m}(.))\,.$$

Da mit Lemma 10.13 $\overline{A^m} \in \mathbf{\Sigma_0^{1,b}}$ ist, folgt mit ($\mathbf{\Sigma_0^{1,b}}$-CA) die Behauptung. □

In den letzten vier Abschnitten nutzen wir Erweiterungen dieses halbformalen Systems aus, um zu zeigen, daß bestimmte Versionen des vollen Induktionsaxioms, des kleinen Fermatschen Satzes, des Wilsonschen Satzes sowie einer erststufigen Komprehension in $\mathbf{U_2^w}$ nicht beweisbar sind.

11 Das volle Induktionsaxiom

Wir zeigen, daß das volle Induktionsaxiom nicht in $\mathbf{U_2^w}$ herleitbar ist. Dies ist in $\mathbf{U_2^1}$ beweisbar, da in [Buss 1986] 9.5 Satz 15 gezeigt wird, daß sogar $\mathbf{U_2^1} \vdash (\mathbf{\Delta_1^{1,b}}\text{-IND})$ gilt.

11.1 Satz

$\mathbf{U_2^w} \nvdash 0 \in \alpha \wedge \forall x\,(x \in \alpha \to \mathrm{S}x \in \alpha) \to c \in \alpha$ für eine freie Variable c.

Der Beweis vollzieht sich in mehreren Schritten. Zuerst definieren wir ein neues Fragment **I**, in dem α wie ein Prädikatszeichen und c wie eine Konstante behandelt werden, die nie Eigenvariable eines Schlusses sein dürfen und auch nicht zu den freien Variablen gezählt werden.

I entsteht aus $\mathbf{U_2^w}$ durch Hinzufügen des Axioms

$$0 \in \alpha$$

und des Schlusses (α-Schritt):

$$\Gamma, s \in \alpha \implies \Gamma, \mathrm{S}s \in \alpha$$

für beliebige Terme s. Dabei heißt s der *Hauptterm* dieses Schlusses.
Diese zusätzlichen Axiome und Regeln sind so angelegt, daß sie die Prämisse des Induktionsaxioms beweisen.

11.2 Lemma

$\mathbf{I} \vdash 0 \in \alpha \wedge \forall x\,(x \in \alpha \to \mathrm{S}x \in \alpha)$. □

Sei $\mathbf{I} - \mathsf{rg} := \mathbf{U_2^w} - \mathsf{rg}$. Analog zum Eliminationssatz 4.13 läßt sich auch hier zeigen:

11.3 Lemma

$\mathbf{I} \vdash_r^m \Gamma \implies \mathbf{I} \vdash_1 \Gamma$. □

Die Idee zur Nichtbeweisbarkeit des Induktionsaxioms ist die folgende. Angenommen, es wäre herleitbar, dann folgt in **I** unter Ausnutzung der zusätzlichen Axiome und Regeln $\mathbf{I} \vdash c \in \alpha$ und damit $\mathbf{I} \vdash_1 c \in \alpha$. Mit Hilfe der neuen Regel (α-Schritt) gelangen wir wie folgt zu einem einfachen Komplexitätsmaß des Beweises.
Bei der Einbettung einer formalen Herleitung in ein halbformales System werden bei einem Schluß mit Variablenbedingung an eine Eigenvariable b in die Teilherleitung zu diesem Schluß beliebige natürliche Zahlen für b eingesetzt. Nun haben wir den Vorteil,

daß in $\mathbf{I} \vdash\!\!\!\frac{m}{1} c \in \alpha$ solch ein Schluß nur eine Anwendung von ($\forall\leq$) oder ($\mathbf{\Sigma^{1,w}}$-LIND) gewesen sein kann, daher liefert uns der Hauptterm des Schlusses eine obere Schranke für die in die Teilherleitung einzusetzenden natürlichen Zahlen. Damit lassen sich bis auf die Parametervariablen alle wesentlichen freien Variablen von Haupttermen beschränken. In Abhängigkeit der Parametervariablen c geben wir dann den *Speicher* dieses Beweises an, der den Bereich der Hauptterme umfaßt. Die Mächtigkeit dieses Speichers ist ein Maß für die Anzahl der Hauptterme. Wir werden feststellen, daß es ein Polynom $\mathrm{p}(c)$ gibt, so daß die Mächtigkeit des Speichers für $c = n$ durch $\mathrm{p}(|n|)$ beschränkt ist.
Zum Widerspruch kommen wir, indem wir für jedes n den Beweis von $\underline{n} \in \alpha$ in ein halbformales System übersetzen. Dort treten keine freien Individuenvariablen mehr auf, deshalb können wir beim Einbetten die Induktionsregel eliminieren. In dem halbformalen System läßt sich vollständige Schnittelimination beweisen. Wir erhalten eine schnittfreie Herleitung von $\underline{n}\in\alpha$, die aber nur mit mindestens n (α-Schritt) Anwendungen möglich ist. Also beträgt die Anzahl der Hauptterme mindestens $n \approx 2^{|n|}$. Dies steht für hinreichend großes n im Gegensatz zu der obigen Festellung.

Um nun in dem Widerspruchsbeweis fortzufahren, müssen wir die für die Definition des Speichers benötigten Informationen aus einer formalen Herleitung von $\mathbf{I} \vdash\!\!\!\frac{m}{1} c \in \alpha$ gewinnen. Dazu zeichnen wir in der Menge aller möglichen Herleitungen von $\mathbf{I} \vdash\!\!\!\frac{m}{1} c \in \alpha$ spezielle aus, indem wir zu Normalherleitungen mit Schranken $\frac{\vec{b}\,|\,\vec{t}}{S}\!\!\mid\!\!\frac{m}{1}\ \Gamma$ für gewisse $\vec{b}$, $\vec{t}$ und S übergehen. Die hier angestrebte Normalform entspricht der „normale Beweise mit Schranken“ aus [Takeuti 1991] und der „freie Variablennormalform“ aus [Takeuti 1987]. In Bezug auf eine feste Herleitung bedeute $\frac{\vec{b}\,|\,\vec{t}}{S}\!\!\mid\!\!\frac{m}{1}\ \Gamma$:

- m und ist eine obere Schranken der Herleitungslänge.
- Die 1 besagt, daß alle Schnittformeln den Rang Null haben (also durch 1 beschränkt werden). Dies gilt schon für alle Herleitungen mit $\mathbf{I} \vdash\!\!\!\frac{m}{1} c \in \alpha$.
- Γ ist eine endliche Menge von $\mathbf{\Sigma^{1,w}}$-Formeln.
- Zu b_i gibt es in der Herleitung genau einen Schluß mit einer Variablenbedingung, wo b_i Eigenvariable ist, dem sogenannten *Eliminationsschluß von* b_i. Der Eliminationsschluß muß also eine Anwendung von ($\forall\leq$) oder ($\mathbf{\Sigma^{1,w}}$-LIND) sein.

  Mithin müssen die Eigenvariablen $\vec{b}$ paarweise verschieden sein, was sich in der Variablenbedingung E1) in der nachstehenden Definition wiederspiegelt.
- Alle im Beweis auftretenden freien Variablen sind entweder Parametervariablen (d. h. treten in der Endformelmenge Γ auf) oder Eliminationsvariablen und diese beiden Gruppen sind disjunkt, was später in den Variablenbedingungen E2) bis E4) ausgenutzt wird (c zählt nicht zu den freien Variablen und kann daher immer auftreten).

– Die Eliminationsvariablen sind bezüglich ihres Auftretens in der Herleitung von oben nach unten geordnet, d. h. tritt b_i in der Teilherleitung, die zum Eliminationsschluß von b_j führt, auf, so ist $i < j$.

– Jedem b_i ist der Term t_i zugeordnet. Dabei muß $|t_i|$ der Hauptterm des Eliminationsschlusses von b_i sein. Das geht in dieser Form, da diese Terme in den entsprechenden Schlüssen alle scharf beschränkt sind. Es liegt also eine der folgenden Situationen vor:

$$\frac{\Lambda, \neg A(b_i), A(\mathrm{S}b_i)}{\Lambda, \neg A(0), A(|t_i|)} \quad \text{mit} \quad b_i \notin \mathsf{FV}(\Lambda, A(|t_i|))$$

oder

$$\frac{\Lambda, b_i \not\leq |t_i|, A(b_i)}{\Lambda, \forall x{\leq}|t_i|\, A(x)} \quad \text{mit} \quad b_i \notin \mathsf{FV}(\Lambda, \forall x{\leq}|t_i|\, A(x)) \ .$$

Mit dem vorherigen Punkt bezüglich der Anordnung der Eigenvariablen erhalten wir in beiden Fällen

$$b_1, \ldots, b_i \notin \mathsf{FV}(t_i) \ ,$$

wodurch die nachfolgende Variablenbedingung E3) begründet ist.

– Die Hauptterme der (α-Schritt)-Anwendungen werden in S notiert.

11.4 Definition

Seien $\mathcal{V}$ eine endliche Menge von freien Variablen, $k, l, m < \omega$, $b_1, \ldots, b_k$ freie Variablen ungleich c und $t_1, \ldots, t_k, s_1, \ldots, s_l$ Terme, $S = \{s_1, \ldots, s_l\}$. Die Variablenbedingung (E)$[\vec{b};\, \vec{t};\, S;\, \mathcal{V}]$ ist genau dann erfüllt, wenn

E1) $b_i \not\equiv b_j$ für $i, j \in \{1, \ldots, k\}$, $i \neq j$

E2) $\mathcal{V} \cap \{b_1, \ldots, b_k\} = \emptyset$

E3) $\mathsf{FV}(t_i) \subset \{b_{i+1}, \ldots, b_k\} \cup \mathcal{V}$ für $1 \leq i \leq k$

E4) $\mathsf{FV}(S) \subset \{b_1, \ldots, b_k\} \cup \mathcal{V}$

gilt. Sei $\Gamma \subset_{\text{fin}} \mathbf{\Sigma^{1,w}}$. Wir schreiben abkürzend (E) für (E)$[\vec{b};\, \vec{t};\, S;\, \mathsf{FV}(\Gamma)]$. Die *Normalherleitung mit Schranken* $\frac{\vec{b}\,|\,\vec{t}}{S}\big|\frac{m}{1}\ \Gamma$ sei induktiv definiert durch:

(a) Ist Γ ein Axiom von $\mathbf{I}$, so gelte für $m < \omega$ beliebig $\frac{|}{\emptyset}\big|\frac{m}{1}\ \Gamma$. (E) ist trivialerweise erfüllt.

(b) Gilt $\frac{\vec{b}\,|\,\vec{t}}{S}\big|\frac{m'}{1}\ \Lambda$, ist $\Lambda \implies \Gamma$ ein $(\vee)$, $(\exists{\leq})$, $(\forall^2)$, $(\exists^2)$ oder ($\mathbf{\Sigma^{1,w}}$-CA)-Schluß und ist $\mathsf{FV}_1(\Lambda) = \mathsf{FV}_1(\Gamma)$, so gelte $\frac{\vec{b}\,|\,\vec{t}}{S}\big|\frac{m}{1}\ \Gamma$ für $m > m'$, falls (E) erfüllt ist.

(c) Gelten $\frac{\vec{b}_i \mid \vec{t}_i}{S_i}\big|\frac{m_i}{1}\ \Gamma, A_i$ für $i = 0, 1$, so gelte $\frac{\vec{b}_0, \vec{b}_1 \mid \vec{t}_0, \vec{t}_1}{S_0 \cup S_1}\big|\frac{m}{1}\ \Gamma, A_0 \wedge A_1$ für $m > m_0, m_1$, falls (E) erfüllt ist.

(d) Gelten $\frac{\vec{b}_0 \mid \vec{t}_0}{S_0}\big|\frac{m_0}{1}\ \Gamma, F$ und $\frac{\vec{b}_1 \mid \vec{t}_1}{S_1}\big|\frac{m_1}{1}\ \Gamma, \neg F$, sind die freien Individuenvariablen von F in $\mathsf{FV}(\Gamma)$ enthalten, damit die in der Herleitung auftretenden freien Individuenvariablen allesamt entweder Eigenvariable oder Parametervariable sind, und ist $F \in \mathbf{\Sigma^{1,w}}$ vom $\vee$-Typ, so gelte $\frac{\vec{b}_0, \vec{b}_1 \mid \vec{t}_0, \vec{t}_1}{S_0 \cup S_1}\big|\frac{m}{1}\ \Gamma$ für $m > m_0, m_1$, falls (E) erfüllt ist.

(e) $\frac{\vec{b} \mid \vec{t}}{S}\big|\frac{m'}{1}\ \Gamma, b \not\leq |t|, F(b) \implies \frac{\vec{b}, b \mid \vec{t}, t}{S}\big|\frac{m}{1}\ \Gamma, \forall x{\leq}|t|\, F(x)$ für $m > m'$, falls $b \notin \mathsf{FV}(\Gamma, \forall x{\leq}|t|\, F(x))$ und (E) erfüllt ist.

(f) $\frac{\vec{b} \mid \vec{t}}{S}\big|\frac{m'}{1}\ \Gamma, \neg F(b), F(\mathrm{S}b) \implies \frac{\vec{b}, b \mid \vec{t}, t}{S}\big|\frac{m}{1}\ \Gamma, \neg F(0), F(|t|)$ für $m > m'$, falls $b \notin \mathsf{FV}(\Gamma, F(|t|))$ und (E) erfüllt ist.

(g) $\frac{\vec{b} \mid \vec{t}}{S}\big|\frac{m'}{1}\ \Gamma, s \in \alpha \implies \frac{\vec{b} \mid \vec{t}}{S \cup \{s\}}\big|\frac{m}{1}\ \Gamma, \mathrm{S}s \in \alpha$ für $m > m'$, falls (E) erfüllt ist.

Die Definition zeigt, daß aus $\frac{\vec{b} \mid \vec{t}}{S}\big|\frac{m}{1}\ \Gamma$ die Variablenbedingung (E)$[\vec{b}; \vec{t}; S; \mathsf{FV}(\Gamma)]$ folgt.

Die Verbindung zwischen **I** und der Normalherleitung mit Schranken stellt der Satz 11.7 her. Dazu werden zuerst zwei technische Lemmata formuliert. Sie bilden den Kern für die Erfüllung der Variablenbedingung in dem Satz.

