Ludwig-Maximilians-Universität München
Mathematisches Institut

Diplomarbeit

Eine gemeinsame Verallgemeinerung von Realisierbarkeitsmodellen und Heyting-Algebra-bewerteten Modellen für konstruktive Mengenlehre CZF

Albert Ziegler

Betreuer	:	Prof. Dr. Wilfried Buchholz
Eingereicht am	:	

Hiermit erkläre ich, diese Arbeit selbstständig und unter Benutzung keiner anderen als den angegebenen Quellen verfasst zu haben.

Inhaltsverzeichnis

Kapitel 1

Einleitung

Eine der bekanntesten Eigenschaften der klassischen Zermelo-Fraenkelschen Mengenlehre ZFC ist, dass sie, obwohl sie für fast jede Frage, die auf anderen Gebieten forschende Mathematiker interessiert, eine Antwort zu haben scheint (und also eine geeignete Fundierung der Mathematik ist), dennoch in hohem Maße unvollständig ist. Man muss keine gödelschen Lügnerkonstruktionen anwenden, um unentscheidbare Sätze zu finden, sondern viele der natürlich aus dem Gebiet der Mengenlehre wachsenden Fragen sind in ZFC (und a forteriori ZF) unentscheidbar: Die Kontinuumshypothese, Prinzipien der kombinatorischen Mengenlehre wie $\diamondsuit$ oder Martins Axiom, die Souslin-Hypothese oder große Kardinalzahlaxiome (vorausgesetzt, sie sind überhaupt konsistent).

Dies mag zunächst als Schwachpunkt der Theorie erscheinen, insofern dass man ZFC für eine fahrlässige Unterbestimmung des Mengenuniversums halten mag, und man könnte geneigt sein, dieses System durch ein vollständigeres (wie ZFC+$V = L$) zu ersetzen. Tatsächlich begeht aber nur ein verschwindender Bruchteil der Mengentheoretiker diesen Weg. Ein Teil begründet dies mit einem quasi-platonischen Argument des Vertrauens in die Gültigkeit der ZF(C)[1] Axiome, das sich nicht auf Axiome wie $V=L$ erstreckt.

Der größte Teil wird allerdings darauf hinweisen, dass die vermeintliche Schwäche schon längst als Stärke erkannt wurde. Wer $V = L$ als Axiom annimmt, beschränkt sich auf solche Welten, in denen die Kontinuumshypothese gilt und in denen es keine messbaren Kardinalzahlen gibt und verpasst so viel untersuchenswerte Struktur. Außerdem ist für die restliche Mathematik durchaus auch die Möglichkeit interessant, unterschiedliche Axiome anzunehmen (etwa das Axiom der Determiniertheit für die Spieltheorie oder die Lebesguemessbarkeit aller Teilmengen der reellen Zahlen).

Ein überaus bedeutender Anteil der Impulse der modernen Mengenlehre wurde durch den Wunsch zur Untersuchung von relativen Modellen der Mengenlehre gegeben. Diese gehen von einem bereits existierenden Modell aus und transformieren es in ein anderes, über das eventuell mehr ausgesagt werden kann. Üblicherweise wird dies „von innen“ ausgeführt, das heißt es wird nicht von einer Menge ausgegangen, die Modell ist, und dann eine anderes Modell konstruiert, sondern man arbeitet in dem Modell und gibt eine Klasse an, die wieder die Eigenschaften eines Modells der Mengenlehre hat.

[1] Die Bezeichnung „ZF(C)“ soll andeuten, dass die gemachten Aussagen sowohl für ZF als auch für ZFC gelten.

Diese Modellkonstruktionen schulen nicht nur die Intuition über Universen und geben Einblicke in das Zusammenspiel verschiedener Prinzipien, sondern liefern ganz konkrete Unabhängigkeits- und Konsistenzresultate. Dabei spielt es keine Rolle, wenn die Konstruktion außer finitistischen Methoden die Mengenlehre im Hintergrund verwendet. Denn kann man in ZF(C) ausgehend von einem Modell für ZF(C) eines für ZF(C)+Γ konstruieren, so gilt

$$ZF(C) \vdash Cons(ZF(C)) \to Cons(ZF(C) + \Gamma)$$

Wäre nun ZF(C)+Γ inkonsistent, so wäre dies auch ein Theorem von ZF(C) und also wäre

$$ZF(C) \vdash \neg Cons(ZF(C))$$

Dann wäre aber schon ZF(C) inkonsistent (etwa nach dem Satz von Löb [18]). Also ist ZF(C)+Γ relativ konsistent[2].

Die ersten relativen Modelle für klassische Mengenlehre zeichneten sich dadurch aus, dass sie – unter Verwendung der natürlichen Elementschaftsbeziehung – das Universum verkleinerten, also auf bestimmte Mengen harmloserer Art beschränkten, über die man viele Aussagen treffen konnte (beispielsweise die konstruktiblen Mengen in Gödels L). Da es mit Gödels L ein kleinstes solches inneres Modell gibt, ist der Anwendbarkeit dieser Methode Schranken aufgelegt. Was in L nicht gilt, kann man in keinem inneren Modell zeigen, da eventuell L schon das ganze Universum und das innere Modell also wieder L sein könnte. Um weitere Resultate zu erzielen, mussten also Verfahren entwickelt werden, die das Universum vergrößern.

Dies gelang Cohen mit seiner berühmten Forcing-Konstruktion, die sich als überaus mächtig erwiesen hat. Hierbei wird eine Klasse an Namen, die auf eine partielle Ordnung Bezug nehmen, erzeugt, in die das Universum V natürlicherweise eingebettet werden kann, und auf denen eine etwas komplexere Elementrelation (und Logik) definiert wird[3]. Auf Grund geeigneter Einbettungstheoreme kann man sich auf Boolesche Algebren als partielle Ordnungen beschränken. Dann besteht die Klasse der Namen, also das Universum des Modells, aus Mengen, deren Elemente erblich mit Elementen der Booleschen Algebra bewertet sind. Man gibt den Mengen des konstruierten Modells also gewissermaßen mehr Information zu jedem Element mit: Während eine Menge im Hintergrund zu jedem Element nur die Information hat, *dass* es darin liegt, hat eine Menge des Modells auch die Information *wie sehr*.

Ähnlich wie ZF(C) als Fundament der klassischen Mathematik dient, wurde Aczels Theorie CZF als Fundament der konstruktiven Mathematik konzipiert. Es enthält jene Prinzipien, die (fast) allen konstruktiven Mathematikern gemein sind, und kann je nach Bedarf einer einzelnen Schule um einige ergänzt werden – Brouwersche Intuitionisten würden etwa das FAN-Theorem hinzunehmen wollen, russische Konstruktivisten die Churchsche These oder Markovs Prinzip und

[2]Dieser Beweis der relativen Konsistenz durch Kontraposition ist nicht unkonstruktiv, da es sich bei Konsistenz um eine negative Aussage handelt.

[3]Dies ist nicht identisch mit Cohens ursprünglichem Zugang zu Forcing, motiviert aber die im folgenden ausgeführten Konstruktionen besser.

Analytiker der Bishopschen Schule vermissen vermutlich ein Auswahlprinzip wie DC. Gerade die Eigenschaft, viele sinnvolle und interessante Erweiterungen zu besitzen (überhaupt hat CZF ja viel mehr Erweiterungen als ZF), die grundlegenden Konstruktionen aber ausführen zu können und dabei beweistheoretisch eine relativ niedrige Stärke zu haben, verheißt Hoffnung auf eine spannende Theorie der Modelle.

Die Forcing-Konstruktion kann in Kontexten mit intuitionistischer Logik übernommen und sogar verallgemeinert werden. Man kann nämlich bei den Booleschen Algebren auf die Forderung, in ihnen müsse das ausgeschlossene Dritte gelten, verzichten und also Heyting-Algebren betrachten. Leider sind in einer prädikativen Theorie wie CZF Heyting-Algebren (oder gar Boolesche Algebren) äußerst rar. Mittels des Zusammenhangs von Heyting-Algebren zu formalen Topologien hat Gambino allerdings die Forcing-Konstruktion erfolgreich auf CZF adaptiert [15].

Eine weitere Methode um Modelle konstruktiver Theorien zu gewinnen ist die von Kleene für die Heyting-Arithmetik eingeführte Realisierbarkeit. Ein Realisierer einer Formel ist hierbei eine Art Algorithmus, der den konstruktiven Inhalt einer Formel zu fassen sucht. Will man diese Methode auf die Mengenlehre adaptieren, konstruiert man ein Universum, in dem jedes Element einer Menge mit einem Realisierer, der intuitiv gesprochen den Grund angibt, aus dem das Element in der Menge ist, gegeben ist (auf erbliche Weise). McCarty [20] entwickelte dies für die extensionale, aber unprädikative Mengenlehre IZF und Rathjen [22] adaptierte diese Methode für die konstruktive Theorie CZF. Damit erzielte er nicht nur zahlreiche Unabhängigkeitsresultate sondern auch viele andere interessante Ergebnisse (etwa die $\vee$- und die $\exists^\omega$ Eigenschaft von CZF), was die Bedeutung dieser Methode unterstreicht.

Diese Arbeit ist angeregt durch eine Vermutung von Peter Aczel, dass diese beiden Hauptmethoden für relative Modellkonstruktionen gemeinsam verallgemeinert werden könnten (und für höherstufige Logik entwickelt er derartiges impredikativ [4]). Dies ist in der Tat der Fall und diese gemeinsame Verallgemeinerung soll vorgestellt und untersucht werden.

Dabei wird zunächst in Kapitel 2 kurz auf die Theorie CZF und die anderen Theorien (etwa IZF) eingegangen, die Theorien werden vorgestellt und einige wesentliche Tatsachen wiederholt. Im dritten Kapitel werden die im Folgenden wesentlichen algebraischen Strukturen eingeführt. Applikative Strukturen entsprechen der Realisierbarkeitstheorie und Heyting-Algebren und formale Topologien der konstruktiven Erweiterung von Forcing. Indem man eine formale Topologie mit zusätzlicher Struktur aufrüstet, erhält man die algebraische Struktur namens *applikative Topologie*. Da diese Struktur hier erstmals eingeführt wird, werden einige im Späteren wichtige Eigenschaften über sie hergeleitet, insbesondere ihre Fähigkeiten zum Betreiben von Rekursionstheorie.

Die eigentliche Modellkonstruktion erfolgt im Kapitel 4. Zunächst wird das Modell definiert, das eine applikative Struktur als freien Parameter hat, und anschließend wird gezeigt, dass in ihm Prädikatenlogik und CZF gilt, sofern dies im Hintergrunduniversum zutrifft. Dieses Resultat wird sogar nicht nur für CZF gezeigt, sondern auch für IZF und einige Zwischentheorien, für alle die die vorgestellte Methode also relative Modelle zu liefern im Stande ist. Dieser Abschnitt ist relativ aufwändig, da die Beweise deutlich komplizierter als in den Spezialfällen der Heyting-Modelle und der Realisierbarkeit sind. Danach werden einige Absolutheitsresultate betrachtet, was einerseits schon als direktes Studieren der erhaltenen Modelle zu zählen ist, andererseits aber auch als Erweiterung der Modellkonstruktion auf weitere Theorien gesehen werden kann. Die dort eingeführte Absolutheit in natürlichen Zahlen ist ein wichtiges Hilfsmittel zum Arbeiten mit den Modellen. Das Kapitel schließt mit einfachen Eigenschaften der realisierten Elementbeziehung und Gleichheit.

Anschließend wird in Kapitel 5 gezeigt, inwiefern Heyting-Modelle (erster Abschnitt) und Realisierbarkeitsmodelle (zweiter Abschnitt) Spezialfälle der eingeführten Techniken sind. Es werden Eigenschaften der applikativen Topologie isoliert, unter denen sich einiges so verhält wie bei Realisierbarkeitsmodellen, die aber doch noch recht allgemein sind.

Die Motivation für Verallgemeinerungen in der Mathematik ist meist der gesteigerte Überblick durch stärkere Abstraktion, verbunden mit erhöhter Ökonomie, die dadurch resultiert, dass man ehedem Getrenntes als Spezialfälle des selben ansieht und die Eigenschaften der Spezialfälle nur einmal, für die Verallgemeinerung, entwickeln muss. Allerdings schwingt natürlich stets die Hoffnung mit, dies könne auch neue Resultate ermöglichen und Anwendungen finden, die mit keinem der Spezialfälle erhalten werden können. Diese Hoffnung wird sich im Kapitel 6 über konkrete Modelle als gerechtfertigt herausstellen. An einigen Beispielen sollen hier applikative Topologien angegeben werden, die weder von Heyting-Algebren noch von applikativen Strukturen herrühren. Die mit ihnen konstruierten Modelle führen zu einigen Äquikonsistenz- und Unabhängigkeitsresultaten, die nach Wissen des Autors neu sind und auch nicht ohne weiteres mit den bekannten Methoden erzielbar sind.

Kapitel 2

Die Theorie CZF

CZF wurde 1978 von Peter Aczel in [5] als konstruktives und prädikatives Fundament der Mengenlehre eingeführt, also für die selbe Rolle, die die klassische Mengenlehre ZFC bezüglich der klassische Mathematik übernimmt. Sie ist schnell zu einer Standardtheorie der konstruktiven Mengenlehre geworden. Als ihre konstruktive Rechtfertigung wird meist ihre Einbettbarkeit in Martin-Löfsche Typentheorie angegeben [29].

Eine gute Referenz für CZF ist [1]. Falls nicht anders angegeben, stammen alle Definitionen und nichttrivialen Resultate über CZF samt Beweis mit nur kleinen Änderungen daraus.

2.1 Axiome

2.1.1 Logische Axiome und einfache Konventionen

CZF ist eine intuitionistische Theorie der ersten Stufe mit Gleichheit. Ihre Sprache enthält abzählbar viele Variablen, für die verschiedenste lateinische und griechische Buchstaben mit Variationen (wie Strichen oder Akzenten), besonders jedoch a, b, c, x, y und z, Mitteilungszeichen sind[1]. Sie enthält die Aussagenkonstante[2] $\bot$, die Junktoren $\wedge$, $\vee$ und $\rightarrow$ und die Quantoren $\forall$ und $\exists$. Die Sprache soll das Zeichen $=$ enthalten, das als logisches Zeichen aufgefasst wird[3].

Klammern sind wie üblich enthalten und es werden die gängigen Klammerkonventionen verwendet, also binden $\wedge$ und $\vee$ etwa stärker als $\rightarrow$, $A \rightarrow B \rightarrow C$ ist zu lesen als $A \rightarrow (B \rightarrow C)$, $A \wedge B \wedge C$ bedeutet $(A \wedge B) \wedge C$ und dergleichen. Gesondert erwähnt werden sollte noch die Konvention, dass in Abwesenheit von Klammern der Bereich des Quantors $\forall x$ kleinstmöglich ist; $\forall x\ \phi \wedge \psi$ bedeutet also etwa $(\forall x \phi) \wedge \psi$. Sind quantifizierte Variable und Matrix des Quantors jedoch durch einen Punkt getrennt, so soll der Bereich des Quantors größtmöglich sein; $\forall x.\phi \wedge \psi$ bedeutet also etwa etwa $\forall x(\phi \wedge \psi)$. Im Allgemeinen sind später eingeführte Klammerkonventionen stärker als früher eingeführte, insbesondere

[1] Tatsächlich werden an späterer Stelle sogar Mitteilungszeichen verwendet, die keine Buchstaben sind, etwa $\leq$. Dies wird dann aber offensichtlich sein.

[2] Dies ist eigentlich nicht notwendig, da man sich diese Aussage auch als $\forall xy.x = y$ definieren könnte.

[3] Das bedeutet, dass die Gleichheitsregeln nicht zu den Axiomen von CZF sondern zu den Regeln des logischen Kalküls gezählt werden.

die zu den Quantoren stärker als die zu den Junktoren. Die Klammerkonvention zu $\Vdash$, die mit der Realisierbarkeit eingeführt wird, wird noch stärker sein.

Wir verwenden $\top$ für $\forall x\ x = x$ und $\neg\phi$ für $\phi \to \bot$. Andere Schreibweisen, wie $\phi \leftarrow \psi, \exists! x\ \phi$ oder $\forall x \in a\ \phi$, werden auf die offensichtliche und übliche Weise verwendet.

Die Sprache von CZF hat ein zweistelliges Relationszeichen, nämlich $\in$, wobei wir $a \in b$ statt $\in (a, b)$ schreiben.

Mit $\phi[x := t]$, soll die Formel bezeichnet sein, die aus der Formel ϕ entsteht, in der man alle freien Vorkommnisse von x durch t ersetzt. Mit der Schreibweise $\phi(x)$ ist nur gemeint, dass in Zukunft $\phi(t)$ als $\phi[x := t]$ gelesen werden soll. Dabei kann t eine Variable oder ein Klassenterm sein:

Ein Klassenterm ist ein Ausdruck der Gestalt $\{x|\phi\}$, wobei ϕ eine beliebige Formel ist. Klassenterme werden wir in Formeln syntaktisch wie freie Variablen verwenden. Formeln mit Klassentermen sind nur Abkürzungen für entsprechende längere Formeln in der Sprache von CZF, wobei

- $x \in \{y|\phi\}$ eine Abkürzung ist für $\phi[y := x]$
- $x = \{y|\phi\}$ eine Abkürzung ist für $\forall z \in x\ \phi(z) \wedge \forall z.\phi(z) \to z \in x$
- $\{y|\phi\} = x$ eine Abkürzung ist für $\forall z \in x\ \phi(z) \wedge \forall z.\phi(z) \to z \in x$
- $\{y|\phi\} \in x$ eine Abkürzung ist für $\exists z \in x\ z = \{y|\phi\}$
- $\{y|\phi\} \in \{y|\psi\}$ eine Abkürzung ist für $\exists z.\ z = \{y|\phi\} \wedge z \in \{y|\psi\}$
- $\{y|\phi\} = \{y|\psi\}$ eine Abkürzung ist für $\forall z.\ z \in \{y|\phi\} \leftrightarrow z \in \{y|\psi\}$
- $\{y|\phi\} \subseteq \{y|\psi\}$ eine Abkürzung ist für $\forall z.\ z \in \{y|\phi\} \to z \in \{y|\psi\}$

Die Quantoren laufen nicht über Klassenterme. Insbesondere wird man für t Klassenterm aus $\forall x\ \phi(x)$ nicht auf $\phi[x := t]$ und aus $\phi(t)$ nicht auf $\exists x\ \phi(x)$ schließen können. Mit Aussagen wie „Für alle Klassen ...“ oder „Es gibt eine Klasse ...“ meinen wir die entsprechende metasprachliche Aussage wie „Für alle Formeln gilt für den von ihnen definierten Klassenterm ...“. Dabei soll Existenz einer Formel die Angebbarkeit einer solchen beinhalten. Ohne damit ontologische Voraussetzungen zu implizieren, wird von „Klassen“ als das, was von Klassentermen bezeichnet wird, gesprochen — ebenso, wie von „Mengen“ als das, was die Variablen bezeichnen, gesprochen wird. Mit der Ausdrucksweise, eine Klasse mit dem entsprechenden Klassenterm $\{y|\phi\}$ sei eine Menge, ist die Aussage $\exists x\ x = \{y|\phi\}$ gemeint. Mengen a werden mit der Klasse mit Klassenterm $\{y|y \in a\}$ identifiziert. Die Rechtfertigung dafür nimmt man daraus, dass die Aussage $\forall x\ \{y|y = a\} = x$ ableitbar ist. Den Klassenterm $\{y|\bot\}$ kürzt man mit $\emptyset$ ab und bezeichnet die entsprechende Klasse als leere Klasse. Den Klassenterm $\{y|\top\}$ kürzt man mit V ab und bezeichnet die entsprechende Klasse als Allklasse. Für eine Menge a bezeichnet man mit $P(a)$ die Potenzklasse $\{x|x \subseteq a\}$.

Klassenterme der Form $\{x|\phi(x)\}$ können freie Variablen enthalten, x wird allerdings als gebunden betrachtet. In der Zukunft soll im Falle einer drohenden Variablenkollision stets automatisch eine gebundene Umbenennung geschehen, ohne dass dies explizit erwähnt wird.

CZF ist eine intuitionistische Theorie erster Stufe mit Gleichheit, ein Kalkül (im Hilbert-Stil) dafür ist etwa [20]:

1. $\phi \to (\psi \to \phi)$
2. $(\phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))$
3. $\phi \to (\psi \to (\phi \wedge \psi))$
4. $(\phi \wedge \psi) \to \phi$
5. $(\phi \wedge \psi) \to \psi$
6. $\phi \to (\phi \vee \psi)$
7. $\psi \to (\phi \vee \psi)$
8. $(\phi \vee \psi) \to (\phi \to \theta) \to (\psi \to \theta) \to \theta$
9. $(\phi \to \psi) \to (\phi \to \neg\psi) \to \neg\phi$
10. $\phi \to \neg\phi \to \psi$
11. $\forall x\phi(x) \to \phi[z]$ für z frei für x in ϕ
12. $\phi[z] \to \exists x\phi(x)$ für z frei für x in ϕ
13. $\forall x\ x = x$
14. $\forall xy.\ x = y \to y = x$
15. $\forall xyz.\ x = y \to y = z \to x = z$
16. $\forall xyz.\ x = y \to y \in z \to x \in z$
17. $\forall xyz.\ x = y \to y \ni z \to x \ni z$

Der Kalkül enthält drei Inferenzregeln:

1. $\phi, \phi \to \psi \vdash \psi$
2. $\phi \to \psi(y) \vdash \phi \to \forall x\psi(x)$ für y frei für x in ϕ und nicht frei in ϕ und ψ
3. $\phi(y) \to \psi \vdash \exists x\phi(x) \to \psi$ für y frei für x in ϕ und nicht frei in ϕ und ψ

2.1.2 $CZF_{-,-}$

Die Axiome von CZF ergeben sich aus den Axiomen der Zermelo-Fraenkel-Mengenlehre ZF, indem jedes dieser Axiome durch ein klassisch dazu äquivalentes ersetzt wird, das aber eine prädikative und konstruktive Aussage ist.

Die Grundaxiome über Extensionalität, Paar- und Vereinigungsmengen werden übernommen:

Extensionalitätsaxiom $\forall a, b.\ \forall c{\in}a\ c{\in}b \wedge \forall c{\in}b\ c{\in}a \to a = b$

Paarmengenaxiom $\forall a, b\exists c\ c = \{x | x = a \vee x = b\}$

Ein solches c (das nach Extensionalität eindeutig ist) bezeichnet man mit $\{a, b\}$.

Vereinigungsmengenaxiom $\forall a\exists b\ b = \{x | \exists y{\in}a\ x{\in}y\}$

Dieses ebenfalls eindeutige b bezeichnet man mit $\bigcup a$. $\bigcup\{a, b\}$ wird auch kurz $a \cup b$ geschrieben.

Δ_0-Separation $\forall a \exists b\ b = \{x | x \in a \wedge \phi(x)\}$ (für alle ϕ beschränkte Formel, b nicht frei in $\phi(x)$)

Δ_0-Separation ist eine Abschwächung des klassischen Axioms der vollen Separation. Im Unterschied zur klassischen Mengenlehre wird nämlich nur für Δ_0-Formeln (auch beschränkte Formeln) ϕ, also solche, in denen alle Quantoren durch Mengen beschränkt sind, mithin nur in der Form $\exists a \in b$ bzw. $\forall a \in b$ vorkommen, Aussonderung gefordert.

Diese Einschränkung entspricht dem Prinzip der Prädikativität: Um zu neuen Mengen zu gelangen, kann man nicht von einem bereits vollendeten Mengenuniversum ausgehen. Die Aussonderung nach einer unbeschränkten Formel würde allerdings die neue Menge $\{x | x \in a \wedge \phi(x)\}$ einführen, was das Mengenuniversum, auf das $\phi(x)$ Bezug nehmen würde, ändert. So wären die Elemente der Menge von einer Eigenschaft der sich durch die Einführung dieser Menge ändernden Gesamtheit aller Mengen abhängig.

Das klassische Fundierungsaxiom würde das ausgeschlossene Dritte implizieren. Es wird darum durch das in intuitionistischer Logik schwächere Prinzip der Mengeninduktion (Set Induction) ersetzt:

Mengeninduktion $\forall a(\forall b{\in}a\ \phi(b) \rightarrow \phi(a)) \rightarrow \forall a \phi(a)$

Das Unendlichkeitsaxiom sollte so formuliert werden, dass es eine kleinste induktive Menge gibt. Im Gegensatz zu Systemen mit voller Separation kann man aus einer beliebigen induktiven Menge sonst nämlich nicht per Aussonderung eine kleinste solche erhalten:

Unendlichkeitsaxiom $\exists \omega.(\emptyset \in \omega \wedge \forall n{\in}\omega\ n \cup \{n\} \in \omega) \wedge \forall \omega'.$
$(\emptyset \in \omega' \wedge \forall n{\in}\omega'\ n \cup \{n\} \in \omega') \rightarrow \omega \subseteq \omega'$

Der Zeuge für diese Aussage wird auch in Zukunft mit ω bezeichnet und die Menge der natürlichen Zahlen genannt. $n \cup \{n\}$ wird auch mit $n + 1$ bezeichnet.

Die Theorie, die nur die bisherigen Axiome enthält, heiße $CZF_{-,-}$. Sie reicht für die folgende Modellkonstruktion bereits aus[4], wie sie auch überhaupt für viele andere, einfache mengentheoretischen Konstruktionen genügt. Die beiden weiteren Axiome von CZF werden auch oft abgeschwächt oder verstärkt betrachtet. Darum sollen hier mehrere Erweiterungen von $CZF_{-,-}$ zugleich definiert werden, die bis zu eine Variation des Ersetzungsschemas und bis zu eine Variation des Potenzmengenaxioms enthalten.

Vorher einige Eigenschaften und Definitionen:

Definition 1. *Zu a und b Mengen sei das Paar (a, b) definiert als $\{\{a\}, \{a, b\}\}$. Es gilt:*

$$(a, b) = (c, d) \leftrightarrow a = c \wedge b = d$$

Es sei $x \times y = \{(a, b) | a \in x \wedge b \in y\}$. Dies ist eine Menge, falls x und y Mengen sind. Eine Teilklasse r von $x \times y$ heißt Relation von x nach y, und es sei

[4] wenn auch nicht zum Beweis des Konsistenzsatzes für CZF für diese Modelle

- $r^{-1} := \{(b,a)|(a,b) \in r\}$
- $r[X] := \{b \in y | \exists a \in X\ (a,b) \in r\}$
- $r(a) := b$, *falls* $\exists! b'\ (a,b') \in r \wedge (a,b) \in r$
- $r : x \rightrightarrows y$, *falls* $\forall a \in x\ \exists b \in y\ (a,b) \in r$. *Ein solches* r *nennt man auch mehrwertige Funktion oder mv-Funktion oder totale Relation.*
- $r : x \leftleftarrows\!\!\rightrightarrows y$, *falls* $r : x \rightrightarrows y \wedge r^{-1} y \rightrightarrows x$
- $r : x \to y$, *falls* $\forall a \in x\ \exists b \in y\ r(a) = b$. *Ein solches* r *nennt man auch Funktion.*
- $r : x \hookrightarrow y$, *falls* $r : x \to y \wedge \forall b \in y\ \forall a, a' \in x.\ (a,b) \in r \wedge (a',b) \in r \to a = a'$. *Ein solches* r *nennt man injektiv.*
- $r : x \twoheadrightarrow y$, *falls* $r : x \to y \wedge r^{-1} : y \rightrightarrows x$. *Ein solches* r *nennt man surjektiv.*
- $r : x \leftrightarrow y$, *falls* $r : x \twoheadrightarrow y \wedge r : x \hookrightarrow y$, *was äquivalent ist zu* $r : x \to y \wedge r^{-1} : y \to x$. *Ein solches* r *nennt man bijektiv.*

In Übereinstimmung mit dem üblichen mathematischen Sprachgebrauch wird manchmal auch $r^{-1}y$ *verwendet für* $r^{-1}[\{y\}]$ *und* $r^{-1}(Y)$ *für* $r^{-1}[Y]$, *dies wird aber aus dem Zusammenhang hervorgehen. Steht statt* r *eine Formel* $\phi(x,y)$ *mit zwei ausgezeichneten Variablen, so ist gemeint, dass die durch diese Formel definierte Klassenrelation*

$$\{(x,y)|\phi(x,y)\}$$

die betreffende Eigenschaft hat. Falls x *und* y *Klassen sind, werden die Zeichen analog verwendet.*

Beweis. Dies findet sich etwa in [1]. q.e.d.

2.1.3 Variationen des Ersetzungsschemas

Klassische Mengenlehre enthält das Ersetzungsschema (Replacement), also

Ersetzungsschema $\forall a.\ \phi : a \to V \to \exists b\ \phi : a \twoheadrightarrow b$ für alle Formeln ϕ

Allerdings kann man gerade in konstruktiven Umgebungen häufig nicht die Rechtseindeutigkeit einer Klasse zeigen, aber dennoch ihre Totalität. Daher ist das Kollektionsschema (Collection) besser anwendbar:

Kollektionsschema $\forall a.\ \phi : a \rightrightarrows V \to \exists b\ \phi : a \rightrightarrows b$ für alle Formeln ϕ

Verfügt man über unbeschränkte Separation, so kann man für den Fall, dass ϕ funktional ist, aus einem solchen b das Bild von a unter ϕ aussondern, aber sonst lässt sich daraus nicht ohne weiteres Ersetzung herleiten, was allerdings doch auch in konstruktiven Kontexten ein äußerst wichtiges Prinzip ist. Darum verwendet man das folgende Schema der starken Kollektion (Strong Collection), das die beiden vorigen impliziert:

Schema der starken Kollektion $\forall a.\ \phi : a \rightrightarrows V \rightarrow \exists b\ \phi : a \leftleftarrows\!\rightrightarrows b$ für alle Formeln ϕ

In der Zukunft besteht Bedarf an einer Aussage, die Strong Collection ähnelt, jedoch mehr abwechselnde Quantoren hat. Nach dem Wissen des Autors ist diese Aussage neu, aber sie ist weder überraschend noch schwer zu beweisen:

Proposition 2. *Unter Annahme von Collection und $CZF_{-,-}$ gilt für beliebige Formeln ϕ*

$$\forall a \in \alpha\ \exists b \in \beta\ \forall c \in \gamma\ \exists d\ \phi \rightarrow \exists \delta\ \forall a \in \alpha\ \exists b \in \beta\ \forall c \in \gamma\ \exists d \in \delta\ \phi$$

Beweis. Sei die Prämisse der Implikation erfüllt. Wegen Collection gilt

$$\forall a \in \alpha\ \exists b \in \beta\ \exists \delta'\ \forall c \in \gamma\ \exists d \in \delta'\ \phi$$

Also

$$\forall a \in \alpha\ \exists \delta'\ \exists b \in \beta\ \forall c \in \gamma\ \exists d \in \delta'\ \phi$$

Nach abermaliger Anwendung von Collection erhält man

$$\exists \delta''\ \forall a \in \alpha\ \exists \delta' \in \delta''\ \exists b \in \beta\ \forall c \in \gamma\ \exists d \in \delta'\ \phi$$

Wenn man insbesondere $\delta = \bigcup \delta''$ wählt ergibt sich:

$$\exists \delta\ \forall a \in \alpha\ \exists b \in \beta\ \forall c \in \gamma\ \exists d \in \delta\ \phi$$

Q.E.D.

2.1.4 Variationen des Potenzmengenaxioms

Klassische Mengenlehre verwendet das Potenzmengenaxiom, um ihr Universum durch überabzählbare Mengen zu bereichern:

Potenzmengenaxiom $\forall a \exists b\ b = P(a)$

Dies wird jedoch vielfach als imprädikativ empfunden, da hier auf einen Streich viele Mengen zusammengefasst werden, die „noch gar nicht konstruiert“ sind. Ausgehend von der Potenzmenge könnte man wieder mit Δ_0-Separation neue Teilmengen konstruieren, was zu einem imprädikativen Zirkel führt. Außerdem wäre in $CZF_{-,-}$ zusammen mit der Aussage, die die Existenz der Potenzmenge der natürlichen Zahlen fordert, offenbar Zahlentheorie zweiter Stufe einbettbar.