11.5 Lemma

Sei $a \notin \vec{b}$ und u ein Term mit $\mathsf{FV}(u) \cap \vec{b} = \emptyset$, dann gilt

$$\frac{\vec{b} \mid \vec{t}}{S}\big|\frac{m}{1}\ \Gamma \implies \frac{\vec{b} \mid \vec{t}_a(u)}{S_a(u)}\big|\frac{m}{1}\ \Gamma a(u)\,.$$

Beweis durch Induktion nach m:

Wir begründen, daß aus (E') := (E)$[\vec{b}; \vec{t}; S; \mathsf{FV}(\Gamma)]$ mit der Voraussetzung $\mathsf{FV}(u) \cap \vec{b} = \emptyset$ die Gültigkeit von (E) := (E)$[\vec{b}; \vec{t}_a(u); S_a(u); \mathsf{FV}(\Gamma a(u))]$ folgt.

Die Eigenschaft E1) $b_i \not\equiv b_j$ für $i, j \in \{1, \ldots, k\}$, $i \neq j$, wird von der Ersetzung nicht betroffen, da nach Voraussetzung schon $a \notin \vec{b}$ gilt. Dies nutzen wir auch aus, um mit der zweiten Voraussetzung $\mathsf{FV}(u) \cap \vec{b} = \emptyset$ E2) zu zeigen:

$$\mathsf{FV}(\Gamma a(u)) \cap \vec{b} \subset (\mathsf{FV}(\Gamma) \cap \vec{b}) \cup (\mathsf{FV}(u) \cap \vec{b}) = \emptyset\,.$$

Für E3) nutzen wir E'3) aus:

$$\mathsf{FV}(t_i\, a(u)) \subset (\mathsf{FV}(t_i) / \{a\}) \cup \mathsf{FV}(u) \subset \{b_{i+1}, \ldots, b_k\} \cup \mathsf{FV}(\Gamma a(u))$$

und für E4) die Eigenschaft E'4):

$$\mathsf{FV}(S_a(u)) \subset (\mathsf{FV}(S) / \{a\}) \cup \mathsf{FV}(u) \subset \vec{b} \cup \mathsf{FV}(\Gamma a(u))\ .$$ □

11.6 Lemma

Für $a \notin \vec{b} \cup \mathsf{FV}(\Gamma)$ und $b \in \{b_1, \ldots, b_k\}$ gilt

$$\frac{\vec{b} \mid \vec{t}}{S} \Big|\!\frac{m}{1}\ \Gamma \implies \frac{\vec{b}_b(a) \mid \vec{t}_b(a)}{S_b(a)} \Big|\!\frac{m}{1}\ \Gamma\,.$$

Beweis durch Induktion nach m:

Es gibt ein $i \in \{1, \ldots, k\}$ mit $b = b_i$. Dann liefert uns (E') $:=$ (E)$[\vec{b};\, \vec{t};\, S;\, \mathsf{FV}(\Gamma)]$

$$\begin{aligned} \vec{b}_b(a) &= b_1, \ldots, b_{i-1}, a, b_{i+1}, \ldots, b_k \\ \vec{t}_b(a) &= t_1{}_b(a), \ldots, t_{i-1}{}_b(a), t_i, \ldots, t_k\,, \end{aligned} \tag{1}$$

denn für $j \geq i$ gilt mit E'3) $\mathsf{FV}(t_j) \subset \{b_{j+1}, \ldots, b_k\} \cup \mathsf{FV}(\Gamma)$ und mit E'2) $b \notin \{b_{j+1}, \ldots, b_k\} \cup \mathsf{FV}(\Gamma)$, mithin $b \notin \mathsf{FV}(t_j)$. Wir zeigen nun (E) $:=$ (E)$[\vec{b}_b(a);$ $\vec{t}_b(a);\, S_b(a);\, \mathsf{FV}(\Gamma)]$.

E1) folgt aus der Voraussetzung $a \notin \vec{b}$ und E2) aus $a \notin \mathsf{FV}(\Gamma)$.

Um E3) zu zeigen, nutzen wir (1) und E'3) aus. Wir unterscheiden zwei Fälle. Für $1 \leq j < i$ ist

$$\mathsf{FV}\Big(t_j{}_b(a)\Big) \subset \{b_{j+1}, \ldots, b_{i-1}, a, b_{i+1}, \ldots, b_k\} \cup \mathsf{FV}(\Gamma)$$

und für $i \leq j \leq k$

$$\mathsf{FV}\Big(t_{jb}(a)\Big) \subset \{b_{j+1}, \ldots, b_k\} \cup \mathsf{FV}(\Gamma)\,.$$

Schließlich erhalten wir E4) aus E'4):

$$\mathsf{FV}\Big(S_b(a)\Big) \subset \{b_1, \ldots, b_{i-1}, a, b_{i+1}, \ldots, b_k\} \cup \mathsf{FV}(\Gamma)\,. \qquad \square$$

Aus einer fest gewählten Herleitung von $\mathbf{I} \mid\!\frac{m}{1}\ \Gamma$ läßt sich immer eine Normalherleitung mit Schranken konstruieren. Dazu nennen wir die Eigenvariablen so um, daß sie jeweils von allen anderen in der Herleitung auftretenden Variablen verschieden sind. Dies ist möglich, da die Eigenvariablen in ihren Eliminationsschlüssen einer geeigneten Variablenbedingung unterliegen. Nun ersetzen wir alle Individuenvariablen (zu denen c nicht zählt), die durch einen Schluß eliminiert werden (d. h. sie treten in der Konklusion nicht mehr auf) ohne dort Eigenvariable zu sein, durch Null. Jetzt brauchen wir nur noch die Eigenvariablen $\vec{b}$ und deren zugeordneten Hauptterme $\vec{t}$ sowie alle Hauptterme von (α-Schritt)-Anwendungen S notieren und erhalten so eine Normalherleitung mit Schranken und der Eigenschaft (E)$[\vec{b};\, \vec{t};\, S;\, \mathsf{FV}(\Gamma)]$.

11.7 Satz (Existenz einer Normalherleitung mit Schranken)

Sei $\Gamma \subset \mathbf{\Sigma^{1,w}}$ und gelte $\mathbf{I} \mid\!\frac{m}{1}\ \Gamma$, dann gibt es eine Normalherleitung mit Schranken von Γ, d. h. es existieren gewisse $\vec{b}, \vec{t}$ und S mit

$$\frac{\vec{b} \mid \vec{t}}{S} \Big|\!\frac{m}{1}\ \Gamma\,.$$

Beweis durch Induktion nach m:

(i) Ist Γ ein Axiom, so ist nichts zu zeigen.

(ii) Der letzte Schluß war $(\vee)$, $(\exists\leq)$, $(\forall^2)$ oder $(\exists^2)$ der Gestalt

$$\mathbf{I} \vdash^{m'}_{1} \Lambda \implies \mathbf{I} \vdash^{m}_{1} \Gamma$$

für ein $m' < m$. Die Induktionsvoraussetzung liefert die Existenz gewisser $\vec{b}, \vec{t}$ und S mit

$$\frac{\vec{b} \mid \vec{t}}{S} \vdash^{m'}_{1} \Lambda .$$

Es ist wegen $\mathsf{FV}_1(\Lambda) \subset \mathsf{FV}_1(\Gamma)$ und Lemma 11.6 auch ohne Einschrnkung $(\mathrm{E})[\vec{b};\ \vec{t};\ S;\ \mathsf{FV}(\Gamma)]$ erfüllt, also erhalten wir durch Anwendung des gleichen Schlusses

$$\frac{\vec{b} \mid \vec{t}}{S} \vdash^{m}_{1} \Gamma .$$

(iii) Als letzter Schluß lag ($\mathbf{\Sigma^{1,w}}$-CA) vor:

$$\mathbf{I} \vdash^{m'}_{1} \Gamma, F(A(.)) \implies \mathbf{I} \vdash^{m}_{1} \Gamma, \exists\phi\, F(\phi)$$

mit $m' < m$ und $A \in \mathbf{\Sigma^{1,w}}$. Die Induktionsvoraussetzung liefert für $\Lambda := \Gamma, F(A(.))$ die Existenz gewisser $\vec{b}, \vec{t}$ und S mit

$$\frac{\vec{b} \mid \vec{t}}{S} \vdash^{m'}_{1} \Lambda .$$

Für $\mathsf{FV}_1(\Lambda) \setminus \mathsf{FV}_1(\Gamma) = \{d_1, \ldots, d_n\}$ erhalten wir durch Induktion nach n unter Ausnutzung von Lemma 11.5

$$\frac{\vec{b} \mid \vec{t}_{\vec{d}}(\vec{0})}{S_{\vec{d}}(\vec{0})} \vdash^{m}_{1} \Lambda_{\vec{d}}(\vec{0}) .$$

Nun ist wegen $\mathsf{FV}_1\left(\Lambda_{\vec{d}}(\vec{0})\right) = \mathsf{FV}_1(\Gamma)$ auch $(\mathrm{E})[\vec{b};\ \vec{t}_{\vec{d}}(\vec{0});\ S_{\vec{d}}(\vec{0});\ \mathsf{FV}(\Gamma)]$ erfüllt, also erhalten wir durch ($\mathbf{\Sigma^{1,w}}$-CA)

$$\frac{\vec{b} \mid \vec{t}_{\vec{d}}(\vec{0})}{S_{\vec{d}}(\vec{0})} \vdash^{m}_{1} \Gamma, \exists\phi\, F(\phi) .$$

(iv) Lag ein $(\wedge)$-Schluß vor, etwa

$$\mathbf{I} \vdash^{m_i}_{1} \Gamma, A_i \quad \text{für} \quad i = 0, 1 \implies \mathbf{I} \vdash^{m}_{1} \Gamma, A_0 \wedge A_1$$

mit $m_0, m_1 < m$, so liefert die Induktionsvoraussetzung

$$\frac{\vec{b}_i \mid \vec{t}_i}{S_i} \vdash^{m_i}_{1} \Gamma, A_i$$

für $i = 0, 1$ und gewisse $\vec{b}_0, \vec{t}_0, S_0$ und $\vec{b}_1, \vec{t}_1, S_1$.

Nach Lemma 11.6 können wir ohne Einschränkung annehmen, daß $\vec{b}_0 \cap \vec{b}_1 = \emptyset$ und $\vec{b}_0, \vec{b}_1 \cap \mathsf{FV}(A_0 \wedge A_1) = \emptyset$ sind. Damit sind E1), E2) und E3) für (E)$[\vec{b}_0, \vec{b}_1;\ \vec{t}_0, \vec{t}_1;\ S_0 \cup S_1;\ \mathsf{FV}(\Gamma, A_0 \wedge A_1)]$ klar. Für E4) beobachten wir

$$\begin{array}{rcl} \mathsf{FV}(S_0 \cup S_1) & = & \mathsf{FV}(S_0) \cup \mathsf{FV}(S_1) \\ & \overset{\text{IV}}{\subset} & (\vec{b}_0 \cup \mathsf{FV}(\Gamma, A_0)) \cup (\vec{b}_1 \cup \mathsf{FV}(\Gamma, A_1)) \\ & = & \vec{b}_0, \vec{b}_1 \cup \mathsf{FV}(\Gamma, A_0 \wedge A_1)\ . \end{array}$$

Mithin

$$\tfrac{\vec{b}_0, \vec{b}_1 \mid \vec{t}_0, \vec{t}_1}{S_0 \cup S_1} \big|\!\!\frac{m}{1}\ \Gamma, A_0 \wedge A_1\ .$$

(v) Der letzte Schluß war ein (Schnitt):

$$\mathbf{I} \mid\!\!\frac{m_0}{1}\ \Gamma, A \quad \text{und} \quad \mathbf{I} \mid\!\!\frac{m_1}{1}\ \Gamma, \neg A \implies \mathbf{I} \mid\!\!\frac{m}{1}\ \Gamma$$

mit $m_0, m_1 < m$ und $\mathbf{I}\text{-}\mathsf{rg}(A) = 0$, also $A \in \mathbf{\Sigma}^{\mathbf{1,w}}$. Ohne Einschränkung sei A vom $\vee$-Typ, dann gilt mit der Induktionsvoraussetzung

$$\tfrac{\vec{b}_0 \mid \vec{t}_0}{S_0} \big|\!\!\frac{m_0}{1}\ \Gamma, A \qquad \text{und} \qquad \tfrac{\vec{b}_1 \mid \vec{t}_1}{S_1} \big|\!\!\frac{m_1}{1}\ \Gamma, \neg A$$

für gewisse $\vec{b}_0, \vec{t}_0, S_0$ und $\vec{b}_1, \vec{t}_1, S_1$.

Analog zu (iii) können wir ohne Einschränkung annehmen, daß $\mathsf{FV}(A) \subset \mathsf{FV}(\Gamma)$ gilt. Die gleiche Argumentation wie unter (iv) zeigt, daß ohne Einschränkung $\vec{b}_0 \cap \vec{b}_1 = \emptyset$ und (E)$[\vec{b}_0, \vec{b}_1;\ \vec{t}_0, \vec{t}_1;\ S_0 \cup S_1;\ \mathsf{FV}(\Gamma)]$ wegen $\mathsf{FV}(\Gamma, A) = \mathsf{FV}(\Gamma, \neg A) = \mathsf{FV}(\Gamma)$ erfüllt sind. Mithin

$$\tfrac{\vec{b}_0, \vec{b}_1 \mid \vec{t}_0, \vec{t}_1}{S_0 \cup S_1} \big|\!\!\frac{m}{1}\ \Gamma\ .$$

(vi) Es lag ($\forall\leq$) als letzter Schluß vor:

$$\mathbf{I} \mid\!\!\frac{m'}{1}\ \Gamma, b \not\leq |t|, F(b) \implies \mathbf{I} \mid\!\!\frac{m}{1}\ \Gamma, \forall x{\leq}|t|\ F(x)$$

mit $b \notin \mathsf{FV}(\Gamma, \forall x{\leq}|t|\ F(x))$ und $m' < m$. Dies ist der einzig mögliche ($\forall\leq$)-Schluß, da nur scharf beschränkte Formeln hergeleitet werden. Die Induktionsvoraussetzung produziert

$$\tfrac{\vec{b} \mid \vec{t}}{S} \big|\!\!\frac{m'}{1}\ \Gamma, b \not\leq |t|, F(b)$$

für gewisse $\vec{b}, \vec{t}$ und S. Insbesondere gilt (E') $:=$ (E)$[\vec{b};\ \vec{t};\ S;\ \mathsf{FV}(\Gamma, b \not\leq |t|, F(b))]$.

Nun überlegen wir uns, daß (E) $:=$ (E)$[\vec{b}, b;\ \vec{t}, t;\ S;\ \mathsf{FV}(\Gamma, \forall x{\leq}|t|\ F(x))]$ erfüllt ist.

Nach E'2) gilt $\vec{b} \cap \mathsf{FV}(b \not\leq |t|) = \emptyset$, also ist $b \notin \vec{b}$. Mit E'1) ist dann auch gezeigt, daß die Variablen $b_1, \ldots, b_k, b$ paarweise verschieden sind, mithin E1).

Die Variablenbedingung $b \notin \mathsf{FV}(\Gamma, \forall x{\leq}|t|\ F(x))$ und E'2) zeigen

$$\mathsf{FV}(\Gamma, \forall x{\leq}|t|\ F(x)) \cap \{b_1, \ldots, b_k, b\} = \emptyset\ .$$

Also haben wir E2). Für E'3) beobachten wir einerseits

$$\begin{array}{rcl} \mathsf{FV}\,(t_i) & \overset{\text{E}'3)}{\subset} & \{b_{i+1},\ldots,b_k\} \cup \mathsf{FV}\,(\Gamma, b \not\leq |t|, F(b)) \\ & = & \{b_{i+1},\ldots,b_k,b\} \cup \mathsf{FV}\,(\Gamma, \forall x{\leq}|t|\; F(x)) \;. \end{array}$$

Andererseits gilt trivialerweise schon

$$\mathsf{FV}\,(t) \subset \mathsf{FV}\,(\forall x{\leq}|t|\; F(x)) \;.$$

Ebenso erhalten wir E4):

$$\begin{array}{rcl} \mathsf{FV}\,(S) & \overset{\text{E}'4)}{\subset} & \{b_1,\ldots,b_k\} \cup \mathsf{FV}\,(\Gamma, b \not\leq |t|, F(b)) \\ & = & \{b_1,\ldots,b_k,b\} \cup \mathsf{FV}\,(\Gamma, \forall x{\leq}|t|\; F(x)) \;. \end{array}$$

Mithin

$$\tfrac{\vec{b},b \mid \vec{t},t}{S} \big|\!\!\frac{m}{1} \; \Gamma, \forall x{\leq}|t|\; F(x) \,.$$

(vii) Der letzte Schluß war ($\mathbf{\Sigma^{1,w}}$-LIND):

$$\mathbf{I} \mid\!\!\frac{m'}{1} \; \Gamma, \neg F(b), F(\mathrm{S}b) \implies \mathbf{I} \mid\!\!\frac{m}{1} \; \Gamma, \neg F(0), F(|t|)$$

mit $b \notin \mathsf{FV}\,(\Gamma, F(0))$ und $m' < m$. Dann liefert die Induktionsvoraussetzung für gewisse $\vec{b}, \vec{t}$ und S

$$\tfrac{\vec{b} \mid \vec{t}}{S} \big|\!\!\frac{m'}{1} \; \Gamma, \neg F(b), F(\mathrm{S}b) \,.$$

Mit Lemma 11.5 können wir ohne Einschränkung $b \notin \mathsf{FV}\,(\Gamma, F(|t|))$ annehmen. Nun zeigt man wie unter (vi) (E)$[\vec{b}, b;\, \vec{t}, t;\, S;\, \mathsf{FV}\,(\Gamma, \neg F(0), F(|t|))]$. Also gilt

$$\tfrac{\vec{b},b \mid \vec{t},t}{S} \big|\!\!\frac{m}{1} \; \Gamma, \neg F(0), F(|t|) \,.$$

(viii) Zuletzt lag ein (α-Schritt) vor:

$$\mathbf{I} \mid\!\!\frac{m'}{1} \; \Gamma, s \in \alpha \implies \mathbf{I} \mid\!\!\frac{m}{1} \; \Gamma, \mathrm{S}s \in \alpha$$

mit $m' < m$. Dann liefert die Induktionsvoraussetzung

$$\tfrac{\vec{b} \mid \vec{t}}{S} \big|\!\!\frac{m'}{1} \; \Gamma, s \in \alpha$$

für gewisse $\vec{b}, \vec{t}$ und S. Es folgt (E)$[\vec{b};\, \vec{t};\, S \cup \{s\};\, \mathsf{FV}\,(\Gamma, \mathrm{S}s \in \alpha)]$, mithin

$$\tfrac{\vec{b} \mid \vec{t}}{S \cup \{s\}} \big|\!\!\frac{m}{1} \; \Gamma, \mathrm{S}s \in \alpha \,. \qquad \square$$

Wir haben nun aus der Existenz einer Herleitung $\mathbf{I} \mid\!\!\frac{m}{1} \; \Gamma$ die Existenz einer Normalherleitung mit Schranken $\tfrac{\vec{b} \mid \vec{t}}{S} \big|\!\!\frac{m}{1} \; \Gamma$ gefolgert. Dadurch haben wir genug Informationen gewonnen, um den Speicher solch einer Herleitung angeben zu können, der alle für die

Einbettung ins halbformale System benötigten Hauptterme von (α-Schritt)-Anwendungen umfaßt.

Wir nutzen die Variablenbedingung (E)$[\vec{b};\,\vec{t};\,S;\,\mathcal{V}]$, speziell E3) $\mathsf{FV}(t_i) \subset \{b_{i+1},\ldots,b_k\} \cup \mathcal{V}$, aus, indem wir sukzessive b_i in $t_1,\ldots,t_{i-1}$ „monoton“, d. h. mit Hilfe der Funktion σ aus 3.12, durch $|t_i|$ ersetzen.
Sind $\vec{b}$ und $\vec{t}$ k-Tupel, dann definieren wir durch Rekursion für $i = k,\ldots,1$ kanonische Beschränkungsterme $T_i[\vec{t}] \in \mathbf{L}^{\emptyset}_{\mathbf{BA}}$ zu t_i durch

$$T_i[\vec{t}] \;:\equiv\; \sigma[t_i]_{b_{i+1},\ldots,b_k}(|T_{i+1}[\vec{t}]|,\ldots,|T_k[\vec{t}]|)\,.$$

Wir beobachten durch Induktion nach i für $i = k,\ldots,1$, daß aus der Eigenschaft E3): $\mathsf{FV}(t_i) \subset \{b_{i+1},\ldots,b_k\} \cup \mathcal{V}$

$$\mathsf{FV}\left(T_i[\vec{t}]\right) \subset \mathcal{V} \tag{1}$$

folgt.

Nun sind wir in der Lage, zu einer gegebenen Normalherleitung $\frac{\vec{b}\,|\,\vec{t}}{S}\big|\frac{m}{1}\;\Gamma$ aus der Variablenbedingung (E)$[\vec{b};\,\vec{t};\,S;\,\mathsf{FV}(\Gamma)]$ den *Speicher* zu definieren, der alle für die Einbettung ins halbformale System benötigten Hauptterme umfaßt.
Dazu gelte (E)$[\vec{b};\,\vec{t};\,S;\,\mathcal{V}]$, die freien Individuenvariablen in $\mathcal{V}$ seien in $\{a_1,\ldots,a_n\}$ enthalten und es gelte $\{a_1,\ldots,a_n\} \cap \{b_1,\ldots,b_k\} = \emptyset$.

11.8 Definition

Für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$ sei $\mathrm{Sp}^{\vec{b};\vec{t};S}_{\vec{a}}(l,\vec{n})$ die Menge

$$\left\{s(\vec{b}) \;\middle|\; s \in S_{c,\,\vec{a}}(l,\vec{n}) \text{ und } b_i \le |T_i[\vec{t}]_{c,\,\vec{a}}(l,\vec{n})| \text{ für } i = 1,\ldots,k\right\}.$$

An dieser Stelle bestimmen wir die Mächtigkeit des Speichers, unser gesuchtes Maß. Sei $\#(M)$ die Mächtigkeit der Menge M.

11.9 Lemma

Es gibt ein geeignetes Polynom p mit

$$\#\left(\mathrm{Sp}^{\vec{b};\vec{t};S}_{\vec{a}}(l,\vec{n})\right) \le \mathrm{p}(|l|,|\vec{n}|)$$

für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$.

Beweis:

Zu $T_i[\vec{t}](c,\vec{a})$ gibt es ein geeignetes Polynom $\mathrm{p}_i(c,\vec{a})$, so daß

$$\forall l \quad \forall \vec{n} \quad |T_i[\vec{t}](l,\vec{n})| \le \mathrm{p}_i(|l|,|\vec{n}|)$$

gilt. Damit erhalten wir

$$
\begin{aligned}
&\#\Big(\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l,\vec{n})\Big)\\
&\quad\le\ \#(S)\cdot(|T_1[\vec{t}](l,\vec{n})|+1)\cdot\ldots\cdot(|T_k[\vec{t}](l,\vec{n})|+1)\\
&\quad\le\ \#(S)\cdot(\mathrm{p}_1(|l|,|\vec{n}|)+1)\cdot\ldots\cdot(\mathrm{p}_k(|l|,|\vec{n}|)+1)\\
&\quad=\ \mathrm{p}(|l|,|\vec{n}|)
\end{aligned}
$$

für ein geeignetes Polynom $\mathrm{p}(c,\vec{a})$. □

Wir haben nun, ausgehend von einer Herleitung $\mathbf{I}\mid\!\frac{m}{1}\ c\in\alpha$, eine Normalherleitung mit Schranken $\frac{\vec{b}\downarrow\vec{t}}{S}\mid\!\frac{m}{1}\ c\in\alpha$ für gewisse $\vec{b},\vec{t},S$ und ein Polynom $\mathrm{p}(c)$ gefunden, so daß der zu dieser Herleitung konstruierte Speicher $\mathrm{Sp}^{\vec{b};\vec{t};S}(n)$ durch $\mathrm{p}(|n|)$ beschränkt ist. Uns bleibt noch zu zeigen, daß der Speicher wirklich alle für die Einbettung ins halbformale System benötigten Hauptterme von (α-Schritt)-Anwendungen umfaßt und daß sich diese Menge bei der Schnittelimination nicht vergrößert. Um dann zu einem Widerspruch zu kommen, müssen wir abschließend begründen, daß die Anzahl der für eine schnittfreie Herleitung von $n\in\alpha$ im halbformalen System benötigten Hauptterme linear zu n und damit exponentiell zu $|n|$ wächst. Darum kann sie für große n nicht durch $\mathrm{p}(|n|)$ beschränkt werden.

Dazu passen wir das schon definierte halbformale System aus Abschnitt 11 für $\mathbf{U}_{\mathbf{2}}^{\mathbf{i}}$ an das Fragment $\mathbf{I}$ an, indem wir zusätzliche Axiome und Regeln angeben. Dabei wird besonderen Wert auf die Kontrolle der Hauptterme aus den (α-Schritt)-Schlüssen durch M gelegt.

11.10 Induktive Definition des halbformalen Systems $M\mid\!\frac{m}{\rho}\ \Gamma$ für $\mathbf{I}$.

Seien $M\subset_{\mathrm{fin}}\mathbb{N}$, $m'<m<\omega$, $\rho<\omega\cdot 2$ und $\Gamma\subset\mathbf{\Sigma^{1,b}}$ ohne freie Individuenvariablen. Wir fügen der Definition 10.3 folgendes Axiom und folgenden Schluß hinzu.

zusätzliches Axiom:

(c) Für $s^{\mathbf{N}}=0$ gelte $M\mid\!\frac{m}{\rho}\ \Gamma,s\in\alpha$.

zusätzlicher Schluß:

(α-Schritt) $M\mid\!\frac{m'}{\rho}\ \Gamma,\underline{i}\in\alpha$ und $i\in M$, $t^{\mathbf{N}}=i+1\ \Longrightarrow\ M\mid\!\frac{m}{\rho}\ \Gamma,t\in\alpha$

Wir beobachten, daß für das neue Axiom und den neuen Schluß wieder das Strukturschlußlemma und das Gleichheitslemma aus Abschnitt 11 gelten. Damit läßt sich in analoger Weise der Eliminationssatz beweisen.

11.11 Eliminationssatz

$M\mid\!\frac{m}{\rho}\ \Gamma\ \Longrightarrow\ M\mid\!\frac{}{0}\ \Gamma$. □

Um zu begründen, daß wir mit der Wahl unserer Definition des Speichers und des halb-

formalen Systems richtig liegen, zeigen wir zuerst den Einbettungssatz. Der wesentliche Punkt dabei ist die Ersetzung der Induktionsschlüsse durch Schnitte.

11.12 Lemma

Es gelte $(\mathrm{E})[b_1,\ldots,b_k;\ t_1,\ldots,t_k;\ S;\ \mathcal{V}]$, die Individuenvariablen von $\mathcal{V}$ seien in $\{a_1,\ldots,a_n\}$ enthalten und es gelte $\{a_1,\ldots,a_n\}\cap\{b_1,\ldots,b_k\}=\emptyset$.

Seien $l\in\mathbb{N}$, $\vec{n}\in\mathbb{N}^n$ und $\hat{t}_\iota := T_\iota[\vec{t}]_{C,\,\vec{a}}(l,\vec{n})^{\mathbf{N}}$ für $\iota=1,\ldots,k$, dann gilt für $0\le i-1\le j\le k$, $T\subset S$, $\Gamma\subset\mathbf{\Sigma^{1,w}}$ mit $\mathsf{FV}(\Gamma)\subset\mathcal{V}\cup\{b_{j+1},\ldots,b_k\}$ und $r_\iota\le|\hat{t}_\iota|$ für $\iota=1,\ldots,k$

$$\frac{b_i,\ldots,b_j\mid t_i,\ldots,t_j}{T}\Big|\frac{m}{1}\ \Gamma \implies \mathrm{Sp}^{\vec{b};\vec{t};S}_{\vec{a}}(l,\vec{n})\vdash\Gamma_{C,\,\vec{a},\,\vec{b}}(\underline{l},\underline{\vec{n}},\underline{\vec{r}})\,.$$

Beweis durch Induktion nach m:

Abkürzend sei $\mathrm{Sp}(l,\vec{n}) := \mathrm{Sp}^{\vec{b};\vec{t};S}_{\vec{a}}(\underline{l},\underline{\vec{n}})$, $F' :\equiv F_{C,\,\vec{a},\,\vec{b}}(\underline{l},\underline{\vec{n}},\underline{\vec{r}})$ und $t' :\equiv t_{C,\,\vec{a},\,\vec{b}}(\underline{l},\underline{\vec{n}},\underline{\vec{r}})$.

(i) Ist Γ ein Axiom, so ist in jedem Fall Γ' ein Axiom des halbformalen Systems, und es gilt $\mathrm{Sp}(l,\vec{n})\vdash\Gamma'$.