Eine vielfach verwendete Abschwächung, die immer noch einen großen Teil der erwünschten Anwendungen des Potenzmengenaxioms bewahrt, ist das etwas technisch anmutende Teilmengensammelschema (Subset Collection):

Subset Collection $\forall a, b\, \exists B\, \forall u.\ \phi(x, y) : a \rightrightarrows b \rightarrow \exists b' \in B \phi(x, y) : a \leftleftarrows\!\rightrightarrows b'$ für alle Formeln ϕ mit a, b, b' und B nicht frei in $\phi(x, y)$

B kann man als Teilmenge der Potenzklasse von b auffassen in dem Sinne, dass $CZF_{-,-}$ zeigt, dass wenn es so ein B gibt, dieses geschnitten mit der (Δ_0-definierbaren) Potenzklasse von b auch die in der Formel geforderte Eigenschaft hat. Es wird also nicht die volle Potenzklasse als Menge postulier, sondern nur die Zusammenfassung von Teilmengen, deren Komplexität gewissermaßen durch die von a und ϕ beschränkt ist. Dürfte man für a die Allklasse V einsetzen, so würde schon für $\phi(x, y) \leftrightarrow x = y$ das Potenzmengenaxiom impliziert.

Eine handliche Variante von Subset Collection erhält man, indem man den Zusammenhang zwischen Teilmengen und totalen Relationen ausnutzt. Offenbar sind die abtrennbaren Teilmengen[5] einer Menge A in direkter Korrespondenz zu den Funktionen dieser Menge in die 2. Die beliebigen Teilmengen stehen in engem (bitotalem) Zusammenhang mit den totalen Relationen von A in die 2, dabei entspricht der Relation r die Teilmenge $\{a \in A | r(a) = 1\}$. Insofern ist die Behauptung, für zwei Mengen bildete die Klasse der totalen Relationen zwischen ihnen eine Menge, äquivalent zum Potenzmengenaxiom[6]. Und es ist Subset Collection äquivalent zu:

Fullness $\forall A, B \exists C. \forall r : A \rightrightarrows B \; \exists r' \in C. \; r' \subseteq r \wedge r' : A \rightrightarrows B$

Beweis. Siehe [1]. Man beachte, dass Fullness→Subset Collection das Schema der starken Kollektion benötigt. q.e.d.

Ein solches C heißt voll in $mv(A, B) := \{r | r : A \rightrightarrows B\}$.

Fullness ebenso wie Subset Collection verspricht die Existenz einer Menge, ohne Hinweise zu geben, wie eine solche zu spezifizieren sei. Rathjen [24] vermutet, dass es keine Formel gibt, die auf genau eine solche Menge zutrifft und die eine volle Menge also spezifizieren könnte. Dies stünde in starkem Kontrast zu typischen Existenzaxiomen der Mengenleere wie den Axiomen der Paarmenge, Vereinigung, (beschränkten) Separation, Unendlichkeit, Ersetzung oder Potenzmenge und ist gerade für eine konstruktive Theorie kein Gütemerkmal. Darum wird gerade in letzter Zeit verstärkt über Fullness nachgedacht, insbesondere durch die Untersuchung von Abschwächungen.

Da die Funktionen $\subseteq$-minimale totale Relationen sind, enthält eine volle Menge alle Funktionen. Die Forderung, dass die Funktionen[7] zwischen zwei Mengen wiederum eine Menge bilden, ist also eine solche Abschwächung und postuliert die Existenz einer spezifizierbaren Menge:

Exponentiation $\forall A, B \; \exists C. \; C = {}^A B$

Es ist dabei ${}^A B := \{f | f : A \to B\}$. Exponentiation reicht für viele Zwecke aus, etwa für die Existenz von überabzählbaren (genauer: nicht abzählbaren) Mengen, ist aber auch für manche Anwendungen etwa in der Analysis nicht stark genug. Zum Beispiel kann es nicht zeigen, dass die Dedekindschen reellen Zahlen eine Menge bilden [19]. Dennoch ist es nicht allzuweit sogar von Potenzmengenaxiom entfernt:

---

[5] A ist abtrennbare Teilmenge von B, wenn jedes Element von A in B liegt oder nicht in B liegt.

[6] Die Rückrichtung erfolgt über Betrachtung der Potenzmenge des kartesischen Produkts der beiden Mengen.

[7] Man beachte, dass die Eigenschaft, eine Funktion zu sein, nur beschränkte Quantoren enthält.

Proposition 3. *Das Potenzmengenaxiom ist in $CZF_{-,-}$+Exponentiation äquivalent zu der Aussage, dass $P(\{\emptyset\})$ eine Menge ist.*

Beweis. Dies folgt leicht aus der Einsicht, dass die Potenzklasse einer Menge a isomorph ist zu der Klasse der Funktionen von a nach $P(1)$ [1]. Q.E.D.

Vor kurzem schlugen Schuster, Ishihara und Crosilla in [11] eine Abschwächung von Fullness vor, die zusammen mit Exponentiation zu Fullness äquivalent ist und viele praktische Konsequenzen von Fullness, wie die Existenz der Dedekind-reellen Zahlen, impliziert. Der Name stammt aus einer topologischen Veranschaulichung des Axioms.

Refinement $\forall A, B\ \exists D.\ \forall r : A \rightrightarrows B\ \exists r' \in C. r' \subseteq r \wedge \forall b \in B\ r'^{-1}(b) \in D$

Vor kurzem wurde allerdings vom Autoren gezeigt [30], dass Refinement doch Exponentiation impliziert und also zu Fullness äquivalent ist:
Beweis. [30] Q.E.D.

Beweisbar nicht äquivalent zu Fullness ist das dazu duale sehr schwache ImageCollection [31], ein schwaches Auswahlprinzip, das den Teil von Fullness fassen soll, der eine nichtspezifizierbare Menge postuliert. Es gilt auch tatsächlich, dass Fullness äquivalent zu Exponentiation und ImageCollection ist.

ImageCollection Für alle A, B gibt es ein E, so dass
$\forall r : A \rightrightarrows B\ \exists r' \in C.\ r' \subseteq r \wedge \forall a \in A\ \{b \in B | (a, b) \in r\} \in E$

2.1.5 $CZF_{X,Y}$

Definition 4. *Es sei die Theorie $CZF_{X,Y}$ die Theorie $CZF_{-,-}$ zusammen mit*

- *dem Ersetzungsschema (Replacement), falls X=R*
- *dem Kollektionsschema (Collection), falls X=C*
- *dem Schema der starken Kollektion (Strong Collection), falls X=S*
- *dem Exponentiationsaxiom (Exponentiation), falls Y=E*
- *dem ImageCollection-Axiom, falls Y=I*
- *dem Teilmengensammelschema (Subset Collection), falls Y=S*
- *dem Potenzmengenaxiom, falls Y=P*

$CZF_{X,Y} + Sep$ sei diese Theorie mit dem vollen Separationsschema.

Nun sei CZF gleich $CZF_{S,S}$. Die intuitionistische Mengenlehre IZF, mit der etwa [20] arbeitet, ist $CZF_{C,P} + Sep$. Wenn im Folgenden eine Aussage der Mengenlehre als Theorem bezeichnet wird, so ist damit gemeint, dass die Aussage in CZF ableitbar ist.

Es werden im Folgenden typische Mengenoperationen wie $a \cup b$, $a \cap b$ oder $a \setminus b$ verwendet. Diese bezeichnen die offensichtlichen Klassenterme. Aus den Axiomen von CZF kann man herleiten, dass es sich um Mengen handelt.

Außerdem werden im Folgenden leicht zu zeigende und bekannte Tatsachen im Zusammenhang mit CZF vorausgesetzt. Einige, die entweder nicht bekannt, sehr interessant oder im Folgenden so wichtig sind, dass dies gerechtfertigt erscheint, sollen aber im folgenden Abschnitt noch erwähnt werden.

2.2 Einige Tatsachen

2.2.1 Δ_0-Separation

Aus dem Schema Δ_0-Separation lässt sich das Schnittmengenaxiom herleiten, welches postuliert, dass es zu zwei Mengen a, b jeweils eine Schnittmenge $a \cap b = \{x | x \in a \wedge x \in b\}$ gibt. Außerdem lässt sich herleiten, dass die leere Klasse eine Menge ist. Obwohl diese beiden Aussagen sehr viel schwächer erscheinen, gilt auch die Umkehrung:

Proposition 5. *Aus $CZF_{-,-}$ mit Schnittmengenaxiom und der Aussage, dass die leere Klasse eine Menge ist, lässt sich jede Instanz der Δ_0-Separation herleiten.*

Beweis. Siehe [1]. q.e.d.

2.2.2 Ordinalzahlen

Definition 6. 1. *Eine Klasse α heißt **transitiv**, wenn*

$$\forall a, b.\ a \in b \in \alpha \rightarrow a \in \alpha$$

2. *Zu einer Klasse a sei die **transitive Hülle** von a definiert als*

$$TC(a) := \{x | \forall b \supseteq a.\ b \text{ transitiv} \rightarrow x \in b\} = \bigcap_{a \subseteq b \text{ transitiv}} b$$

Dies ist die Klasse der Elemente von a, der Elemente der Elemente von a usw[8]*. Falls a eine Menge ist, so ist $TC(a)$ auch eine Menge. Das Mengeninduktionsschema kann erweitert werden zu:*

$$\forall x (\forall y \in TC(x)\ \phi(y) \rightarrow \phi(x)) \rightarrow \forall x \phi(x)$$

3. *Eine Menge, die transitiv ist, und deren Elemente alle transitiv sind, nennt man **Ordinalzahl**. Elemente von Ordinalzahlen sind wieder Ordinalzahlen und die Klasse aller Ordinalzahlen bezeichnet man mit On. ω ist eine Ordinalzahl. Die Vereinigung einer Menge von Ordinalzahlen ist wieder eine Ordinalzahl.*

Beweis. Zu finden in [1] q.e.d.

In der klassischen Mengenlehre sind Ordinalzahlen sowie die Klasse der Ordinalzahlen wohlgeordnet, und das ist eine zentrale und überaus nützliche Eigenschaft, die im Umgang mit Ordinalzahlen vielfach ausgenutzt wird und von vielen klassischen Mengentheoretikern sehr als das Wesen von Ordinalzahlen ausmachend angesehen wird. In CZF kann dies allerdings nicht gezeigt werden, nicht einmal, dass Ordinalzahlen trichotom geordnet sind. Allerdings sind sie durch $\in$ partiell geordnet[9]. Die wichtige Eigenschaft, dass man über Ordinalzahlen Induktion betreiben kann, gilt allerdings auch konstruktiv:

---

[8] Dies kann man formal ausdrücken als

$$\bigcup_{n \in \omega} \{x | \exists f : n+1 \rightarrow V.\ \forall m \in n\ f(m+1) \in f(m) \wedge f(0) \in a \wedge f(n) = x\}$$

[9] Genauer gesagt ist die durch $\in$ gegebene Relation irreflexiv und transitiv. Partielle Ordnungen werden später etwas anders als reflexive Strukturen definiert.

Lemma 7.

$$\forall \alpha \in On(\forall \beta \in \alpha\ \phi(\beta) \to \phi(\alpha)) \to \forall \alpha \in On\ \phi(\alpha)$$

Beweis. Dies ist klar mit Mengeninduktion über $\phi(x) \wedge x \in On$. q.e.d.

Natürliche Zahlen

Die Menge ω, die vom Unendlichkeitsaxiom gefordert wird, ist ein wichtiges Beispiel für eine Ordinalzahl. Diese Menge der von-Neumann-natürlichen Zahlen stimmt mit unserer Intuition der natürlichen Zahlen insofern überein, als dass CZF offenbar beweist, dass sie die (zweitstufigen) Axiome der Peano-Arithmetik erfüllt, wobei der Null die leere Menge und der Nachfolgeroperation die Abbildung $x \mapsto x + 1 = x \cup \{x\}$ entspricht. Die durch $\in$ gegebene Relation zwischen natürlichen Zahlen ist genau die auf ihnen bekannte $<$-Relation.

Die natürlichen Zahlen haben die wichtige Eigenschaft, diskret zu sein, das heißt es gilt

$$\forall n, m \in \omega.\ n = m \vee n \neq m$$

Dies zeigt man leicht durch Induktion über m und n [1]. Man zeigt sogar die Verstärkung

$$\forall n, m \in \omega.\ n = m \vee n \in m \vee n \ni m$$

Dies findet sich in [1].

Der klassische Begriff der Endlichkeit spaltet sich unter einem konstruktiven Gesichtspunkt in viele Facetten auf ([1], [27]), die natürlichste (und zugleich stärkste) Fassung ist wohl die folgende:

Definition 8. *Eine Menge a heißt* ***endlich****, falls*

$$\exists n \in \omega \exists f : n \leftrightarrow a$$

Die klassische Eigenschaft, dass bewohnte Mengen natürlicher Zahlen ein kleinstes Element haben, ist konstruktiv nicht mehr gültig und kann auch oft durch das Induktionsprinzip hinreichend ersetzt werden. Allerdings gilt sie dennoch für endliche Teilmengen der natürlichen Zahlen:

Proposition 9. *Jede nichtleere endliche Teilmenge natürlicher Zahlen hat ein minimales und ein maximales Element.*

Beweis. Dies wird durch Induktion über die zur Teilmenge bijektive natürliche Zahl gezeigt. Für die 0 ist die Aussage trivialerweise erfüllt, denn dann ist die Teilmenge nicht nichtleer. Für 1 ist das auch noch klar. Falls die Teilmenge zwei Elemente enthält, ist entweder das eine größer oder das andere, dann ist das größere das Maximum und das andere das Minimum. Der Fall mehrerer Elemente kann offenbar induktiv auf den von zweien zurückgeführt werden, denn

$$max(M \dot{\cup} \{a\}) = max(\{max(M)\} \dot{\cup} \{a\})$$

und analog für das Minimum. q.e.d.

Man kann jeder Menge x einen Rang $rk(x) \in On$ zuordnen, der die „Höhe“ des Elements misst und der die folgende Formel erfüllt

$$rk(x) = \bigcup \{rk(y) \cup \{rk(y)\} | y \in x\}$$

Dies geht aus dem nächsten Kapitel hervor.

2.2.3 Induktive Definitionen

Induktive Definitionen sind Abschlüsse einer Klasse gegenüber einer bestimmten Operation. [1] empfiehlt, die Elemente des Abschlusses als die mit einem allgemeinen Kalkül herleitbaren verallgemeinerten Formeln zu sehen, wobei man y aus x in einem Schritt herleiten kann, wenn $\Phi(x, y)$ mit der das Kalkül bestimmenden Formel Φ gilt.

Definition 10. *Eine Formel $\Phi(x, y)$ mit zwei ausgezeichneten Variablen x und y heißt **induktive Definition**. Sie induziert einen monotonen Operator Γ_Φ auf Klassen mit*

$$\Gamma_\Phi(Y) := \{y | \exists x \subseteq Y \ \Phi(x, y)\}$$

*Eine Klasse Y heißt **abgeschlossen** unter Γ_Φ, falls $\Gamma_\Phi(Y) = Y$*

Lemma 11. *Für eine induktive Definition $\Phi(x, y)$ gibt es eine kleinste unter Γ_Φ abgeschlossene Klasse J und Klassen J^α für $\alpha \in On$[10] so dass*

- $J = \hat{\bigcup}_{\alpha \in On} J^\alpha$
- $\forall \alpha \in On \ J^\alpha = \Gamma_\Phi(\hat{\bigcup}_{\beta \in \alpha} J^\beta)$

Dabei bedeutet $\hat{\bigcup}$, dass die Vereinigung aufsteigend ist.

Beweis. In [1]. q.e.d.

Die induktive Definition

$$\Phi(x, y) \ :\leftrightarrow \ \exists a, b. \ y = (a, b) \wedge x : a \to V \wedge b = (x[a] \cup \bigcup_{c \in a} \{x(c)\})$$

etwa liefert als kleinste abgeschlossene Klasse die Klassenfunktion $x \mapsto rk(x)$.

[10] also einen Klassenterm mit einer freien Variable α, die auf On beschränkt ist

Kapitel 3

Applikative Topologien

Ziel dieses Kapitels ist, die in dieser Arbeit bedeutsamen algebraischen Strukturen zu definieren und einige zentrale Aussagen über sie herzuleiten. Im Zentrum steht dabei die neu eingeführte Struktur der applikativen Topologie. Ausgehend von solch einer applikativen Topologie wird ein Modell der Mengenlehre konstruiert werden; seine Eigenschaften werden dabei kritisch davon abhängen, welche applikative Topologie verwendet wird.

Um auf die Definition hinzuleiten, werden zunächst applikative Strukturen und formale Topologien definiert. In einem gewissen Sinne werden sich beide als Grundlagen für applikative Topologien herausstellen, deren Definition anschließend gegeben wird. Danach werden einige zentrale Fakten über die Theorie der applikativen Topologien angegeben und abschließend einige Beispiele diskutiert, mit denen später Modelle der konstruktiven Mengenlehre konstruiert werden.

3.1 Applikative Strukturen

Die Methode der Realisierbarkeitsmodelle liefert Modelle von CZF in Abhängigkeit von so genannten applikativen Strukturen, Mengen mit einer partiellen Verknüpfung, die man Anwendung oder Applikation nennt, und die bestimmte Axiome erfüllen. Applikative Strukturen entsprechen Modellen für den un-ge-typ-ten λ-Kalkül (rein formal sind es allerdings keine).

Folgend Currys Zugang zur Behandlung von ungetypten Applikationsstrukturen wird ihre Theorie allerdings nicht definiert, indem man Abstraktion in die Syntax aufnimmt und Konversionsregeln axiomatisiert, sondern indem einige ausgezeichnete Kombinatoren gefordert werden, mit denen man dann λ-Terme definieren kann.

Definition 12. *Eine **applikative Struktur** (auch partielle kombinatorische Algebra oder Schönfinkel-Algebra) ist eine Menge A mit einer (durch eine Menge gegebenen) partiellen binären Verknpfung $\circ$ (Applikation)*[1] *und zwei verschiedenen ausgezeichneten Elementen k und $s \in A$, so dass gilt:*

- $\forall a, b \in A\ (k \circ a) \circ b = a$

[1] Mit einem Ausdruck der Form $a \circ b$ in einer Aussage soll in diesem Abschnitt zugleich die Behauptung enthalten sein, dass dies überhaupt definiert ist. Dies ist nicht selbstverständlich, da $\circ$ ja nur partiell sein muss.

- $\forall a, b, c \in A\ \exists d \in A\ (s \circ a) \circ b = d$
- $\forall a, b, c \in A\ (\exists d \in A\ (s \circ a \circ b \circ c = d \vee a \circ c \circ (b \circ c) = d)) \to s \circ a \circ b \circ c = a \circ c \circ (b \circ c)$

In applikativen Strukturen wird die Verknüpfung linksassoziativ geschrieben, also steht $a_1 \circ ... \circ a_n$ für $(...(a_1 \circ a_2) \circ a_3) \circ a_4)... \circ a_n$. Wie üblich wird ohne Gefahr von Verwechslungen die applikative Struktur meist nur durch ihre Trägermenge bezeichnet und ihre ausgezeichneten Elemente und die Verknüpfung auch für verschiedene applikative Strukturen stets mit s, k und $\circ$ bezeichnet, in verwechslungsträchtigen Situationen allenfalls mit der Bezeichnung der Struktur als Index gekennzeichnet.

Applikative Strukturen sind also genau die Modelle von APP, der intuitionistischen Theorie erster Stufe mit Gleichheit als logischem Zeichen[2] deren Sprache nur das dreistellige Relationszeichen App enthält und die mit den folgenden vier Axiomen axiomatisiert ist:

1. $\forall a, b, c, d.\ App(a, b, c) \wedge App(a, b, d) \to c = d$
2. $\exists k \forall a \exists c \forall b.\ App(k, a, c) \wedge App(c, b, a)$
3. $\exists s \forall a, b, c\ \exists d, e\ (App(s, a, d) \wedge App(d, b, e)) \wedge$
   $(\exists f. App(e, c, f) \vee \exists g, h.\ App(a, c, g) \wedge App(b, c, h) \wedge App(g, h, f))$
   $\to (App(e, c, f) \wedge \exists g, h App(a, c, g) \wedge App(b, c, h) \wedge App(g, h, f))$
4. $\exists a, b a \neq b$

Definiert man in einem Modell $\mathbf{M}$ dieser Theorie dann

$$a \circ b = c \leftrightarrow \mathbf{M} \models App[a, b, c]$$

und wählt man für k und s zwei beliebige Zeugen des ersten beziehungsweise zweiten Axioms, erhält man offenbar eine applikative Struktur. Nicht offensichtlich ist nur, dass dann $k \neq s$ gilt. Aber sei $a \neq b \in M$ und angenommen, es wäre $k = s$. Es würde folgen:

$$\begin{aligned} a &= k \circ a \circ b \\ &= (k \circ k) \circ (k \circ k) \circ a \circ b \\ &= s \circ k \circ k \circ k \circ a \circ b \\ &\doteq k \circ k \circ k \circ k \circ a \circ b \\ &= (k \circ k \circ k) \circ k \circ a \circ b \\ &= k \circ k \circ a \circ b \\ &= k \circ (k \circ k \circ k) a \circ b \\ &\doteq k \circ (s \circ k \circ k) \circ a \circ b \\ &= k \circ b \circ (k \circ b) = b, \end{aligned}$$

was ein Widerspruch ist (wo $k = s$ einging wurde dies mit einem Punkt über dem Gleichheitszeichen gekennzeichnet). Man beachte, dass tatsächlich alle angegebenen Applikationen definiert waren.

[2]das heißt, das Zeichen für Gleichheit wird durch die wirkliche Gleichheit interpretiert

Oft wird von applikativen Strukturen sehr viel mehr gefordert, beispielsweise Elemente, die den natürlichen Zahlen entsprechen, Elemente, die Paare kodieren können, die Fallunterscheidungen ausführen und so fort. Dies macht es sehr umständlich, eine applikative Struktur tatsächlich ausführlich anzugeben, erleichtert jedoch die Formulierung von Theoremen über applikative Strukturen. Letztendlich spielt das jedoch keine Rolle, da die beiden Kombinatoren k und s kombinatorisch vollständig[3] sind und man sich mit ihnen Paare, natürliche Zahlen und alles, was man in applikativen Strukturen gerne ausdrücken würde, problemlos definieren kann. Später werden die Beispiele hierfür angegeben, die für diese Arbeit wesentlich sind.

3.1.1 Applikationsterme

In applikativen Strukturen kann eine Applikation durchaus undefiniert sein, trotzdem möchte man gerne über komplexere Terme sprechen, ohne stets Aussagen über die Definiertheit der einzelnen Teilterme zu machen. Applikationsterme werden deswegen als syntaktisches Hilfsmittel eingeführt und entsprechen auch nach einer Belegung der Variablen nicht unbedingt einem Element der applikativen Struktur, sondern können auch undefiniert sein.

Definition 13. *Sei A eine applikative Struktur. Die* ***Applikationsterme*** *t* ***über*** *A und die Mengen $FV(t)$ ihrer freien Variablen sind induktiv definiert:*

1. *Für eine natürliche Zahl n ist $(0, n)$ ein Applikationsterm mit $FV((0, n)) = \{n\}$ und wird mit v_n abgekürzt. Die Buchstaben v, w und Variationen, manchmal aber auch andere Buchstaben, dienen als Mitteilungszeichen für diese Applikationsterme.*

2. *Für jedes Element von A ist $(1, a)$ ein Applikationsterm mit $FV((1, a)) = \emptyset$, der mit a abgekürzt wird.*

3. *Sind t_1 und t_2 Applikationsterme, so auch das geordnete Tripel $(2, t_1, t_2)$, das mit $t_1 t_2$ abgekürzt wird. Seine freien Variablen sind $FV(t_1) \cup FV(t_2)$.*

Bemerkung 14.

1. *Der erste Fall entspricht einfach einer Kodierung von abzählbar vielen Variablen. Die genaue Wahl der Details ist unerheblich, wichtig ist nur, dass man einem Applikationsterm ansehen kann, wie er zu Stande gekommen ist, auch wenn natürliche Zahlen, Elemente von A und Paare von bereits vorher konstruierten Termen zusammenfallen sollten.*

2. *$FV(t) = \emptyset$ ist offenbar äquivalent dazu, dass zur Herleitung von "t ist Applikationsterm"der erste Fall der induktiven Definition nicht herangezogen wurde. Solche Applikationsterme heißen geschlossen.*

3. *Durch Induktion über die Definition zeigt man leicht, dass $FV(t)$ eine endliche Menge natürlicher Zahlen ist. Insbesondere hat sie also auch ein Maximum.*

[3] in dem Sinne, dass sie λ-Abstraktion erlauben und auch in dem Sinne, dass für jede Turing-Maschine ein Term in der applikativen Struktur angebbar ist, so dass der Wert des Terms (und seine Definiertheit) auf einfache Weise mit dem Ergebnis der Turing-Maschine korrespondiert.

Üblicherweise werden Applikationsterme unabhängig von einer applikativen Struktur syntaktisch zu der Theorie APP eingeführt, wobei die Variablen, s und k den Induktionsanfang bilden. Ähnlich wie in dem hier gewählten Zugang wird dann Definiertheit von Applikationstermen definiert. Für die Zwecke dieser Arbeit scheint dem Autoren allerdings die hier gewählte Weise erheblich geeigneter um technische Exaktheit zu gewährleisten. Überlässt man die Details dem Leser, kommt die andere Methode allerdings zu kürzeren Definitionen.

Die zentrale Eigenschaft eines Applikationsterms ist, dass ihm ein Element der betreffenden applikativen Struktur entsprechen kann. Er kann aber auch undefiniert sein. Die wichtigste Relation zwischen zwei Applikationstermen ist auch nicht unbedingt, dass sie das selbe Element denotieren, sondern dass die Definiertheit von einem die Definiertheit des anderen und die Übereinstimmung ihrer Denotationen impliziert. Dies wird mit dem Zeichen $\simeq$ ausgedrückt. Um dies für Applikationsterme mit freien Variablen zu definieren, benötigt man zuerst das Konzept von Einsetzungen von Elementen der applikativen Struktur in einen Applikationsterm, das analog zum Verfahren für übliche Terme ist.

Definition 15. *Sei t ein Applikationsterm über A, $a \in A$, $b \in \omega$. Dann ist der Applikationsterm $t[v_b := a]$ induktiv definiert:*

1. $v_i[v_b := a] = a$, *falls* $i = b$
2. $v_i[v_b := a] = v_i$, *falls* $i \neq b$
3. $\hat{a}[v_b := a] = \hat{a}$, *falls* $\hat{a} \in A$
4. $(t_1 t_2)[v_b := a] = t_1[v_b := a] t_2[v_b := a]$

Sind $a_0, ..., a_n \in A, b_0, ..., b_n \in \omega$, *so schreibt man kürzer:*

- $t[v_{b_0} =: a_0, ..., v_{b_n} =: a_n]$ *für* $t[v_{b_0} =: a_0]...[v_{b_n} =: a_n]$
- $t[a_0, ..., a_n]$ *für* $t[v_0 =: a_0, ..., v_n =: a_n]$

Bemerkung 16. 1. $FV(t[v_{b_0} =: a_0, ..., v_{b_n} =: a_n]) = FV(t) \setminus \{b_0, ..., b_n\}$

2. *Ist σ Permutation von $\{b_0, ..., b_n\}$ und sind die b_i paarweise verschieden, so ist*

$$t[v_{b_{\sigma(0)}} =: a_{\sigma(0)}, ..., v_{b_{\sigma(n)}} =: a_{\sigma(n)}] = t[v_{b_0} =: a_0, ..., v_{b_n} =: a_n]$$

3. *Ist $i \notin FV(t)$, so ist $t[v_i := a] = t$.*
Dies erhält man direkt durch Induktion über den Aufbau von t.

Definition 17. 1. *Sei M die Menge der geschlossenen Applikationsterme über A. Dann ist die Denotationsrelation V auf $M \times A$ induktiv definiert:*

   (a) $V(a, a)$

   (b) $V(t, a) \wedge V(s, b) \wedge c = a \circ b \to V(ts, c)$

2. *Sei t ein geschlossener Applikationsterm über A. t **denotiert**, in Zeichen $t \downarrow$, falls $\exists a \in A\ V(t, a)$. So ein a heißt **Denotat** von t.*

3. *Sei t ein beliebiger Applikationsterm über A. t **denotiert**, in Zeichen $t \downarrow$, falls für alle $a_0, ..., a_{max(FV(t))} \in A$ gilt: $t[a_0, ..., a_{max(FV(t))}] \downarrow$. Man spricht allerdings nicht von einem Denotat eines Terms mit freien Variablen.*

4. *Seien t_1, t_2 Applikationsterme über A. Man sagt t_1 und t_2* ***denotieren gleich****, in Zeichen $t_1 \simeq t_2$, falls für alle $a_0, ..., a_{max(FV(t_1) \cup FV(t_2))}, a \in A$ gilt:*

$$V(t_1[a_0, ..., a_{max(FV(t_1) \cup FV(t_2))}], a) \to V(t_2[a_0, ..., a_{max(FV(t_1) \cup FV(t_2))}], a)$$
$$V(t_2[a_0, ..., a_{max(FV(t_1) \cup FV(t_2))}], a) \to V(t_1[a_0, ..., a_{max(FV(t_1) \cup FV(t_2))}], a)$$

Bemerkung 18. *1. Durch Induktion über die Definion von geschlossenen Termen sieht man: Denotiert ein Term, so ist das Denotat eindeutig.*

2. *Zwei Terme t und s denotieren genau dann gleich, wenn für alle $\vec{a}$, so dass $t[\vec{a}]$ und $s[\vec{a}]$ geschlossen sind, gilt: Wenn einer der beiden geschlossenen Terme $t[\vec{a}]$ und $s[\vec{a}]$ denotiert, so denotieren sie beide und ihr Denotat stimmt überein.*

3. *Falls in Zukunft ein Applikationsterm an einer Stelle steht, wo ein Element der applikativen Struktur zu erwarten ist, also wenn behauptet wird, auf ihn träfe eine Eigenschaft zu, die nur für Elemente der applikativen Struktur definiert wurde oder offensichtlicherweise für die Applikationsterme selbst nicht gilt, so ist dies stets zu lesen als: Der Applikationsterm denotiert und auf sein Denotat trifft die Eigenschaft zu. Dies entspricht der Situation in freier Logik, wenn ein eventuell undefinierter Term in ein Prädikat eingesetzt wird.*

Ein Beispiel für gleich denotierende Terme, die aber nicht stets denotieren, sind $svv'w$ und $(vw)(v'w)$ für x, y, z Variablen. Das dritte Axiom applikativer Strukturen ist äquivalent zu der Tatsache, dass die beiden Terme gleich denotieren. Dass sie jedoch überhaupt denotieren, ist für nichttriviale applikative Strukturen allerdings stets falsch, nämlich zum Beispiel immer, wenn vw oder $v'w$ nicht denotiert[4], können beide Terme gar nicht denotieren. Dass svw jedoch denotiert, ist gerade die Aussage des zweiten Axioms.

Man beachte, dass bei den obigen Definitionen die Axiome der applikativen Strukturen keine Rolle gespielt haben, ebensowenig wie die ausgezeichneten Elemente k und s. Tatsächlich kann man sie für beliebige Strukturen mit partieller binärer Verknüpfung einführen und sie werden genauso für applikative Topologien verwendet werden.

Die Verwendung von Applikationstermen erleichtert viele Beweise, wie sich im folgenden Abschnitt zeigen wird.

3.1.2 Einige denotierende Applikationsterme

Applikative Strukturen sind mächtig in dem Sinne, dass sie Applikationsterme enthalten, die Mächtiges tun[5]. Insbesondere sind sie abgeschlossen gegenüber λ-Abstraktion.

[4]Genauer: Wenn v und w durch die Elemente a und b substituiert werden, und ab nicht denotiert; analog für $v'w$

[5]Dies ist ein erstes Beispiel der im dritten Teil der vorigen Bemerkung getroffenen Konvention: Natürlich sind die Applikationsterme nicht Elemente der applikativen Struktur, aber sie denotieren, und ihre Denotate sind Elemente der applikativen Struktur, die „mächtiges tun".