(ii) Gilt $\frac{b_i,\ldots,b_j\mid t_i,\ldots,t_j}{T}\Big|\frac{m'}{1}\ \Lambda$ für ein $m'<m$ und ist $\Lambda \implies \Gamma$ ein $(\vee)$, $(\forall^2)$ oder ein $(\exists^2)$-Schluß, so gilt nach Induktionsvoraussetzung

$$\mathrm{Sp}(l,\vec{n})\vdash\Lambda'\,.$$

Mit dem entsprechenden Schluß im halbformalen System folgt

$$\mathrm{Sp}(l,\vec{n})\vdash\Gamma'\,.$$

(iii) War der letzte Schluß eine ($\mathbf{\Sigma^{1,w}}$-CA)-Anwendung, so lag ohne Einschränkung die Prämisse

$$\frac{b_i,\ldots,b_j\mid t_i,\ldots,t_j}{T}\Big|\frac{m'}{1}\ \Gamma,F(A(.))$$

für ein $m'<m$ und $A(a)\in\mathbf{\Sigma^{1,w}}$ vor. Hier liefert die Induktionsvoraussetzung

$$\mathrm{Sp}(l,\vec{n})\vdash\Gamma',F(A(.))'\,.$$

Dann folgt mit Satz 10.15, der ($\mathbf{\Sigma^{1,w}}$-CA) im halbformalen System beweist,

$$\mathrm{Sp}(l,\vec{n})\vdash\Gamma'\,.$$

(iv) Als letzter Schluß lag vor:

$$\frac{b_i,\ldots,b_j\mid t_i,\ldots,t_j}{T}\Big|\frac{m'}{1}\ \Gamma,F(s)$$
$$\implies \frac{b_i,\ldots,b_j\mid t_i,\ldots,t_j}{T}\Big|\frac{m}{1}\ \Gamma,s\not\le t,\exists x{\le}t\,F(x)$$

mit $m'<m$. Dann liefert die Induktionsvoraussetzung

$$\mathrm{Sp}(l,\vec{n})\vdash\Gamma',F'(s')\,.$$

Für $s'^{\mathbf{N}} \leq t'^{\mathbf{N}}$ produziert ($\exists\leq$) mit einem Strukturschluß 10.4

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', s' \not\leq t', \exists x{\leq}t'\, F'(x)\,,$$

im anderen Fall ist dies ein Axiom (a).

(v) Gelten

$$\frac{b_i,\ldots,b_s \mid t_i,\ldots,t_s}{T_0}\Big|\frac{m_0}{1}\ \Gamma_0 \quad \text{und} \quad \frac{b_{s+1},\ldots,b_j \mid t_{s+1},\ldots,t_j}{T_1}\Big|\frac{m_1}{1}\ \Gamma_1\,,$$

$i-1 \leq s \leq j$, $m_0, m_1 < m$ und ist $\Gamma_0 \ \&\ \Gamma_1 \implies \Gamma$ ein ($\wedge$) oder (Schnitt)-Schluß, so gilt nach Voraussetzung und wegen der zusätzlichen Variablenbedingung im Schnitt

$$\mathsf{FV}(\Gamma_0,\Gamma_1) \subset \mathcal{V} \cup \{b_{j+1},\ldots,b_k\}$$

sowie $T_0 \subset T \subset S$ und $T_1 \subset T \subset S$. Also ist die Induktionsvoraussetzung anwendbar. Sie liefert

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma'_i\,.$$

Mit dem ursprünglichen Schluß folgt die Behauptung.

(vi) Der letzte Schluß hatte die Gestalt:

$$\frac{b_i,\ldots,b_{j-1} \mid t_i,\ldots,t_{j-1}}{T}\Big|\frac{m'}{1}\ \Gamma, b_j \not\leq |t_j|, F(b_j)$$
$$\implies \frac{b_i,\ldots,b_j \mid t_i,\ldots,t_j}{T}\Big|\frac{m}{1}\ \Gamma, \forall x{\leq}|t_j|\, F(x)$$

mit $m' < m$, $b_j \notin \mathsf{FV}(\Gamma, \forall x{\leq}|t_j|\, F(x))$ und $i \leq j$. Nach Voraussetzung gilt

$$\begin{aligned}\mathsf{FV}(\Gamma, b_j \not\leq |t_j|, F(b_j)) &= \mathsf{FV}(\Gamma, \forall x{\leq}|t_j|\, F(x)) \cup \{b_j\}\\ &\subset \mathcal{V} \cup \{b_j,\ldots,b_k\}\,.\end{aligned}$$

Also liefert die Induktionsvoraussetzung für $d \leq |\hat{t}_j|$

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', \underline{d} \not\leq |t'_j|, F'(\underline{d})\,. \tag{1}$$

Nun beobachten wir wegen E3) $\mathsf{FV}(t_j) \subset \mathcal{V} \cup \{b_{j+1},\ldots,b_k\}$ mit Lemma 3.12 über die Monotonie von σ

$$\begin{aligned}\big(t'_j\big)^{\mathbf{N}} &= \big(t_j\, c, \vec{a}, b_{j+1},\ldots,b_k(l,\vec{n},r_{j+1},\ldots,r_k)\big)^{\mathbf{N}}\\ &\leq \big(\sigma[t_j]_c, \vec{a}, b_{j+1},\ldots,b_k(l,\vec{n},|\hat{t}_{j+1}|,\ldots,|\hat{t}_k|)\big)^{\mathbf{N}}\\ &= \big(T_j[\vec{t}]_{c,\,\vec{a}}(l,\vec{n})\big)^{\mathbf{N}}\\ &= \hat{t}_j\,.\end{aligned}$$

Also gilt für alle $d \leq |t'_j|^{\mathbf{N}}$ insbesondere (1) und mit Axiom (a) $\vdash \underline{d} \leq |t'|$, mithin erhalten wir

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', F'(\underline{d})\,.$$

Dann folgt mit $(\forall\leq)$

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', \forall x{\leq}|t'_j|\, F'(x)\,.$$

(vii) Der letzter Schluß war:

$$\frac{b_i,\ldots,b_{j-1} \mid t_i,\ldots,t_{j-1}}{T}\Big|^{m'}_{1}\ \Gamma, \neg F(b_j), F(\mathrm{S}b_j)$$
$$\Longrightarrow\ \frac{b_i,\ldots,b_j \mid t_i,\ldots,t_j}{T}\Big|^{m}_{1}\ \Gamma, \neg F(0), F(|t_j|)$$

mit $m' < m$, $b_j \notin \mathsf{FV}(\Gamma, F(|t_j|))$, $F(a) \in \mathbf{\Sigma^{1,w}}$ und $i \leq j$. Wie unter (v) produziert die Induktionsvoraussetzung für $d \leq |t'_j|^{\mathbf{N}}$

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', \neg F'(\underline{d}), F'(\mathrm{S}\underline{d})\,.$$

Aus diesem folgt durch endlich viele Schnitte

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', \neg F'(0), F'(\underline{|t'_j|^{\mathbf{N}}})\,,$$

also zeigt das Gleichheitslemma 10.5

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', \neg F'(0), F'(|t'_j|)\,.$$

(viii) Der letzter Schluß sah wie folgt aus:

$$\frac{b_i,\ldots,b_j \mid t_i,\ldots,t_j}{T}\Big|^{m'}_{1}\ \Gamma, t \in \alpha$$
$$\Longrightarrow\ \frac{b_i,\ldots,b_j \mid t_i,\ldots,t_j}{T\cup\{t\}}\Big|^{m}_{1}\ \Gamma, \mathrm{S}t \in \alpha$$

mit $m' < m$. Nach Voraussetzung ist $T \cup \{t\} \subset S$, insbesondere gilt $T \subset S$ und $t \in S$. Die Induktionsvoraussetzung liefert also

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', t' \in \alpha\,.$$

Wegen

$$\begin{aligned} t' &\equiv t_{\mathcal{C},\vec{a},\vec{b}}(l,\vec{n},\vec{r}) \\ &\in \Big\{ s(\vec{b}) \mid s \in S_{\mathcal{C},\vec{a}}(l,\vec{n}) \text{ und } b_\iota \leq |T_\iota[\vec{t}]_{\mathcal{C},\vec{a}}(l,\vec{n})| \text{ für } \iota = 1,\ldots,k \Big\} \\ &= \mathrm{Sp}(l,\vec{n}) \end{aligned}$$

folgt mit einem (α-Schritt)

$$\mathrm{Sp}(l,\vec{n}) \vdash \Gamma', \mathrm{S}t' \in \alpha\,. \qquad \square$$

Als Spezialfall dieses Lemmas erhalten wir den Einbettungssatz.

11.13 Einbettungssatz

Sei $\Gamma \subset \mathbf{\Sigma^{1,w}}$, die Individuenvariablen von Γ seien in $\{a_1, \ldots, a_n\}$ enthalten, es sei $\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_k\} = \emptyset$ und es gelte $\frac{\vec{b} \mid \vec{t}}{S} \Big|\!\frac{m}{1}\ \Gamma$, dann gilt für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$

$$\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l, \vec{n}) \mid\!- \Gamma_{c,\,\vec{a}}(\underline{l}, \underline{\vec{n}})\,.$$ □

Die Begründung dafür, daß mindestens n (α-Schritt)-Schlüsse zur schnittfreien Herleitung von $\underline{n} \in \alpha$ benötigt werden, liegt im Beschränkungssatz.
Sei $\mathrm{Min}(s_1, \ldots, s_l) := \mathrm{Min}\left({s_1}^{\mathbf{N}}, \ldots, {s_l}^{\mathbf{N}}\right)$.

11.14 Beschränkungssatz

$$M \mid\!\frac{m}{0}\ s_1 \in \alpha, \ldots, s_l \in \alpha \implies \{0, \ldots, \mathrm{Min}(s_1, \ldots, s_l) - 1\} \subset M\,.$$

Beweis durch Induktion nach m:

Ist $\mathrm{Min}(s_1 \ldots, s_l) = 0$, so ist die Behauptung trivial. Sei also $\mathrm{Min}(s_1 \ldots, s_l) > 0$, dann kann kein Axiom vorliegen, und der letzte Schluß muß ein (α-Schritt) gewesen sein:

$$M \mid\!\frac{m'}{0}\ s_1 \in \alpha, \ldots, s_l \in \alpha, t \in \alpha \implies M \mid\!\frac{m}{0}\ s_1 \in \alpha, \ldots, s_l \in \alpha$$

mit $t^{\mathbf{N}} + 1 = {s_i}^{\mathbf{N}}$ für ein $i \in \{1, \ldots, l\}$, $t^{\mathbf{N}} \in M$ und $m' < m$.

Falls $t^{\mathbf{N}} \geq \mathrm{Min}(s_1 \ldots, s_l)$ ist, so folgt aus der Induktionsvoraussetzung

$$\begin{aligned} &\{0, \ldots, \mathrm{Min}(s_1, \ldots, s_l) - 1\} \\ &= \{0, \ldots, \mathrm{Min}(s_1, \ldots, s_l, t) - 1\} \\ &\subset M\,. \end{aligned}$$

Ist $t^{\mathbf{N}} < \mathrm{Min}(s_1 \ldots, s_l)$, so folgt aus $t^{\mathbf{N}} + 1 = {s_i}^{\mathbf{N}}$

$$\mathrm{Min}(s_1 \ldots, s_l) = t^{\mathbf{N}} + 1$$

und daraus mit der Induktionsvoraussetzung und $t^{\mathbf{N}} \in M$

$$\begin{aligned} &\{0, \ldots, \mathrm{Min}(s_1, \ldots, s_l) - 1\} \\ &= \{0, \ldots, t^{\mathbf{N}}\} \\ &= \{0, \ldots, \mathrm{Min}(s_1, \ldots, s_l, t) - 1, t^{\mathbf{N}}\} \\ &\subset M\,. \end{aligned}$$ □

Nun sind wir in der Lage, den begonnenen Widerspruchsbeweis zu vollenden.

Satz 11.1

$\mathbf{U_2^w} \not\vdash 0 \in \alpha \wedge \forall x\,(x \in \alpha \to \mathrm{S}x \in \alpha) \to c \in \alpha$, wobei c eine freie Variable ist.

Beweis:

Angenommen, es gilt $\mathbf{U_2^w} \vdash 0 \in \alpha \wedge \forall x\,(x \in \alpha \to \mathrm{S}x \in \alpha) \to c \in \alpha$. Wir führen diese Annahme zum Widerspruch.

Da $\mathbf{U_2^w}$ ein Teilsystem von $\mathbf{I}$ ist und mit Lemma 11.2 $\mathbf{I} \vdash 0{\in}\alpha \wedge \forall x\,(x{\in}\alpha \to \mathrm{S}x{\in}\alpha)$ gilt, folgt $\mathbf{I} \vdash c \in \alpha$. Partielle Schnittelimination 11.3 ergibt daraus

$$\mathbf{I} \vdash_{\overline{1}} c \in \alpha\,.$$

Nun zeigt der Satz 11.7 über die Existenz einer Normalherleitung

$$\frac{\vec{b}\,|\,\vec{t}}{S}\Big|_{\overline{1}}\; c \in \alpha \tag{1}$$

für gewisse $\vec{b}, \vec{t}$ und S. Damit konstruieren wir den Speicher $\mathrm{Sp}^{\vec{b};\vec{t};S}(n)$ und ein geeignetes Polynom p, so daß

$$\#\Big(\mathrm{Sp}^{\vec{b};\vec{t};S}(n)\Big) \leq \mathrm{p}(|n|)$$

für beliebiges n gilt.

Durch Einbettung 11.13 der Normalherleitung (1) in das halbformale System und anschließender Schnittelimination 11.11 erhalten wir

$$\mathrm{Sp}^{\vec{b};\vec{t};S}(n) \vdash_{\overline{0}} \underline{n} \in \alpha$$

für alle $n \in \mathbb{N}$. Das ist mit dem Beschränkungssatz 11.14 nur möglich, wenn

$$\{0, \ldots, n-1\} \subset \mathrm{Sp}^{\vec{b};\vec{t};S}(n)$$

ist, also gilt

$$n = \#\{0, \ldots, n-1\} \leq \#\Big(\mathrm{Sp}^{\vec{b};\vec{t};S}(n)\Big) \leq \mathrm{p}(|n|)\,.$$

Mithin ist

$$2^{|n|} = 2^{\lceil \log_2(n+1) \rceil} \leq 2 \cdot (n+1) \leq 2 \cdot \mathrm{p}(|n|) + 2\,,$$

was für hinreichend großes n zum Widerspruch führt. □

Wir übertragen dieses Widerspruchsprinzip auf zwei zahlentheoretische Aussagen, den Kleinen Fermatschen Satz sowie den Satz von Wilson. Für den kleinen Fermatschen Satz rechnen wir $\mathrm{Rem}(c^{p-1}, p)$ mit der Rekursionsgleichung

$$\mathrm{Rem}(c^{i+1}, p) = \mathrm{Rem}(c \cdot \mathrm{Rem}(c^i, p), p)$$

aus, die die Grundlage für die (α-Schritt)-Regel dort sein wird. Analog zu $\mathbf{I}$ ist die Anzahl der (α-Schritt)-Anwendungen, die zur Berechnung von $\mathrm{Rem}(c^{p-1}, p)$ im halbformalen System benötigt werden, linear zu p, was $\mathbf{U_2^w}$-Herleitungen allgemein nicht liefern können.

12 Der kleine Fermat

Der kleine Fermatsche Satz ist die zahlentheoretische Aussage

$$c^{p-1} \equiv 1 \mod p$$

für Primzahlen p und $0 < c < p$. Er läßt sich in $\mathbf{L}^{\mathbf{P}}_{\mathbf{BA}}$ formulieren, indem wir rekursiv c^i in der kleinsten Restklasse modulo p, also $\mathrm{Rem}(c^i, p)$, mit Hilfe von α ausrechnen, d. h. α mit

$$\langle i, a\rangle \in \alpha \leftrightarrow a = \mathrm{Rem}(c^i, p)$$

festlegen, und anschließend $\langle p \dot{-} 1, 1\rangle \in \alpha$ fordern. Dabei nutzen wir die Rekursionsgleichung

$$\mathrm{Rem}(c^{i+1}, p) = \mathrm{Rem}(\mathrm{Rem}(c^i, p) \cdot c, p)$$

aus, die den Zusammenhang $c^{i+1} \equiv c^i \cdot c \mod p$ übersetzt.
$KleinFermat$ sei der $\mathbf{L}^{\mathbf{P}}_{\mathbf{BA}}$-Satz

$$\begin{aligned}\forall p\, \forall x{<}p \Big[& 0 < x \wedge (1 < p \wedge \forall y{<}p\, (1 < y \to \mathrm{Rem}(p, y) \neq 0)) \\ & \wedge \forall y\, (\langle 0, y\rangle \in \alpha \leftrightarrow y = 1) \\ & \wedge \forall i\, \forall y{<}p\, (\langle i, y\rangle \in \alpha \leftrightarrow \langle \mathrm{S}i, \mathrm{Rem}(x \cdot y, p)\rangle \in \alpha) \\ & \to \langle p \dot{-} 1, 1\rangle \in \alpha \Big] .\end{aligned}$$

In [Takeuti 1991] §3 Theorem 2 wird

$$\mathbf{U}^{\mathbf{1}}_{\mathbf{2}} \vdash KleinFermat$$

gezeigt. Wir beweisen hier analog zu Abschnitt 11

12.1 Satz

$$\mathbf{U}^{\mathbf{w}}_{\mathbf{2}} \nvdash KleinFermat\,.$$

Sei $\mathbf{F}$ ein neues Fragment, in dem α wie ein Prädikatszeichen und p, c wie Konstanten behandelt werden, d. h. sie dürfen nie Eigenvariable sein und auch nicht mehr zu den freien Variablen gezählt werden.

$\mathbf{F}$ entsteht aus $\mathbf{U_2^w}$, indem wir die Axiome

$$1 < p$$
$$1 < s \wedge s < p \to \mathrm{Rem}(p, s) \neq 0$$
$$0 < c$$
$$c < p$$
$$\langle 0, 1\rangle \in \alpha$$
$$\langle 0, s\rangle \in \alpha \to s = 1$$

und die Schlüsse (α-Rückschritt):

$$\Gamma, \langle \mathrm{S}s, \mathrm{Rem}(t \cdot c, p)\rangle \in \alpha \implies \Gamma, t \not< p, \langle s, t\rangle \in \alpha$$

und (α-Schritt):

$$\Gamma, \langle s, t\rangle \in \alpha \implies \Gamma, \langle \mathrm{S}s, \mathrm{Rem}(t \cdot c, p)\rangle \in \alpha$$

für beliebige Terme s, t hinzufügen, wobei bei (α-Schritt) s der Hauptterm des Schlusses ist. Nun sind die Axiome und Regeln von $\mathbf{F}$ so angelegt, daß sie die Prämisse von $KleinFermat$ beweisen.

12.2 Lemma

$$\begin{aligned}\mathbf{F} \vdash\ & c < p \wedge 0 < c \wedge (1 < p \wedge \forall y{<}p\,(1 < y \to \mathrm{Rem}(p, y) \neq 0))\\ & \wedge \forall y\,(\langle 0, y\rangle \in \alpha \leftrightarrow y = 1)\\ & \wedge \forall i\,\forall y{<}p\,(\langle i, y\rangle \in \alpha \leftrightarrow \langle \mathrm{S}i, \mathrm{Rem}(c \cdot y, p)\rangle \in \alpha)\end{aligned}$$

Beweis:

Die ersten vier neuen Axiome von $\mathbf{F}$ zeigen

$$c < p \wedge 0 < c \wedge (1 < p \wedge \forall y{<}p\,(1 < y \to \mathrm{Rem}(p, y) \neq 0))\,.$$

Die nächsten beiden Axiome liefern

$$\forall y\,(\langle 0, y\rangle \in \alpha \leftrightarrow y = 1)\,.$$

Für den letzten Teil überlegen wir uns, daß aus dem logischen Axiom $\langle a, b\rangle \notin \alpha, \langle a, b\rangle \in \alpha$ mit einer (α-Schritt) und zwei ($\vee$)-Anwendungen

$$\langle a, b\rangle \in \alpha \to \langle \mathrm{S}a, \mathrm{Rem}(b \cdot c, p)\rangle \in \alpha \tag{1}$$

und aus dem logischen Axiom $\langle \mathrm{S}a, \mathrm{Rem}(b \cdot c, p)\rangle \notin \alpha, \langle \mathrm{S}a, \mathrm{Rem}(b \cdot c, p)\rangle \in \alpha$ mit einer (α-Rückschritt) und zwei ($\vee$)-Anwendungen

$$\langle \mathrm{S}a, \mathrm{Rem}(b \cdot c, p)\rangle \in \alpha \to \langle a, b\rangle \in \alpha \tag{2}$$

folgt. Durch (1) und (2) erhalten wir den fehlenden letzten Teil der Prämisse

$$\forall i\,\forall y{<}p\,(\langle i, y\rangle \in \alpha \leftrightarrow \langle \mathrm{S}i, \mathrm{Rem}(c \cdot y, p)\rangle \in \alpha)\,. \qquad \square$$

Sei $\mathbf{F} - \mathsf{rg} := \mathbf{U}_{\mathbf{2}}^{\mathbf{w}} - \mathsf{rg}$. Die partielle Schnittelimination für $\mathbf{F}$ läßt sich wie in 4.13 zeigen.

12.3 Lemma

$\mathbf{F} \vdash_r^m \Gamma \implies \mathbf{F} \vdash_1 \Gamma$. □

Zum Beweis des Satzes 12.1 nehmen wir $\mathbf{U}_{\mathbf{2}}^{\mathbf{w}} \vdash \mathit{KleinFermat}$ an. Dann zeigen die letzten beiden Lemmata $\mathbf{F} \vdash_1 \langle p \dot{-} 1, 1\rangle \in \alpha$.
Wir lesen wieder durch Auswahl einer Normalherleitung mit Schranken charakteristische Größen ab, mit deren Hilfe wir einen Speicher definieren, der alle für die Einbettung in ein halbformales System benötigten Hauptterme beschränkt. Dazu ändern wir in der Definition 11.4 der Normalherleitung mit Schranken die Klauseln (a) und (g) ab zu

(a') Ist Γ ein Axiom von $\mathbf{F}$, so gelte für $m < \omega$ beliebig $\frac{|}{\emptyset}|_1^m \Gamma$.

(g') $\frac{\vec{b}\,|\,\vec{t}}{S}|_1^{m'} \Gamma, \langle \mathrm{S}s, \mathrm{Rem}(t \cdot c, p)\rangle \in \alpha \implies \frac{\vec{b}\,|\,\vec{t}}{S}|_1^{m} \Gamma, t \not< p, \langle s, t\rangle \in \alpha$ für $m > m'$.

(h') $\frac{\vec{b}\,|\,\vec{t}}{S}|_1^{m'} \Gamma, \langle s, t\rangle \in \alpha \implies \frac{\vec{b}\,|\,\vec{t}}{S\cup\{s\}}|_1^{m} \Gamma, \langle \mathrm{S}s, \mathrm{Rem}(t \cdot c, p)\rangle \in \alpha$ für $m > m'$.

Damit erhalten wir aus $\mathbf{F} \vdash_1^m \Gamma$ die Existenz einer Normalherleitung mit Schranken wie im letzten Abschnitt, da die wesentlichen Schritte der Umbenennung von Eigenvariablen sowie der Ersetzung „überflüssiger" Variablen durch 0 von den neuen Axiomen und Regeln nicht tangiert werden.

12.4 Satz (Existenz einer Normalherleitung mit Schranken)

Sei $\Gamma \subset \mathbf{\Sigma}^{\mathbf{1,w}}$ und gelte $\mathbf{F} \vdash_1^m \Gamma$, dann gibt es eine Normalherleitung mit Schranken von Γ, d. h. es existieren gewisse $\vec{b}, \vec{t}$ und S mit

$\frac{\vec{b}\,|\,\vec{t}}{S}|_1^{m} \Gamma$. □

Wir definieren den Speicher zu einer Normalherleitung $\frac{\vec{b}\,|\,\vec{t}}{S}|_1^{m} \Gamma$ wie in Abschnitt 11 und geben die Abschätzung der Mächtigkeit des Speichers nach oben hin an. Die freien Variablen von Γ seien in $\{a_1, \ldots, a_n\}$ mit $\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_k\} = \emptyset$ enthalten.

12.5 Definition

Für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$ sei $\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l, \vec{n})$ die Menge

$$\Big\{ s(\vec{b}) \mid s \in S_{p,\,c,\,\vec{a}}(l, 1, \vec{n}) \text{ und } b_i \le |T_i[\vec{t}]_{p,\,c,\,\vec{a}}(l, 1, \vec{n})| \text{ für } i = 1, \ldots, k \Big\}.$$

12.6 Lemma

Es gibt ein geeignetes Polynom p mit

$$\#\Big(\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l,\vec{n})\Big) \leq \mathrm{p}(|l|,|\vec{n}|)$$

für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$. □

Zwecks Abschätzung des Speichers nach unten betten wir Normalherleitungen mit Schranken in ein passendes halbformales System ein. Dazu geben wir die zusätzlichen Axiome und Regeln an, die dem halbformalen System aus Abschnitt 10 zugefügt werden.

12.7 Induktive Definition des halbformalen Systems $M \mid\!\!\frac{m}{\rho}\ \Gamma$ für $\mathbf{F}$

Seien $M \subset_{\mathrm{fin}} \mathbb{N}$, $m' < m < \omega$, $\rho < \omega \cdot 2$ und $\Gamma \subset \mathbf{\Sigma^{1,b}}$ ohne freie Individuenvariablen. Wir erweitern die Definition 10.3 um folgende Axiome und Schlüsse.

zusätzliche Axiome:

(c) Für $s^{\mathbf{N}} = \langle 0,1\rangle$ gelte $M \mid\!\!\frac{m}{\rho}\ \Gamma, s \in \alpha$.

(d) Ist $s^{\mathbf{N}} \neq \langle i,1\rangle$ für beliebiges i, dann gelte $M \mid\!\!\frac{m}{\rho}\ \Gamma, s \notin \alpha$.

zusätzliche Schlüsse:

(α-Rückschritt) $M \mid\!\!\frac{m'}{\rho}\ \Gamma, \langle \mathrm{S}\underline{i}, \underline{j}\rangle \in \alpha$ und $s^N = \langle i,j\rangle \implies M \mid\!\!\frac{m}{\rho}\ \Gamma, s \in \alpha$

(α-Schritt) $M \mid\!\!\frac{m'}{\rho}\ \Gamma, \langle \underline{i}, \underline{j}\rangle \in \alpha$ und $i \in M$, $s^N = \langle i+1, j\rangle \implies M \mid\!\!\frac{m}{\rho}\ \Gamma, s \in \alpha$

Um das Reduktionslemma in analoger Weise zu Abschnitt 10 zu beweisen, zeigen wir folgende zusätzliche Inversion.

12.8 Lemma

Gilt $M \mid\!\!\frac{m}{\rho}\ \Gamma, s \in \alpha$ und $s^{\mathbf{N}} \neq \langle i,1\rangle$ für alle i, so folgt $M \mid\!\!\frac{m}{\rho}\ \Gamma$.

Beweis durch Induktion nach m:

Die Fälle, wo etwas zu tun ist, sind die, in denen $s \in \alpha$ Hauptformel des letzten Schlusses ist. Dafür gibt es drei Möglichkeiten.

(i) Es liegt ein Gleichheitsaxiom vor. Dann gibt es einen Term t mit $s^{\mathbf{N}} = t^{\mathbf{N}}$ und $(t \notin \alpha) \in \Gamma$. Aus der Voraussetzung folgt $t^{\mathbf{N}} \neq \langle i,1\rangle$ für beliebiges i, also ist Γ ein Axiom (d).

(ii) Der letzte Schluß war ein (α-Rückschritt), also gibt es $i,j \in \mathbb{N}$ und $m' < m$, so daß $s^{\mathbf{N}} = \langle i,j\rangle$ und $M \mid\!\!\frac{m'}{\rho}\ \Gamma, t \in \alpha$ für $t :\equiv \langle \mathrm{S}\underline{i}, \underline{j}\rangle$ gilt. Mit der zweiten Voraussetzung ist $j \neq 1$, also produziert die Induktionsvoraussetzung $M \mid\!\!\frac{m'}{\rho}\ \Gamma$.

(iii) Lag als letzter Schluß ein (α-Schritt) vor, dann gibt es $i,j \in \mathbb{N}$ und $m' < m$, so daß $s^{\mathbf{N}} = \langle i+1, j\rangle$ und $M \mid\!\!\frac{m'}{\rho}\ \Gamma, t \in \alpha$ für $t :\equiv \langle \underline{i}, \underline{j}\rangle$ gilt. Wieder zeigt

die zweite Voraussetzung, daß es kein k mit $s^{\mathbf{N}} = \langle k, 1\rangle$ gibt, also liefert die Induktionsvoraussetzung $M \mid\!\frac{m'}{\rho}\, \Gamma$. □

12.9 Eliminationssatz

$M \mid\!\frac{m}{\rho}\, \Gamma \implies M \mid\!\frac{}{0}\, \Gamma$.