Lemma 19. *Sei t ein Applikationsterm über einer applikativen Struktur A. Dann gibt es für $n \in \omega$ einen Applikationsterm $\lambda v_n.t$, so dass gilt:*

- $FV(\lambda v_n.t) = FV(t) \setminus \{n\}$
- $(\lambda v_n.t) \downarrow$
- $(\lambda v_n.t)v_n \simeq t$

Wie üblich schreibt man $\lambda v_{n_1} ... v_{n_k}.t$ für $\lambda v_{n_1}....\lambda v_{n_k}.t$. Im Gegensatz zu Quantoren spielt die Reihenfolge der Variablen bei der λ-Abstraktion allerdings eine Rolle.

Beweis. Induktion über den Aufbau von t, folgend [13].

1. $t = v_n$: Definiere $\lambda v_n.t$ als skk. Dies hat keine freien Variablen, denotiert und $skkv_n \simeq (kv_n)(kv_n) \simeq v_n$.
2. $t = v_m, m \neq n$: Definiere $\lambda v_n.t$ als kv_m. Dies hat die gleichen freien Variablen wie t, denotiert und $kv_m v_n \simeq v_m$.
3. $t = a \in A$: Definiere $\lambda v_n.t$ als ka. Dies hat keine freien Variablen, denotiert und $kav_n \simeq a$.
4. $t = t_1 t_2$: Definiere $\lambda v_n.t$ als $s(\lambda v_n.t_1)(\lambda v_n.t_2)$. Dies denotiert nach Axiom und Induktionsvoraussetzung und hat als freie Variablen die selben wie t außer v_n. Und $s(\lambda v_n.t_1)(\lambda v_n.t_2)v_n \simeq ((\lambda v_n.t_1)v_n)((\lambda v_n.t_1)v_n) \simeq t_1 t_2 = t$ nach Induktionsvoraussetzung.

Q.E.D.

Über λ-Abstraktion konstruierte Terme werden im Verlauf dieser Arbeit vielfach verwendet werden. Dies rührt vor allem daher, dass λ-Terme intuitiv leichter verständlich und manipulierbar sind als die länglichen Ausdrücke, die in k und s geschrieben sind.

Mit diesem Werkzeug könnten wir nun leicht einiges an Rekursionstheorie betreiben, zeigen, dass in applikativen Strukturen das Fixpunktlemma gilt, Paare kodieren, natürliche Zahlen definieren und beweisen, dass jede partiell rekursive Funktion durch einen denotierenden Term repräsentiert wird [29]. An dieser Stelle sind diese Beweise allerdings nicht aufgeführt, da wir derartige Resultate erst für applikative Topologien benötigen, wo die Beweise sowieso in abgewandelter Form benötigt werden. Um die Macht der λ-Abstraktion zu illustrieren, soll nur ein Resultat bewiesen werden, das für applikative Topologien so nicht gilt:

Proposition 20. *Jede applikative Struktur A enthält eine abzählbar unendliche Teilmenge*[6]*.*

Beweis. Definiere eine Einbettung f von ω in die Applikationsterme über A induktiv:

- $f(0) = k$

[6] Also eine Teilmenge, die zu der Menge der natürlichen Zahlen bijektiv ist. Gäbe es nur eine Surjektion von den natürlichen Zahlen auf die Menge, so würde man sie als aufzählbar bezeichnen.

- $f(n+1) = \lambda v_0.v_0 s(f(n))$

Diese hat die Eigenschaft, dass $f(n{+}1)(k(skk)) \simeq k(skk)s(f(n)) \simeq skk(f(n)) \simeq k(f(n))(k(f(n))) \simeq f(n)$

Die Werte unter f sind alle geschlossen und denotieren, zu zeigen ist, dass sie auch alle verschieden sind. Durch Induktion über n wird bewiesen, dass für alle $n \in \omega$ die ersten n Werte verschieden sind. Der Induktionsanfang ist klar; seien also die ersten n Werte verschieden, es soll gezeigt werden, dass der Wert von $f(n+1)$ mit keinem von ihnen bereinstimmt. Würde er mit dem Denotat eines $f(m{+}1)$ übereinstimmen, so wären auch die Denotate von $f(n{+}1)(k(skk))$ und $f(m{+}1)(k(skk))$ die selben, im Widerspruch zur Induktionsvoraussetzung. Also kann das Denotat von $f(n+1)$ höchstens mit dem von $f(0)$ zusammenfallen, also $k \simeq f(n+1)$ gelten. Also wäre $kk \simeq f(n+1)k \simeq ks(f(n)) \simeq s$. Also wäre auch $s \simeq ksk \simeq kkksk \simeq sksk \simeq kk(sk) \simeq k$, und das ist nicht der Fall. Q.E.D.

Diese Folge hat die schöne Eigenschaft, dass es ein Element der applikativen Struktur gibt, nämlich das Denotat von $\lambda v_1 v_0.v_0 s v_1$, das angewandt auf ein Glied dessen Nachfolger ergibt, und ein Element, nämlich $\lambda v_1.v_1(k(skk))$, das zu jedem Glied ungleich 0 den Vorgänger liefert. Dies wird später dazu verwendet werden, um die natürlichen Zahlen in den konstruierten Modellen der Mengenlehre zu wiederzufinden.

3.1.3 Beispiele für applikative Strukturen

Die Beispiele in diesem Kapitel dienen nicht allein der Illustration der oben gemachten Definitionen, sondern werden an späterer Stelle, wenn es um Realisierbarkeitsmodelle geht, wieder auftauchen. Allerdings sind sie, auch wenn sie ihren Platz schon in diesem Kapitel haben, bis zu diesem Punkt nicht bedeutsam und dieses Kapitel kann ohne Verlust bis dorthin zurückgestellt werden.

3.1.4 Kleenes erstes Modell

Dies ist sicher der Prototyp für applikative Strukturen. Sowohl die Struktur selbst als auch die aus ihr entstehenden Realisierbarkeitsmodelle sind gut erforscht.

Kleenes erstes Modell werden wir mit Kl bezeichnen. Seine Trägermenge sind die natürlichen Zahlen, die man mit der Menge der Turing-Maschinen identifiziert (man kann auch ein anderes Modell für partiell rekursive Funktionen nach Wahl verwenden; siehe auch [7] zu den verwendeten Begriffen) denkt, so dass jedes Element eine Doppelrolle erhält: Einerseits als Index einer partiell rekursiven Funktion und andererseits als natürliche Zahl, auf die man die Funktion anwenden kann. Die Applikation ist die Anwendung dieser Funktion auf das Argument, das heißt, man definiert

$$e \circ f = g \leftrightarrow \{e\}f \simeq g$$

Wobei $\{e\}f \simeq g$ dafür steht, dass die Turing-Maschine mit Index e auf die Eingabe f angesetzt mit dem Ergebnis g terminiert. Für k wähle man den Index einer Turing-Maschine, die jede Eingabe in eine Turing-Maschine umschreibt, welche unabhängig von ihrer Eingabe dies als Ausgabe gibt. Für s wähle man den Index einer Turing-Maschine, die die für s geforderte Eigenschaft hat, ein Programm

x zu einem Programm umzuschreiben, das ein Programm y umschreibt in ein Programm, das auf seine Eingabe x anwendet und das Ergebnis als Programm interpretiert, das es auf das Ergebnis anwendet, das man erhält, wenn man y auf die Eingabe anwendet. Dies ist zwar als Turing-Maschine sicherlich nicht leicht zu beschreiben, aber es steht außer Frage, dass es eine solche Turing-Maschine gibt.

3.1.5 Kleenes zweites Modell

Dies ist eine weniger offensichtliche applikative Struktur, deren Grundmenge ${}^{\omega}\omega$ die totalen Funktionen von den natürlichen Zahlen in sich selbst sind. Sie wird ausführlicher etwa in [23] beschrieben. Wir identifizieren die natürlichen Zahlen ω mit der Menge ${}^{<\omega}\omega$ endlicher Folgen natürlicher Zahlen vermöge der rekursiven Funktion

$$(\tau : ln(\tau) \to \omega) \mapsto \Pi_{i<ln(\tau)} p_i^{\tau(i)} \in \omega$$

Dann entspricht 1 der leeren Folge und 2^n der Folge mit dem einzigen Element n. Sei $* : \omega \times \omega \to \omega$ die Konkatenationsfunktion, also die Funktion, die angewandt auf die Folgen $\langle a_0, ..., a_n\rangle$ und $\langle b_0, ..., b_m\rangle$ die Folge $\langle a_0, ..., a_n, b_0, ..., b_m\rangle$ ergibt; wie üblich wird hier $\tau * \sigma$ statt $*(\tau, \sigma)$ geschrieben. Diese Bezeichnung soll auch verwendet werden, falls die zweite Folge gar nicht endlich ist, $\tau * \alpha$ bezeichnet also für $\alpha : \omega \to \omega$ die Funktion der natürlichen Zahlen auf sich selbst, die an Stellen kleiner der Länge von τ mit τ übereinstimmt, und an den anderen Stellen n gleich $\alpha(n - lh(\tau))$ ist.

Für $\alpha \in {}^{\omega}\omega$ schreibt man $\bar{a}(n)$ für $\langle a_0, ..., a_{n-1}\rangle$. Wir definieren jetzt drei Operationen auf der Menge der totalen Funktionen der natürlichen Zahlen in sich selbst, die erste total nach ω, die zweite total in die partiellen Funktionen von ω nach ω und die dritte partiell nach ${}^{\omega}\omega$:

$$\alpha \diamond \beta = m \leftrightarrow \exists n.\ \alpha(\bar{\beta}(n)) = m + 1 \land \forall i < n\ \alpha(\bar{\beta}(i)) = 0$$
$$(\alpha \mid \beta)(n) = \alpha \diamond (\langle n\rangle * \beta)$$
$$\alpha \circ \beta = \gamma \leftrightarrow \forall n (\alpha \mid \beta)(n) = \gamma(n)$$

Die letzte Operation sei die Applikationsoperation für Kleenes zweites Modell. Man beachte, dass sie genau dann definiert ist, wenn $\alpha \mid \beta$ total ist und dann damit übereinstimmt.

3.2 Formale Topologien

3.2.1 Partielle Ordnungen

Definition 21. *Eine* ***partiell geordnete Menge (Pomenge, partielle Ordnung)*** *ist ein Menge A mit einer binären Relation $\leq \subseteq A \times A$, die durch eine Menge gegeben ist und folgende Axiome erfüllt:*

1. *$\leq$ ist reflexiv, also $\forall a \in A\ a \leq a$*
2. *$\leq$ ist transitiv, also $\forall a, b, c \in A\ a \leq b \to b \leq c \to a \leq c$*

Man sagt auch, $\leq$ sei eine partielle Ordnung von oder auf A.

Bemerkung 22. 1. *Wie üblich werden partielle Ordnungen mit ihren Trägern identifiziert und verschiedene partielle Ordnungen auf verschiedenen Mengen meist mit dem selben Zeichen $\leq$ bezeichnet.*

2. *Falls A oder $\leq$ keine Mengen sondern Klassen sind, aber dennoch die Forderungen 1 und 2 der Definition erfüllt sind, spricht man auch von Poklasse.*

3. *Die partiellen Ordnungen auf einer festen Menge A bilden offenbar eine Struktur, die später als eine Heyting-Mengenalgebra bezeichnet wird mit kleinsten Element $\{(a,a)|a \in A\}$, wo $\leq$ äquivalent zu $=$ ist, und mit größtem Element $A \times A$, wo zwei Objekte stets in der Relation stehen.*

4. *Falls $a \in A$ Element einer partiell geordneten Menge ist, so schreibt man ${}^{\leq}a$ für die Menge $\{b \in A | b \leq a\}$ der Elemente in A, die in der partiellen Ordnung Vorgänger von A sind. Für $B \subseteq A$ schreibt man ${}^{\leq}B$ für $\bigcup\{{}^{\leq}b | b \in B\}$. $a \supseteq A \mapsto {}^{\leq}B$ ist eine Abschlussoperation auf dem Verband der Teilmengen von A im Sinne der folgenden Definition.*

Definition 23. *Eine **Abschlussoperation** Φ auf einem Mengenverband (der meist eine Klasse ist) ist eine (meist durch eine Klasse) gegebene Abbildung dieses Verbandes auf sich selbst, die zwei Eigenschaften für alle Mengen A in dem Verband erfüllt:*

1. $A \subseteq \Phi(A)$ *(Reflexivität)*

2. $\Phi(\Phi(A)) = \Phi(A)$ *(Idempotenz)*

3.2.2 Formale Topologien

Formale Topologien sind partiell geordnete Mengen mit einer weiteren Relation. Denkt man sich die Elemente der formalen Topologie als offene Mengen einer klassischen Topologie, so entspricht die partielle Ordnung der Ordnung durch Inklusion. Die weitere Relation $\lhd$ entspricht der Aussage, dass eine offene Menge durch eine Menge offener Mengen überdeckt wird und heißt entsprechend Überdeckungsrelation.

Definition 24. *Eine formale Topologie ist eine partiell geordnete Menge $(S, \leq)$ mit einer Relation $\lhd$ zwischen Elementen von S und Teilmengen von S, die die folgende vier Axiome erfüllt:*

1. $a \in p \to a \lhd p$

2. $a \leq b \lhd p \to a \lhd p$

3. $a \lhd p \to \forall x \in p\, x \lhd q \to a \lhd q$

4. $a \lhd p, q \to a \lhd {}^{\leq}p \cap {}^{\leq}q$

Bemerkung 25. 1. *Man verwendet $\lhd$ in formalen Topologien auch als Relation zwischen zwei Teilmengen der Trägermenge, indem man definiert:*

$$p \lhd q :\leftrightarrow \forall x \in p\, x \lhd q$$

Damit kann man dann das dritte Axiom umschreiben zu: $a \lhd p \lhd q \to a \lhd q$

2. *Falls $P \subseteq S$ eine Klasse ist, so verwendet man $a \lhd P$ für $\exists p \subseteq P\ a \lhd P$*

3. *Man beachte, dass wegen dem zweiten und dritten Axiom $a \leq b$ impliziert, dass $a \lhd b$ gilt.*

4. *Üblicherweise definiert man die Struktur einer formalen Topologie stärker, als dies hier getan wird, nämlich mit einem Positivitätsprädikat und oft einer Operation, die dem Schnitt entspricht. Dies ist allerdings in diesem Kontext überflüssig. Die obige Definition stammt aus [15].*

Definition 26. *Wir definieren den Operator $P(S) \ni A \mapsto\ ^{\lhd}A \subseteq S$ durch*

$$x \in\ ^{\lhd}A \leftrightarrow x \lhd A$$

Für Klassen $A \subseteq S$ bezeichnen wir mit $^{\lhd}A$ die Klasse

$$\{x \in S | \exists B \subseteq A\ x \in\ ^{\lhd}B\}$$

mit Teil 2 der letzten Bemerkung erfüllt dies auch die Bedingung

$$x \in\ ^{\lhd}A \leftrightarrow x \lhd A$$

Offenbar handelt es sich hierbei um eine Abschlussoperation (wegen dem ersten und dritten Axiom) mit $\forall A \subset S.\ ^{\lhd}A \subseteq\ ^{\leq}A \subseteq A$, die allerdings nicht auf der Potenzmenge, sondern auf der Gesamtheit der Teilklassen operiert.

So wie es für klassische Topologien das einfache Beispiel der Potenzmenge einer Menge gibt, also die so genannte diskrete Topologie, in der alle Mengen offen sind, so gibt es auch für formale Topologien das einfache Beispiel der durch $=$ gegebenen partiellen Ordnung, wobei $\lhd$ durch $\in$ gegeben ist.

Jeder klassischen Topologie, die eine Klasse sein darf, aber eine Basis besitzen muss, die eine Menge ist, entspricht eine formale Topologie, indem man eine Basis als Trägermenge nimmt, und $\leq$ über die Inklusion von Basiselementen und $\lhd$ über die Überdeckung eines Basiselements durch eine Menge von Basiselementen definiert. Diskreten Topologien entspricht dann, falls man als Basis die Menge aller Einermengen von Elementen des topologischen Raums nimmt, gerade dieses einfache Beispiel, das darum im Folgenden auch mit diskreter formaler Topologie bezeichnet werden soll. Allerdings können auch nichtdiskrete klassische Topologien zu diskreten formalen Topologien führen. Zum Beispiel führt eine Topologie, in der der Raum durch die Menge der Basiselemente (die aber keine Singletons sein müssen) ohne $\emptyset$ zerlegt ist, stets zu einer diskreten formalen Topologie, obwohl es sich formal nicht um eine diskrete klassische Topologie handeln muss.

Die genaue Formulierung und der Beweis der Korrespondenz zwischen klassischer und formaler Topologie steht noch aus:

Proposition 27. *Sei eine Menge B Basis einer Topologie auf A, also:*

1. $\forall b \in B\ b \subseteq A$

2. $\emptyset \in B$

3. $\forall b, b' \in B\ b \cap b' \in B$

Dann ist $(B, \subseteq, \lhd)$ eine formale Topologie[7]*, wobei $\lhd$ definiert ist durch*

$$b \lhd p \leftrightarrow b \subseteq \bigcup p$$

Dies soll als die (A, B) entsprechende formale Topologie bezeichnet werden.

Beweis.

1. Offenbar ist $\forall b \in B\ b \subseteq b$, also $b \in p \to b \lhd p$.
2. Falls $a \leq b \lhd p$, so $a \subseteq b \subseteq \bigcup p$, also $a \lhd p$.
3. Falls $a \lhd p$, also $a \subseteq \bigcup p$, und $\forall b \in p\ b \lhd q$, also $b \subset \bigcup q$, dann $a \subset \bigcup q$, also $a \lhd q$.
4. Sei $a \lhd p, q$. Dann ist $a \subseteq \bigcup p \cap \bigcup q = \bigcup \{b \cap b' | b \in p \cap b' \in q\} \subset {}^{\leq}p \cap {}^{\leq}q$.

q.e.d.

Eine für unsere Zwecke weit wichtigere Quelle für Beispiele formaler Topologien sind jedoch nicht die klassischen Topologien, sondern Heyting-Algebren.

3.2.3 Heyting-Algebren

Heyting-Algebren sind das intuitionistische Analogon zu Booleschen Algebren. Es sind algebraische Strukturen mit Verknüpfungen, die den logischen Konnektiven entsprechen. Man kann sich eine Heyting-Algebra gut vorstellen als Gesamtheit von möglichen Ereignissen in einer Welt mit intuitionistischer Logik. Zu Ereignissen A und B gibt es auch das Ereignis „A und B“, und falls das Ereignis „$A(x)$“ von x abhängt, kann man das Ereignis „Es gibt ein $x \in X$, so dass $A(x)$“ betrachten.

Eine typische Heyting-Algebra ist die Klasse der Wahrheitswerte

$$\Omega = \{p | p \subseteq 1\}$$

Allgemein ist über halbwegs interessante Heyting-Algebren in CZF nur sehr selten herleitbar, dass es sich um Mengen handle, auch wenn dies in stärkeren Theorien (mit Potenzmengenaxiom) üblicherweise gilt.

Definition 28. *1. Eine Poklasse H mit Klassenoperationen $\bigvee : P(H) \to H$ und $\wedge : H \times H \to H$ heißt* ***Frame****, wenn die folgenden Gesetze gelten:*

(a) Es gibt ein größtes Element, also $\exists \top \in H\ \forall a \in H\ a \leq \top$, dieses Element wird stets mit $\top$ bezeichnet[8]*.*

[7]Es wurde hier die $\leq$-Relation als Relation und nicht als Menge angegeben, letzteres wäre natürlich nicht "$\subseteq$", sondern genauer $\{(b, b') \in B \times B | b \subseteq b'\}$.

[8]Obwohl $\top$ formal nicht zur algebraischen Struktur der Heyting-Algebra gehört, werden wir hier die gleichen Notationskonventionen benutzen, also insbesondere die größten Elemente verschiedener Heyting-Algebren bei Verwechslungssicherheit alle so bezeichnen, ohne diese Bezeichnung für die einzelnen Heyting-Algebren einzuführen. Die folgenden Forderungen führen zu analogen Konventionen. Die Bezeichnungen für die Elemente, deren Existenz gefordert wird, werden im Existenzquantor eingeführt. Dies führt dazu, dass dort im Laufe dieser Definition und der nächsten Proposition Zeichenketten stehen werden, die üblicherweise nicht als Mitteilungszeichen für Variablen gewählt würden. Man beachte, dass die Existenz dieses ausgezeichneten Elementes nicht als kanonisch gefordert wurde. In Abwesenheit von Auswahl kann man diese Konvention also nur führen, wenn man nur endlich viele Heyting-Algebren gleichzeitig betrachtet. Dies wird allerdings im Folgenden stets eingehalten, anderenfalls wäre es nicht nachteilig, $\top$ als Teil der Struktur einer Heyting-Algebra zu fordern.

(b) *Es existieren binäre Infima, also*

$$\forall a, b, c \in H.\ c \leq a \wedge b \leftrightarrow c \leq a \wedge c \leq b$$

(c) *Es existieren beliebige Suprema*[9]*, also*

$$\forall p \subseteq H, c \in H.\ \forall a \in p\ a \leq c \leftrightarrow \bigvee p \leq c$$

(d) *Es gilt das Distributivgesetz, also*

$$\forall a \in H, p \subseteq H.\ a \wedge \bigvee p = \bigvee \{a \wedge x | x \in p\}$$

2. *Ein Frame $(H, \leq)$ mit einer Menge $g \subseteq H$ heißt* ***Heyting-Algebra*** *mit* ***Generatormenge*** *g, wenn für alle $a \in H$ die Klasse $\{x \in g | x \leq a\}$ eine Menge ist und ihr Supremum gleich a ist.*

Die Definition einer Heyting-Algebra wird meist anders gegeben und der Begriff wird oft schwächer verwendet, so dass das, was hier Heyting-Algebra genannt wird, als mengenerzeugte Heyting-Algebra bezeichnet wird. Man fordert dann zusätzlich zu den Eigenschaften eines Frames die Punkte 1 bis 3 der folgenden Proposition als Axiome. Selten verlangt man auch $\bigvee$ nicht als Operation, die jeder Menge ein Supremum zuweist, sondern nur die Existenz eines solchen (analog für $\wedge$). In Abwesenheit von starken Auswahlprinzipien ist dies jedoch ungleich schwächer.

Gambino [15] bezeichnet die Struktur, die wir Heyting-Algebra nennen, als mengenerzeugten (set-generated) Frame, um zu verdeutlichen, dass die Axiome nur die eines Frames und die Erzeugungsaxiome sind. Allerdings zeigt die folgende Proposition, dass es sich um vollständige Heyting-Algebren handelt (mit einer Generatormenge). Die Differenzierung zwischen mengenerzeugten Heyting-Algebren und Heyting-Algebren schlechthin wird hier nicht getroffen, da nur erstere zur Konstruktion von Modellen der Mengenlehre hilfreich sind. Außerdem findet man zu den meisten relevanten Beispielen eine erzeugende Menge.

In Heyting-Algebren sind die typischen Heyting-Operationen alle definierbar:

Proposition 29. *Sei $(H, \leq, g)$ eine Heyting-Algebra. Es ist $\bigvee$ monoton steigend im Sinne*

$$\forall p, q\ p \subseteq q \rightarrow \bigvee p \leq \bigvee q$$

Es ist $\wedge$ monoton steigend im Sinne

$$\forall a, b, c\ a \leq b \rightarrow a \wedge c \leq b \wedge c.$$

Sei $a \in H, b \in H, p \subseteq H$ Menge. Dann gilt:

1. $\exists a \vee b\ \in\ H\ \forall c \in H.\ a \vee b \leq c \leftrightarrow a \leq c \wedge b \leq c$
2. $\exists \bigwedge p\ \in\ H\ \forall c \in H.\ \forall d \in p\ c \leq d \leftrightarrow c \leq \bigwedge p$
3. $\exists a \rightarrow b\ \in\ H\ \forall c \in H\ (c \wedge a \leq b) \leftrightarrow (c \leq a \rightarrow b)$

[9] also Suprema beliebiger Mengen. Der folgende Allquantor läuft ja nicht über Klassen.

Alle in der Definition geforderten und in dieser Proposition behaupteten Elemente sind eindeutig in dem Sinne, dass, falls zwei Elemente $a, b \in H$ die selbe Nummer erfüllen, auch $a \leq b \leq a$ gilt.

Beweis. Sei $p \subseteq q$. Es ist $\bigvee p \leq \bigvee q \leftrightarrow \forall a \in p\ a \leq \bigvee q \leftarrow \forall a \in q\ a \leq \bigvee q \leftrightarrow \bigvee q \leq \bigvee q$, und das ist der Fall.

Sei $a \leq b$. Dann ist $a \wedge c \leq b \wedge c \leftrightarrow (a \wedge c \leq b) \wedge (a \wedge c \leq c)$. Also ist nur noch zu zeigen, dass stets $x \wedge y \leq x$ und $\leq y$. Aber $x \wedge y \leq x \wedge y \leftrightarrow (x \wedge y \leq x) \wedge (x \wedge y \leq y)$.

1. Setze $a \vee b = \bigvee \{a, b\}$.

2. Setze $\bigwedge p = \bigvee \{x \in g | \forall y \in p\ x \leq y\}$. Denn falls $b \in p$, so wegen der Monotonie $\bigvee \{x \in g | \forall y \in p\ x \leq y\} \leq \bigvee \{x \in g | x \leq b\} = b$, also

$$a \leq \bigwedge p \rightarrow \forall b \in p\ a \leq b$$

Wenn andererseits $\forall y \in p\ a \leq y$, so wegen Monotonie

$$a = \bigvee \{x \in g | x \leq a\} \leq \bigvee \{x \in g | \forall y \in p\ x \leq y\}$$

3. Setze $a \rightarrow b = \bigvee \{x \in g | x \wedge a \leq b\}$. Ist dann $c \wedge a \leq b$, so wegen Monotonie $c = \bigvee \{c\} \leq a \rightarrow b$. Ist umgekehrt $c \leq \bigvee \{x \in g | x \wedge a \leq b\}$, so wegen Monotonie

$$c \wedge a \leq \bigvee \{x \in g | x \wedge a \leq b\} \wedge a = \bigvee \{x \wedge a | x \in g \wedge (x \wedge a \leq b)\} \leq \bigvee \{x \in g | x \leq b\} = b$$

4. Setze $\perp = \bigvee \emptyset$, dann ist $\forall c \in H \perp \leq c$.

Die Eindeutigkeit jeder Heyting-Operation folgt, indem man ein Element, das die definierenden Gleichungen erfüllt, nimmt und die definierende Gleichung für ein anderes solches Element auf dieses erste spezialisiert. Stets folgt, dass das eine Element $\leq$ dem anderen ist. So sieht man auch, dass zwei verschiedene $\bigvee$- oder $\wedge$-Operationen auch eindeutig sind bis auf gegenseitige Kleinergleichheit. Q.E.D.

Teile dieses Beweises sind in [15] skizziert.

Wenn wir Bezeichnungen wie $\bigwedge p$ verwenden, obwohl diese ja gar nicht eindeutig sind, meinen wir die Definitionen wie aus dem Beweis. Mit $\top$, was auch nicht eindeutig ist, meinen wir bei Heyting-Algebren $\bigwedge \emptyset$, bei einfachen Frames meinen wir einen festen Zeugen für $\exists \top \in A\ \forall a \in a\ a \leq \top$. Da wir stets nur endlich viele Frames auf einmal betrachten, wird es dabei nie Probleme mit Auswahl geben.

Heyting-Algebren modellieren intuitionistische Logik auf die selbe Weise, wie Boolesche Algebren klassische Logik modellieren. Man wähle eine beliebige Heyting-Algebra A und übersetze eine Formel Θ der intuitionistischen Prädikatenlogik in einen Klassenterm $\bar{\Theta}$ von CZF wie folgt:

$\overline{P_i(x_1, ..., x_{\sharp(i)})} = \{x \in A | (x_1, ..., x_{\sharp(i)}) \in v_i\}$ für P_i, v_i die i-te Prädikatskonstante (mit Stelligkeit $\sharp(i)$) bzw Variable.

$\overline{\Phi \star \Psi} = \bar{\Phi} \star \bar{\Psi}$ für $\star$ ein Junktor (auf der rechten Seite als Heyting-Verknüpfung interpretiert)

$\overline{Qx\Phi(x)} = \dot{Q}\{x | \overline{\Phi(x)} = A\}$ für Q ein Quantor ($\dot{\exists} = \bigvee, \dot{\forall} = \bigwedge$)

Es verwende Θ keine Prädikatenkonstante einer höheren Nummer als n. Dann ist Θ genau dann ableitbar, wenn in CZF ableitbar ist:

$$\forall v_1 \subseteq A^{\sharp(P_1)}, ..., v_n \subseteq A^{\sharp(P_n)} \bar{\Theta} \geq \top$$

Auf explizite Angabe des Beweises durch einfache Induktion wird verzichtet, da später noch viel stärkere Resultate bewiesen werden.

3.2.4 Heyting-Algebren und formale Topologien

Definition 30. *Eine formale Topologie $(S, \leq, \lhd)$*[10] *heißt* ***separierbar****, falls die Relation $\lhd$ separierbar ist, also*

$$\forall a \exists b\, b = \{(x,y) \in a | x \lhd y\}$$

Dies ist häufig der Fall, wenn die Relation $\lhd$ beispielsweise Δ_0-definierbar ist, oder wenn die Topologie auf die unten angegebene Weise aus einer Heyting-Algebra hervorgeht. Insbesondere werden die später eingeführten mengenartigen formalen Topologien diese Eigenschaft haben. In Anwesenheit von voller Separation gilt Separierbarkeit ebenfalls immer. Insbesondere ist bei einer separierbaren formalen Topologie S stets

$$^{\lhd}p = \{x \in S | x \lhd p\}$$

eine Menge für jede Teilmenge $p \subseteq S$.

Definition 31.

1. *Sei $(S, \leq, \lhd)$ eine formale Topologie. Dann sei $H(S)$ definiert als die Klasse aller $A \subseteq S$ so dass $A = {}^{\lhd}A$. Es sei für eine Menge $A \subseteq H(S)$ und $a, b \in H(S)$ definiert: $\bigvee A = {}^{\lhd}\bigcup A$, $a \wedge b = a \cap b$. Es sei $g = \{^{\lhd}\{s\} | s \in S\}$.*

2. *Sei $(H, \leq, \bigvee, \wedge, g)$ eine Heyting-Algebra, so sei $S(H)$ gleich g mit der kleinergleich-Relation $\leq$ von H und der Überdeckungsrelation*

$$g \ni x \lhd p \subseteq g \leftrightarrow \exists y \in p\; y = y \wedge x \leq \bigvee p$$

Dass diese beiden Zuordnungen zu Funktoren zwischen den nur metatheoretisch definierbaren Kategorien der Heyting-Algebren und der separierbaren formalen Topologien führen, ist zwar korrekt, aber nur mit viel Aufwand zu beweisen. Wir benötigen nur die folgende, auch starke Aussage:

Theorem 32.

1. *Sei H eine Heyting-Algebra, dann ist $S(H)$ eine separierbare formale Topologie und $H(S(H)) \cong H$.*

2. *Sei S eine separierbare formale Topologie. Dann ist $H(S)$ eine Heyting-Algebra, und es gilt:*

$$S/(x \lhd \{y\} \wedge y \lhd \{x\}) \cong S(H(S)),$$

wobei $X/(\Phi(x,y))$ die Quotientenstruktur bezeichnet, bei der durch die Relation $\Phi(x,y)$ dividiert wurde.

[10] Die Tripelschreibweise ist eigentlich nicht angemessen, da es sich bei $\lhd$ ja um eine Klasse handelt. In Zukunft werden endliche Tupel von Klassen jedoch auch mit der gleichen Schreibweise wie die objekttheoretischen Tupel von Mengen geschrieben.

Dabei bedeutet Isomorphie von algebraischen Strukturen wie üblich die Existenz einer bijektiven Abbildung der Trägerstrukturen, die mit den zur algebraischen Struktur gehörenden Konstanten, Operationen und Relationen verträglich ist.