Beweis:

Wir schauen uns noch einmal das Reduktionslemma an. In den Axiom-Fällen müssen wir zusätzlich $F \equiv s \notin \alpha$ mit $s^{\mathbf{N}} \neq \langle i, 1\rangle$ für alle i betrachten. Hier greift nun das gerade bewiesene Lemma, angewandt auf die zweite Voraussetzung, und ein anschließender Strukturschluß.

Bei den Schlüssen gibt es keine neuen Fälle zu betrachten, da die Hauptformeln der neuen Schlüsse nicht vom $\vee$-Typ sind. Damit ist der Beweis des Reduktionslemmas abgeschlossen. Der Eliminationssatz folgt hieraus wie in 10.9. □

Um den Einbettungssatz wie in 11.13 zu erhalten, begründen wir, daß die neuen Axiome und Regeln von **F** einbettbar sind. Sei q eine Primzahl. Aus einem beliebigen Term s entstehe s', indem die freien Variablen von s durch beliebige, eventuell verschiedene Zahlterme und p, c durch $\underline{q}, 1$ ersetzt werden.
Da q eine Primzahl ist, sind

$$(1 < p)p(\underline{q})\,,\ (0 < c)c(1)\,,\ (c < p)c, p(1, \underline{q})$$

wahre Primformeln und somit Axiome des halbformalen Systems. Ist s ein beliebiger Term mit $1 < s'^{\mathbf{N}} < q$, so ist

$$\mathrm{Rem}(\underline{q}, s') \neq 0$$

eine wahre Primformel, da q eine Primzahl ist und somit nicht von $s'^{\mathbf{N}}$ geteilt wird. Das Axiom $\langle 0, 1\rangle \in \alpha$ ist auch eins des halbformalen Systems.
Für das letzte Axiom sei s ein beliebiger Term. Ist $s'^{N} = 1$, so gilt $\emptyset \mid\!\frac{0}{0}\, s = 1$ mit dem Axiom (a). Ansonsten ist $s'^{\mathbf{N}} \neq 1$, also liefert ein Axiom (d) $\emptyset \mid\!\frac{0}{0}\, \langle 0, s'\rangle \notin \alpha$. In beiden Fällen folgt mit einem ($\vee$)-Schluß

$$\emptyset \mid\!\frac{1}{0}\, \langle 0, s'\rangle \in \alpha \to s' = 1\,.$$

Die Regel (α-Rückschritt) und (α-Schritt) im halbformalen System sind als Einbettung der entsprechenden Regeln des formalen Systems **F** definiert.
Damit erhalten wir analog zu 11.13 den Einbettungssatz für **F**.

12.10 Einbettungssatz

Sei $\Gamma \subset \mathbf{\Sigma^{1,w}}$, die Individuenvariablen von Γ seien in $\{a_1, \ldots, a_n\}$ enthalten, $\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_k\} = \emptyset$ und es gelte $\frac{\vec{b} \mid \vec{t}}{S} \mid\!\!\frac{m}{1}\ \Gamma$, dann gilt für $\vec{n} \in \mathbb{N}^n$ und Primzahlen q

$$\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(q, \vec{n}) \vdash \Gamma_{p,\, c,\, \vec{a}}(\underline{q}, 1, \underline{\vec{n}})\,. \qquad \square$$

Der Beschränkungssatz für dieses halbformale System sieht wie folgt aus.

12.11 Beschränkungssatz

$$M \mid\!\!\frac{m}{0}\ \langle s_1, t_1\rangle \in \alpha, \ldots, \langle s_k, t_k\rangle \in \alpha \implies \{0, \ldots, \mathrm{Min}(s_1, \ldots, s_k) - 1\} \subset M\,.$$

Beweis:

Der Beweis ist dergleiche wie für 11.14. Als zusätzlichen Fall haben wir die Möglichkeit eines (α-Rückschritt) als letzten Schluß. Ohne Einschränkung lag die Prämisse

$$M \mid\!\!\frac{m'}{0}\ \langle s_1, t_1\rangle \in \alpha, \ldots, \langle s_l, t_l\rangle \in \alpha, \langle \mathrm{S}\underline{i}, \underline{j}\rangle \in \alpha$$

mit $\langle i, j\rangle = \langle s_l, t_l\rangle^{\mathbf{N}}$ für ein $l \in \{1, \ldots, k\}$ und $m' < m$ vor. Dann ist aber $\mathrm{Min}(s_1, \ldots, s_k) = \mathrm{Min}(s_1, \ldots, s_k, \mathrm{S}\underline{i})$, also folgt die Behauptung schon aus der Induktionsvoraussetzung. $\square$

Wir haben nun alle Punkte erfüllt, um den Widerspruchsbeweis zu vollenden.

Satz 12.1

$\mathbf{U_2^w} \nvdash \mathit{KleinFermat}\,.$

Beweis:

Angenommen, $\mathit{KleinFermat}$ ist in $\mathbf{U_2^w}$ herleitbar. Da $\mathbf{F}$ eine Erweiterung von $\mathbf{U_2^w}$ ist, folgt mit Lemma 12.2 $\mathbf{F} \vdash \langle p \dot{-} 1, 1\rangle \in \alpha$ und mit der partiellen Schnittelimination 12.3

$$\mathbf{F} \mid\!\!\frac{}{1}\ \langle p \dot{-} 1, 1\rangle \in \alpha\,.$$

Dann existieren mit Satz 12.4 $\vec{b}, \vec{t}, S$ mit

$$\frac{\vec{b} \mid \vec{t}}{S} \mid\!\!\frac{}{1}\ \langle p \dot{-} 1, 1\rangle \in \alpha\,. \tag{1}$$

Mit der Definition des Speichers $\mathrm{Sp}^{\vec{b};\vec{t};S}(n)$ 12.5 und der anschließenden Abschätzung 12.6 gibt es ein geeignetes Polynom p, so daß

$$\#\Big(\mathrm{Sp}^{\vec{b};\vec{t};S}(n)\Big) \leq \mathrm{p}(|n|)$$

für beliebige n gilt.

Wir wenden die Schnittelimination 12.9 auf die Einbettung 12.10 der Normalher-

leitung (1) in das halbformale System an und erhalten

$$\mathrm{Sp}^{\vec{b};\vec{t};S}(q) \mid\!\!\frac{}{0}\ \langle \underline{q} \dot{-} 1, 1\rangle \in \alpha$$

für alle Primzahlen q. Also muß mit dem Beschränkungssatz 12.11

$$\{0, \ldots, q-2\} \subset \mathrm{Sp}^{\vec{b};\vec{t};S}(q)$$

gelten. Das liefert uns folgende Abschätzung des Speichers:

$$q = \#\{0, \ldots, q-2\} + 1 \leq \#\Big(\mathrm{Sp}^{\vec{b};\vec{t};S}(q)\Big) + 1 \leq \mathrm{p}(|q|) + 1\,.$$

Mithin ist

$$2^{|q|} \leq 2 \cdot \mathrm{p}(|q|) + 3\,,$$

was für hinreichend große Primzahlen q zum Widerspruch führt. □

Im nächsten Abschnitt wenden wir wie angekündigt die Methode aus Abschnitt 11 auf den Satz von Wilson an. Diesmal benutzt die (α-Schritt)-Regel die Rekursionsgleichung

$$\mathrm{Rem}((i+1)!, p) = \mathrm{Rem}((i+1) \cdot \mathrm{Rem}(i!, p), p)\,,$$

um $\mathrm{Rem}((p-1)!, p)$ auszurechnen. Wieder ist die Zahl dieser (α-Schritt)-Anwendungen, die im halbformalen System zur Berechnung von $\mathrm{Rem}((p-1)!, p)$ benötigt werden, linear in p. Dies steht im Gegensatz zu der von $\mathbf{U}_{\mathbf{2}}^{\mathbf{w}}$-Herleitungen bereitgestellten Größenordnung der Anzahl spezieller Regelanwendungen.

13 Der Satz von Wilson

Für natürliche Zahlen i sei $i! := i \cdot (i-1) \cdot \ldots \cdot 1$. Der Satz von Wilson ist die zahlentheoretische Aussage

$$(p-1)! \equiv -1 \mod p$$

für Primzahlen p. Analog zu dem kleinen Fermat'schen Satz läßt sich der Satz von Wilson formulieren. $Wilson$ sei der $\mathbf{L}^{\mathbf{P}}_{\mathbf{BA}}$-Satz

$$\begin{aligned}\forall p \Big[& (1 < p \wedge \forall x{<}p\,(1 < x \to \mathrm{Rem}(p,x) \neq 0)) \\ & \wedge \forall y\,(\langle 0, y\rangle \in \alpha \leftrightarrow y = 1) \\ & \wedge \forall i\,(\mathrm{S}i < p \to \forall x{<}p\,(\langle i, x\rangle \in \alpha \leftrightarrow \langle \mathrm{S}i, \mathrm{Rem}((\mathrm{S}i)\cdot x, p)\rangle \in \alpha)) \\ & \to \langle p \dot{-} 1, p \dot{-} 1\rangle \in \alpha \Big] .\end{aligned}$$

In [Takeuti 1991] §3 Theorem 1 wird

$$\mathbf{U}^{\mathbf{1}}_{\mathbf{2}} \vdash Wilson$$

gezeigt. Wir beweisen hier analog zu Abschnitt 12

13.1 Satz

$$\mathbf{U}^{\mathbf{w}}_{\mathbf{2}} \nvdash Wilson\,.$$

Sei **W** ein neues Fragment, in dem α wie ein Prädikatszeichen und p wie eine Konstante behandelt werden, d. h. sie dürfen nie Eigenvariable sein und auch nicht mehr zu den freien Variablen gezählt werden.

W entsteht aus $\mathbf{U}^{\mathbf{w}}_{\mathbf{2}}$, indem wir die Axiome

$$\begin{aligned}& 1 < p \\ & 1 < s \wedge s < p \to \mathrm{Rem}(p,s) \neq 0 \\ & \langle 0, 1\rangle \in \alpha \\ & \langle 0, s\rangle \in \alpha \to s = 1\end{aligned}$$

und die Schlüsse (α-Rückschritt):

$$\Gamma, \langle \mathrm{S}s, \mathrm{Rem}((\mathrm{S}s)\cdot t, p)\rangle \in \alpha \implies \Gamma, t \not< p, \mathrm{S}s \not< p, \langle s, t\rangle \in \alpha$$

und (α-Schritt):

$$\Gamma, \langle s, t\rangle \in \alpha \implies \Gamma, \langle \mathrm{S}s, \mathrm{Rem}((\mathrm{S}s)\cdot t, p)\rangle \in \alpha$$

für beliebige Terme s, t hinzufügen, wobei bei (α-Schritt) s der Hauptterm des Schlusses ist. Nun sind die Axiome und Regeln von $\mathbf{W}$ so angelegt, daß sie die Prämisse von $Wilson$ beweisen.

13.2 Lemma

$$\begin{aligned}\mathbf{W} \vdash\ & (1 < p \wedge \forall x{<}p\,(1 < x \to \mathrm{Rem}(p, x) \neq 0)) \\ & \wedge \forall x\,(\langle 0, x\rangle \in \alpha \leftrightarrow x = 1) \\ & \wedge \forall i\,(\mathrm{S}i < p \to \forall x{<}p\,(\langle i, x\rangle \in \alpha \leftrightarrow \langle \mathrm{S}i, \mathrm{Rem}((\mathrm{S}s)\cdot x, p)\rangle \in \alpha))\end{aligned}$$ □

Sei $\mathbf{W} - \mathsf{rg} := \mathbf{U}^{\mathbf{w}}_{\mathbf{2}} - \mathsf{rg}$. Die partielle Schnittelimination für $\mathbf{W}$ läßt sich wie in 4.13 zeigen.

13.3 Lemma

$$\mathbf{W} \mid\!\!\frac{m}{r}\ \Gamma \implies \mathbf{W} \mid\!\!\frac{}{1}\ \Gamma$$ □

Zum Beweis des Satzes 12.1 nehmen wir $\mathbf{U}^{\mathbf{w}}_{\mathbf{2}} \vdash Wilson$ an. Dann zeigen die letzten beiden Lemmata $\mathbf{W} \mid\!\!\frac{}{1}\ \langle p \dot{-} 1, p \dot{-} 1\rangle \in \alpha$.
Wir lesen wieder durch Auswahl einer Normalherleitung mit Schranken charakteristische Größen ab, mit deren Hilfe wir einen Speicher definieren, der alle für die Einbettung in ein halbformales System benötigten Hauptterme beschränkt. Dazu ändern wir in der Definition 11.4 der Normalherleitung mit Schranken die Klauseln (a) und (g) ab zu:

(a') Ist Γ ein Axiom von $\mathbf{W}$, so gelte für $m < \omega$ beliebig $\frac{\bot \mid m}{\emptyset \mid 1}\ \Gamma$.

(g') $\frac{\vec{b} \mid \vec{t} \mid m'}{S \mid 1}\ \Gamma, \langle \mathrm{S}s, \mathrm{Rem}((\mathrm{S}s)\cdot t, p)\rangle \in \alpha \implies \frac{\vec{b} \mid \vec{t} \mid m}{S \mid 1}\ \Gamma, t \not< p, \mathrm{S}s \not< p, \langle s, t\rangle \in \alpha$ für $m > m'$.

(h') $\frac{\vec{b} \mid \vec{t} \mid m'}{S \mid 1}\ \Gamma, \langle s, t\rangle \in \alpha \implies \frac{\vec{b} \mid \vec{t}}{S \cup \{s\} \mid 1}\ \Gamma, \langle \mathrm{S}s, \mathrm{Rem}((\mathrm{S}s)\cdot t, p)\rangle \in \alpha$ für $m > m'$.

13.4 Satz (Existenz einer Normalherleitung mit Schranken)

Sei $\Gamma \subset \mathbf{\Sigma^{1,w}}$ und gelte $\mathbf{W} \mid\!\!\frac{m}{1}\ \Gamma$, dann gibt es eine Normalherleitung mit Schranken von Γ, d. h. es existieren gewisse $\vec{b}, \vec{t}$ und S mit

$$\frac{\vec{b} \mid \vec{t} \mid m}{S \mid 1}\ \Gamma.$$ □

Wir definieren den Speicher zu einer Normalherleitung $\frac{\vec{b} \mid \vec{t} \mid m}{S \mid 1}\ \Gamma$ wie in Abschnitt 11 und geben die Abschätzung der Mächtigkeit des Speichers nach oben hin an. Die freien Variablen von Γ seien in $\{a_1, \ldots, a_n\}$ mit $\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_k\} = \emptyset$ enthalten.