Dieses Theorem zeigt, dass formale Topologien, mit denen man im Vergleich zu Heyting-Algebren, die intuitiv gesehen Interpretationen für Formeln liefern (wie das letzte Resultat des letzten Abschnitts andeutet), leicht arbeiten kann, mit diesen eng verwandte Strukturen sind, obwohl der Träger einer formalen Topologien eine Menge sein muss. Ein enger Zusammenhang zwischen formalen Topologien und Heyting-Algebren ist bekannt [9], [25]. Auch Gambino formuliert in seinem Artikel über Heyting-Algebra-bewertete Modelle von CZF [15] ein Theorem, das besagt, dass Heyting-Algebren von formalen Topologien herrühren und verwendet, dass beliebige formale Topologien stets zu Heyting-Algebren führen. Allerdings ist diese zweite von ihm gebrachte Aussage, wie später noch gezeigt werden wird, in der dort behaupteten Allgemeinheit nicht korrekt.

Man beachte, dass man sich der vielleicht als unästhetisch einzuschätzenden Assymetrie des Theorems entledigen hätte können, wenn man bei formalen Topologien und Heyting-Algebren noch $x \lhd \{y\} \wedge y \lhd \{x\} \to x = y$ und $x \leq y \wedge y \leq x \to y = x$ gefordert hätte (bei Heyting-Algebren nur die zweite Bedingung) — sicher kein unnatürliches Axiom, das die wesentlichen Beispiele auch erfüllen. Dies wäre zwar unproblematisch gewesen, da in dieser Arbeit nie Eigenschaften wesentlich werden, die nicht erhalten bleiben, wenn man durch die Relation $x \leq y \wedge y \leq x$ beziehungsweise ihr Analogon für $\lhd$ teilt. Allerdings wäre die schönere Formulierung des obigen Theorems auch der einzige Vorteil dieser Klausel gewesen, was den Aufwand, diese Bedingung für Kandidaten der wesentlichen algebraischen Strukturen stets nachzuprüfen, in den Augen des Autors nicht gerechtfertigt hätte. Außerdem strebt man ja danach, Theoreme über algebraische Strukturen mit möglichst wenigen Axiomen zu formulieren.

Das Theorem muss noch bewiesen werden:
Beweis.

1. Offenbar ist $S(H) \subseteq H$ eine durch $\leq$ partiell geordnete Menge. Die weiteren Bedingungen an eine formale Topologie rechnet man einfach nach:

   (a) $a \in p \to a \leq \bigvee p \to a \lhd p$

   (b) $a \leq b \lhd p \to a \leq b \leq \bigvee p \to a \leq \bigvee p \to a \lhd p$

   (c) $a \lhd p \lhd q \to a \leq \bigvee p \wedge \forall b \in p\, b \leq \bigvee q \to a \leq \bigvee p \leq \bigvee q \to a \lhd q$

   (d) Sei $a \lhd q, p$, also $a \leq \bigvee q, \bigvee p$, so folgt $a \leq \bigvee {}^{\leq}p,\ {}^{\leq}q$ und damit

   $$a \leq \bigvee {}^{\leq}p \wedge \bigvee {}^{\leq}q = \bigvee \{b \wedge c | b \in {}^{\leq}p, c \in {}^{\leq}q\} = \bigvee ({}^{\leq}p \cap {}^{\leq}q)$$

   Also $a \lhd {}^{\leq}p \cap {}^{\leq}q$.

   Es ist noch die Isomorphie zwischen H und $H(S(H))$ zu zeigen. Der Isomorphismus f ist definiert durch $f(x) = \{a \in g | a \leq x\}$, diese Teilmenge von g liegt in $H(S(H))$, denn wäre $y \lhd f(x)$, so $y \leq \bigvee f(x) = f(x)$ und also $y \in f(x)$. Die Abbildung ist injektiv, denn es gibt das Linksinverse $\bigvee$, denn $\bigvee\{a \in g | a \leq x\} = x$ nach den Forderungen an die Mengenerzeugung. Sie ist surjektiv, denn $\bigvee$ ist auch ein rechtsinverses, da für eine Menge A

mit $A = {}^{\lhd}A$ gilt:

$$f(\bigvee A) = \{a \in g | a \leq \bigvee A\} = \{a \in g | a \lhd A\} = {}^{\lhd}A = A$$

Die Abbildung f erhält binäre Infima:

$$f(x \wedge y) = \{z \in g | z \leq x \wedge z \leq y\} = f(x) \cap f(y)$$

Sie erhält beliebige Suprema:

$$\begin{aligned} f(\bigvee p) &= \\ \{x \in g | x \leq \bigvee p\} &= \\ \{x \in g | x \lhd p\} &= \\ \{x \in g | x \lhd \bigcup_{a \in p} \{y \in g | y \leq a\}\} &= \\ {}^{\lhd}\bigcup_{a \in p} f(a) &= \\ \bigvee \{f(a) | a \in p\}, & \end{aligned}$$

wobei das letzte $\bigvee$ natürlich das $\bigvee$ in $H(S(H))$ bezeichnet. Man beachte, dass für $A \in H(S(H))$ insbesondere $\bigvee A = {}^{\lhd}\bigcup f(\bigvee A)$ eine Menge ist, was aus der Definition keineswegs direkt ersichtlich ist.

Das Bild von g unter f ist wieder ein Mengenerzeugendensystem, weil f ein Isomorphismus von Frames ist. Damit ist f ein Isomorphismus von Heyting-Algebren.

2. Es soll gezeigt werden, dass $H(S)$ eine Heyting-Algebra ist. Natürlich ist es eine Poklasse mit $\leq = \subseteq$ und $(a \leq b \wedge c) \leftrightarrow (a \leq b) \wedge (a \leq c)$, dies gilt stets für Mengen. Man beachte, dass $a \wedge b$ überhaupt stets in $H(S)$ liegt. Um zu zeigen, dass dies auch für $\bigvee A$ (mit $A \subseteq H(S)$) gilt, benötigt man die Separierbarkeitsvorausssetzung, dass ${}^{\lhd}\bigcup A$ eine Menge ist. Dass dies die Supremumsbedingung erfüllt, rechnet man nach, wobei eingeht, dass $X \mapsto {}^{\lhd}X$ eine Abschlussoperation ist und somit $X \subseteq Y \leftrightarrow {}^{\lhd}X \subseteq Y$, falls $Y = {}^{\lhd}Y$. Also für $b \in H(S)$:

$$\bigvee A \leq b \leftrightarrow {}^{\lhd}\bigcup A \subseteq b = {}^{\lhd}b \leftrightarrow \bigcup A \subseteq b \leftrightarrow \forall a \in A a \subseteq b \leftrightarrow \forall a \in A a \leq b$$

Es gilt auch das Distributivgesetz:

$$b \wedge \bigvee A = b \cap {}^{\lhd}A = {}^{\lhd}(b \cap \bigcup A) = {}^{\lhd}\bigcup \{a \cap b | a \in A\} = \bigvee \{a \wedge b | a \in A\}$$

Also ist $H(S)$ ein Frame, es ist noch zu zeigen, dass g ein Mengenerzeugendensystem ist. Um zu sehen, dass es sich überhaupt um eine Menge handelt, benötigt man die Erkenntnis, dass seine Elemente ${}^{\lhd}\{s\}, s \in S$ wegen der Voraussetung der Separierbarkeit Mengen sind. Es ist offenbar

$$\{ {}^{\lhd}s | s \in S,\ {}^{\lhd}\{s\} \leq a\} \text{ für } a \in H(S)$$

stets wie benötigt eine Menge, und es gilt, unter starker Ausnutzung der Abschlusseigenschaften:

$$\bigvee\{{}^{\lhd}\{s\}|s\in S,\ {}^{\lhd}\{s\}\leq a\} = {}^{\lhd}\bigcup_{s\in S\wedge s\in a}{}^{\lhd}s = {}^{\lhd}a = a$$

Also ist $H(S)$ tatsächlich Heyting-Algebra.

Zu zeigen bleibt die behauptete Isomorphie. Der Quotient von S soll mit S' bezeichnet werden. Das Element des Quotienten, das von einem Element x herrührt - also seine Äquivalenzklasse - wird mit $\bar{x}$ bezeichnet.

Der Isomorphismus f ist gegeben durch $f(\bar{x}\in S') = {}^{\lhd}\{x\}\in S(H(S))$. Dies ist wohldefiniert, denn falls $x \lhd \{y\} \wedge y \lhd \{x\}$, so auch ${}^{\lhd}\{x\} = {}^{\lhd}\{y\}$. Er ist injektiv, denn falls ${}^{\lhd}\{x\} = {}^{\lhd}\{y\}$, so ist $x \lhd \{y\} \wedge y \lhd \{x\}$. Die Abbildung ist auch surjektiv, denn die Trägermenge von $S(H(S))$ ist ja das Mengenerzeugendensystem von $H(S)$, und das sind genau die ${}^{\lhd}\{x\}$ für $x \in S$. Zu zeigen ist die Strukturerhaltung bezüglich $\leq$ und $\lhd$. Ist $x \leq y$, so $x \lhd \{y\}$ und also ${}^{\lhd}\{x\} \leq {}^{\lhd}\{y\}$, denn in $S(H(S))$ war $\leq$ gerade durch $\subseteq$ definiert. Ist $x \lhd p$, so $x \lhd \bigcup_{y\in p}{}^{\lhd}y$, also $x \in {}^{\lhd}\bigcup_{y\in p}{}^{\lhd}y$, somit ${}^{\lhd}x \leq \bigvee\{{}^{\lhd}y|y \in p\}$, mithin $f(\bar{x}) \lhd \{f(\bar{y})|y \in p\}$. Damit ist f ein Isomorphismus.

Q.E.D.

Heyting-Algebren sind Klassen, aber ihre ganze Struktur ist schon in formalen Topologien enthalten, deren Träger Mengen sind. Allerdings kann bei Topologien mit mindestens zwei unterschiedlichen Elementen die Relation $\lhd$ gar nicht beweisbar durch eine Menge gegeben sein, denn in dieser Menge müsste jede Menge von Paaren enthalten sein, deren erste Komponente das eine Element wäre und deren zweite Komponente eine Menge wäre, die dieses eine Element enthielte und eventuell auch das zweite (mit b bezeichnet) — daraus könnte man aber die Menge $\Omega = \{p \subseteq 1\} \cong \{p \subseteq \{b\}\}$ bilden, und deren Existenz ist äquivalent zum Potenzmengenaxiom, das in CZF ja nicht beweisbar ist, da die Stärke von CZF unterhalb der Stärke von zweitstufiger Zahlentheorie liegt [23].

Dennoch ist die Überdeckungsrelation in vielen Beispielen sehr einfach, bei diskreten Topologien etwa durch die Elementschaftsbeziehung gegeben. Zwar ist die Elementschaftsrelation in nichttrivialen Verbänden nicht durch eine Menge gegeben, aber dennoch muss man von einer diskreten formalen Topologie nur die Trägermenge und keine Klasse kennen, um sie festzulegen, so man eben um ihre Diskretheit weiß. Dies wird nun etwas verallgemeinert: Wir definieren *mengenartige* (set-presentable bei [15]) formale Topologien, bei denen wir $\lhd$ in Abhängigkeit von einem Parameter, der eine Menge ist, mit dem Wissen um die Mengenartigkeit bestimmen können.

Definition 33. *Eine* ***mengenartige*** *formale Topologie ist eine partiell geordnete Menge $(S, \leq)$ mit einer Funktion $R : S \to P(P(S))$, die eine Menge ist, so dass S eine formale Topologie wird mit der Überdeckungsrelation, die gegeben ist durch:*

$$a \lhd p \leftrightarrow \exists u\in R(a)\ u \subseteq p$$

Die einer mengenartigen formalen Topologie zugeordnete formale Topologie wird mit dieser identifiziert.

Das heißt, R gibt zu jedem Element einige „Basisüberdeckungen“ an. Bei einer diskreten Topologie könnte man etwa $R(x) = \{\{x\}\}$ wählen. Man beachte, dass in einer Theorie wie IZF, in der Aussonerung und Potenzmengenaxiom vorliegen, jede formale Topologie mengenartig ist.

Mengenartige formale Topologien S haben die Eigenschaft, dass für Mengen $A \subseteq S$ stets ${}^{\lhd}A = \{s \in S | \exists u \in R(s)\ u \subseteq A\}$ eine Menge ist und also $H(S)$ eine Heyting-Algebra ist. Umgekehrt kann man aber nicht von jeder Heyting-Algebra beweisen, dass die ihr entsprechende Topologie mengenartig ist. Dies kann man mit der später angegebenen Modellkonstruktion aus Heyting-Algebren zeigen [15], allerdings nicht dadurch, dass ein Gegenmodell angegeben wird, sondern dadurch, dass man unter der Annahme, man könnte von einer bestimmten Topologie beweisen, dass sie mengenartig wäre, die Existenz eines Modells zeigt, die in CZF nicht beweisbar sein kann, da in ihm $Cons(CZF)$ gilt.

3.3 Applikative Topologien

Die in dieser Arbeit neu eingeführte Struktur der applikativen Topologie ist eine Art Mischung aus einer formalen Topologie und einer applikativen Struktur und wird verwendet, um ein Modell der konstruktiven Mengenlehre anzugeben.

Zur besseren Formulierbarkeit der von dieser algebraische Struktur geforderten Axiome werden wir bei Strukturen mit partiellen binären Verknüpfungen die Applikationsterme, wie sie in Sektion 3.1.1 eingeführt wurden, mit all ihren Notationen verwenden.

3.3.1 Definition

Definition 34. *Eine **schwache applikative Topologie** ist eine separierbare formale Topologie $(S, \leq, \lhd)$ mit einer Teilmenge $\nabla \subseteq S$, zwei ausgezeichneten Elementen $k \in \nabla$ und $s \in \nabla$ und einer partiellen binären Verknüpfung $\circ$, die Applikation genannt wird, und die folgenden Axiome erfüllt:*

1. $\forall x \in p, y \in q\ xy\downarrow \rightarrow (a \lhd p \wedge b \lhd q) \rightarrow ab\downarrow\ \wedge ab \lhd \{xy | x \in p, y \in q\}$
2. $\forall x, y \in S.\ xy\downarrow \rightarrow x, y \in \nabla \rightarrow xy \in \nabla$
3. $\forall x, y \in S.\ kxy\downarrow \wedge kxy \lhd \{x\}$
4. $\forall x, y \in S\ sxy\downarrow$
5. $\forall x, y, z \in S.((xz)(yz)\downarrow \vee sxyz\downarrow) \rightarrow (sxyz\downarrow \wedge (xz)(yz)\downarrow \wedge sxyz \lhd \{(xz)(yz)\})$
6. $\nexists e \in \nabla\ e \lhd \emptyset$

Bemerkung 35. *Bei einer (schwachen) applikativen Topologie sind folgende Konventionen, die an die Konvention zu $\simeq$ angelehnt sind, sehr hilfreich. Man erinnere sich, dass $V(t, a)$ bedeutet, dass t ein geschlossener Applikationsterm ist und den Wert a hat. Seien t, t' Applikationsterme, p, p' Mengen von Applikationstermen.*

1. *$t \trianglelefteq t'$ steht für*

$$\forall a.(V(t, a) \rightarrow \exists b.\ a \lhd \{b\} \wedge V(t', b)) \wedge (V(t', b) \rightarrow \exists a.\ a \lhd \{b\} \wedge V(t, b))$$

2. $p\downarrow$ *steht für* $\forall a\in p\ a\downarrow$

3. pp' *steht für* $\{ab|a\in p, b\in p'\}$

Damit schreiben sich die Forderungen an schwache applikative Topologien einfacher als:

1. $pp'\downarrow, a\lhd p, b\lhd p' \to ab\lhd pp'$

2. $xy\downarrow, x\in\nabla, y\in\nabla \to xy\in\nabla$

3. $kxy \unlhd x$

4. $sxy\downarrow$

5. $sxyz \unlhd xz(yz)$

6. $\nabla\ni x\lhd\emptyset \to \bot$

Man sieht, dass die Applikation ähnlichen Bedingungen genügt wie in applikativen Strukturen, allerdings gilt statt dem starken $\simeq$ nur die schwache Relation $\unlhd$, die keine Äquivalenzrelation ist, sondern nur eine partielle Ordnungsrelation[11]. Außerdem dürfen in applikativen Topologien k und s übereinstimmen. In vielen Beispielen tun sie dies durchaus, ohne dadurch die applikative Topologie zu trivialisieren. Der im Kapitel zu applikativen Strukturen angegebene Beweis, dass aus den restlichen Axiomen applikativer Strukturen und der Existenz zweier verschiedener Elemente folgt, dass $k\neq s$, stützt sich nämlich wesentlich darauf, dass man in applikativen Strukturen die Axiome für $\simeq$ und nicht nur für die partielle Ordnungsrelation $\unlhd$ zur Verfügung hat.

Schwache applikative Topologien reichen aus, um Modelle einer elementaren Mengenlehre ohne das Subset Collection Schema zu konstruieren. Eigentlich will man jedoch mit (starken) applikativen Topologien arbeiten.

Definition 36. *Eine (starke)* ***applikative Topologie*** *ist ein Septupel* $(S,\leq,r,\circ,\nabla,k,s)$*, so dass* $(S,\leq,r)$ *eine mengenartige formale Topologie bildet, deren Überdeckungsrelation mit* $\lhd$ *bezeichnet sei, und so dass* $(S,\leq,\lhd,\circ,\nabla,k,s)$ *eine schwache applikative Topologie bildet. Es werden Konventionen analog zum Verhältnis der mengenartigen formalen Topologien zu den allgemeinen formalen Topologien verwendet.*

Bevor wir zentrale Eigenschaften über applikative Topologien herleiten, benötigen wir zwei Definitionen: Wir wollen Substitutionen auch für allgemeine Applikationsterme durchführen und nicht nur konstante Terme substituieren, und wir führen eine weitere Bezeichnung ein für Terme, die sich bezüglich ∇ günstig verhalten.

Definition 37. *Für Applikationsterme* t,t' *ist* $t[v_i := t']$ *induktiv definiert:*

1. $v_i[v_i := t'] = t'$

2. $v_j[v_i := t'] = v_j$ *für* $j\neq i$

3. $a[v_i := t'] = a$ *für* $a\in S$

[11] die wegen der Separierbarkeit auf $S\times S$ stets durch eine Menge gegeben ist

4. $t_1t_2[v_i := t'] = t_1[v_i := t']t_2[v_i := t']$

Definition 38. *Wir sagen, ein Applikationsterm t **überzeugt**, in Zeichen $t!$, falls für alle Folgen $(a_i)_{i\in FV(t)}$ in ∇ gilt:*

$$t[(v_i := a_i)_{i\in FV(t)}]\downarrow \to t[(v_i := a_i)_{i\in FV(t)}] \in \nabla$$

Insbesondere überzeugen Applikationsterme, bei deren Aufbau nur solche Elemente aus S verwendet wurden, die in ∇ liegen, wie k und s. Hätte man Applikationsterme unabhängig von der Struktur eingeführt, so würden alle Applikationsterme überzeugen. Man beachte, dass die Eigenschaft, zu überzeugen, bei Substitution erhalten bleibt, also

$$t! \to s! \to t[v_i := s]!$$

Mit dieser Definition kann man das zweite Axiom umschreiben als:

$$v_1v_2\downarrow$$

3.3.2 Einige Eigenschaften

Wie applikative Strukturen verfügen applikative Topologien über die Fähigkeit der λ-Abstraktion und man kann die λ-Terme genauso definieren. Wichtig ist nicht nur, dass sie stets denotieren, sondern auch, dass sie überzeugen, also in ∇ liegen.

Lemma 39. *Sei t ein Applikationsterm über einer schwachen applikativen Topologie S. Dann gibt es für $n\in\omega$ einen Applikationsterm $\lambda v_n.t$, so dass gilt:*

- $FV(\lambda v_n.t) = FV(t) \setminus \{n\}$
- $(\lambda v_n.t)\downarrow$
- $(\lambda v_n.t)!$ *falls alle Konstanten von t aus ∇ sind*
- $(\lambda v_n.t)v_n \trianglelefteq t$

Beweis. Induktion über den Aufbau von t.

1. $t = v_n$: Definiere $\lambda v_n.t$ als skk. Dies hat keine freien Variablen, denotiert und überzeugt und $skkv_n \trianglelefteq (kv_n)(kv_n) \trianglelefteq v_n$.

2. $t = v_m, m \neq n$: Definiere $\lambda v_n.t$ als kv_m. Dies hat die gleichen freien Variablen wie t, denotiert und überzeugt und $kv_mv_n \trianglelefteq v_m$.

3. $t = a\in A$: Definiere $\lambda v_n.t$ als ka. Dies hat keine freien Variablen, denotiert und überzeugt und $kav_n \trianglelefteq a$.

4. $t = t_1t_2$: Definiere $\lambda v_n.t$ als $s(\lambda v_n.t_1)(\lambda v_n.t_2)$. Dies denotiert und überzeugt nach Axiomen und Induktionsvoraussetzung und hat als freie Variablen die selben wie t, nur ohne v_n. Und

$$s(\lambda v_n.t_1)(\lambda v_n.t_2)v_n \trianglelefteq ((\lambda v_n.t_1)v_n)((\lambda v_n.t_1)v_n) \trianglelefteq t_1t_2 = t$$

nach Induktionsvoraussetzung.

Q.E.D.

Insbesondere folgt aus dem vierten Punkt die formal etwas stärkere Konversionsregel: Falls $n \in FV(t)$ oder $t' \downarrow$, so

$$(\lambda v_n.t)t' \trianglelefteq t[v_n := t']$$

Denn $(\lambda v_n.t)t' = (\lambda v_n.t)v_n[v_n := t'] \trianglelefteq t[v_n := t']$. Die letzte Umformung gilt, falls t' denotiert oder falls $n \in FV(t)$, also wenn die Denotiertheit der rechten Seite tatsächlich die der linken impliziert (dass wenn beide Denotate existieren, sie auch gleich sind, ist klar).

Wir werden auch in Zukunft die Bezeichnung $\lambda v_n.t$ für den im Beweis dieses Lemmas angegebenen Term verwenden. Überhaupt werden wir nach einem Existenzlemma und Angabe eines Zeugen im Beweis künftig die Bezeichnung des behaupteten Elements/Terms der applikativen Topologie für den im Beweis angegebenen Zeugen verwenden, eventuell nach einer Umbenennung der gebundenen Variablen zu neuen Nummern (der λ-Operator zählt hier als bindend).

In applikativen Strukturen ist die Existenz eines Fixpunktterms ganz wesentlich (dies entspricht dem effektiven Rekursionssatz oder der effektiven Variante des Fixpunktsatz von Kleene in der Rekursionstheorie). Dieser denotiert zu einem Element, das auf ein Element a angewandt einen Fixpunkt der Anwendung von a liefert (genauer: ein Element, das ein Fixpunkt dieser Anwendung ist, sofern diese überhaupt denotiert). Dieses Resultat ist etwa in [20] bewiesen.

In applikativen Topologien funktioniert dieser Beweis nicht, auch wenn man $\simeq$ durch $\trianglelefteq$ ersetzt, da dieses „in verschiedene Richtungen“ angewandt würde, so aber natürlich nicht mehr transitiv ist. Alles, was man so zeigen kann, wäre, dass das gefundene Element auf ein Element a angewandt etwas liefert, was mit einem Fixpunkt der Anwendung von a eine gemeinsame Überdeckung durch ein einziges Element hat. Für die wesentlichen Anwendungen ist dies jedoch nicht hilfreich.

Es besteht ein feiner Unterschied zwischen dem Theorem für applikative Strukturen und der folgenden Aussage, die zwar deutlich schwächer ist insofern, als dass der Fixpunktfinder nicht in der applikativen Struktur selbst behauptet wird, sondern nur als Fixpunkt*term* vorliegt, was aber bei genauem Hinschauen für viele Zwecke ausreicht. Unumgänglich für die Anwendbarkeit ist die Formulierung der zweiten Eigenschaft des Fixpunktterms als Eigenschaft für alle Terme, und nicht nur alle Elemente der Struktur. Sonst könnte der Fixpunktterm etwa eine stets undenotierender Term sein, was aber nichts nützt.

Lemma 40. *Sei S eine schwache applikative Topologie. Dann existiert ein Applikationsterm τ^{fix} über S mit v_1 als einziger freien Variable, so dass*

1. $\tau^{fix}!$

2. $\forall t\ \tau^{fix}[v_1 := t] \trianglelefteq t(\tau^{fix}[v_1 := t])$

Beweis. Setze $\tau^{fix} = ((\lambda v_2.v_1(v_2v_2))(\lambda v_2.v_1(v_2v_2)))$, dies überzeugt. Da die Ersetzung von v_2 durch eine andere Variable ungleich v_1 die syntaktische Form des Terms nicht ändert, kann man ohne Einschränkung verlangen, dass v_2 keine freie Variable in t ist. Dann ist für $a \in S$

$$\begin{aligned} \tau^{fix}[v_1 := t] = \\ (\lambda v_2.t(v_2 v_2))(\lambda v_2.t(v_2 v_2)) \trianglelefteq \\ t((\lambda v_2.t(v_2 v_2))(\lambda v_2.t(v_2 v_2))) = \\ t(\tau^{fix}[v_1 := t]) \end{aligned}$$

Q.E.D.

Offenbar gibt es ein Element von S, das auf ein $a \in S$ angewandt immerhin einen $\trianglelefteq$-Vorgänger von a angewandt auf den substituierten Fixpunktterm ergibt, nämlich $\lambda v_1.\tau^{fix}$. Es selbst ist aber kein Fixpunkt, nicht einmal in dem schwachen Sinne, dass es ein $\trianglelefteq$-Vorgänger dessen, was man erhält, wenn man a auf es anwendet, sei.

Das folgende Lemma wirkt vielleicht unnötig speziell, ist aber von großer Anwendbarkeit.

Lemma 41. *Seien x und y voneinander und von v_1 verschiedene Variablen, v_1 nicht frei in t, x frei in t. Dann gilt*

$$t^{fix}[v_1 := \lambda xy.t] \downarrow$$

Beweis. Es ist

$$\begin{aligned} \tau^{fix}[v_1 := \lambda xy.t] \trianglelefteq \\ (\lambda xy.t)(\tau^{fix}[v_1 := \lambda xy.t]) = \\ ((\lambda xy.t)(\tau^{fix}))[v_1 := \lambda xy.t] \trianglelefteq \\ (\lambda y.t)[x := \tau^{fix}][v_1 := \lambda xy.t] \downarrow \end{aligned}$$

Q.E.D.

Wie in applikativen Strukturen stellen applikative Topologien Werkzeuge zur Fallunterscheidung und Paarbildung bereit. Die Definitionen in [6], der dies in applikativen Strukturen zeigt, wurden etwas abgeändert, um weniger Terme definieren zu müssen - insbesondere agieren die Projektoren, die einem Paar die linke beziehungsweise rechte Komponente zuweisen, nun auch als Wahrheitswerte, abhängig von denen Fallunterscheidungen getroffen werden. Dies führt zu einer deutlichen Vereinfachung und ist nach Meinung des Autoren in rekursionstheoretischen Kontexten auch natürlicher als die gängige Praxis, Wahrheitswerte mit den beiden ersten natürlichen Zahlen zu identifizieren.

Lemma 42. *Sei S eine schwache applikative Topologie. Es gibt p, D, l und r in ∇, so dass für alle $a, b \in S$ gilt:*

1. $l(pab) \trianglelefteq a$
2. $r(pab) \trianglelefteq b$
3. $Dlab \trianglelefteq a$
4. $Drab \trianglelefteq b$

Beweis. Setze $l = \lambda v_1.v_1 k$, $r = \lambda v_2.v_2(k(skk))$, $p = \lambda v_3 v_4 v_5.v_5 v_3 v_4$, $D = \lambda v_6 v_7 v_8.v_6(p v_7 v_8)$. Dann gilt

1. $l(pab) = (\lambda v_1.v_1 k)(pab) \trianglelefteq pabk \trianglelefteq kab \trianglelefteq a$
2. $r(pab) \trianglelefteq pab(k(skk)) \trianglelefteq k(skk)ab \trianglelefteq (skk)b \trianglelefteq kb(kb) \trianglelefteq b$
3. $Dlab \trianglelefteq l(pab) \trianglelefteq a$
4. $Drab \trianglelefteq r(pab) \trianglelefteq b$

Q.E.D.

Korollar 43. *Ist $x \trianglelefteq l$, $y \trianglelefteq r$, so*

1. $Dxab \trianglelefteq a$

2. $Dyab \trianglelefteq b$

Beweis. Da $Dlab$ und $Drab$ denotieren, folgt aus Axiom 1 der applikativen Topologie, dass $Dxab \trianglelefteq Dlab$ und $Dyab \trianglelefteq Drab$ ist. Q.E.D.

Man kann l und r als die entscheidbaren, klassischen Wahrheitswerte 0 und 1 interpretieren, die den Fallunterscheidungsoperator D dirigieren können. Mit ihm kann man auch die bekannten Booleschen Funktionen basteln, $\lambda v_0.Dv_0 rl$ etwa entspricht der auf den klassischen Wahrheitswerten selbstinversen Nicht-Funktion.

Uns ist daran gelegen, die natürlichen Zahlen in unsere Struktur S einzubetten, dies ist für applikative Topologien nicht viel anders als für applikative Strukturen [6], [20] und es gibt viele Methoden, dies zu tun, die alle Vor- und Nachteile haben. Gütekriterien könnten etwa sein, kurze Ausdrücke (in s und k) zu erhalten oder leicht zeigen zu können, dass alle rekursiven Funktionen implementierbar sind. Die hier entwickelte Variante hat den Vorteil, dass man den Zahlen sehr direkt ansehen kann, ob sie 0 sind oder nicht, und leicht ihre Nachfolger und Vorgänger bestimmen kann.

Wir definieren für ein $n \in \omega$ induktiv $\underline{n} \in \nabla$:

$$\underline{0} = plr$$

$$\underline{n+1} = pr\underline{n}$$

Dies sind alles in ∇ denotierende Terme. Man sieht, dass $l\underline{n}$ angibt, ob n gleich oder ungleich 0 ist. Man sieht, dass es $s_N \in \nabla$ gibt, so dass $s_N \underline{n} \trianglelefteq \underline{n+1}$, nämlich das Denotat von $\lambda v_0.prv_0$. Es gibt auch ein $p_N \in \nabla$ mit $p_N \underline{n+1} \trianglelefteq \underline{n}$ und $p_N \underline{0} \trianglelefteq \underline{0}$, nämlich

$$\lambda v_0.D(lv_0)\underline{0}(prv_0)$$

(Man beachte dabei, dass stets $l\underline{n}\downarrow$ und $r\underline{n}\downarrow$, sonst würde eventuell zwar der Term denotieren, auf den die Fallunterscheidung weist, aber nicht der andere, und damit $p_N \underline{n}$ nicht.)

Man kann auch testen, ob eine Zahl kleiner als eine andere ist. Es sei

$$d_{\leq} := \tau^{fix}[v_1 := \lambda vxy.D(lx)(\lambda zz'.l)(D(ly)(\lambda zz'.r)(\lambda zz'.vzz'))(p_N x)(p_N y)]$$

Dann gilt

$$n \leq m \to d_{\leq}\underline{n}\underline{m} \trianglelefteq l$$
$$n > m \to d_{\leq}\underline{n}\underline{m} \trianglelefteq r$$

Dies zeigt man durch Induktion über $min(n,m)$. Der Induktionsanfang ist klar, denn ist $n = 0$, so entscheidet die äußere Fallunterscheidung für etwas $\trianglelefteq l$, und ist dies nicht der Fall, aber $m = 0$, so entscheidet die innere für etwas $\trianglelefteq r$. Hierbei muss man beachten, dass der Teilterm $(\lambda zz'.vzz')$ ohne Voraussetzung über Denotiertheit von v stets denotiert, sonst wäre die Fallunterscheidungseigenschaft von D nicht ausnutzbar

Seien also $n, m > 0$ und die Aussage für alle kleineren Minima bewiesen, so gilt

$$\begin{aligned}&d_{\leq}\underline{n}\underline{m}\\ \trianglelefteq\ &(D(l\underline{n})(\lambda zz'.l)(D(l\underline{m})(\lambda zz'.r)(((d(l\underline{n})(\lambda zz'd_{\leq}zz'))))(p_N\underline{n})(p_N\underline{m})))\\ \trianglelefteq\ &d_{\leq}(p_N\underline{n})(p_N\underline{m})\end{aligned}$$

Und dies erfüllt nach Induktionsvoraussetzung die gewünschte Beziehung.

Man beachte die Denotiertheit aller Teilterme (die sehr einfach über die Induktion mitbewiesen wird) — wäre auf diese nicht zu achten (sondern nur auf Denotiertheit der Teilterme, die tatsächlich bei einer „lazy evaluation“-Berechnung des Ergebnisses benötigt werden), so hätte man den Term einfacher wählen können als

$$\tau^{fix}[v_1 := \lambda vxy.D(lx)r(d(ly)l((v(p_N x)(p_N y)))$$

Für die Zukunft setzen wir noch $e_{\leq} = \lambda x.d_{\leq}x \in \nabla$.

Dies wird für unsere Zwecke genügen. Es ist anzumerken, dass es sich übrigens um keine echte Einbettung in dem Sinne, dass die Abbildung $n \mapsto \underline{n}$ injektiv wäre, handelt. Dies ist zwar oft, aber nicht immer gegeben, etwa nicht, falls $k = s$ gilt. Dies tritt bei sehr natürlichen Beispielen auf, wie der nächste Abschnitt zeigt. Wenn die Abbildung allerdings in einem starken Sinne injektiv ist, ergeben sich einige interessante Folgerungen, wie im Kapitel über unterscheidende applikative Topologien demonstriert wird.

3.3.3 Einige Beispiele

Die trivale applikative Struktur ist offenbar $S = \nabla = \{0\}$ mit $k = s = 0$ und $0 \circ 0 = 0$, $0 \lhd p \leftrightarrow 0 \in p$. Es gibt aber interessantere Beispiele. Verändert man etwa in der trivialen applikativen Struktur nur die Definition von $\lhd$ zu $0 \lhd p \leftrightarrow \neg 0 \notin p$, so erhält man offenbar eine andere Struktur, die dennoch zumindest eine schwache applikative Struktur ist (alle Axiome sind offenbar erfüllt, $\{0 \in S | 0 \lhd p\}$ ist stets eine Menge, da $\lhd$ durch eine Δ_0-Formel definiert ist). Mengenartig ist die Topologie jedenfalls zumindest nicht offensichtlich (in CZF ist auch nicht beweisbar, dass sie es wäre, denn das mit ihr erhaltene Modell realisiert das ausgeschlossene Dritte, die beweistheoretische Stärke von CZF wird durch das ausgeschlossene Dritte aber stark erhöht; könnte man beweisen, dass die Struktur eine starke applikative Topologie wäre, so könnte man die Existenz eines Klassenmodells für CZF+EM in CZF zeigen [15]). Man kann mithin nicht behaupten, dass es sich um eine starke applikative Struktur handle.

Die Struktur der applikativen Topologien soll in einem gewissen Sinne eine gemeinsame Verallgemeinerung der applikativen Strukturen und Heyting-Algebren sein, da die damit konstruierten Modelle eine gemeinsame Verallgemeinerung der Modelle aus applikativen Strukturen und Heyting-Algebren werden sollen.

Proposition 44. *Ist* $(A, \circ, k, s)$ *eine applikative Struktur, so erhält man mit* $\nabla = A$, $a \lhd p \leftrightarrow a \in p$ *und* $r(a) = \{\{a\}\}$ *eine starke applikative Topologie.*

Beweis. Alle Axiome sind offensichtlich erfüllt. Q.E.D.

Dieses erste Beispiel war mit einer diskreten Topologie versehen (triviale $\lhd$-Relation) und ging von applikativen Strukturen aus. Das folgende Beispiel verfügt in dieser Beziehung über mehr Struktur und basiert auf Heyting-Algebren:

Proposition 45. *Sei* $(H, \leq, \bigvee, \wedge, g)$ *eine mengenerzeugte Heyting-Algebra, so dass*

$$\top \in g \wedge \forall x, y \in g \; x \wedge y \in g$$

Sei $\tilde{\nabla}$ *ein Heyting-Algebra Filter*[12]*. Dann ist* $S(H)$ *mit* $k = s = \top$, $a \circ b = a \wedge b$ *und* $\nabla = \tilde{\nabla} \cap g$ *eine schwache applikative Topologie.*

Die Bedingungen an g sind hierbei nicht wirklich Einschränkungen, denn wenn man von einer beliebigen Generatormenge g von H ausgeht, dann erfüllt die vergrößerte Menge

$$g' := \{a_0 \wedge ... \wedge a_{n-1} | n \in \omega, \forall i \in n . a_i \in g \vee a_i = \top\}$$

die beiden Eigenschaften $\top \in g'$ und $x, y \in g' \to x \wedge y \in g'$ offenbar. Und wie jede Obermenge einer Generatormenge ist g' wieder eine Generatormenge.

Zum Beweis der Proposition:
Beweis. Es wurde in der Sektion über formale Topologien gezeigt, dass $S(H)$ eine formale Topologie ist. Nach der Wahl von g ist $\circ$ wohldefiniert und sogar total auf $S(H) = g$. Es ist $k = s = \top \in g \cap \tilde{\nabla} = \nabla$ und für $x, y \in \nabla = \tilde{\nabla} \cap g$ gilt $x \wedge y \in \tilde{\nabla} \cap g = \nabla$ wegen der Abgeschlossenheit der beiden Mengen gegenüber $\wedge$. Wegen der Abgeschlossenheit von $\tilde{\nabla}$ ist ∇ auch abgeschlossen gegenüber $\trianglelefteq$ und kein Element von ∇ wird von der leeren Menge überdeckt. Für $x, y, z \in S(H) = g$ gilt

1. $kxy = x \wedge y \leq x = \bigvee\{x\} \to kxy \lhd \{x\}$
2. $sxyz = (x \wedge y \wedge) z \leq \bigvee\{(x \wedge y)(x \wedge z)\}$

Damit ist alles gezeigt. Q.E.D.

Konstruktionen

Man kann aus alten applikativen Topologie neue machen. Es ist die Kategorie der applikativen Topologien zum Beispiel abgeschlossen gegenüber kartesischen Produkten[13].

[12] also $\tilde{\nabla} \ni a \leq b \to b \in \tilde{\nabla}$, $\top \in \tilde{\nabla}$ und $a, b \in \tilde{\nabla} \to a \wedge b \in \tilde{\nabla}$

[13] Schwache applikative Topologien sind Klassen (wegen $\lhd$) und so wäre ihre Kategorie umständlich zu definieren und sehr metatheoretisch, es wird darum auf eine genaue Ausführung dieser Aussage verzichtet.

Proposition 46. *Seien S und T schwache applikative Topologien. Dann ist $S \times T$ eine schwache applikative Topologie mit:*

1. $(a,b) \leq (c,d)$ *gdw*[14] $a \leq c \wedge b \leq d$
2. $(a,b) \lhd p$ *gdw* $a \lhd p^{-1}[T] \wedge b \lhd p[S]$
3. $(a,b) \circ (c,d) = (e,f)$ *gdw* $a \circ c = e \wedge b \circ d = f$,
4. $(a,b) \in \nabla$ *gdw* $a \in \nabla \wedge b \in \nabla$

Sind S und T sogar starke applikative Topologien, dann ist $S \times T$ starke applikative Topologie mit

$$r(a,b) = \{u \times v | u \in r(a), v \in r(b)\}$$

Beweis. Es bleiben $k, s \in \nabla$. Da $\lhd$ komponentenweise definiert wurde, folgen auch die anderen Axiome sofort, unter Beachtung, dass $(a,b)(c,d) \downarrow \leftrightarrow ac \downarrow \wedge bd \downarrow$. Q.E.D.

Eine weitere natürliche Konstruktion sind Quotienten:

Proposition 47. *Sei S eine schwache applikative Topologie und R eine durch eine Menge gegebene Äquivalenzrelation auf S, so dass gilt:*

$$aRb \rightarrow a \circ b = c \rightarrow aRc$$

$$aRb \rightarrow cRd \rightarrow a \leq c \rightarrow b \leq c$$

$$aRb \rightarrow a \lhd \{c \in S | \exists d \in S.\ cRd \wedge d \in p\} \rightarrow b \lhd p$$

Dann ist der Quotient

$$S/R := \{\bar{a} | a \in S\}$$

mit

$$\bar{a} := \{b \in S | bRa\}$$

eine schwache applikative Topologie mit ausgezeichneten Elementen $\bar{k}$ und $\bar{s}$ und

1. $\bar{a} \leq \bar{b}$ *gdw* $a \leq b$
2. $\bar{a} \lhd p$ *gdw* $a \lhd \bigcup p$
3. $\bar{a} \circ \bar{b} = \bar{c}$ *gdw* $a \circ b = c$
4. $e \in \nabla$ *gdw* $\exists a \in e\ a \in \nabla$

Ist S sogar eine starke applikative Topologie, dann ist der Quotient dies auch mit

$$r(e) = \bigcup_{a \in e} \{\{\bar{b} | b \in u\} | u \in r(a)\}$$

[14] genau dann, wenn

Beweis. Bekanntermaßen sind Quotienten von Mengen durch durch Mengen gegebene Äquivalenzrelationen wieder Mengen ([1]). Die Verknüpfung $\circ$ und die Relationen $\leq$ und $\lhd$ sind wegen der Bedingung an die Äquivalenzrelation wohldefiniert. Offenbar ist $\lhd$ immer noch separabel, da die Definition für $\lhd$ der neuen Topologogie Δ_0-definierbar in der Relation $\lhd$ der alten Topologie ist.

Auch in der neuen Struktur impliziert $e \leq f \in p$, dass $e \lhd p$. Falls $e \lhd p \lhd q$, so ist wieder $e \lhd q$. Falls $e \lhd p, q$, also $\forall a \in e a \lhd \bigcup p, \bigcup q$, so ist $\forall a \in e a \lhd {}^{\leq}\bigcup p \cap {}^{\leq}\bigcup q$. Es ist aber

$$ {}^{\leq}\bigcup p = \{x \in S | \exists \bar{y} \in p x \leq y\} = \bigcup {}^{\leq}p $$

Also ist $\forall a \in e a \lhd \bigcup({}^{\leq}p \cap {}^{\leq}q)$, also $e \lhd {}^{\leq}p \cap {}^{\leq}q$. Damit ist gezeigt, dass es sich überhaupt um eine formale Topologie handelt.

Es ist auch eine applikative Topologie. Offenbar sind $\bar{s}, \bar{k} \in \nabla$ und es ist ∇ abgeschlossen gegenüber $\circ$. Die Axiome über s und k sind offenbar auch erfüllt, und kein Element von ∇ wird von der leeren Menge überdeckt.

Seien $\bar{a} \lhd p, \bar{b} \lhd q$ mit $\forall e \in p, f \in q ef\downarrow$. Dann gilt auch für alle $a' \in \bigcup p, b' \in \bigcup q$, dass $a'b'$ denotiert, da $\bar{a'}\bar{b'}$ dies tut. Also ist wegen $a \lhd \bigcup p$, $b \lhd \bigcup q$ auch

$$ ab \lhd \{xy | x \in \bigcup p, y \in \bigcup q\} = \bigcup \{\bar{x}\bar{y} | \bar{x} \in p, \bar{y} \in q\} $$

Also nach Voraussetzung $\bar{a}\bar{b} \lhd \{ef | e \in p, f \in q\}$. Damit sind alle Eigenschaften einer schwachen applikativen Topologie gezeigt. Für starkes S ist $\lhd$ gegeben durch r, denn

$$
\begin{aligned}
& e \lhd p \leftrightarrow \\
\leftrightarrow\ & \exists a \in e a \lhd \bigcap p \\
\leftrightarrow\ & \exists a \in e, u \in r_S(a) u \subseteq \bigcap p = \{\bar{b} | b \in \bigcap p\} \\
\leftrightarrow\ & \exists a \in e, u \in r_S(a) \{\bar{b} | b \in u\} \subseteq \{\bar{b} | b \in \bigcap p\} = p \\
\leftrightarrow\ & \exists u \in r_{S/R}(e) u \subseteq p
\end{aligned}
$$

Q.E.D.

Weitere Beispiele werden später noch auf natürliche Weise auftauchen.

Kapitel 4

Modelle für CZF

4.1 Konstruktion eines Modells

Wir werden in diesem Abschnitt eine schwache applikative Topologie S festhalten und von ihr ausgehend ein Modell für CZF konstruieren.

Ein Modell für eine logische Theorie wie CZF besteht üblicherweise aus zwei Teilen: Einem Universum $V(S)$, über dessen Elemente die Quantoren laufen, und einer Interpretation der Sätze in diesem. Es wird dabei jedem Satz Ψ der Sprache der Mengenlehre ein Satz Ψ^S zugewiesen, dessen Quantoren auf $V(S)$ (und manche auf S) beschränkt sein werden[1]. Um zu zeigen, dass es sich um ein Modell von CZF handelt, müssen drei Dinge gezeigt werden:

1. Es handelt sich um ein Modell der intuitionistischen Logik, das bedeutet, die in ihm erfüllten Sätze bilden eine Theorie, sind also unter logischer Folgerung abgeschlossen: $\Gamma \vdash \Psi$ und $CZF \vdash \Gamma^S$ (elementweise) impliziert $CZF \vdash \Psi^S$.

2. In dem Modell gilt CZF: $CZF \vdash \Psi$ impliziert $CZF \vdash \Psi^S$.

3. Das Modell ist nichttrivial: $CZF \vdash \perp^S$ impliziert $CZF \vdash \perp$.

Dies sind natürlich Aussagen, die in unserer Metatheorie (etwa PRA) getroffen und bewiesen werden. Γ in Forderung 1 kann auf endliche Satzmengen beschränkt werden.

Allerdings ist die Konstruktion nicht nur in dieser Hinsicht interessant, die zwar Konsistenzresultate ermöglicht, aber den Begriff „Modell“ nicht stark genug ausnutzt. Mit einer höheren Metatheorie als PRA, die über Mengenlehre verfügt, kann man nämlich die unten angegebene Modellkonstruktion wirklich als relative Modellkonstruktion verstehen, also als Verfahren, aus einem Modell von CZF ein anderes Modell von CZF zu erstellen. Dies ist intuitiv leichter fassbar als die Zuordnung der Sätze, so dass in der klassischen Mengenlehre beispielsweise fast ausschließlich diese Sichtweise verwendet wird. In konstruktivem oder intuitionistischem Kontext, wo Konsistenz und Modellexistenz durchaus nicht übereinstimmen [21], ist dies aber eine echt stärkere Aussage.

[1] Demnach wäre Ψ^S nur eine Δ_0-Formel (also beschränkt), falls $V(S)$ eine Menge wäre - dies wird aber nicht der Fall sein.

4.1.1 Das Universum

Da CZF nicht seine eigene Konsistenz beweisen kann, der Satz

$$\exists M M \models CZF$$

diese aber implizieren würde, kann ein Modell von CZF, das wir innerhalb von CZF konstruieren wolle, nicht in CZF beweisbar eine Menge sein. Es spricht aber nichts dagegen, eine Klasse $V(S)$ als Universum eines Modells zu finden.

Das einfachste Modell von CZF ist das Mengenuniversum $V = \{x|x = x\}$ mit der Interpretation $\Phi^V = \Phi$ selbst. Wie in der klassischen Mengenlehre ist dessen Universum V mit der bekannten Konstruktion von von Neumann in „Schichten“ $V_\alpha, \alpha \in On$ einteilbar, die rekursiv definiert werden:

$$V_\alpha := \hat{\bigcup}_{\beta \in \alpha} P(V_\beta)$$

In ZF oder IZF sind die V_α, wie man induktiv zeigt, aufsteigende Mengen und man kann $V = \hat{\bigcup}_{\alpha \in On} V_\alpha$ als Vereinigung ordinalzahlvieler Mengen definieren[2]. In CZF sind wegen der Abwesenheit des Potenzmengenaxioms die einzelnen Stufen des Mengenuniversums bereits schon Klassen. Um die Klassen V_α exakt zu definieren, verwendet man darum am besten das im Kapitel über CZF eingeführte Instrumentarium der induktiven Definitionen.

Die hier passende induktive Definition ist die Klasse

$$\Phi = \{(x, a)|a \subseteq x\}$$

Dann gibt es wegen dem Theorem zur induktiven Definition von Klassen die Klassen

$$V^\alpha = \Gamma_\Phi(\hat{\bigcup}_{\beta \in \alpha} V^\beta) = P(\hat{\bigcup}_{\beta \in \alpha} V^\beta)$$

Definiert man nun

$$V_\alpha := \hat{\bigcup}_{\beta \in \alpha} V^\beta,$$

so ist V_α eine Hierarchie wie gewünscht:

$$V_\alpha = \hat{\bigcup}_{\beta \in \alpha} V^\beta = \hat{\bigcup}_{\beta \in \alpha} P(\hat{\bigcup}_{\gamma \in \beta} V^\gamma) = \hat{\bigcup}_{\beta \in \alpha} P(V_\beta)$$

Nun hat

$$V = \hat{\bigcup}_{\alpha \in On} V^\alpha = \hat{\bigcup}_{\alpha \in On} V_\alpha$$

die Eigenschaft, dass Teilmengen von V wieder in V liegen (also $P(V) \subseteq V$). Man kann induktiv zeigen, dass alle Mengen in V liegen, damit ist also V wirklich die Allklasse. Um dies mit $\in$-Induktion beweisen zu können, müssen wir zeigen,

[2]Wir hatten V eigentlich schon als die Allklasse eingeführt. Da wir beweisen können, dass dieses neue V auch die Allklasse definiert, werden wir den selben Buchstaben verwenden und die alte Definition vorerst zurückstellen.

dass $\forall b.\ \forall a \in b\ a \in V\ \rightarrow\ b \in V$ gilt. Aber dies heißt ja nichts anderes als $\forall b.\ b \subseteq V \rightarrow b \in V$, und es ist ja $P(V) \subseteq V$.

Dieses "Modell" von CZF ist natürlich so einfach, dass es uninteressant ist, da genau die selben Sätze gelten wie im Ursprungsmodell selbst und CZF genau die Sätze zeigt, von denen es auch zeigt, dass sie im Modell gelten. Stellt man sich die Modellkonstruktionen als Methode vor, mit einer mengentheoretischen Metatheorie aus echten Klassenmodellen von CZF andere zu konstruieren, so wäre das so erhaltene Modell einfach das ursprüngliche.

Folgend McCartys Konstruktion [20]verbreitern wir also das Modell. Eine Menge in unserem Modell soll nicht nur Elemente enthalten, sondern zu jedem Element auch einen Grund angeben können, warum dieses Element darin liegt. Eine intuitive Vorstellung wäre, dass ein Grund, warum 5 in ω liegt, etwa sein könnte, dass „5 ist eine natürliche Zahl“ gilt, oder ein Grund, warum a in $b \cap c$ liegt die Kombination von Gründen, dass a in b liegt und dass a in c liegt, ist. Was ein Grund sein kann, soll allgemein gelassen werden und wir sagen einfach, dass die Elemente von S Kandidaten für solche Gründe sind. In unserem konstruierten Modell besteht eine Menge also (ähnlich etwa zu Forcing-Konstruktionen [10], [17]) aus Paaren, deren erste Komponente aus S ist und deren zweite Komponente ein Element der Menge, also ein zuvor konstruiertes Element des Modells, ist. Es ist zwar nicht unumgänglich, macht aber vieles einfacher, wenn wir fordern, dass die Menge dieser Gründe unter $\lhd$ abgeschlossen sein soll.

Um diese intuitive Erklärung formal zu machen:

Theorem 48. *Es gibt eindeutig bestimmte Klassen $(V(S)_\alpha)_{\alpha \in On}$, so dass*

$$V(S)_\alpha = \hat{\bigcup}_{\beta\in\alpha} \{x \subseteq S \times V(S)_\beta | \forall a \in x[S]\ x^{-1}a = {}^{\lhd}x^{-1}a\}$$

Es sei dann

$$V(S) = \hat{\bigcup}_{\alpha\in On} V(S)_\alpha$$

Die $V(S)_\alpha$ werden die Schichten des Universums genannt.

Beweis. Das Resultat entspricht [22] und auch der Beweis geht analog (nur die induktive Definition ist abgeändert):

Die Eindeutigkeit ist klar nach Induktion über $\alpha \in On$. Zur Existenz:

Betrachte die induktive Definition

$$\Phi_S = \{(x, a) | a \subseteq S \times x \wedge \forall y \in x\ a^{-1}y = {}^{\lhd}a^{-1}y\}$$

Nach dem Theorem zur induktiven Definition von Klassen gibt es dann $V(S)^\alpha$, so dass

$$V(S)^\alpha = \Gamma_\Phi(\hat{\bigcup}_{\beta\in\alpha} V(S)^\beta),$$

wobei Γ_Φ der Klassenoperator zu der induktiven Definition sei. Definiere

$$V(S)_\alpha = \hat{\bigcup}_{\beta\in\alpha} V(S)^\alpha$$

Dann gilt:

$$
\begin{aligned}
V(S)_\alpha &= \hat{\bigcup}_{\beta\in\alpha} V(S)^\alpha \\
&= \hat{\bigcup}_{\beta\in\alpha} \Gamma_\Phi(\hat{\bigcup}_{\gamma\in\beta} V(S)^\gamma) \\
&= \hat{\bigcup}_{\beta\in\alpha} \Gamma_\Phi(V(S)_\alpha) \\
&= \hat{\bigcup}_{\beta\in\alpha} \{x \subseteq S \times V(S)_\beta | \forall a \in x[S]\ x^{-1}a = {}^{\lhd}x^{-1}a\}
\end{aligned}
$$

Die Gerichtetheit der Vereinigungen ist überall klar. Q.E.D.

Es bildet in einer separierbaren formalen Topologie allgemein der Operator $X \mapsto {}^{\lhd}X$ Mengen auf Mengen ab. Darum ist insbesondere für $x, y \in V(S)$ die Klasse $\{e \in S | e \lhd x^{-1}(y)\}$ eine Menge. Hätte man nicht die Separierbarkeit gefordert, so könnte der Mengenreichtum des Modells aber stark eingeschränkt sein. Also hätte man in einem von einer nicht separierbaren Topologie ausgehenden Modell nur noch kleine Bruchstücke von CZF realisieren können.

Eine Alternative wäre, auf die Forderung zu verzichten, dass x nur in $V(S)$ sein könne, wenn $x^{-1}a = {}^{\lhd}(x^{-1}a)$. Tatsächlich wären die entstehenden Strukturen unter Separierbarkeitsannahme äquivalent, einige Beweise aber deutlich umständlicher. Dennoch wollen wir bei der Definition von Mengen in $V(S)$ nur ungern stets dazu schreiben, dass wir unter $\lhd$ abschließen. Wir führen deshalb eine Kurzschreibweise für den Abschluss einer Menge unter $\lhd$ ein:

Definition 49. *Zu einer Menge a sei $S(a)$ die Menge $\{(e, b) | b \in a[S] \wedge e \lhd a^{-1}b\}$.*

Dies ist eine Menge, obwohl $\{(e, b) | e \lhd a^{-1}b\}$ dies nicht sein muss, denn es kann ja sein, dass die leere Menge manche Elemente der schwachen applikativen Topologie überdeckt.

Das folgende Lemmas entspricht [22], 3.5:

Lemma 50. *In CZF gilt:*

$$\forall a \subseteq S \times V(S).\ \forall (e, b) \in a\ a^{-1}b = {}^{\lhd}a^{-1}b \rightarrow a \in V(S)$$

Beweis. Jedes Element der Menge a ist mit der Terminologie des letzten Beweises in einem $V(S)^\alpha$. Sei A nach Strong Collection eine Sammlung solcher α, so dass für jedes Element in a ein $\alpha \in A$ existiert, so dass das Element in $V(S)^\alpha$ liegt. Da A eine Menge von Ordinalzahlen ist, gibt es eine Ordinalzahl $\beta \supseteq A$, etwa $\hat{\bigcup}_{\alpha\in A} \alpha + 1$. Damit ist

$$a \subseteq \hat{\bigcup}_{\alpha\in\beta} S \times V(S)^\alpha)$$

und also $a \in V(S)^\beta$, da es die Bedingung $\forall (e, b) \in a\ a^{-1}b = {}^{\lhd}a^{-1}b$ erfüllt. Q.E.D.

Das Universum $V(S)$ ist in einem intuitiven Sinne breiter als das Mengenuniversum V. Dies kann formal ausgedrückt werden als:

Lemma und Definition 51. *Es gibt genau eine injektive Abbildung $x \mapsto x^k$ von V nach $V(S)$ mit*

$$x^k = S(\{(k, y^k) | y \in x\})$$

Diese Abbildung hat die surjektive Abbildung $x \mapsto x^\nabla$ von $V(S)$ nach V als Linksinverses, wobei dies die eindeutig bestimmte Abbildung ist mit

$$x^\nabla = \{y | \exists a \in \nabla\ (a, y) \in x\}$$

Beweis. Diese Abbildungen sind natürlich echte Klassen. Die Existenzen sind einfache Folgerungen der Theorie der induktiven Definitionen. Etwa erhält man die erste Abbildung als die kleinste Fixklasse der induktiven Operation Φ_k, die definiert ist als die Klasse aller Paare (x, a), so dass es c und d gibt mit

$$a = (c, S(d)) \wedge \forall e \in c \exists f ((e, f) \in x \wedge (k, f) \in d) \wedge \forall f \in d \exists e \in c, f'\ (f = (k, f') \wedge (e, f) \in x)$$

Man zeigt durch $\in$-Induktion, dass $\Gamma^\alpha_{\Phi_k}$ eine funktionale Klasse von V^α nach $V(S)^\alpha$ ist, die die geforderte Gleichung erfüllt. Analog hält man es mit der zweiten Abbildung. Die Eindeutigkeit ist ebenfalls klar durch Mengeninduktion. Q.E.D.

Diese injektive Abbildung wird als Einbettung des Mengenuniversums V nach $V(S)$ auch später noch wiederholt vorkommen, da sie ein Monomorphismus von Modellen der Mengenlehre ist, also die $\in$-Struktur erhält. Die surjektive „Vergiss"-Abbildung unterschlägt die Gründe, aus denen ein Element in einer Menge liegt.

Offenbar ist $V(S) \subseteq V$, aber die Inklusion wird (für nichttriviales S) kein Monomorphismus sein. In diesem Sinne ist $V(S)$ als Mengenuniversum größer, auch wenn es dies als Klasse nicht ist.

Die injektive Abbildung ist eine gemeinsame Verallgemeinerung der in [22] von Rathjen verwendeten Abbildung $x \mapsto x^{st}$ und der von Gambino in [15] verwendeten Abbildung $x \mapsto \hat{x}$.

4.1.2 Realisierbarkeit

Wir definieren eine Relation $e \Vdash \phi$ zwischen Elementen von S und Sätzen $\phi[a_1, ..., a_n]$ in der Sprache der Mengenlehre mit dem zusätzlichen Relationssymbol $\dot{\in}$ mit Parametern[3] in $V(S)$ über den Aufbau der Formel mit Nebeninduktion über die Stufe der Parameter in $V(S) = \hat{\bigcup}_{\alpha \in On} V(S)_\alpha$ für die atomaren Formeln. Diese Definition geht von der Idee her auf McCarty zurück, ist allerdings mit einigen Feinheiten versehen, die durch die Verwendung der applikativen Topologien einfließen.

Es wird hier und im Folgenden die Konvention verwendet, dass der Bereich von $\Vdash$ so lang wie möglich ist, ohne Elemente aus S oder die Symbole $\lhd$, $\leq$ und $\Vdash$ zu enthalten. Dadurch kann auf viele Klammern verzichtet werden.

Definition 52. *Die Beziehung $e \Vdash \phi$, in Worten „e realisiert ϕ", für Sätze ϕ mit Parametern in $V(S)$ ist induktiv definiert:*

[3] Falls man eine exorbitante Metatheorie verwenden will, kann man die „Sätze mit Parametern" verstehen als Sätze in einer Sprache, die um Konstanten für jedes Element von V(S) erweitert ist. Dies ist wohl auch die intuitive Vorstellung die man haben sollte, und McCarty in [20] etwa verfährt so. In PRA kann man allerdings eine so reiche Sprache natürlich nicht kodieren, dies ist aber auch gar nicht nötig. Um genau zu sein (s.u.), weist diese Definition nur einer Formel ϕ mit freien Variablen $v_1, ..., v_n$ eine Formel $e \Vdash \phi$ mit gleichen freien Variablen zu, diese freien Variablen werden die Parameter in $V(A)$ genannt und die Formeln werden nur in Fällen betrachtet, in denen vorausgesetzt wird, dass sie in $V(S)$ liegen (meist explizit, manchmal implizit).

1. $e \Vdash \bot$, *falls* $e \lhd \emptyset$
2. $e \Vdash x \mathrel{\dot\in} y$, *falls* $e \lhd y^{-1}x$
3. $e \Vdash x \in y$, *falls* $e \lhd \{f \in S | \exists z \in Bi(y).\, lf \Vdash z \mathrel{\dot\in} y \wedge rf \Vdash x = y\}$
4. $e \Vdash x = y$, *falls* $\forall z \in Bi(x)\, \forall f \Vdash z \mathrel{\dot\in} x\; lef \Vdash z \in y$ *und* $\forall z \in Bi(y)\, \forall f \Vdash z \mathrel{\dot\in} y\; ref \Vdash z \in x$
5. $e \Vdash \phi \wedge \psi$, *falls* $le \Vdash \phi \wedge re \Vdash \psi$
6. $e \Vdash \phi \vee \psi$, *falls* $e \lhd \{f \in S | (lf \unlhd l \wedge rf \Vdash \phi) \vee (lf \unlhd r \wedge rf \Vdash \psi)\}$
7. $e \Vdash \phi \to \psi$, *falls* $\forall f \in S.\; f \Vdash \phi \to ef \Vdash \psi$
8. $e \Vdash \forall x \phi(x)$, *falls* $\forall a \in V(S) e \Vdash \phi[a]$
9. $e \Vdash \exists x \phi(x)$, *falls* $e \lhd \{f \in S | \exists a \in V(S)\; f \Vdash \phi[a]\}$

Dies sieht nach einer gewaltigen Erweiterung der Sprache aus, deren Konsequenzen nicht unbedingt klar sind. Deswegen werden wir dies nur als Schreibweise verwenden - eigentlich weisen wir hier induktiv über ihren Aufbau nur jeder Formel $\phi(x_1, ..., x_n)$ eine Formel $\dot\phi(e, x_1, ..., x_n)$ zu (die nur betrachtet wird für $e \in S$ und $x_1, ..., x_n \in V(S)$). Hierbei ist die Nebeninduktion im Fall für $\in$ und $=$ nicht ohne weiteres unproblematisch, da die Auflösung der Schreibweise $e \Vdash x \in y$ oder $x = y$ wieder ein $\Vdash x \in y$ oder $\Vdash x = y$ erhält.

Sauberer wäre es, Klassen $R_\in$ und $R_=$ zu definieren, und dann zu bestimmen, dass $e \Vdash x \in y$, falls $(e, x, y) \in R_\in$, und $e \Vdash x = y$, falls $(e, x, y) \in R_=$. Dies werden wir auch tun und dann zeigen, dass diese saubere Definition mit der anderen, von der man nicht direkt sieht, dass es sich um eine gültige Definition handelt, übereinstimmt.

Da wir simultane rekursive Definitionen nicht formal eingeführt haben, werden wir eine Klasse R, und anschließend $R_\in(e, x, y) \leftrightarrow R(0, e, x, y)$ und $R_=(e, x, y) \leftrightarrow R(1, e, x, y)$ definieren. Wir definieren R als kleinste Fixklasse der induktiven Definition Φ, die als Vereinigung der zwei Klassen Φ_0 und Φ_1 gegeben ist.

Es sei Φ_0 die Klasse aller $(a, (0, e, x, y))$, so dass

$$e \lhd \{f \in S | \exists x' \in Bi(y).\, lf \lhd y^{-1}x' \wedge (1, rf, x, x') \in a\}$$

Es sei Φ_1 die Klasse aller $(a, (1, e, x, y))$, so dass

$$\forall f, z.(f \lhd x^{-1}z \wedge z \in Bi(x) \to (0, lef, z, y) \in a) \wedge (f \lhd y^{-1}z \wedge z \in Bi(y) \to (0, ref, z, x) \in a)$$

Man sieht sofort, dass eine Klasse, die Fixpunkt dieser induktiven Definition ist, nach Definition von $e \Vdash x \in y$ falls $(e, x, y) \in R_\in$ und $e \Vdash x = y$, falls $(e, x, y) \in R_=$, eine Satzmenge liefert, die unter den Punkten 1 und 2 der obigen Definition abgeschlossen ist. Ebenso sieht man, dass die Satzmenge der mit den Punkten 1 und 2 der obigen Definition herleitbaren $\Vdash$-Aussagen mit atomaren Formeln auf der rechten Seite eine Teilklasse der Satzmenge ist, die man erhält, wenn man $\Vdash \phi$ für atomare Formeln ϕ über R definiert hätte. Damit stimmt die der kleinsten Fixpunktklasse entsprechende Satzmenge mit den Sätzen überein, die man mit der obigen Definition herleiten kann.