13.5 Definition

Für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$ sei $\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l,\vec{n})$ die Menge

$$\Big\{ s(\vec{b}) \mid s \in S_{p,\,\vec{a}}(l,\vec{n}) \text{ und } b_i \leq |T_i[\vec{t}]_{p,\,\vec{a}}(l,\vec{n})| \text{ für } i = 1,\ldots,k \Big\}.$$

13.6 Lemma

Es gibt ein geeignetes Polynom p mit

$$\#\Big(\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l,\vec{n})\Big) \leq \mathrm{p}(|l|,|\vec{n}|)$$

für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$. □

Zwecks Abschätzung des Speichers nach unten betten wir Normalherleitungen mit Schranken in ein passendes halbformales System ein. Dazu ändern wir das halbformale System aus Abschnitt 10 wie folgt ab.

13.7 Induktive Definition des halbformalen Systems $M_p \mid\!\!\frac{m}{\rho}\ \Gamma$ für $\mathbf{W}$

Seien $M \subset_{\mathrm{fin}} \mathbb{N}$, p eine Primzahl, $m' < m < \omega$, $\rho < \omega \cdot 2$ und $\Gamma \subset \mathbf{\Sigma^{1,b}}$ ohne freie Individuenvariablen. Wir ersetzen in der Definition 10.3 M durch M_p und fügen folgende Axiome und Schlüsse hinzu.

zusätliche Axiome:

(c) Für $s^{\mathbf{N}} = \langle 0,1\rangle$ gelte $M_p \mid\!\!\frac{m}{\rho}\ \Gamma, s \in \alpha$.

(d) Ist $s^{\mathbf{N}} \neq \langle i, \mathrm{Rem}(i!,p)\rangle$ für beliebiges i, dann gelte $M_p \mid\!\!\frac{m}{\rho}\ \Gamma, s \notin \alpha$.

zusätzliche Schlüsse:

(α-Rückschritt) $M_p \mid\!\!\frac{m'}{\rho}\ \Gamma, \langle \mathrm{S}\underline{i}, \mathrm{Rem}((\mathrm{S}\underline{i}) \cdot \underline{j}, \underline{p})\rangle \in \alpha$ und $s^N = \langle i,j\rangle$, $i+1<p$,
$j<p \implies M_p \mid\!\!\frac{m}{\rho}\ \Gamma, s \in \alpha$

(α-Schritt) $M_p \mid\!\!\frac{m'}{\rho}\ \Gamma, \langle \underline{i}, \underline{j}\rangle \in \alpha$ und $i \in M$, $s^N = \langle i+1, \mathrm{Rem}((i+1)\cdot j, p)\rangle$
$\implies M_p \mid\!\!\frac{m}{\rho}\ \Gamma, s \in \alpha$

Um nun wie in Abschnitt 12 fortzufahren, zeigen wir folgende zusätzliche Inversion.

13.8 Lemma

Gilt $M_p \mid\!\!\frac{m}{\rho}\ \Gamma, s \in \alpha$ und $s^{\mathbf{N}} \neq \langle i, \mathrm{Rem}(i!,p)\rangle$ für alle i, so folgt $M_p \mid\!\!\frac{m}{\rho}\ \Gamma$.

Beweis durch Induktion nach m:

Die Fälle, wo etwas zu tun ist, sind die, in denen $s \in \alpha$ Hauptformel des letzten Schlusses ist. Dafür gibt es drei Möglichkeiten.

(i) Es liegt ein Gleichheitsaxiom vor. Dann gibt es einen Term t mit $s^{\mathbf{N}} = t^{\mathbf{N}}$ und

$(t \notin \alpha) \in \Gamma$. Aus der Voraussetzung folgt $t^{\mathbf{N}} \neq \langle i, \mathrm{Rem}(i!, p)\rangle$ für beliebiges i, also ist Γ ein Axiom (d).

(ii) Der letzte Schluß war ein (α-Rückschritt), also gibt es $i, j \in \mathbb{N}$ und $m' < m$, so daß $s^{\mathbf{N}} = \langle i, j\rangle$, $i+1<p$, $j<p$ und $M_p \mid\!\frac{m'}{\rho}\, \Gamma, t \in \alpha$ für $t :\equiv \langle \mathrm{S}\underline{i}, \mathrm{Rem}((\mathrm{S}\underline{i}) \cdot \underline{j}, p)\rangle$ gilt. Aus der zweiten Voraussetzung folgt $j \neq \mathrm{Rem}(i!, p)$, also gilt wegen $j < p$

$$j \not\equiv i! \mod p\,.$$

Da $0 < i + 1 < p$ ist, gibt es $l \in \mathbb{N}$ mit $l \cdot (i + 1) \equiv 1 \mod p$. Damit folgt

$$(i + 1) \cdot j \not\equiv (i + 1)! \mod p\,,$$

also ist $\mathrm{Rem}((i + 1) \cdot j, p) \neq \mathrm{Rem}((i + 1)!, p)$. Dann produziert die Induktionsvoraussetzung $M_p \mid\!\frac{m'}{\rho}\, \Gamma$.

(iii) Lag als letzter Schluß ein (α-Schritt) vor, so gibt es $i, j \in \mathbb{N}$ und $m' < m$, so daß $s^{\mathbf{N}} = \langle i + 1, \mathrm{Rem}((i + 1) \cdot j, p)\rangle$ und $M_p \mid\!\frac{m'}{\rho}\, \Gamma, t \in \alpha$ für $t :\equiv \langle \underline{i}, \underline{j}\rangle$ gilt. Wäre $j = \mathrm{Rem}(i!, p)$, so würde

$$\begin{aligned} \mathrm{Rem}((i + 1) \cdot j, p) &= \mathrm{Rem}((i + 1) \cdot \mathrm{Rem}(i!, p), p) \\ &= \mathrm{Rem}((i + 1)!, p) \end{aligned}$$

im Widerspruch zur zweiten Voraussetzung folgen. Daher liefert die Induktionsvoraussetzung $M_p \mid\!\frac{m'}{\rho}\, \Gamma$. □

13.9 Eliminationssatz

$M_p \mid\!\frac{m}{\rho}\, \Gamma \implies M_p \mid\!\frac{}{0}\, \Gamma$. □

Den Einbettungssatz für **W** erhalten wir analog zu 12.10.

13.10 Einbettungssatz

Sei $\Gamma \subset \mathbf{\Sigma^{1,W}}$, die Individuenvariablen von Γ seien in $\{a_1, \ldots, a_n\}$ enthalten, $\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_k\} = \emptyset$ und es gelte $\frac{\vec{b}\,|\,\vec{t}}{S} \big|\!\frac{m}{1}\, \Gamma$, dann gilt für $\vec{n} \in \mathbb{N}^n$ und Primzahlen q

$$\left(\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(q, \vec{n})\right)_q \vdash \Gamma_{p,\vec{a}}(\underline{q}, \underline{\vec{n}})\,.$$ □

Der Beschränkungssatz für dieses halbformale System sieht wie folgt aus, der Beweis ist dergleiche wie für 12.11.

13.11 Beschränkungssatz

$M_p \mid\!\frac{m}{0}\, \langle s_1, t_1\rangle \in \alpha, \ldots, \langle s_k, t_k\rangle \in \alpha \implies \{0, \ldots, \mathrm{Min}(s_1, \ldots, s_k) - 1\} \subset M$. □

Wir haben nun alle Punkte erfüllt, um den Widerspruchsbeweis zu vollenden.

Satz 13.1

$\mathbf{U_2^w} \nvdash Wilson\,.$

Beweis:

Angenommen, *Wilson* gelte in $\mathbf{U_2^w}$. Wie in Abschnitt 12 erhalten wir auch hier aus den gezeigten Lemmata und Sätzen

$$\mathbf{W} \vdash_1 \langle p \dot{-} 1, p \dot{-} 1\rangle \in \alpha$$

und damit

$$\frac{\vec{b}\,|\,\vec{t}}{S} \vdash_1 \langle p \dot{-} 1, p \dot{-} 1\rangle \in \alpha \tag{1}$$

für gewisse $\vec{b}, \vec{t}, S$. Wieder gibt es ein Polynom p mit

$$\#\Big(\mathrm{Sp}^{\vec{b};\vec{t};S}(n)\Big) \leq \mathrm{p}(|n|)$$

für beliebige n.

Andererseits folgt aus (1) für Primzahlen q

$$\Big(\mathrm{Sp}^{\vec{b};\vec{t};S}(q)\Big)_q \vdash_0 \langle \underline{q} \dot{-} 1, \underline{q} \dot{-} 1\rangle \in \alpha\,,$$

mithin

$$\{0, \ldots, q-2\} \subset \mathrm{Sp}^{\vec{b};\vec{t};S}(q)\,.$$

Kombinieren wir die Abschätzungen, so erhalten wir

$$2^{|q|} \leq 2 \cdot \mathrm{p}(|q|) + 3\,,$$

was für hinreichend große Primzahlen q zum Widerspruch führt. □

Wir nutzen die schwache Größenordnung der Anzahl spezieller Regelanwendungen in $\mathbf{U_2^w}$-Herleitungen auch im nächsten Abschnitt aus. Dort zählen wir die Beispiele in $(\exists\leq)$-Anwendungen, die zu einer festgelegten Formel $\exists x{\leq}2 \cdot c\,F(x)$ führen. Diese Zahl wird im halbformalen System linear zu c sein, wodurch wir zu einem Widerspruch gelangen.

14 Komprehension in der ersten Stufe

Wie schon in der Bemerkung zu Satz 5.9 angedeutet, ist eine Komprehension in der Form

$$\exists x{\le}2\cdot c\,\forall y{<}|c|\,(\mathrm{Bit}(y,x)=1 \leftrightarrow y\in\alpha)$$

nicht in $\mathbf{U_2^w}$ herleitbar. Daß dies in $\mathbf{U_2^1}$ gilt, lt sich durch L-Induktion nach a in

$$\exists x{\le}2\cdot c\,\forall y{<}|c|\,(y\le a \to (\mathrm{Bit}(y,x)=1 \leftrightarrow y\in\alpha))$$

zeigen ([Takeuti 1991] §3 Punkt 1).

14.1 Satz

$$\mathbf{U_2^w} \not\vdash \exists x{\le}2\cdot c\,\forall y{<}|c|\,(\mathrm{Bit}(y,x)=1 \leftrightarrow y\in\alpha)\,.$$

Zur Abkürzung definieren wir die Formel

$$Ktrl(a,c) \;:\equiv\; \forall y{<}|c|\,(\mathrm{Bit}(y,a)=1 \leftrightarrow y\in\alpha)\,.$$

Sei $\mathbf{K}$ das Fragment $\mathbf{U_2^w}$, in dem α wie ein Prädikatszeichen und c wie eine Konstante behandelt werden, d. h. sie dürfen nie Eigenvariable sein und auch nicht mehr zu den freien Variablen gezählt werden. In $\mathbf{K}$ werden für beliebige Terme s die $(\exists\le)$-Schlüsse der Gestalt

$$\Gamma, Ktrl(s,c) \quad\Longrightarrow\quad \Gamma, s\not\le 2\cdot c, \exists x{\le}2\cdot c\,Ktrl(x,c)$$

mit (α-Kontroll) bezeichnet und nicht mehr zu $(\exists\le)$ gezählt. Der Term s heißt dann wieder Hauptterm des Schlusses.

Sei $\mathbf{K}-\mathsf{rg} := \mathbf{U_2^w}{-}\mathsf{rg}$. Zum Beweis des Satzes 14.1 nehmen wir $\mathbf{U_2^w} \vdash \exists x{\le}2{\cdot}c\,Ktrl(x,c)$ an. Dann zeigt partielle Schnittelimination $\mathbf{K} \vdash_1 \exists x{\le}2\cdot c\,Ktrl(x,c)$.

Wir lesen wieder durch Auswahl einer Normalherleitung mit Schranken charakteristische Größen ab, mit deren Hilfe wir einen Speicher definieren, der alle für die Einbettung in ein halbformales System benötigten Hauptterme beschränkt. Dazu ändern wir in der Definition der Normalherleitung mit Schranken 11.4 die Klauseln (a) und (g) ab zu

(a') Ist Γ ein Axiom von $\mathbf{K}$, so gelte für $m<\omega$ beliebig $\frac{\;|\;}{\emptyset}\Big|\frac{m}{1}\;\Gamma$.

(g') $\frac{\vec{b}\,|\,\vec{t}}{S}\Big|\frac{m'}{1}\;\Gamma, Ktrl(s,c) \quad\Longrightarrow\quad \frac{\vec{b}\,|\,\vec{t}}{S\cup\{s\}}\Big|\frac{m}{1}\;\Gamma, s\not\le 2\cdot c, \exists x{\le}2\cdot c\,Ktrl(x,c)$ für $m>m'$.

Dabei ist für die Klausel (b) zu berücksichtigen, daß die (α-Kontroll)-Schlüsse nicht mehr zu $(\exists\le)$ zählen.

Damit erhalten wir aus $\mathbf{K} \mid\!\frac{m}{1}\ \Gamma$ die Existenz einer Normalherleitung mit Schranken wie in Abschnitt 11.

14.2 Satz (Existenz einer Normalherleitung mit Schranken)

Sei $\Gamma \subset \mathbf{\Sigma^{1,w}}$ und gelte $\mathbf{K} \mid\!\frac{m}{1}\ \Gamma$, dann gibt es eine Normalherleitung mit Schranken von Γ, d. h. es existieren gewisse $\vec{b}, \vec{t}$ und S mit

$\frac{\vec{b}\mid\vec{t}}{S} \mid\!\frac{m}{1}\ \Gamma$. □

Wir definieren den Speicher zu einer Normalherleitung $\frac{\vec{b}\mid\vec{t}}{S} \mid\!\frac{m}{1}\ \Gamma$ wie in Abschnitt 11 und geben die Abschätzung der Mächtigkeit des Speichers nach oben hin an. Die freien Variablen von Γ seien in $\{a_1, \ldots, a_n\}$ mit $\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_k\} = \emptyset$ enthalten.