Mit anderen Worten: Man kann $e \Vdash \phi(a_1, ..., a_n)$ für atomare (und damit alle) ϕ wirklich als Abkürzung für eine Formel $\dot{\phi}(e, x_1, ..., x_n)$ lesen, die man sogar auf primitiv rekursive Weise aus ϕ erhält[4].

Man bemerke, dass sich die Realisierbarkeitsrelation für die atomaren Formeln in der Sprache der Mengenlehre wie folgt vereinfachen lässt:

$(e \Vdash x \in y)$ gdw $e \lhd \{f \in S | \exists z \in V(S).(lf, z) \in y \wedge rl \Vdash x = z\}$

$(e \Vdash x = y)$ gdw für alle $f \in S, z \in V(S)$ gilt: $((f, z) \in x \to lef \Vdash z \in y)$ und $((f, z) \in y \to ref \Vdash z \in x)$

Dies ist unmittelbar ersichtlich. Wäre allerdings bei der Definition $V(S)$ auf die Abgeschlossenheit der $x^{-1}y$ für $y \in Bi(x)$ gegenüber $\lhd$ nicht bestanden worden, wäre es keineswegs klar. Jedoch wäre die dadurch gegebene Definition zu der eigentlichen immer noch insofern gleichwertig, als dass die selben Sätze realisiert würden. Dies ist verwandt mit der Situation im späteren Korollar 60.

Die $e \in S$ mit $e \Vdash \phi$ kann man sich als Begründungen vorstellen, warum ϕ gelten sollte. Bei der Konstruktion unseres Modells müssen wir aber sagen, was wir darunter verstehen wollen, dass ein Satz in dem Modell gilt, ohne dass der Grund noch kümmert. Wir werden dies sagen, wenn es einen überzeugenden[5] Grund gibt:

Definition 53. *Wir sagen der Satz ϕ gilt in $V(S)$ oder $V(S)$ (manchmal auch ungenau S) realisiert ϕ, in Zeichen $V(S) \models \phi$ oder $\Vdash \phi$, falls*

$$\exists e \in \nabla e \Vdash \phi$$

Klassen von Realisierern

Wir wollen natürlich herausfinden, welche Sätze von einer applikativen Topologie S realisiert werden und werden dieser Frage viel Zeit widmen. Zunächst ist jedoch die Beschäftigung mit dem umgekehrten Probkem weiterführend: Wir interessieren uns für die Elemente von S, die ein festgehaltenes ϕ realisieren.

Definition 54. *Sei ϕ ein Satz mit Parametern in $V(S)$. Dann sei $[\![\phi]\!]$ definiert als die Klasse*

$$[\![\phi]\!] = \{e \in S | e \Vdash \phi\}$$

Die Definition der Realisierbarkeit gibt uns keinen Grund zur Annahme, wir könnten zeigen, dass diese eine Menge bilden (in Spezialfällen wird dies allerdings gelten). Aber auch wenn diese Elemente Klassen bilden, haben jene Klassen doch eine einfache Form:

Theorem 55. *Sei ϕ ein Satz der Mengenlehre mit Parametern in $V(S)$. Dann gilt*

$$^{\lhd}[\![\phi]\!] = [\![\phi]\!]$$

[4]Man beachte, dass für den atomaren Fall die Formel $\dot{\phi}$ einfach hinschreibbar ist als die Zugehörigkeit eines Tupels zu einer Klasse, die ja einfach eine bestimmte Formel ist. Diese Formel wurde nicht explizit angegeben und wäre auch sehr unhandlich, aber das Theorem über die induktive Definition von Klassen zeigt, dass man sie finden kann (und der Beweis zeigt, wie).

[5]im Sinne der Definition 38

Beweis. Dies wird durch Induktion über den Aufbau von ϕ bewiesen. Sei $A := [\![\phi]\!]$

1. ϕ ist $\bot$: Die Realisierer dieser Formel sind gerade durch die Anwendung der Abschlussoperation $X \mapsto {}^{\lhd}X$ definiert.

2. ϕ ist $x\dot{\in}y$: Ebenso.

3. ϕ ist $x \in y$: Ebenso.

4. ϕ ist $x = y$: Sei

$$e \lhd \{f \in S | \forall z \in V(S) \forall g \in S.(z \in Bi(x) \wedge g \Vdash z\dot{\in}x \rightarrow lfg \Vdash z \in y) \wedge (z \in Bi(y) \wedge g \Vdash z\dot{\in}y \rightarrow rfg \Vdash z \in x)\}$$

Sei also $z \in V(S)$ und $g \in S$, dann (weil Überdecktheit von einer Menge die Überdecktheit von Obermengen impliziert):

$$e \lhd \{f \in S | z \in Bi(x) \wedge g \Vdash z\dot{\in}x \rightarrow lfg \Vdash z \in y\}$$

$$e \lhd \{f \in S | z \in Bi(x) \wedge g \Vdash z\dot{\in}y \rightarrow rfg \Vdash z \in x\}$$

Sei $g \lhd z\dot{\in}x, z \in Bi(x)$. Dann gilt für $B := \{f \in S | g \Vdash z\dot{\in}x \rightarrow lfg \Vdash z \in y\}$, dass $\forall f \in B \; lfg \Vdash z \in y$, insbesondere $\forall f \in B \; lfg \downarrow$. Also gilt nach dem ersten Axiom applikativer Topologien:

$$leg \lhd \{lfg | f \in B\} = \{lfg | lfg \in A'\}$$

mit $A' = [\![z \in y]\!]$. Da nach Induktionsvoraussetzung $A = {}^{\lhd}A$ gilt, ist:

$$leg \lhd \{lfg | lfg \in A'\} = \{lfg | lfg \lhd A'\} \lhd A'$$

Also folgt nach nochmaliger Anwendung der Induktionsvoraussetzung $A = {}^{\lhd}A$ nun $leg \in A'$, mithin

$$leg \Vdash z \in y$$

Durch Implikationseinführung (es wurde zuvor $g \lhd z\dot{\in}x$ angenommen) erhalten wir für e allgemein:

$$g \lhd z\dot{\in}x \rightarrow leg \Vdash z \in y$$

Damit ist $e \in B$.

Die analoge Beweisführung mit y und z vertauscht liefert auch

$$e \in \{f \in S | z \in Bi(x) \wedge g \Vdash z\dot{\in}y \rightarrow rfg \Vdash z \in x\}$$

Da dies alles unabhängig von z und g war, gilt nach Alleinführung:

$$e \in \{f \in S | \forall z \in V(S) \forall g \in S.(z \in Bi(x) g \Vdash z\dot{\in}x \rightarrow lfg \Vdash z \in y) \wedge (z \in Bi(y) \wedge g \Vdash z\dot{\in}y \rightarrow rfg \Vdash z \in x)\}$$

Und dies war zu zeigen.

5. ϕ ist $\psi \wedge \theta$: Sei also

$$e \lhd \{f \in S | lf \Vdash \psi \wedge rf \Vdash \theta\}$$

Für Elemente f der Menge auf der rechten Seite denotiert offenbar lf und rf, also

$$le \lhd \{lf \in S | lf \Vdash \psi \wedge rf \Vdash \theta\} \subseteq \{f \in S | f \Vdash \psi\}$$

$$re \lhd \{rf \in S | lf \Vdash \psi \wedge rf \Vdash \theta\} \subseteq \{f \in S | f \Vdash \theta\}$$

Da die Mengen auf der rechten Seite nach Induktionsvoraussetzung gegenüber $X \mapsto {}^{\lhd}X$ abgeschlossen sind, folgt

$$le \Vdash \psi \wedge re \Vdash \theta$$

Also $e \in [\![\psi \wedge \theta]\!]$, was zu zeigen war.

6. ϕ ist $\psi \vee \theta$: Die Realisierer dieser Formel sind gerade definiert durch die Anwendung der Abschlussoperation $X \mapsto {}^{\lhd}X$.

7. ϕ ist $\psi \to \theta$: Sei also

$$e \lhd \{f \in S | \forall g \in S. g \Vdash \psi \to fg \Vdash \theta\}$$

Sei $g \in S$ mit $g \Vdash \psi$. Da e von einer Obermenge erst recht überdeckt wird, gilt

$$e \lhd \{f \in S | fg \Vdash \theta\}$$

Da für all die f in der Menge auf der rechten Seite $fg\downarrow$, ist

$$eg \lhd \{fg \in S | fg \Vdash \theta\} \subseteq [\![\theta]\!]$$

Also gilt für alle $g \in S$ mit $g \Vdash \psi$ damit $eg \Vdash \theta$. Somit ist $e \in [\![\phi \to \theta]\!]$.

8. ϕ ist $\forall x \psi(x)$: Sei darum

$$e \lhd \{f \in S | \forall x \in V(S) f \Vdash \psi[x]\}$$

Also ist für alle $x \in V(S)$ auch $e \lhd [\![\psi[x]]\!]$, damit wegen der Induktionsvoraussetzung $e \Vdash \psi[x]$. Folglich $e \Vdash \forall x \psi(x)$.

9. ϕ ist $\exists x \psi(x)$: Dies ist ebenso wie die Fälle $\dot\in$, $\in$ und $\vee$ trivial.

Q.E.D.

Dies hat zur Folge, dass man ohne Einschränkung annehmen kann, dass

$$\forall e \in \nabla\ \forall f \in S.\ e \trianglelefteq f \to f \in \nabla$$

Denn geht man von der applikativen Topologie mit ∇ über zu der mit

$$\nabla' = \{f | \exists e \in \nabla\ e \trianglelefteq f\},$$

so sind immer noch die selben Sätze realisiert. Diese Annahme werden wir im Folgenden treffen, sie wird aber nur selten relevant.

4.2 Der Konsistenzsatz für die Prädikatenlogik

Ziel dieses Abschnitts ist es, zu zeigen, dass die realisierten Sätze eine relativ widerspruchsfreie Theorie bilden, also dass sie unter logischer Ableitung abgeschlossen sind und der Widerspruch nur realisiert wird, wenn er aus den Axiomen von CZF schon ableitbar wäre. Dies ist nicht nur ein essentielles Gütekriterium, sondern wird viele Nachweise der Realisiertheit von konkreten Sätzen deutlich erleichtern.

4.2.1 Formulierung und Beweis

Satz 56. $\perp$ *ist nicht realisiert*[6].

Beweis. Kein Element von ∇ wird von der leeren Menge überdeckt. Q.E.D.

Satz 57. *Sei ϕ ein mit intuitionistischer Logik ableitbarer Satz der Prädikatenlogik mit $\dot\in, \in$ und $=$ sowie mit Parametern in $V(S)$. Dann ist ϕ realisiert.*

Wir verwenden wieder den intuitionistischen Kalkül aus dem Kapitel über CZF mit den folgenden Axiomen(schemata), die um das Zeichen $\dot\in$ erweitert sind:

1. $\phi \to (\psi \to \phi)$
2. $(\phi \to (\psi \to \theta)) \to ((\phi \to \psi) \to (\phi \to \theta))$
3. $\phi \to (\psi \to (\phi \wedge \psi))$
4. $(\phi \wedge \psi) \to \phi$
5. $(\phi \wedge \psi) \to \psi$
6. $\phi \to (\phi \vee \psi)$
7. $\psi \to (\phi \vee \psi)$
8. $(\phi \vee \psi) \to (\phi \to \theta) \to (\psi \to \theta) \to \theta$
9. $(\phi \to \psi) \to (\phi \to \neg\psi) \to \neg\phi$
10. $\phi \to \neg\phi \to \psi$
11. $\forall x \phi(x) \to \phi[z]$ für z frei für x in ϕ
12. $\phi[z] \to \exists x \phi(x)$ für z frei für x in ϕ
13. $\forall x\, x = x$
14. $\forall xy.\, x = y \to y = x$
15. $\forall xyz.\, x = y \to y = z \to x = z$
16. $\forall xyz.\, x = y \to y \dot\in z \to x \dot\in z$
17. $\forall xyz.\, x = y \to y \ni z \to x \ni z$

Der Kalkül enthält drei Inferenzregeln:

[6] Genauer: $CZF \vdash\!\!\!\nvdash \perp$.

1. $\phi, \phi \to \psi \vdash \psi$
2. $\phi \to \psi(y) \vdash \phi \to \forall x\psi(x)$ für y frei in x und nicht frei in ϕ und ψ
3. $\phi(y) \to \psi \vdash \exists x\phi(x) \to \psi$ für y frei in x und nicht frei in ϕ und ψ

Beweis. Der Beweis verläuft induktiv über die Ableitung. Da viele Fakten zu überprüfen sind, wird er etwas umfangreich sein, aber die einzelnen Fälle sind oft kurz, wenn auch manchmal deutlich länger als es entsprechende Beweise für Realisierbarkeit mit applikativen Strukturen wären. Das den vorigen Abschnitt abschließende Theorem über die Abgeschlossenheit von Realisiererklassen unter $\lhd$ wird vielfach verwendet werden.

Wir beginnen mit den drei Inferenzregeln und zeigen: Wenn CZF beweist, dass die Voraussetzungen realisiert sind, beweist es auch, dass die Folgerung realisiert ist.

1. Falls $e \Vdash \phi$ und $f \Vdash \phi \to \psi$ mit $e, f \in \nabla$, so ist nach Definition der Realisierbarkeit $ef \Vdash \psi$ und da es also denotiert ist $ef \in \nabla$.
2. Falls $e \in \nabla$ mit $e \Vdash \phi \to \psi(y)$, so gilt für jedes $g \in S$ mit $g \Vdash \phi$, dass $eg \Vdash \psi(y)$, also lässt sich nach eben jener Inferenzregel in CZF schließen, dass $eg \Vdash \forall x\psi(x)$. Folglich $e \Vdash \phi \to \forall x\psi(x)$.
3. Falls $e \in \nabla$ mit $CZF \vdash e \Vdash \phi(y) \to \psi$, so $CZF, g \in S \vdash g \Vdash \phi(y) \to eg \Vdash \psi$, darum (man beachte die Variablenbedingung!)

   $$CZF, g \in S \vdash \exists a \in V(S)\ e \Vdash \phi(a) \to eg \Vdash \psi$$

   also $CZF \vdash \forall g \in S\ g \Vdash \exists x\phi(x) \to eg \Vdash \psi$. Somit $e \Vdash \exists x\phi(x) \to \psi$

Nun die rein logischen Axiome, also diejenigen außer den Gleichheitsregeln, deren Nachweis mit anderen Methoden durchgeführt wird und die deshalb gesondert gruppiert werden:

1. Dies wird realisiert durch $k \in \nabla$. Denn für Realisierer $f \Vdash \phi$ und $e \Vdash \psi$ ist $kfe \trianglelefteq f \Vdash \phi$.
2. Dies wird realisiert durch $s \in \nabla$. Denn für Realisierer $e \Vdash \phi \to (\psi \to \theta)$, $f \Vdash \phi \to \psi$ und $g \Vdash \phi$ gilt: $sefg \trianglelefteq eg(fg)$ und da $fg \Vdash \psi$ gilt $eg(fg) \Vdash \theta$.
3. Dies wird realisiert durch $p \in \nabla$. Denn für $e \Vdash \phi$ und $f \Vdash \psi$ gilt: $lpef \trianglelefteq e \Vdash \phi$ und $rpef \trianglelefteq f \Vdash \psi$.
4. Dies wird realisiert durch $l \in \nabla$. Denn für $e \Vdash \phi \wedge \psi$ gilt $le \Vdash \phi$.
5. Dies wird realisiert durch $r \in \nabla$. Denn für $e \Vdash \phi \wedge \psi$ gilt $re \Vdash \psi$.
6. Dies wird realisiert durch $\lambda x.plx \in \nabla$. Denn für $e \Vdash \phi$ ist $(\lambda x.plx)e \trianglelefteq ple \Vdash \phi \vee \psi$, denn $lple \trianglelefteq l \wedge rple \lhd e \Vdash \phi$, also $ple \in \{f \in S | (lf \lhd l \wedge rf \Vdash \phi) \vee (lf \trianglelefteq r \wedge rf \Vdash \psi)\}$, ple wird also insbesondere von dieser Menge überdeckt.
7. Dies wird realisiert durch $\lambda x.prx \in \nabla$. Denn für $e \Vdash \psi$ ist $(\lambda x.prx)e \trianglelefteq pre \Vdash \phi \vee \psi$, denn $lpre \trianglelefteq r \wedge rpre \lhd e \Vdash \psi$, also $pre \in \{f \in S | (lf \lhd l \wedge rf \Vdash \phi) \vee (lf \trianglelefteq r \wedge rf \Vdash \psi)\}$, pre wird also insbesondere von dieser Menge überdeckt.

8. Dies würde man gerne realisieren durch $\lambda xyz.D(lx)(y(rx))(z(rx)) \in \nabla$. Dies ist aber an manchen möglichen Eingabestellen (e,f,g) mit $e \Vdash \phi \vee \psi$, $f \Vdash \phi \rightarrow \theta$ und $g \Vdash \psi \rightarrow \theta$ eventuell gar nicht definiert, denn falls etwa le nach links zeigt, kann durchaus die rechte Alternative, $g(re)$, undefiniert sein. D leistet sozusagen nur eager evaluation, wir bräuchten aber lazy evaluation[7].

   So müssen wir also unnötige Berechnungen selbst vermeiden, und man wählt statt dem obigen problematischen lieber den Term

   $$\lambda xyz.(D(lx)yz)rx \in \nabla$$

   als Realisierer. Sei dann $e \Vdash \phi \vee \psi$, $f \Vdash \phi \rightarrow \theta$ und $g \Vdash \psi \rightarrow \theta$. Es ist

   $$(\lambda xyz.(D(lx)yz)rx)efg \trianglelefteq (D(le)fg)(re)$$

   Es gilt:

   $$e \lhd \{h \in S | (lh \lhd l \wedge rh \Vdash \phi) \vee (lh \trianglelefteq r \wedge rh \Vdash \psi)\} =: A$$

   Für Elemente $h \in A$ ist $lh \downarrow$, $rh \downarrow$ sowie $lh \trianglelefteq l$ oder $lh \trianglelefteq r$. Also ist $D(lh)fg\downarrow$ und $\trianglelefteq f$ bzw g, je nachdem, ob $lh \trianglelefteq l$ oder r.

   Im ersten Fall ist $(D(lh)fg)(rh) \Vdash \theta$, im zweiten ebenso $(D(lh)fg)(rh) \Vdash \theta$, stets also gilt $(D(lh)fg)(rh)\downarrow$. Also folgt aus der obigen Gleichung mit dem ersten Axiom applikativer Topologien:

$$(D(le)fg)(re) \lhd \{(D(lh)fg)(rh) \in S | (lh \lhd l \wedge rh \Vdash \phi) \vee (lh \trianglelefteq r \wedge rh \Vdash \psi)\} \subseteq \{h | h \Vdash \theta\}$$

   Also auch $(D(le)fg)(re) \Vdash \theta$, dies war zu zeigen.

9. Dies wird realisiert durch $\lambda xyz.yz(xz) \in \nabla$ (man bedenke, dass $\neg\psi$ nur eine Abkürzung ist für $\psi \rightarrow \bot$). Dann ist für $e \Vdash \phi \rightarrow \psi$, $f \Vdash \phi \rightarrow (\psi \rightarrow \bot)$, $g \Vdash \phi$:

   $$(\lambda xyz.yz(xz))efg \trianglelefteq fg(eg)$$

   Und $eg \Vdash \psi$ und $fgh \Vdash \bot$, falls $h \Vdash \psi$. Also wäre $fg(eg) \Vdash \bot$.

10. Dies wird realisiert durch $\lambda xy.yx$. Denn wenn $e \Vdash \phi$ und $f \Vdash \phi \rightarrow \bot$, so gilt

    $$(\lambda xy.yx)ef \trianglelefteq fe \lhd \emptyset \subseteq [\![\psi]\!]$$

11. Die letzten beiden Axiomenschemata 11 und 12 sind durch $\lambda x.x$ realisiert wegen der Wahl der Realisiertheitsbeziehung für Quantoren.

Nun fehlen noch die Gleichheitsregeln.

Die in diesem Beweis angegebenen Realisierer werden auch im Folgenden mit den ihnen hier gegebenen Namen bezeichnet.

[7] Dieses Problem scheint [20] zu übersehen, wenn er im Kapitel 2.5.5. dieses Axiom der Prädikatenlogik als eines von zwei Beispielen realisiert. Die hier vorgeschlagene Lösung würde auch diese kleine Unkorrektheit beheben.

1. $\forall x\ x = x$ wird durch $e_r := \tau^{fix}[v_1 := \lambda v.p(\lambda w.pw(lv))(\lambda w.pw(lv))] \in \nabla$ realisiert. Dies liegt in ∇, da es überzeugt und denotiert, letzteres wegen

   $$e_r \trianglelefteq p(\lambda w.pw(le_r))(\lambda w.pw(le_r))$$

   und dies denotiert.

   Man zeigt $\forall \alpha \in On\ \forall a \in V(S)_\alpha\ e_r \Vdash a = a$ durch Induktion über die Stufe $\alpha \in On$. Sei dies also schon für $\beta \in \alpha$ bewiesen. Nun soll also für $a \in V(S)_\alpha$ gezeigt werden:

   (a) $\forall z \in Bi(a)\ \forall f \Vdash z\ \dot{\in}\ a\ le_r f \Vdash z \in a$

   (b) $\forall z \in Bi(a)\ \forall f \Vdash z\ \dot{\in}\ a\ re_r f \Vdash z \in a$

   Sei also $f \Vdash z \dot{\in} a$ und $z \in Bi(a)$, also $z \in V(S)_\beta$ für ein $\beta \in \alpha$. Also nach Induktionsvoraussetzung $e \Vdash z = z$. Anwenden kann man die Induktionsvoraussetzung, da nach Konstruktion von $V(S)$ Elemente von $Bi(a)$ aus einer tieferen Schicht als a stammen. Nun gilt wegen der Definition von e:

   $$\begin{aligned} le_r f &\trianglelefteq \\ l((\lambda v.p(\lambda w.pw(lv))(\lambda w.pw(lv)))e_r)f &\trianglelefteq \\ l(p(\lambda w.pw(le_r))(\lambda w.pw(le_r)))f &\trianglelefteq \\ (\lambda w.pw(le_r))f &\trianglelefteq \\ pf(le_r) & \end{aligned}$$

   Insbesondere $l(le_r f) \trianglelefteq f$ und $r(le_r f) \trianglelefteq e_r \Vdash z = z$ (man beachte, dass alles denotiert). Also $le_r f \Vdash z \in a$. Analog $re_r f \Vdash z \in a$. Damit sind die beiden obigen Formeln gezeigt.

2. $\forall xy x = y \to y = x$ wird etwa durch $e_s := \lambda x.p(rx)(lx) \in \nabla$ realisiert (dieser Term stimmt mit dem in [20] für übliche Realisierbarkeit angegebenen überein). Denn sei $a, b \in V(S)$, $f \Vdash a = b$. Dann

   $$(\forall z \in Bi(a)\ \forall g \Vdash z \dot{\in} a\ lfg \Vdash z \in b) \wedge (\forall z \in Bi(b)\ \forall g \Vdash z \dot{\in} b\ rfg \Vdash z \in a)$$

   Somit gilt für $z \in Bi(b), z' \in Bi(a), g \Vdash z \dot{\in} b, g' \Vdash z' \dot{\in} a$:

   $$l(e_s f)g \trianglelefteq l(p(rf)(lf))g \trianglelefteq rfg \Vdash z \in a$$

   $$r(e_s f)g' \trianglelefteq r(p(rf)(lf))g' \trianglelefteq lfg \Vdash z' \in b$$

   Also $e_s f \Vdash b = a$

3. $\forall xyz.x = y \to y = z \to x = y$ wird etwa realisiert durch

   $$e_t := \tau^{fix}[v_1 := \lambda vxy.pe_1 e_2]$$

   mit

   $$e_1 = \lambda z.p(l(ly(l(lxz))))(v(r(lxz))(r(ly(l(lxy)))))$$

   $$e_2 = \lambda z.p(l(rx(l(ryz))))(v(e_s(r(ryz)))(e_s(r(rx(l(ryy))))))$$

[20] verwendet simultane Rekursion in der applikativen Struktur, um etwas kürzere Terme zu erhalten, obwohl er die Gleichheitsaxiome etwas komplexer (wenn auch logisch äquivalent) formuliert. Dies ist jedoch nicht nötig, wenn auch die Lesbarkeit dieses Terms zu wünschen übrig lässt[8]. Der Term e_t denotiert aus dem gleichen Grund wie e_r.

Dass

$$\forall \alpha \in On\, \forall x, y, z \in V(A)_\alpha\; e_t \Vdash (x = y \to y = z \to x = z)$$

gilt, wird durch Induktion über α bewiesen. Sei dies also schon für alle $\beta \in \alpha$ bekannt. Sei $f \Vdash x = y$ und $g \Vdash y = z$ und $x, y, z \in V(S)_\alpha$.

Sei $h \Vdash w \dot{\in} x$, $w \in Bi(x)$. Wir wollen zeigen, dass $l(e_t f g)h \Vdash w \in z$. Wir wissen:

$$lfh \lhd \{i | \exists w' \in Bi(y).li \Vdash w' \dot{\in} y, ri \Vdash w = w'\} =: A$$

Und für alle $i \in A$, $w' \in Bi(y)$ passend dazu so dass $li \Vdash w' \dot{\in} y \wedge ri \Vdash w = w'$ gilt:

$$lg(li) \lhd \{j | \exists w'' \in Bi(z) lj \Vdash w'' \dot{\in} z, rj \Vdash w' = w''\}$$

Die folgende Kette wird unten begründet[9]:

$$\begin{aligned}
l(e_t f g)h &\unlhd p(l(lg(l(lfh))))(e_t(r(lfh))(r(lg(l(lfh))))) \\
&\lhd \{p(l(lg(li)))(e_t(ri)(r(lg(li))))|i \in A\} \\
&\subseteq \{p(l(lg(li)))(e_t m(r(lg(li))))|\exists w' \in Bi(y).li \Vdash w' \dot{\in} y, ri \Vdash w = w', m \Vdash w = w'\} \\
&\lhd \{p(lj)(e_t m(rj))|\exists w' \in Bi(y), w'' \in Bi(z). \\
&\quad li \Vdash w' \dot{\in} y, ri \Vdash w = w', lj \Vdash w'' \dot{\in} z, rj \Vdash w' = w'', m \Vdash w = w'\} \\
&\subseteq \{pab | \exists w'' \in Bi(z).a \Vdash w'' \dot{\in} z, b \Vdash w = w''\} \\
&\subseteq \{e | e \Vdash w \in z\}
\end{aligned}$$

Die erste Zeile folgt aus den Eigenschaften von τ^{fix} und λ. Es gilt die Umformung zur zweiten Zeile wegen dem ersten Axiom applikativer Topologien, denn jeder Term in der Menge denotiert. Dies sieht man daraus, dass jeder dieser Terme von den Termen in der Menge der vierten Zeile überdeckt wird, indem man das erste Axiom abermals, und zwar zur Umformung zur vierten Zeile, anwendet, was man kann, da in der vierten Zeile alle Terme denotieren. Dies folgt nun wiederum aus der Induktionsvoraussetzung, die nochmals angewandt wird, um zur fünften Zeile zu gelangen.

Also ist $l(e_t f g)h \Vdash w \in z$ gezeigt.

[8]Nach Ansicht des Autoren ist es übrigens einfacher, sich zu überlegen, was für ein Term die Aussage realisieren könnte und dann auf den angegebenen zu kommen, als zu versuchen, ihn nachzuvollziehen.

[9]Um die Formeln nicht übermäßig lang zu gestalten, wurde hier die Konvention verwendet, dass freie Variablen in einem Klassenterm existenzquantifiziert gedacht werden sollen.

Sei nun umgekehrt $h \Vdash w \dot{\in} z, w \in Bi(z)$. Wir wollen zeigen, dass $r(e_t fg)h \Vdash w \in x$. Wir wissen:

$$rgh \lhd \{i | \exists w' \in Bi(y).li \Vdash w' \dot{\in} y, ri \Vdash w' = w\} =: A$$

Und für alle $i \in A$, w' passend dazu so dass $li \Vdash w' \in y \wedge ri \Vdash w' = w$ gilt:

$$rf(li) \lhd \{j | \exists w'' \in Bi(x).lj \Vdash w'' \dot{\in} x, rj \Vdash w'' = w'\}$$

Analog zu oben erhält man:

$$\begin{aligned}
&r(e_t fg)h \trianglelefteq p(l(rf(l(rgh))))(e_t(e_s(r(rgh)))(e_s(r(rf(l(rgh))))))\\
&\lhd \{p(l(rf(li)))(e_t(e_s(ri))(e_s(r(rf(li)))))| i \in A\}\\
&\subseteq \{p(l(rf(li)))(e_t m(e_s(r(rf(li)))))| \exists w' \in Bi(y).li \Vdash w' \dot{\in} y, ri \Vdash w = w', m \Vdash w = w'\}\\
&\lhd \{p(lj)(e_t m(e_s(rj)))| \exists w' \in Bi(y), w'' \in Bi(x).li \Vdash w' \dot{\in} y, ri \Vdash w = w', lj \Vdash w'' \dot{\in} x, e_s(rj) \Vdash w'' = w', m \Vdash w = w'\}\\
&\subseteq \{pab | \exists w'' \in Bi(x).a \Vdash w'' \dot{\in} x, b \Vdash w = w''\}\\
&\subseteq \{e | e \Vdash w \in x\}
\end{aligned}$$

Damit ist $r(e_t fg)h \Vdash w \in z$ gezeigt und insgesamt $e_t \Vdash x = y \to y = z \to x = z$.

4. $\forall xyz.\ x = y \to x \in z \to y \in z$ wird etwa realisiert durch $e_\in := \lambda xy.p(ly)(e_t x(ry))$. Denn für $e \Vdash x = y$ gilt $f \Vdash y \in z$, also

$$\begin{aligned}
f &\lhd \{i | \exists w \in Bi(z).li \Vdash w \dot{\in} (z).\ li \Vdash w \dot{\in} z, ri \Vdash x = y\}\\
\to e_\in ef &\lhd \{p(li)m | \exists w \in Bi(z).\ li \Vdash w \dot{\in} z, ri \Vdash x = y, m \Vdash x = w\}\\
&\subseteq \{j | \exists w \in Bi(z).\ lj \Vdash w \dot{\in} z, rj \Vdash x = w\}
\end{aligned}$$

   Man beachte wieder die Anwendbarkeit von Axiom 1 der applikativen Topologien wegen der Denotiertheit aller Terme.

5. $\forall xyz.\ x = y \to z \in x \to z \in y$ wird etwa realisiert durch das Denotat von $e_\ni := \lambda xy.e_\in(ry)(lx(ly))$, denn für $e \Vdash x = yn$ gilt $f \Vdash z \in x$, also

$$f \lhd \{i | \exists w \in Bi(x).li \Vdash w \dot{\in} x, ri \Vdash z = w\}$$

   also $le(li) \Vdash w \in y$ für ein i aus dieser Menge und entsprechendes $w \in V(S)$. Dann ist

$$\begin{aligned}
(\lambda xy.e_\in(ry)(lx(ly)))ef &\trianglelefteq e_\in(rf)(le(lf))\\
\lhd \{e_\in(ri)(le(li)) | \exists w \in Bi(x).li \Vdash w \dot{\in} x, ri \Vdash z = w\}&\\
\subseteq \{e_\in ab | \exists w \in V(S).a \Vdash z = w, b \Vdash w \in y\}&\\
\subseteq \{e | e \Vdash z \in y\}&
\end{aligned}$$

   Wiederum rechtfertigt die Denotiertheit aller Terme die Anwendbarkeit von Axiom 1.

Damit wäre alles gezeigt. Q.E.D.

Man beachte, dass damit das Schema $x = y \to \phi(x) \to \phi(y)$ für Formeln ϕ, die nicht das Zeichen $\dot\in$ enthalten, realisiert wird, was uns berechtigen wird, zu sagen, dass das Fragment der realisierten Formeln ohne $\dot\in$ eine extensionale Mengenlehre ist, sobald $\forall xy.\forall z(z \in x \leftrightarrow z \in y) \to x = y$ realisiert sein wird. Denn eine alternative Formulierung der Axiome der Mengenlehre ist ja, $=$ nicht als logisches Zeichen (mit Gleichheitsaxiomen) zu verwenden, sondern mittels der oben angegebenen Formel als definiertes Zeichen zu betrachten. Dann nennt man das obige Schema Extensionalitätsaxiom. Da es nicht beweisbar ist für $\dot\in$ statt $\in$ (es gibt einfache Gegenbeispiele), wird dieses andere Fragment keine extensionale Mengenlehre bilden, auch wenn dafür einige typische Axiome der Mengenlehre realisiert werden. Vor [20] realisierte man nur intensionale Mengenlehre, und zwar per $\dot\in$ statt $\in$. McCartys Errungenschaft war die Erweiterung der Realisierbarkeitsmodelle für Mengenlehre auf die häufiger genutzten extensionalen Mengenlehren.

Im Gegensatz zu unserem Beweis benötigt [20] das folgende Lemma. Es nutzt aber auch für applikative Topologien, die die Voraussetzung erfüllen, wenig zum induktiven Beweis von Aussagen wie $\Vdash \forall x\, x = x$, da hier Implikationen gezeigt werden müssen, bei denen Schlüsse der Form $(e \Vdash y \dot\in x) \to (f \Vdash y \in x)$ vonnöten sind. Um die Induktionsvoraussetzung anwenden zu können, also y in niedrigerer Stufe als x annehmen zu können, hilft das Lemma nur für $e \in \nabla$. Für applikative Strukturen gibt es die Unterscheidung zwischen Realisierern in ∇ und anderen Realisierern nicht, so dass es dort ausreicht.

Lemma 58. *Angenommen, $S = \nabla$. Sei $\alpha \in On$.*

1. $\forall b \in V(S)_\alpha \exists \beta \in \alpha \forall c.\ \Vdash c \in b \to c \in V(S)_\beta$
2. $\forall a, b \in V(S).(a \in V(S)_\alpha \wedge \Vdash a = b) \to b \in V(S)_\alpha$

Beweis. Der Beweis kann weitgehend übernommen werden. Q.E.D.

Die Situation ist für $\nabla \subsetneq S$ aber nicht so einfach. Denn dann kann durchaus realisiert sein, dass eine Menge einer höheren Stufe Element einer Menge einer echt niedrigeren Stufe ist, wenn die Gründe, aus denen Elemente höherer Stufen in der ersten Menge sind, von der leeren Menge überdeckt sind. Dies führt dazu, dass für die übliche Realisierbarkeit einfache Tatsachen hier recht komplex werden.

4.2.2 Korollare

Für weitere Resultate ist die Definition der Realisierbarkeit mitunter etwas umständlich und man würde gerne die Realisierer für bestimmte Motive, wie beschränkte Quantoren, einfacher definieren. Rathjen [22] geht etwa so vor, dass er beschränkte Quantoren als syntaktisch neue Objekte einführt. Später muss er natürlich beweisen, dass die Realisierbarkeitsklauseln, die er für sie einführt, mit der Logik kompatibel sind, also etwa Realisierer von $\forall x \in a\, \phi$ umgeformt werden können in solche von $\forall x.\ x \in a \to \phi$. Allerdings legt diese elegante Methode den Erleichterungen, die man schaffen kann, eine Schranke auf. In vorliegenden Kontext scheint es darum leichter, zu beweisen, dass man statt bestimmten komplexen Realisierern auch einfache verwenden kann.

Die folgende metatheoretische Standarddefinition (vergleiche etwa [18]) ist zur Formulierung nötig:

Definition 59. *Die Aussagenformen in X und ihre Substitution durch Formeln ϕ sind induktiv definiert:*

1. *X ist eine Aussagenform in X und $X[\phi] = \phi$.*
2. *ψ ist eine Aussagenform in X für ψ Formel und $\psi[\phi] = \psi$.*
3. *Ist Ψ eine Aussagenform in X, so ist auch $\forall x\Psi$ eine Aussagenform in X und $(\forall x\Psi)[\phi] = \forall x(\Psi[\phi])$.*
4. *Ist Ψ eine Aussagenform in X, so ist auch $\exists x\Psi$ eine Aussagenform in X und $(\exists x\Psi)[\phi] = \exists x(\Psi[\phi])$.*
5. *Sind Ψ und Φ Aussagenformen in X, so ist auch $\Psi \wedge \Phi$ eine Aussagenform in X und $(\Psi \wedge \Phi)[\phi] = \Psi[\phi] \wedge \Phi[\phi]$.*
6. *Sind Ψ und Φ Aussagenformen in X, so ist auch $\Psi \vee \Phi$ eine Aussagenform in X und $(\Psi \vee \Phi)[\phi] = \Psi[\phi] \vee \Phi[\phi]$.*
7. *Sind Ψ und Φ Aussagenformen in X, so ist auch $\Psi \to \Phi$ eine Aussagenform in X und $(\Psi \to \Phi)[\phi] = \Psi[\phi] \to \Phi[\phi]$.*

Lemma 60. *(Substitutionslemma) Sei Φ eine Aussagenform in X, ϕ und ψ Formeln. Die freien Variablen aller drei seien in $v_1, ..., v_n$ enthalten. Seien $a, b \in \nabla$, so dass für alle $e \in S$ und für $a_1, ..., a_n \in V(S)$ gilt:*

$$e \Vdash \phi[a_1, ..., a_n] \to ae \Vdash \psi[a_1, ..., a_n]$$

$$e \Vdash \psi[a_1, ..., a_n] \to be \Vdash \phi[a_1, ..., a_n]$$

Dann gilt $\Vdash \Phi[\phi[a_1, ..., a_n]] \leftrightarrow \Vdash \Phi[\psi[a_1, ..., a_n]]$.

Beweis. Sind die Voraussetzungen erfüllt, so gilt offenbar $\Vdash \forall\vec{x}.(\phi(\vec{x}) \to \psi(\vec{x})) \wedge (\phi(\vec{x}) \to \psi(\vec{x}))$. Es gilt nach dem bekannten Substitutionslemma der Prädikatenlogik [12]:

$$\vdash (\forall\vec{x}.(\phi(\vec{x}) \to \psi(\vec{x})) \wedge (\phi(\vec{x}) \to \psi(\vec{x}))) \to (\Phi[\phi[a_1, ..., a_n]] \leftrightarrow \Phi[\psi[a_1, ..., a_n]])$$

Also auch nach obigem Theorem:

$$\Vdash (\forall\vec{x}.(\phi(\vec{x}) \to \psi(\vec{x})) \wedge (\phi(\vec{x}) \to \psi(\vec{x}))) \to (\Phi[\phi[a_1, ..., a_n]] \leftrightarrow \Phi[\psi[a_1, ..., a_n]])$$

Und somit nochmal nach obigem Theorem:

$$\Vdash \Phi[\phi[a_1, ..., a_n]] \leftrightarrow \Phi[\psi[a_1, ..., a_n]]$$

Dies ist (mit obigem Theorem) eine sogar etwas stärkere Aussage als die zu beweisende. Q.E.D.

Man beachte, dass dies auch gelten würde, wäre die Sprache der Formeln, für die die Realisierbarkeitsrelation definiert wird ebenso wie die Definition erweitert, vorausgesetzt, die neuen Formeln erfüllten auch ${}^{\triangleleft}[\![\phi]\!] = [\![\phi]\!]$. Damit sieht man die angekündigte Möglichkeit der Vereinfachung der Realisierbarkeitsdefinition.

Bevor das schon angekündigte Beispiel der beschränkten Quantoren gebracht wird, bietet sich eine Vereinfachung der Realisierung der atomaren Formeln mit $\in$ und $=$ an. Da sonst unsere Beweise nicht einfach durchgegangen wären, wurden in ihren Definitionen stärkere Veränderungen zu den Versionen der Realisierbarkeit mit applikativen Strukturen getroffen, als der Übergang zu applikativen *Topologien* offensichtlicherweise erfordert. Dennoch sind alternative Definitionen oftmals handlicher, und wir würden sie gerne auch verwenden können:

Korollar 61. *Man kann in der Definition der Realisierbarkeit die Klauseln für $\in$ und $=$ ändern zu:*

1. $e \Vdash x \in y$, *falls* $e \lhd \{f \in S | \exists z. lf \Vdash z \dot{\in} y \wedge rf \Vdash x = z\}$
2. $e \Vdash x = y$, *falls* $\forall z \forall f \Vdash z \dot{\in} x \; lef \Vdash z \in y$ *und* $\forall z \forall f \Vdash z \dot{\in} y \; ref \Vdash z \in x$

Dann sind immer noch die selben Sätze realisiert.

Beweis. Technisch korrekt beweist man dies, indem man die Sprache der realisierbaren Formeln erweitert um die Zeichen $\tilde{\in}$ und $\tilde{=}$, deren Realisierer nach den obigen Formeln definiert sind. Dies formuliert man exakt wieder über eine induktive Definition von Klassen, so dass man die Klasse

$$\{(e, x, y, i) | (i = 0 \wedge e \Vdash x \tilde{\in} y) \vee (i = 1 \wedge e \Vdash x \tilde{=} y)\}$$

als kleinsten Fixpunkt einer induktiven Definition, die den beiden obigen Gleichungen folgt (mit $\in$ durch $\tilde{\in}$ ersetzt und analog für $=$), erhält. Man beachte, dass diese induktive Definition nicht so einfach ist, wie die für $\in$ und $=$ aus Definition 50, da man zur Bestimmung der Frage, ob $x \in y$ realisiert ist, eventuell auf Realisierer von $z \in y$ mit z aus einer höheren Stufe als x zurückgreifen muss.

Man sieht mit nur leicht veränderten Beweisen, dass immer noch ${}^{\lhd}[\![\phi]\!] = [\![\phi]\!]$ für alle ϕ gilt. Nach dem Substitutionslemma muss man jeweils zwei Elemente von ∇ finden, die Realisierer von $\tilde{\in}$ auf die von $\in$ bringen und umgekehrt, beziehungsweise analog für $=$.

Es würde ausreichen, hier induktiv vorzugehen, und jeweils als Induktionsannahme vorauszusetzen, es gäbe schon einen Realisierer in ∇, der das Geforderte für die Elemente erfüllt, die den Schluss, es gelte $x \in y$ oder $x \tilde{\in} y$ etc., ermöglicht haben. Allerdings gibt es auch einen Beweis, der ohne dies auskommt, da man mit Rekursion tatsächlich einen Realisierer von

$$\forall xy. (\, x \in y \leftrightarrow x \tilde{\in} y) \wedge (\, x = y \leftrightarrow x \tilde{=} y)$$

finden kann (dass dies stimmt, muss man natürlich auch induktiv nachweisen). Da das eine etwas stärkere Aussage zeigt und dennoch kaum komplizierter ist, werden wir diesen Weg beschreiten.

Es wird behauptet, dass die obige Formel realisiert wird durch

$$e := \tau^{fix}[v_1 := \lambda v. p(p(e_1)(e_2))(p(e_3)(e_4))]$$

mit

$$e_1 = \lambda x. p(lx)(l(rv)(rx))$$

$$e_2 = \lambda x.p(lx)(r(rv)(rx))$$
$$e_3 = \lambda x.p(\lambda y.r(lv)(lxy))(\lambda y.r(lv)(rxy))$$
$$e_4 = \lambda x.p(\lambda y.l(lv)(lxy))(\lambda y.l(lv)(rxy))$$

Da nach Eigenschaften von τ^{fix} dies $\trianglelefteq$ einem offenbar denotierenden Term ist (Paarbildung aus λ-Termen), denotiert e und liegt (da überzeugend) in ∇. Es gelten vier Aussagen:

$$l(le) \trianglelefteq \lambda x.p(lx)(l(re)(rx)) \Vdash\ x \in y \to x \tilde{\in} y$$
$$r(le) \trianglelefteq \lambda x.p(lx)(r(re)(rx)) \Vdash\ x \tilde{\in} y \to x \in y$$
$$l(re) \trianglelefteq p(\lambda y.l(le)(lxy))(\lambda y.l(le)(rxy)) \Vdash\ x = y \to x \tilde{=} y$$
$$r(re) \trianglelefteq p(\lambda y.r(le)(lxy))(\lambda y.r(le)(rxy)) \Vdash\ x \tilde{=} y \to x = y$$

Also sind vier über $f \in S$ allquantifizierte Implikationen zu zeigen, mit Prämissen $f \Vdash x \in y$ etc. Dies soll per Rekursion über die Stufe, in der die Prämisse hergeleitet wurde, geschehen.

1. Sei $f \Vdash x \in y$, also
$$f \lhd \{h \in S | \exists (lh, z) \in y\ rh \Vdash x = y\}$$
Dann nach Induktionsvoraussetzung
$$l(le)f \lhd \{h \in S | \exists (lh, z) \in y\ rh \Vdash x \tilde{=} y\} \subseteq [\![x \tilde{\in} y]\!]$$

2. Sei
$$f \lhd \{h \in S | \exists z \in V(S).lh \Vdash z \dot{\in} y \wedge rh \Vdash z \tilde{=} x\} := A$$
Dann nach Induktionsvoraussetzung
$$\begin{aligned} r(le)f &\trianglelefteq (\lambda x.p(lx)((r(re))(rx)))f \\ &\lhd \{p(lf)((r(re))(rf)) | f \in A\} \\ &\lhd \{pab | \exists z \in V(S).a \Vdash \{g | (g,z) \in y\}, b \Vdash z = x\} \\ &\lhd \{pab | \exists z \in V(S).(a,g) \in y, b \Vdash z = x\} \\ &= \{pab | \exists z \in Bi(y).(a,g) \in y, b \Vdash z = x\} \\ &\subseteq \{e | \exists a, b.le \lhd a, re \lhd b, \exists z \in Bi(y).(a,g) \in y, b \Vdash z = x\} \\ &\subseteq [\![x \in y]\!] \end{aligned}$$

3. Sei $f \Vdash x = y$. Sei $g \Vdash z \dot{\in} x$. Dann ist nach Induktionsvoraussetzung
$$\begin{aligned} l((l(re))f)g &\trianglelefteq l(le)(lfg) \\ &\lhd \{l(le)(lfh) | (h,z) \in x\} \\ &\subseteq \{l(le)i | i \Vdash z \in y\} \\ &\subseteq [\![z \tilde{\in} y]\!] \end{aligned}$$

Die umgekehrte Richtung mit $g \Vdash z \dot{\in} y$ geht analog.

4. Sei $f \Vdash x \tilde{=} y$. Sei $(g, z) \in x$, so $lfg \Vdash z \tilde{\in} y$. Also nach Induktionsvoraussetzung

   $$l((r(re))f)g \trianglelefteq r(le)(lfg) \Vdash \; z \in y$$

   Die umgekehrte Richtung geht analog.

Q.E.D.

In Zukunft werden wir die alternativen Definitionen verwenden, wo es sinnvoll erscheint, eventuell verschiedene im selben Beweis. Nur die selbe Formel werden wir nie auf verschiedene Arten realisieren (dies wäre tatsächlich problematisch). Man bemerke, dass man auch Mischungen aus beiden Definitionen verwenden kann, also etwa $a = b$ durch die unbeschränkte Allquantifikation, aber auf $x \in a, b$ mit beschränkter Allquantifikation, realisieren. Dies alles wird die Gesamtheit der realisierten Sätze sind ändern.

Nun zu der angekündigten Behandlung der beschränkten Quantoren:

Korollar 62. *Man kann in der Definition der Realisierbarkeit folgende Klauseln hinzufügen:*

- $e \Vdash \forall x \in a\, \phi(x)$, *falls* $\forall (f, x) \in a.\ ef \Vdash \phi(x)$
- $e \Vdash \exists x \in a\, \phi(x)$, *falls* $e \lhd \{e' | \exists (le', x) \in a.\ re' \Vdash \phi(x)\}$

Genauer ausgedrückt[10]*: Wenn man beschränkte Quantoren als eigene syntaktische Objekte einführt, deren Realisierbarkeit mit obigen Klauseln definiert ist, so lassen sich die folgenden gewünschten Beziehungen realisieren:*

$$\forall x \in a\ \phi \leftrightarrow \forall x.\ x \in a \to \phi$$

$$\exists x \in a\ \phi \leftrightarrow \exists x.\ x \in a \wedge \phi$$

Die Ersetzung eines beschränkten Quantors als Zusammensetzung aus einem unbeschränkten Quantor mit Beschränkung $x \in a$ durch einen beschränkten Quantor als eigenes syntaktisches Objekt oder umgekehrt ändert nichts an der Realisierbarkeit eines Satzes.

Beweis. Die Abgeschlossenheit der Realisierer von Formeln gegenüber $\lhd$ ist immer noch klar. Es sind vier Realisierer zu finden.

1. $\forall x \in a\ \phi(x) \to \forall x.\ x \in a \to \phi(x)$ wird realisiert durch $\lambda vw.i(v(lw))(rw)$, wobei i ein Realisierer für $\forall xy.\ \phi(y) \to x = y \to \phi(x)$ ist, den man ja angeben kann.

   Denn sei $e \Vdash \forall \in a \phi(x)$, $f \Vdash x \in a$. Dann ist $(lf, z) \in a$ und $rf \Vdash x = z$ für ein $z \in V(S)$. Also

   $$(\lambda vw.i(v(lw))(rw))ef = i(e(lf))(rf) \Vdash \phi(x)$$

   Denn es ist $e(lf) \Vdash \phi(z)$ und $rf \Vdash z = x$.

[10] Denn exakt genommen sind diese Klauseln ja nicht wahr, man kann sie nur „alternativ“ verwenden.

2. $\forall x(x \in a \to \phi(x)) \to \forall x \in a\, \phi(x)$ wird realisiert durch $\lambda vw.v(pwe_r)$. Denn sei $e \Vdash \forall x.x \in a \to \phi(x)$ und sei $(f,x) \in a$. Dann ist $pfe_r \Vdash x \in a$ und also $(\lambda vw.v(pwe_r))ef \trianglelefteq e(pfe_r) \Vdash \phi(x)$.

3. $\exists x \in a\, \phi(x) \to \exists x.\, x \in a \wedge \phi(x)$ wird etwa realisiert durch $\lambda v.p(p(lv)e_r)(rv)$. Denn sei $e \Vdash \exists x \in a\, \phi(x)$, so

$$\begin{aligned}(\lambda v.p(p(lv)e_r)(rv))e \lhd & \{(\lambda v.p(p(lv)e_r)(rv))f | \exists (lf,x) \in a.\, rf \Vdash \phi(x)\} \\ & \lhd\{p(p(lf)e_r)(rf) | \exists (lf,x) \in a.\, rf \Vdash \phi(x)\} \\ & \subseteq [\![\exists x.x \in a \wedge \phi(x)]\!]\end{aligned}$$

   Bei der Umformung zur letzten Zeile wurde ausgenutzt, dass $[\![x \in a]\!]$ und $[\![\phi(x)]\!]$ gegenüber $\lhd$ abgeschlossen sind.

4. $\exists x \in a\phi(x) \leftarrow \exists x.x \in a \wedge \phi(x)$ wird etwa realisiert durch $\lambda v.p(l(lv))(i(rv)(r(lv)))$ mit $i \Vdash \phi(x) \to x = z \to \phi(z)$. Denn sei $e \Vdash \exists x.x \in a \wedge \phi(x)$. Dann

$$\begin{aligned}& (\lambda v.p(l(lv))(i(rv)(r(lv))))e \\ \lhd & \{(\lambda v.p(l(lv))(rv))f | \exists x,z.(l(lf),z) \in a \wedge r(lf) \Vdash x = z \wedge rf \Vdash \phi(x)\} \\ \lhd & \{p(l(lf))(i(rf)(r(lf))) | \exists x,z.(l(lf),z) \in a \wedge r(lf) \Vdash x = z \wedge rf \Vdash \phi(x)\} \\ \subseteq & \{p(l(lf))b | \exists z.(l(lf),z) \in a \wedge b \Vdash \phi(z)\} \\ \lhd & \{e | \exists h,i.le \trianglelefteq h, re \trianglelefteq i, \exists z \in V(S).(h,z) \in a \wedge i \Vdash \phi(z)\} \\ \subseteq & [\![\exists x \in a\phi(x)]\!]\end{aligned}$$

Q.E.D.

Es soll gleich eine interessante Anwendung dieser Charakterisierung der Realisierung gebundener Formeln gegeben werden:

Korollar 63. *Sei ϕ beschränkt. Dann ist $[\![\phi]\!]$ eine Menge.*

Beweis. Dieser Satz, analog zum Satz X in [22], wird induktiv über den Aufbau der Formel ϕ bewiesen. Beachtet man, dass in einer schwachen applikativen Topologie die Operation $X \mapsto {}^{\lhd}X = \{x \in S | \exists u \in r(x)\, \forall y \in u\; y \in X\}$ Mengen X auf Mengen abbildet, ist jeder Fall unmittelbar klar nach der Definition; für beschränkte Quantoren verwendet man das vorige Korollar. Q.E.D.

4.3 Der Konsistenzsatz für CZF

Ziel dieses Abschnitts ist der Beweis des folgenden Theorems:

Theorem 64. *Ist S eine schwache applikative Topologie, so sind alle Axiome von CZF ohne Subset Collection realisiert. Ist S sogar eine applikative Topologie, so ist auch Subset Collection realisiert.*

4.3.1 Der Konsistenzsatz für $CZF_{-,-}$

Es werden nun für jedes Axiom (beziehungsweise für äquivalente Umformungen) Realisierer angegeben. Mit den alternativen Definitionen des letzten Abschnitts ist das Extensionalitätsaxiom unmittelbar realisiert. Dies ist nicht besonders verwunderlich, denn die Realisierungsdefinition für = wurde gerade so gewählt, dass dem so ist.

Lemma 65. *$\lambda v.v$ realisiert $\forall xy.\, \forall z \in x\, z \in y \wedge \forall z \in y\, z \in x \to z = x$, was zum Extensionalitätsaxiom äquivalent ist.*

Beweis. Seien $x, y \in V(S)$ und $e \Vdash \forall z \in x z \in y \wedge \forall z \in y z \in x$. Also $le \Vdash \forall z \in x\ z \in y$, also $\forall (f, z) \in x\ lef \Vdash z \in y$. Analog $\forall (f, z) \in x ref \Vdash z \in x$. Q.E.D.

Lemma 66. *1. $p(pke_r)(pke_r)$ realisiert $\forall xy \exists z.\, x \in z \wedge y \in z$, was zum Paarmengenaxiom äquivalent ist (mit Δ_0-Collection).*

2. $k(k(pke_r))$ realisiert $\forall x \exists y \forall z \in x\, \forall w \in z\, w \in y$, was zum Vereinigungsmengenaxiom äquivalent ist (mit Δ_0-Collection).

Beweis.

1. Sei $x, y \in V(S)$. Sei $z = S(\{(k, x), (k, y)\})$. Dann offenbar $pke_r \Vdash x \in z$, $pke_r \Vdash y \in z$, also

   $$p(pke_r)(pke_r) \in \{e | \exists z e \Vdash x \in z \wedge y \in z\}$$

   Insbesondere wird das Element also von dieser Menge überdeckt.

2. Sei $x \in V(S)$. Sei $y = S(\{(k, w) | \exists (f, v) \in y, (e, w) \in v\})$. Dann gilt offenbar

   $$k(k(pke_r)) \Vdash \forall z \in x \forall w \in z w \in y$$

   denn für $(e, v) \in x$, $(f, w) \in v$ ist $k(k(pke_r))ef \trianglelefteq pke_r \Vdash w \in y$, denn dann ist ja $(k, w) \in y$. Also ist

   $$k(k(pke_r)) \in \{e | \exists y.e \Vdash \forall z \in x \forall w \in z w \in y\}$$

   Insbesondere wird das Element also von dieser Menge überdeckt.

Q.E.D.

Lemma 67. *Sei ϕ eine Formel.*

$$e := p(\lambda xy.p(p(xy))e_r)(\lambda x.p(p(lx)e_r)(rx))$$

realisiert

$$\forall x \exists y.\, \forall z \in x\, (\phi(z) \to z \in y) \wedge \forall z \in y\, (z \in x \wedge \phi(z)),$$

also Δ_0-Kollektion.

Beweis. Sei $x \in V(S)$. Es ist zu zeigen, dass

$$e \lhd \{e' | \exists y.e' \Vdash \forall z \in x \phi(z) \to z \in y \wedge \forall z \in y.z \in x \wedge \phi(z)\}$$

Es soll aber sogar gezeigt werden, dass e in dieser Menge selbst liegt, nämlich mit y definiert als:

$$y := S(\{(pfg) | (f, z) \in x, g \Vdash \phi(z)\})$$

Dies ist eine Menge, da $[\![\phi(z)]\!]$ ja für jedes $z \in x[S]$ eine Menge ist, was wieder eine Menge ist.

Gelte nun $f \Vdash z \dot{\in} x$ und $g \Vdash \phi(z)$. Dann erhält man:

$$\begin{aligned} lefg &\unlhd p(p(fg)e_r) \\ &\in \{h | lh \Vdash z \dot{\in} y, rh \Vdash z = z\} \\ &\subseteq \{h | \exists z'.lh \Vdash z \dot{\in} y, rh \Vdash z' = z\} \\ &\subseteq [\![z \in y]\!] \end{aligned}$$

Sei umgekehrt $f \Vdash z \dot{\in} y$, also $z = pgh$ mit $g \Vdash z \dot{\in} x$ und $h \Vdash \phi(z)$. Dann gilt

$$l(rlf) \unlhd p(lx)e_r \unlhd pge_r \Vdash z \in xr(rlf) \unlhd rx \unlhd h \Vdash \phi(z) \tag{4.1}$$

Q.E.D.

Man beachte, dass die Beschränktheit von ϕ nur eingegangen ist, indem man $[\![\phi]\!] \subseteq S$ als Menge erkannt hat. Falls also volle Separation im Hintergrund vorläge, könnte man auch volle Separation realisieren, weil die Realisiererklasse dann stets eine Menge wäre, da Teilklasse der Menge S.

Lemma 68. *$e := \tau^{fix}[v_1 := \lambda vx.x(k(vx))] \in \nabla$ realisiert $\forall x(\forall y \in x\phi(y) \to \phi(x)) \to \forall x\phi(x)$, also Mengeninduktion.*

Beweis. Es gilt $e!$, aber dass e auch denotiert, folgt erst aus

$$e \unlhd \lambda x.x(k(ex)) \downarrow$$

Sei $f \Vdash \forall x.\forall y \in x\, \phi(y) \to \phi(x)$. Dass für alle $x \in V(S)$ dann $ef \Vdash \phi(x)$ gilt, wird durch Mengeninduktion bewiesen. Sei dies also für alle $x \in V(S)_\beta$ mit $\beta \in \alpha$ gezeigt und sei $x \in V(S)_\alpha$. Es ist

$$\begin{aligned} ef &\unlhd (\lambda x.x(k(ex)))f \\ &\unlhd f(k(ef)) \\ &\Vdash \phi(x) \end{aligned}$$

Denn nach Induktionsvoraussetzung gilt $k(ef) \Vdash \forall y \in x\, \phi(y)$, da $ef \Vdash \phi(y)$ für alle $y \in Bi(x)$. Q.E.D.

Um das Unendlichkeitsaxiom zu realisieren, wird ein Kandidat zur Repräsentation der natürlichen Zahlen benötigt.

Definition 69. *Sei für $n\in\omega$ induktiv definiert:*

$$\bar{n} := S(\{(\underline{i},\bar{i})|i\in n\})\in V(S)$$

Dann sei definiert:

$$\bar{\omega} := \hat{\bigcup}_{n\in\omega}\bar{n} = S(\{(\underline{n},\bar{n})|n\in\omega\})$$

Der folgende Hilfssatz wird die Realisierer und den Beweis etwas abkürzen:

Hilfssatz 70. *Sei*

$$e_+ := \lambda v.p(\lambda w.p(e_{\leq}vw)(D(e_{\leq}vw)e_r(pwe_r)))(p(pve_r)(\lambda w.pwe_r))$$

Für $n = m\cup\{m\}$ mit $n,m\in\omega$ realisiert $e_+\underline{m}$ die Aussage $\bar{n} = \bar{m}\cup\{\bar{m}\}$, also

$$\forall x\in\bar{n}(x = \bar{m}\vee x\in\bar{m})\wedge(\bar{m}\in\bar{n}\wedge\forall x\in\bar{m}\; x\in\bar{n})$$

Beweis. Die Realisierung des rechten Konjunktes verläuft auf die offensichtliche Weise, nur das linke Konkunkt ist nicht trivial. Sei also $(g,l)\in\bar{n}$, folglich $g\trianglelefteq\underline{l}$ und $l\in n$. Da die natürlichen Zahlen diskret sind, ist entweder $l = m$ oder $l\in m$. Im ersten Fall ist

$$l(e_+\underline{m})g \triangleleft pr(p\underline{l}e_r) \Vdash (\bar{l} = \bar{m}\vee\bar{l}\in\bar{m})$$

Denn es ist ja tatsächlich $(\underline{l},\bar{l})\in\bar{m}$. Im zweiten Fall ist

$$l(e_+\underline{m})g \triangleleft pl(\bar{l}e_r) \Vdash (x = \bar{m}\vee l\in\bar{m})$$

Denn es ist ja tatsächlich sogar $\bar{l} = \bar{m}$, also wird es sicherlich durch e_r realisiert. Q.E.D.

Nun kann man zum Unendlichkeitsaxiom schreiten:

Lemma 71. $e := p(p\underline{0}e_r)(\lambda v.p(s_N v)(e_+v))$ *realisiert*

$$\emptyset\in\bar{\omega}\wedge\forall n\in\bar{\omega}\exists m\in\bar{\omega} m = n\cup\{n\}$$

Und $f := \lambda x.p(lx)(D(lx)k(p(p_N x)(e_+(p_N x))))$ realisiert:

$$\forall n\in\bar{\omega}.n = 0\vee\exists m\in\bar{\omega} n = m\cup\{m\}$$

Die Behauptung, es gebe ein x, so dass

$$\emptyset\in x\wedge\forall n\in x\,\exists m\in x\; m = n\cup\{n\}\wedge\forall n\in x.\; n = 0\vee\exists m\in x\; n = m\cup\{m\}$$

ist äquivalent zum Unendlichkeitsaxiom (unter Annahme von Mengeninduktion).

Beweis. Es ist $le\trianglelefteq\underline{0}\in\bar{\omega}^{-1}\emptyset$ und für $(g,\bar{n})\in\omega$ ist $g\trianglelefteq\underline{n}$, also $reg\trianglelefteq\underline{n+1}$ und $\underline{n+1}\in\bar{\omega}^{-1}(\bar{n}\cup\{(\underline{n},\bar{n})\})$. Damit ist wegen des obigen Hilfssatzes die Aussage betreffend e gezeigt.

Außerdem ist n entweder 0 oder nicht. Im ersten Fall gilt $l(fg)\trianglelefteq l(f\underline{0})\trianglelefteq l$ und (man beachte die Denotiertheit sämtlicher Subterme, auf Grund derer man die Fallunterscheidungseigenschaft von d anwenden kann) $r(fg) \trianglelefteq k \Vdash n = 0$, denn der Allquantor in der Definition der Realisierung der Gleichheit läuft leer.

Sei jedoch $n \neq 0$, also $n = m + 1$ für ein $m \in \omega$. Dann ist $l(r(fg)) \trianglelefteq \underline{m}$ und daher $(l(r(fg)), m) \in \bar{\omega}$ und $n = m \cup \{m\}$, also wegen des Hilfssatzes $r(fg) \Vdash \exists m \in \bar{\omega}\; n = m \cup \{m\}$ und die Aussage betreffend f ist gezeigt.