14.3 Definition

Für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$ sei $\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l, \vec{n})$ die Menge

$$\Big\{ s(\vec{b}) \mid s \in S_{C,\,\vec{a}}(l, \vec{n}) \text{ und } b_i \leq |T_i[\vec{t}]_{C,\,\vec{a}}(l, \vec{n})| \text{ für } i = 1, \ldots, k \Big\}.$$

14.4 Lemma

Es gibt ein geeignetes Polynom p mit

$$\#\Big(\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l, \vec{n})\Big) \leq \mathrm{p}(|l|, |\vec{n}|)$$

für $l \in \mathbb{N}$ und $\vec{n} \in \mathbb{N}^n$. □

Zwecks Abschätzung des Speichers nach unten betten wir Normalherleitungen mit Schranken in ein passendes halbformales System ein. Dazu zeichnen wir in dem halbformalen System aus Abschnitt 10 die (α-Kontroll)-Schlüsse aus, die alle benötigten Beispiele für diesen speziellen ($\exists\leq$)-Schluß aufsammeln.

14.5 Induktive Definition des halbformalen Systems $M \mid\!\frac{m}{\rho}\ \Gamma$ für $\mathbf{K}$

Seien $M \subset_{\mathrm{fin}} \mathbb{N}$, $m' < m < \omega$, $\rho < \omega \cdot 2$ und $\Gamma \subset \mathbf{\Sigma^{1,b}}$ ohne freie Individuenvariablen. Wir spezialisieren die Definition 10.3 zu

<u>zusätzliche Schlüsse:</u>

(α-Kontroll) $M \mid\!\frac{m'}{\rho}\ \Gamma, Ktrl(\underline{i}, \underline{n})$ und $i \in M$, $i \leq 2 \cdot n$

$\Longrightarrow$ $M \mid\!\frac{m}{\rho}\ \Gamma, \exists x{\leq}2 \cdot \underline{n}\, Ktrl(x, \underline{n})$

Wir erhalten den Einbettungssatz für $\mathbf{K}$ wir in Abschnitt 11.

14.6 Einbettungssatz

Sei $\Gamma \subset \mathbf{\Sigma^{1,w}}$, die Individuenvariablen von Γ seien in $\{a_1, \ldots, a_n\}$ enthalten, $\{a_1, \ldots, a_n\} \cap \{b_1, \ldots, b_k\} = \emptyset$ und es gelte $\frac{\vec{b}\,|\,\vec{t}}{S}\Big|\frac{m}{1}\ \Gamma$, dann gilt für $\vec{n} \in \mathbb{N}^n$ und $l \in \mathbb{N}$

$$\mathrm{Sp}_{\vec{a}}^{\vec{b};\vec{t};S}(l, \vec{n}) \vdash \Gamma_{c,\vec{a}}(\underline{l}, \underline{\vec{n}})\,. \qquad \square$$

Der Beschränkungssatz für dieses halbformale System benutzt die (α-Kontroll)-Exportation.

14.7 (α-Kontroll)-**Exportation**

Sei $M = \{i_1, \ldots, i_k\}$ für Zahlen $i_1, \ldots, i_k \in \mathbb{N}$, dann gilt

$$M \vdash^{m} \Gamma, \exists x{\le}2 \cdot \underline{n}\, Ktrl(x, \underline{n}) \quad \Longrightarrow \quad \vdash \Gamma, Ktrl(\underline{i_1}, \underline{n}), \ldots, Ktrl(\underline{i_k}, \underline{n})\,.$$

Beweis durch Induktion nach m:

War der letzte Schluß keine (α-Kontroll)-Anwendung, dann folgt die Behauptung aus der Induktionsvoraussetzung mit demgleichen Schluß oder Γ ist ein Axiom, da $\exists x{\le}2 \cdot \underline{n}\, Ktrl(x, \underline{n})$ nicht Hauptformel eines Axioms ist. Bleibt noch der Fall, daß der letzte Schluß eine (α-Kontroll)-Anwendung war, also lag ohne Einschränkung die Prämisse

$$M \vdash^{m'} \Gamma, \exists x{\le}2 \cdot \underline{n}\, Ktrl(x, \underline{n}), Ktrl(\underline{i}, \underline{n})$$

mit $i \in M$ und $i \le 2 \cdot n$ vor. Daraus folgt mit der Induktionsvoraussetzung, da $i \in M = \{i_1, \ldots, i_k\}$ ist, die Behauptung. $\square$

14.8 Beschränkungssatz

$$M \vdash \exists x{\le}2 \cdot \underline{n}\, Ktrl(x, \underline{n}) \quad \Longrightarrow \quad \#M \ge 2^{|n|}\,.$$

Beweis:

Sei $k := \#M$, dann gibt es Zahlen $i_1, \ldots, i_k \in \mathbb{N}$ mit $M = \{i_1, \ldots, i_k\}$. Mit (α-Kontroll)-Exportation folgt

$$\vdash Ktrl(\underline{i_1}, \underline{n}), \ldots, Ktrl(\underline{i_k}, \underline{n})\,.$$

Also zeigt der Korrektheitssatz für das halbformale System

$$\mathbb{N} \models (Ktrl(\underline{i_1}, \underline{n}) \vee \ldots \vee Ktrl(\underline{i_k}, \underline{n}))_{\alpha}(\mathcal{M})$$

für alle $\mathcal{M} \subset \{0, \ldots, |n| - 1\}$.

Gäbe es $\mathcal{M}, \mathcal{N} \subset \{0, \ldots, |n| - 1\}$ und $j \in \{1, \ldots, k\}$ mit $\mathcal{M} \ne \mathcal{N}$ und

$$\mathbb{N} \models \forall y{<}\underline{n}\, (\mathrm{Bit}(y, \underline{i_j}) = 1 \leftrightarrow y \in \mathcal{M}) \tag{1}$$

$$\mathbb{N} \models \forall y{<}\underline{n}\, (\mathrm{Bit}(y, \underline{i_j}) = 1 \leftrightarrow y \in \mathcal{N})\,, \tag{2}$$

dann gibt es $l<|n|$ mit $(l\in\mathcal{M}\leftrightarrow l\notin\mathcal{N})$, da $\mathcal{M}\neq\mathcal{N}$ ist. Ohne Einschränkung sei $l\in\mathcal{M}$. Damit erhalten wir den Widerspruch

$$1\overset{(1)}{=}\mathrm{Bit}(l,i_j)\overset{(2)}{=}0\,.$$

Also ist

$$k\geq\#\Big(\mathcal{P}(\{0,\ldots,|n|-1\})\Big)=2^{|n|}$$

gezeigt. □

Wir haben nun alle Punkte erfüllt, um den Widerspruchsbeweis zu vollenden.

Satz 14.1

$\mathbf{U_2^w}\nvdash\exists x{\leq}2\cdot c\,\forall y{<}|c|\,(\mathrm{Bit}(y,x)=1\leftrightarrow y\in\alpha)$.

Beweis:

Angenommen, es gilt $\mathbf{U_2^w}\vdash\exists x{\leq}2\cdot c\,Ktrl(x,c)$. Mit partieller Schnittelimination folgt

$$\mathbf{K}\vdash_1\exists x{\leq}2\cdot c\,Ktrl(x,c)\,.$$

Dann existieren mit Satz 14.2 $\vec{b},\vec{t},S$ mit

$$\frac{\vec{b}\mid\vec{t}}{S}\Big|_1\ \exists x{\leq}2\cdot c\,Ktrl(x,c)\,. \tag{1}$$

Mit der Definition des Speichers $\mathrm{Sp}^{\vec{b};\vec{t};S}(n)$ 14.3 und der anschließenden Abschätzung 14.4 gibt es ein geeignetes Polynom p, so daß

$$\#\Big(\mathrm{Sp}^{\vec{b};\vec{t};S}(n)\Big)\leq\mathrm{p}(|n|)$$

für beliebige n gilt.

Nun betten wir die Normalherleitung (1) in das halbformale System ein (14.6)

$$\mathrm{Sp}^{\vec{b};\vec{t};S}(n)\vdash\exists x{\leq}2\cdot\underline{n}\,Ktrl(x,\underline{n})\,.$$

Dann liefert der Beschränkungssatz 14.8

$$\#\Big(\mathrm{Sp}^{\vec{b};\vec{t};S}(n)\Big)\geq 2^{|n|}\,.$$

Also erhalten wir

$$2^{|n|}\leq\mathrm{p}(|n|)\,,$$

was für hinreichend großes n zum Widerspruch führt. □

Auf den letzten Seiten ziehen wir die Quintessenz aus dem gesamten Werk.

15 Quintessenz

Wir fassen zum Ende noch einmal die wichtigsten Ergebnisse dieser Arbeit zusammen. Zuerst halten wir die Charakterisierung der Polynomialen Hierarchie in $\mathbf{U_2^{w^\star}}$ aus Teil B fest:

15.1 Hauptsatz für $\mathbf{U_2^{i,w^\star}}$

Ist $i > 0$, so gilt folgende Äquivalenz:

$$\mathrm{A} \in \mathbf{\Delta_i^p} \iff \text{A ist in } \mathbf{\Delta_i^{1,w^\star}} \text{ bezüglich } \mathbf{U_2^{i,w^\star}} \,. \qquad \square$$

Nun wollen wir noch begründen, daß $\mathbf{U_2^1}$ eine echte Erweiterung von $\mathbf{U_2^{w^\star}}$ ist. Wir stellen aufgrund der Definitionen fest, daß $\mathbf{U_2^1}$ eine Erweiterung von $\mathbf{S_2}(\mathcal{A})$ ist. Damit übertragen sich die Resultate aus Abschnitt 9 auf $\mathbf{U_2^1}$, insbesondere

15.2 Lemma

(i) $A(a) \in \mathbf{\Sigma_0^{1,w^\star}} \implies \mathbf{U_2^1} \vdash \exists x{\leq}(4 \cdot t + 1)\, \forall y{\leq}|t|\, (A(y) \leftrightarrow \mathrm{Bit}(y,x) = 1)\,.$

(ii) $\Gamma \subset \mathbf{\Sigma^{1,w^\star}}$ und $\mathbf{U_2^{w^\star}} \vdash \Gamma \implies \mathbf{U_2^1} \vdash \Gamma^\circ\,.$ $\qquad \square$

Die wesentliche neue Überlegung, die wir noch zum Erhalt des obigen Ergebnisses benötigen, ist

15.3 Lemma

Für $F \in \mathbf{\Sigma^{1,w^\star}}$ gilt $\mathbf{U_2^1} \vdash F \leftrightarrow F^\circ\,.$

Beweis durch Induktion nach der Länge von F:

Dazu nutzen wir im interessanten Fall, $F \equiv \mathrm{Q}\phi\, G(\phi^{|t|})$, zum einen die in $\mathbf{U_2^1}$ gegebene Komprehension ($\mathbf{\Sigma_0^b}$-CA) und zum anderen die in $\mathbf{U_2^1}$ beweisbare erststufige Komprehension Lemma 15.2 (i) aus. $\qquad \square$

Fügen wir alle Teile zusammen, so erhalten wir

15.4 Satz

$\mathbf{U_2^{w^\star}} \vdash \Gamma \implies \mathbf{U_2^1} \vdash \Gamma\,.$

Beweis:

Wir überlegen uns, daß alle nicht-logischen Axiome von $\mathbf{U_2^{w^\star}}$ in $\mathbf{U_2^1}$ beweisbar sind. Der einzige nicht offensichtliche Fall ist der, daß ein Induktionsaxiom vorliegt.

Die Induktionsaxiome von $\mathbf{U_2^{w^\star}}$ haben die Gestalt

$$F \equiv A(0) \wedge \forall x\, (A(x) \to A(\mathrm{S}x)) \to A(|t|)$$

für ein $A(a) \in \mathbf{\Sigma^{1,w^\star}}$. Für

$$G \;\equiv\; A(0) \wedge \forall x{\leq}|t|\,(A(x) \to A(\mathrm{S}x)) \to A(|t|)$$

zeigt reine Logik

$$F \leftrightarrow G\,. \tag{1}$$

Damit folgt $\mathbf{U_2^{w^\star}} \vdash G$. Hieraus erhalten wir wegen $G \in \mathbf{\Sigma^{1,w^\star}}$ mit Lemma 15.2 (ii) $\mathbf{U_2^1} \vdash G^\circ$ und daraus mit Satz 15.3 $\mathbf{U_2^1} \vdash G$.

Mit (1) ist F in $\mathbf{U_2^1}$ beweisbar. □

15.5 Korollar

$\mathbf{U_2^1}$ ist eine echte Erweiterung von $\mathbf{U_2^{w^\star}}$.

Beweis:

Dies ist der letzte Satz im Einklang mit einem der Sätze 11.1, 12.1, 13.1 oder 14.1.

□

Literatur

Barwise, Jon

1977 *An Introduction to First-Order Logic*, in: Barwise, J. (Hrsg.), Handbook of Mathematical Logic, S. 5-46

Buss, Samuel R.

1986 *Bounded Arithmetics*, Bibliopolis

Glaß, Thomas

1990 *Partielle Modelle von Theorien imprädikativer Mengenlehre*, Diplomarbeit Münster

Jan Krajíček, Pavel Pudlák und Gaisi Takeuti

1991 *Bounded Arithmetic and the Polynomial Hierarchy*, Annals of Pure and Applied Logic 52, S. 143-153

Pohlers, Wolfram

1989 *Proof Theory: An Introduction*, Springer

Stockmeyer, Larry J.

1976 *The Polynomial-Time Hierarchy*, Theoretical Computer Science 3, S. 1-22

Takeuti, Gaisi

1987 *Proof Theory*, 2. Auflage, North Holland

1988 *Bounded Arithmetic and Truth Definition*, Annals of Pure and Applied Logic 39, S. 75-104

1990a *Sharply Bounded Arithmetic and the Function* $a \dot{-} 1$, Logic and Computation, Contemporary Mathematics 106, American Mathematical Society, S. 281-288

1990b $\mathbf{S}^{\mathbf{i}}_{\mathbf{3}}$ *and* $\mathbf{V}^{\mathbf{i}}_{\mathbf{2}}(\mathbf{BD})$, Archive for Mathematical Logic 29, S. 149-169

1991 *A Second Order Version of* $\mathbf{S}^{\mathbf{i}}_{\mathbf{2}}$ *and* $\mathbf{U}^{\mathbf{1}}_{\mathbf{2}}$, The Journal of Symbolic Logic 56, S. 1038-1063

Savage, John E.

1976 *The Complexity of Computing*, Wiley-Interscience

Schütte, Kurt

1977 *Proof Theory*, Springer

Schwichtenberg, Helmut

1977 *Proof Theory: Some Applications of Cut-Elimination*, in: Barwise, J. (Hrsg.), Handbook of Mathematical Logic, S. 867-895