Nun noch zur Äquivalenz zum Unendlichkeitsaxiom. Gelte die Aussage (die für $a := \bar{\omega}$ realisiert wurde)

$$\emptyset \in a \wedge \forall n \in a\; \exists m \in a\; m = n \cup \{n\} \wedge \forall n \in a.\; n = 0 \vee \exists m \in a\; n = m \cup \{m\}$$

und sei b so, dass

$$\emptyset \in b \wedge \forall n \in b \exists m \in b m = n \cup \{n\}$$

Dann zeigt man $\forall x.\; x \in a \to x \in b$ durch Mengeninduktion. Denn sei dies für die Elemente von x schon gezeigt. Ist $x \in a$, so hat x die Form $y \cup \{y\}$ für ein $y \in a$ und $y \in x$, also $y \in b$. Also $x = y \cup \{y\} \in b$. Oder $x = 0$, und dann ist x sowieso in b.

Die Rückrichtung ist natürlich für unsere Zwecke unbedeutend, aber dennoch: Sei a so, dass

$$\emptyset \in a \wedge \forall n \in a \exists m \in a\, m = n \cup \{n\} \wedge \forall a'.(\emptyset \in a' \wedge \forall n \in a'\; n \cup \{n\} \in a') \to a \subseteq a'$$

Sei dann etwa

$$a' = \{x \in a | x = \emptyset \vee \exists y \in a\; x = y \cup \{y\}\}$$

Dies erfüllt sicherlich die Voraussetzung, denn ist $x \in a'$, so auch $x \cup \{x\}$. Also ist $a \subseteq a'$, also $a = a'$. Q.E.D.

Wir werden in Zukunft ohne die Gesamtheit der realisierten Formeln zu verändern in ihnen stets ω, was ja ein Term ist, der nach Auflösung zu sehr langen Formeln führen würde, durch $\bar{\omega}$, was einfach eine Konstante ist, ersetzen, da realisiert ist $\bar{\omega} = \omega$, wobei dies wieder als Abkürzung für eine recht komplexe Formel zu lesen ist. Auch wenn dies selten erwähnt wird, ist das eine übliche Verfahrensweise, ohne die die Lesbarkeit von Termen, die Formeln realisieren, die über die natürlichen Zahlen sprechen, kaum mehr gegeben wäre.

4.3.2 Paare

Als Anwendung kann man das folgende, höchst nützliche Lemma zeigen.

Definition und Lemma 72. *Sei für $a, b \in V(S)$ definiert:*

$$\langle a, b\rangle := S(\{(l, a), (r, S(\{(l, a), (r, b)\}))\})$$

Dann kann in der Definition der Realisierbarkeit (a, b) durch $\langle a, b\rangle$ ersetzt werden.

Beweis. (a, b) ist ja formal gar nicht in der Syntax von CZF enthalten, sondern statt dessen nur die drei Abkürzungen:

1. $(a, b) = x$ für $\forall y.\; y \in x \leftrightarrow (y = a \vee \forall z. z \in y \leftrightarrow z = a \vee z = b)$

2. $(a, b) \in x$ für $\exists y \in x\, y = (a, b)$

3. $(a, b) \ni x$ für $\exists y.\, x \in y \wedge y = (a, b)$

Mit Extensionalität kann man das umformen zu den handlicheren

1. $x \in (a, b)$ für $x = a \vee ((\forall y \in x\, y = a \vee y = b) \wedge a \in x \wedge b \in x)$

2. $(a, b) = x$ für $\forall y.\, y \in x \leftrightarrow y \in (a, b)$

3. $(a, b) \in x$ für $\exists y \in x\, y = (a, b)$

Es ist klar, dass es ausreicht, zu zeigen, dass die erste Formel nach der Ersetzung realisiert ist:

$$\forall x \in \langle a, b\, \rangle.\, x = a \vee ((\forall y \in x\ y = a \vee y = b) \wedge (a \in x \wedge b \in x))$$

und

$$a \in \langle a, b\rangle \wedge \forall x.(\forall y \in x(y = a \vee y = b) \wedge (a \in x \wedge b \in x)) \rightarrow x \in \langle a, b\rangle$$

Der Rest folgt mit reiner Logik, realisierten Axiomen und dem Lemma 58 nach dem Konsistenzsatz der Prädikatenlogik.

Die erste Formel ist realisiert durch

$$e := \lambda x.px(dxe_r(p(\lambda y.pye_r))(p(ple_r)(pre_r)))$$

Denn sei $(f, x) \in \langle a, b\rangle$, dann

$$(x = a \wedge f \trianglelefteq l) \vee (x = S(\{(l, a), (r, b)\}) \wedge f \trianglelefteq r)$$

Im ersten Fall gilt natürlich

$$l(ef) \trianglelefteq l \wedge r(ef) \trianglelefteq e_r \Vdash x = a$$

Im zweiten Fall gilt für alle $(g, y) \in x$:

$$(y = a \wedge g \trianglelefteq l) \vee (y = b \wedge g \trianglelefteq r)$$

Also

$$l(r(ef)) \trianglelefteq pfe_r \Vdash y = a \vee y = b$$

Außerdem gilt

$$l(r(r(ef))) \trianglelefteq ple_r \Vdash a \in x$$

und

$$r(r(r(ef))) \trianglelefteq pre_r \Vdash b \in x$$

Insgesamt realisiert e also die Formel wie gewünscht.

Das erste Konjunkt der zweiten Formel ist offenbar realisiert durch ple_r. Das zweite ist realisiert durch

$$e' := \lambda v.pr(p(\lambda w.lvw)(\lambda w.Dw(l(rv))(r(rv))))$$

Denn sei $x \in V(S)$ und sei

$$(lf \Vdash \forall y \in xy = a \vee y = b) \wedge (l(rf) \Vdash a \in x) \wedge (r(rf) \Vdash b \in x)$$

Wir behaupten, dass dann

$$(l(e'f), S(\{(l,a),(r,b)\})) \in \langle a, b\rangle \wedge r(e'f) \Vdash x = S(\{(l,a),(r,b)\})$$

Der erste Teil ist dabei trivial, da $l(e'f) \trianglelefteq r$. Der zweite besteht wiederum aus zwei Aussagen:

Sei $(g,z) \in x$. Dann gilt

$$\begin{aligned} & l(r(e'f))g \\ & \trianglelefteq lfg \\ \lhd \{h | (lh \trianglelefteq l \wedge rh \Vdash z = a) \vee (lh \trianglelefteq r \wedge rh \Vdash z = b)\} \subseteq & [\![z \in S(\{(l,a),(r,b)\})]\!] \end{aligned}$$

Sei umgekehrt $(g,z) \in S(\{(l,a),(r,b)\})$, also tritt einer der folgenden Fälle auf:

1. $g \trianglelefteq l$, $z = a$. In diesem Fall

$$r(r(e'f))g \trianglelefteq l(rf) \Vdash a \in x$$

2. $g \trianglelefteq r$, $z = b$. In diesem Fall

$$r(r(e'f))g \trianglelefteq r(rf) \Vdash b \in x$$

Damit ist alles gezeigt. Q.E.D.

4.3.3 Der Konsistenzsatz für $CZF_{X,Y}$

Bisher wurden für dieses Modell und die Aussagen darüber noch nicht die höheren Axiome verwendet — alles Wesentliche, was bisher bewiesen wurde, benötigte nur $CZF_{-,-}$. Dies ändert sich nun, wenn wir die Kollektionsaxiome realisieren wollen. Allgemein benötigt man in etwa diejenigen höheren Axiome von $CZF_{X,Y}$, die man gerade realisieren will. Gerade die Realisierung der Kollektionsaxiome ist für applikative Topologien allerdings deutlich schwerer als für applikative Strukturen.

Variationen von Strong Collection

Die Realisierbarkeit soll zunächst für Variationen des Strong-Collection Schemas von CZF gezeigt werden.

Lemma 73. *Sei ϕ eine Formel. Unter Annahme von Collection gilt:*

$$e := \lambda x.(\lambda y.py(xy))$$

realisiert

$$\forall a.\forall x \in a \exists y \phi(x,y) \to \exists b \forall x \in a \exists y \in b \phi(x,y)$$

also eine beliebige Instanz von Collection.

Beweis. Sei $a \in V(S)$ und $f \Vdash \forall x \in a \exists y \phi(x,y)$, also

$$\forall (g,x) \in a\ fg \lhd \{h | \exists y h \Vdash \phi(x,y)\}$$

Die überdeckende Klasse muss keine Menge sein. Es wurde vereinbart, die Überdeckung durch eine Klasse äquivalent als die Existenz einer überdeckenden Teilmenge festzulegen, mithin

$$\forall (g,x) \in a \exists c.\ fg \lhd c \wedge \forall h \in c \exists y\ h \Vdash \phi(x,y)$$

Mit Collection kann man nun diese y in einer Menge sammeln — man kann aber auch die Paare (g,y) in eine Menge sammeln:

$$\forall (g,x) \in a \exists c. fg \lhd c \wedge \exists Y \forall h \in c \exists (g,y) \in Y h \Vdash \phi(x,y)$$

Da man das „$fg \lhd c \wedge$" unter den Existenzquantor über Y ziehen kann und dann die Existenzquantoren von c und Y vertauschen kann, erhält man nach nochmaliger Anwendung von Collection:

$$\exists B \forall (g,x) \in a \exists c. fg \lhd c \wedge \exists Y \in B \forall h \in c \exists (g,y) \in Y h \Vdash \phi(x,y)$$

Setzt man nun $b := S(\{(g,y) \in \bigcap B | y \in V(S)\})$, so ist dies in $V(S)$ und es gilt

$$\forall (g,x) \in a \exists c. fg \lhd c \wedge \forall h \in c \exists (g,y) \in Bh \Vdash \phi(x,y)$$

Das bedeutet aber wiederum

$$\forall (g,x) \in a\ fg \lhd \{h | \exists (g,y) \in B\ h \Vdash \phi(x,y)\}$$

und also

$$\forall (g,x) \in a\ pg(fg) \lhd \{h | \exists (lh,y) \in B\ rh \Vdash \phi(x,y)\}$$

Darum ist, nämlich für jenes konstruierte B,

$$ef \in \{i | \exists B \forall (g,y) \in a\ ig\{h | \exists (lh,y) \in B\ rh \Vdash \phi(x,y)\}\}$$

Insbesondere wird ef also von dieser Menge überdeckt, was zu zeigen war. Q.E.D.

Lemma 74. *Sei ϕ eine Formel. Unter der Annahme von Strong Collection gilt: $e := \lambda x.p(\lambda y.py(xy))(\lambda y.y)$ realisiert*

$$\forall a. \forall x \in a \exists y \phi(x,y) \to \exists b. \forall x \in a \exists y \in b \phi(x,y) \wedge \forall y \in b \exists x \in a \phi(x,y),$$

also eine beliebige Instanz von Strong Collection.

Beweis. Die Beweisidee ist verwandt mit der des letzten Beweises, allerdings sind die Einzelheiten etwas umständlicher. Dennoch kann der Beweis knapp präsentiert werden, da einige Schritte übereinstimmen.

Sei $a \in V(S)$ und $f \Vdash \forall x \in a \exists y \phi(x,y)$. Wie im obigen Beweis folgt

$$\forall (g,x) \in a \exists c. fg \lhd c \wedge \forall h \in c \exists y\ h \Vdash \phi(x,y)$$

Ähnlich wie zu zuvor sammelt man die $(pg(fg), y)$ per Strong Collection in einer einzigen Menge:

$$\forall (g,x) \in a \exists c. fg \lhd c \wedge \exists Y. \forall h \in c \exists (pg(fg), y) \in Y (h \Vdash \phi(x,y)) \wedge \forall (g', y). g = pg(fg) \wedge \exists h \in ch \Vdash \phi(x,y)$$

Wieder vertauscht man die Existenzquantoren und geht von der Menge, deren Existenz man gezeigt hat, zu deren Vereinigungsmenge über. Alternativ verwendet man die in der Sektion über Strong Collection bewiesene Aussage. So erreicht man schließlich die Existenz eines b, so dass die beiden Aussagen gelten:

$$\forall (g,x) \in a \exists c. fg \lhd c \wedge \forall h \in c \exists (pg(fg), y) \in b\, h \Vdash \phi(x,y)$$

$$\forall y' \in b \exists y \exists (g,x) \in a. y' = (pg(fg), y) \wedge \exists c. fg \lhd c \wedge \forall h \in c\, h \Vdash \phi(x,y)$$

Dies impliziert, dass $S(b) \in V(S)$ und es impliziert jede der beiden Gleichungen eine der folgenden Aussagen:

$$\forall (g,x) \in a\; fg \lhd \{h | \exists (pg(fg), y) \in S(b) h \Vdash \phi(x,y)\}$$

$$\forall (g', y) \in S(b)\; g' \lhd \{h | \exists x. lh \Vdash x \dot{\in} a \wedge rh \Vdash \phi(x)\}$$

Das wiederum zeigt, dass

$$ef \in \{h | \exists b \in V(S). h \Vdash \forall x \in a \exists y \in S(b) \phi(x,y) \wedge \forall y \in S(b) \exists x \in a \phi(x,y)\}$$

Insbesondere wird ef also von der Klasse aller solchen h überdeckt. Dies war zu zeigen. Q.E.D.

Gilt im Hintergrund nur Replacement, so scheint es sehr schwer, Replacement zu realisieren, da die Realisierung der Funktionalität einer Formel nicht die Funktionalität einer Formel in der „wirklichen Welt" impliziert, sondern nur die Eigenschaft, dass zwei Bilder des selben Urbilds auf bestimmt realisierte Weise gleich seien — und das ist nicht ausreichend, um Replacement anwenden zu können. Dem Autor ist darum kein Beweis der Realisiertheit von Replacement aus $CZF_{R,-}$ bekannt.

Abschwächungen des Potenzmengenaxioms

Im folgenden Lemma stammt der gewählte Realisierer aus McCarty, wenn auch der Beweis völlig anders sein muss. Dennoch ist dies erwähnenswert, da hier nach Wissen des Autors zum ersten Mal der Realisierungsterm eines mengentheoretischen Axioms mit einem in der Literatur vorgeschlagenen übereinstimmt, was mitunter darauf zurückzuführen ist, dass applikative Topologien komplexer sind, vielfach aber auch einfach darauf, dass hier viele Anstrengungen und Vereinfachungen unternommen wurden, um möglichst kurze Realisierer und einfache Beweise zu erhalten (etwa Realisierung äquivalenter Aussagen, Ausnutzen der Korollare zum Konsistenzsatz der Prädikatenlogik etc). In der Regel differieren nämlich die hier definierte Realisierbarkeitsdefinition und die klassische weniger darin, andere Terme zu benötigen, sondern mehr darin, dass es wesentlich aufwändiger ist, von den Termen zu beweisen, dass sie die gewünschte Eigenschaft erfüllen. So auch in diesem Fall:

Lemma 75. *Sei ϕ eine Formel. Unter der Annahme des Potenzmengenaxioms gilt: $\Vdash \forall a \exists b \forall c. (\forall d \in c\;\, d \in a) \to c \in b$, also eine zum Potenzmengenaxiom äquivalente Aussage (mit $\Delta_0 - Collection$) ist realisiert.*

Dies ist für gewöhnliche Realisierbarkeitstheorie leicht zu zeigen (mit Lemma 58), aber trickreich für Realisierung durch applikative Topologien (wo dieses Lemma im allgemeinen nicht anwendbar ist). Der Grund ist, dass man eine Menge, die realisierterweise gleich der Potenzklasse sein soll, angeben will, indem man alle Mengen, die realisierterweise Teilmengen sind, zusammenfasst. Dies ist allerdings auch nicht mit Potenzmengenaxiom im Hintergrund möglich, da eine Menge c, die realiserterweise Teilmenge von a ist, in beliebig höheren Stufen $V(S)_\alpha$ liegen kann, da sie Elemente aus hohen Stufen enthält — wenn auch nur mit so schlechten Gründen, dass sie immer noch Teilmenge von a ist.

Vor dem Beweis benötigen wir eine Definition. Sie macht es möglich, im konstruierten Modell darüber zu sprechen, dass ein Element des Modells „im Wesentlichen" in einer bestimmten Stufe liegt. Dazu wird der Teil einer Menge definiert, der in dieser Stufenmenge liegt:

Definition 76. *Es sei $V(S) \times On \ni (a, \alpha) \mapsto a^\alpha \in V(S)_\alpha$ die Abbildung, die induktiv definiert ist durch*

$$a^\alpha = \{(e, \hat{\bigcup}_{\beta\in\alpha} x^\beta) | (e, x) \in a\}$$

Beweis. Existenz, Totalität und Funktionalität folgt durch einfache Induktion über α. Q.E.D.

Für $a \in V(S)_\alpha$ gilt $a^\alpha = a$, wie man durch Induktion über α sofort sieht. Liegt a aber in einer höheren Stufenmenge $V(S)_\beta$, so wird beim Übergang zu a^α gewissermaßen der Überhang abgeschnitten. Wenn realisiert wird, dass $a = a^\alpha$, dann kann das also als eine Zugehörigkeit von a zu $V(S)_\alpha$ „bis auf wenig überzeugende Gründe" interpretiert werden — diese Gründe müssen jedoch nicht direkt Gründe sein, warum ein Element in a liegt, sondern können durchaus tiefer in der transitiven Hülle von a verborgen sein. Die zentrale Eigenschaft ist das folgende Lemma:

Lemma 77. *Sei $a \in V(S)_\alpha, b \in V(S)$. Dann realisiert*

$$e := \tau^{fix}[v_1 := \lambda vx.p(\lambda y.p(l(lxy))(v(r(lxy))))(\lambda y.p(l(rxy))(e_s v(e_s(r(rxy)))))]$$

die Formel $a = b \to a = b^\alpha$. Außerdem realisiert

$$e' := \lambda x.p(\lambda y.p(l(xy))(e(r(xy))))$$

die Formel $\forall x \in a\, x \in b \to \forall x \in a\, x \in b^\alpha$

Beweis. Induktion über α, sei die Tatsache also schon für alle $\beta \in \alpha$ bewiesen. Es ist

$$l(ef)g \trianglelefteq p(l(lfg))(e(r(lfg)))$$

Sei $f \Vdash a = b$. Für $(g, x) \in a$ gibt es ein $\beta' \in \alpha$ mit $x \in V(S)_{\beta'}$. Also gilt nach

Induktionsvoraussetzung (denn $V(S)_{\beta'} \ni x = x^{\beta'}$):

$$\begin{aligned} lfg \lhd \{h | \exists (lh, y) \in b\, rh \Vdash x = y\} \\ \subseteq \{h | \exists (lh, y) \in b\, \forall \alpha > \beta \geq \beta'\, e(rh) \Vdash x = y^\beta\} \\ \subseteq \{h | \exists (lh, y) \in b\, e(rh) \Vdash x = \hat{\bigcup}_{\alpha > \beta \geq \beta'} y^\beta\} \\ = \{h | \exists (lh, y) \in b\, e(rh) \Vdash x = \hat{\bigcup}_{\beta \in \alpha} y^\beta\} \\ \subseteq \{h | \exists (lh, y) \in b^\alpha\, e(rh) \Vdash x = y\} \end{aligned}$$

Von der zweiten zur dritten Zeile wurde verwendet, dass stets gilt:

$$\forall d \in E\; i \Vdash c = d \rightarrow i \Vdash c = \bigcup E$$

Also gilt insgesamt:

$$l(ef)g \lhd [\![x \in b^\alpha]\!]$$

Außerdem analog

$$\begin{aligned} fg \lhd \{h | \exists (lh, y) \in b\, rh \Vdash x = y\} \\ \subseteq \{h | \exists (lh, y) \in b\, e(rh) \Vdash x = \hat{\bigcup}_{\alpha > \beta \geq \beta'} y^\beta\} \\ \subseteq \{h | \exists (lh, y) \in b^\alpha\, e(rh) \Vdash x = y\} \end{aligned}$$

Also

$$e' f \Vdash \forall x \in a x \in b^\alpha$$

D.h. f' ist wie gewünscht.

Umgekehrt sei $(g, \hat{\bigcup}_{\beta \in \alpha} y^\beta) \in b^\alpha$, mit $(g, y) \in b$. Da $\hat{\bigcup}_{\beta \in \alpha} y^\beta \in V(S)_{\beta'}$ für ein $\beta' \in \alpha$, gilt nach Induktionsvoraussetzung

$$\begin{aligned} rfg \lhd \{h | \exists (lh, x) \in a\, rh \Vdash y = x\} \\ \subseteq \{h | \exists (lh, x) \in a\, \forall \alpha' \ni \beta' \in \alpha\; e_s(e(e_s(rh))) \Vdash x^{\alpha'} = \hat{\bigcup}_{\beta \in \alpha} y^\beta\} \\ \subseteq \{h | \exists (lh, x) \in a\; e_s(e(e_s(rh))) \Vdash \hat{\bigcup}_{\beta' \in \alpha' \in \alpha} x^{\alpha'} = \hat{\bigcup}_{\beta \in \alpha} y^\beta\} \\ = \{h | \exists (lh, x) \in a\; e_s(e(e_s(rh))) \Vdash x^\alpha = \hat{\bigcup}_{\beta \in \alpha} y^\beta\} \\ = \{h | \exists (lh, x) \in a\, \forall e_s\; (e(e_s(rh))) \Vdash x = \hat{\bigcup}_{\beta \in \alpha} y^\beta\} \end{aligned}$$

Also

$$r(ef)g \lhd [\![\hat{\bigcup}_{\beta \in \alpha} y^\beta \in a]\!]$$

Also gilt

$$ef \Vdash a = b^\alpha$$

Q.E.D.

Damit kann man nun das Lemma über das Potenzmengenaxiom zeigen:
BEWEIS. Es wird behauptet, dass ein gesuchter Realisierer $\lambda x.pk(e'x)$ wäre, wobei e' wie im letzten Lemma ist.

Sei nämlich $a \in V(S)_\alpha$. Man definiere

$$b := S(\{(k,c)|c \in V(S)_\alpha\})$$

Dies ist eine Menge, denn mit dem Potenzmengenaxiom kann man induktiv zeigen, dass alle $V(S)_\beta$ Mengen sind. Sei nun $c \in V(S)$ und $f \Vdash \forall d \in c\, d \in a$. Wir werden zeigen, dass $ef \trianglelefteq pk(e'f) \Vdash c \in b$. Es gilt

$$pk(e'f) \lhd \{h|(lh, c^\alpha) \in b \wedge rh \Vdash c = c^\alpha\} \subseteq \{h|\exists d(lh, d) \in b\, rh \Vdash c = d\}$$

Damit ist das Potenzmengenaxiom realisiert. Q.E.D.

Diese Maschinerie ist für Subset Collection nicht erforderlich. Allerdings benötigt man für Subset Collection, im Gegensatz zu dem stärkeren Potenzmengenaxiom, tatsächlich applikative Topologien und nicht nur schwache applikative Topologien.

Lemma 78. *Sei S eine (starke) applikative Topologie mit $R : S \to P(P(S))$ als die Funktion, die die Mengenartigkeit der zu Grunde liegenden formalen Topologie bezeugt. Sei ϕ eine Formel. Unter Annahme von Subset Collection gilt:*

$$i := \lambda v.pk(p(\lambda x.p(px(vx))(r(vx)))(\lambda x.p(ly)(r(ry))))$$

realisiert Subset Collection, also

$$\forall a, b \exists c \forall u. \forall x \in a \exists y \in b \phi(x, y, u) \to \exists d \in c. \forall x \in a \exists y \in d \phi(x, y, u) \wedge \forall y \in d \exists x \in a \phi(x, y, u)$$

BEWEIS. Seien $a, b \in V(S)$. Sei

$$b^* := \{(g,d)|(l(rg), d) \in b\} \in V(S)$$

Dies ist in $V(S)$, da für $d \in b^*[S]$ gilt:

$$e \lhd b^{*-1}d \to l(re) \lhd l(rb^*)^{-1}d \subseteq b^{-1}d \to (e,d) \in b^*$$

Es gibt nach Subset Collection eine Menge B von Teilmengen von b^*, so dass für alle $(f,x) \in a$, alle $u \in V(S)$, alle $e \in S$ und alle $S \supseteq v \in r[S]$

$$\forall j \in v \exists (h,y) \in b^*. j = h \wedge (lh, x) \in a \wedge (l(rh), y) \in b \wedge r(rh) \Vdash \phi[x, y, u]$$

impliziert, dass es ein $b^{*'} \in B$ gibt, so dass

$$\forall j \in v \exists (h,y) \in b^{*'}. j = h \wedge (lh, x) \in a \wedge (l(rh), y) \in b \wedge r(rh) \Vdash \phi[x, y, u]$$

und

$$\forall (h,y) \in b^{*'} \exists j \in v. j = h \wedge (lh, x) \in a \wedge (l(rh), y) \in b \wedge r(rh) \Vdash \phi[x, y, u]$$

Die Konjunktion dieser beiden Formeln soll mit $\psi(f, x, u, v, e, b^{*'})$ bezeichnet werden.

Nochmalige Anwendung von Subset Collection liefert für jedes $e \in S$ eine Menge C_e von Teilmengen von B, so das für alle $u \in V(S)$

$$\forall (f,x) \in a \exists b^{*'} \in B \exists v \in r[S].pf(ef) \lhd v \wedge \phi(f,x,u,v,e,b^{*}\ )$$

impliziert, dass es ein $B' \in C$ gibt, so dass

$$\forall (f,x) \in a \exists b^{*'} \in B' \exists v \in r[S].pf(ef) \lhd v \wedge \phi(f,x,u,v,e,b^{*'})$$

und

$$\forall b^{*'} \in B' \exists (f,x) \in a \exists v \in r[S].pf(ef) \lhd v \wedge \phi(f,x,u,v,e,b^{*'})$$

Man setze nun letztendlich

$$c = S(\{(k, S(\{(l,y) | \exists b^{*'} \in B'.(l,y) \in b^{*'}\})) | B' \in \bigcap_{e \in S} C_e\})$$

Dieses $c \in V(S)$ ist nun wie von Subset Collection gefordert.

Denn sei $u \in V(S)$, $e \Vdash \forall x \in a \exists y \in b \phi(x,y,u)$. Also gilt für $(f,x) \in a$:

$$\exists v \in r[S].ef \lhd v \wedge \forall j \in v \exists (lh,y) \in b.j = h \wedge (lh,y) \in b \wedge rh \Vdash \phi[x,y,u]$$

Also

$$\exists v \in r[S].pf(ef) \lhd v \wedge \forall j \in v \exists (h,y) \in b^{*}.j = h \wedge (lh,x) \in a \wedge (l(rh),y) \in b \wedge r(rh) \Vdash \phi[x,y,u]$$

Wegen unserer ersten Anwendung von Subset Collection folgt:

$$\exists v \in r[S].pf(ef) \lhd v \wedge \exists b^{*'} \in B.\psi(f,x,u,v,e,b^{*'})$$

Und damit nach Allquantor-Einführung:

$$\forall (f,x) \in a \exists b^{*'} \in B \exists v \in r[S].pf(ef) \lhd v \wedge \phi(f,x,u,v,e,b^{*'})$$

Es gibt also ein $B' \in C$, so dass die folgenden beiden Aussagen gelten:

$$\forall (f,x) \in a \exists b^{*'} \in B' \exists v \in r[S].pf(ef) \lhd v \wedge \psi(f,x,u,v,e,b^{*'})$$

$$\forall b^{*'} \in B' \exists (f,x) \in a \exists v \in r[S].pf(ef) \lhd v \wedge \psi(f,x,u,v,e,b^{*'})$$

Setze nun $b' = S(\{(l,y) | \exists b^{*'} \in B'.(l,y) \in b^{*'}\})$. Offenbar gilt $(l(ef), b') \in c$, denn $l(ef) \unlhd k$. Der Nachweis der folgenden Behauptung wird den Beweis fertigstellen.

$$r(ie) \Vdash \forall x \in a \exists y \in b' \phi(x,y,u) \wedge \forall y \in b' \exists x \in a \phi[x,y,u]$$

Sei also $(f,x)\in a$. Dann gibt es nach der ersten der beiden Aussagen über B' ein $v\in r[S]$ mit $pf(ef)\lhd v$ und $\psi(f,x,u,v,e,b^{*'})$ für ein $b^{*'}\in B'$, insbesondere gibt es für jedes $j\in v$ ein $(h,y)\in b^{*'}$ mit

$$j = h \wedge (lh,x)\in a \wedge (l(rh),y)\in b \wedge r(rh) \Vdash \phi[x,y,u]$$

Also $pf(ef) \lhd \{j|\exists(j,y)\in b' \wedge r(r(j)) \Vdash \phi[x,y,u]\}$. Damit gilt

$$r(r(ie))f \unlhd p(pf(ef))(r(ef)) \Vdash \exists y\in b'\phi[x,y,u]$$

Sei umgekehrt $(g',y)\in b'$. Also gibt es ein $b^{*'}$ mit $(g,y)\in b^{*'}$ und $g'\lhd b^{*\ -1}y$. Es reicht zu zeigen, dass für alle g mit $(g,y)\in b^{*'}$ folgt, dass $l(r(ie))g \Vdash \exists x\in a\phi[x,y,u]$ gilt, denn da Realisiererklassen unter $\lhd$ abgeschlossen sind, trifft das dann erst recht für g' zu. Sei also $(g,y)\in b^{*'}$, dann gibt es nach der zweiten Gleichung über B' ein $(f,x)\in a$ mit

$$\exists v\in r[S].pf(ef)\lhd v\wedge\forall(h,y')\in b^{*'}\exists j\in v.j = h\wedge(lh,x)\in a\wedge(l(rh'),y)\in b\wedge r(rh) \Vdash \phi[x,y,u],$$

wobei nur das zweite Konjunkt von ψ verwendet wurde. Insbesondere also für $(h,y') := (g,y)$:

$$(lg,x)\in a \wedge r(rg) \Vdash \phi[x,y,u]$$

Dies impliziert

$$l(r(ie))g \unlhd p(lg)(r(rg)) \Vdash \exists x\in a\phi[x,y,u]$$

Q.E.D.

Insbesondere ist das Theorem hiermit bewiesen, ebenso wie ein analoges Theorem für IZF statt CZF.

4.4 Absolutheitsresultate

Definition 79. *Ein Satz ϕ heißt **absolut**, falls $CZF \vdash (\phi \rightarrow\Vdash \phi)$.*

Ist insbesondere ein Kandidat für ein CZF verstärkendes Axiom absolut, so ist die angegebene Modellkonstruktion auch für die um dieses Axiom erweiterte Theorie geeignet. Ergebnisse des letzten Abschnitts kann man auch als Absolutheit einiger Axiome von $CZF_{X,Y}$ über $CZF_{-,-}$ sehen.

4.4.1 REA

Das Axiom der regulären Erweiterungen (regular extension axiom, REA) postuliert die Existenz beliebig großer so genannter regulären Mengen: Mengen, die in einer klassischen Umgebung den V_α mit α regulär entsprechen. Das Axiom ist im Zusammenhang mit induktiven Definitionen hilfreich, da es ermöglicht, induktiv definierte Klassen, deren einzelnen Stufen uniform durch eine Menge beschränkt sind, als Menge zu erkennen [2].

Definition 80. *Eine Menge A heißt **regulär**, falls*

1. *A bewohnt ist, also* $\exists x \in A \top$

2. *A transitiv ist, also* $\forall x \in A \forall y \in x\, y \in A$

3. *A ist ein Modell für zweitstufige Strong Collection, also*

$$\forall a \in A \forall R \subseteq a \times A.\, R : a \rightrightarrows A \to \exists b \in A R : a \leftrightarrows\!\!\rightrightarrows b$$

Man beachte, dass R in der dritten Bedingung eine Menge sein muss, auch wenn das Axiom Strong Collection eine Schema ist, das über Klassen Aussagen trifft. A modelliert zweitstufige Strong Collection also in dem Sinne, dass die zweitstufigen Quantoren über die Teilmengen von A, nicht die Teilklassen laufen sollten — was allerdings wohl sowieso die natürlichere Wahl ist.

Es werden mitunter auch Varianten betrachtet, in denen A nicht zweitstufige Strong Collection, sondern nur zweitstufige Ersetzung oder zweitstufige Collection modellieren soll [1], diese sind jedoch weniger üblich, wenn auch kaum schwächer.

Beispielsweise heißt eine Menge A **schwach regulär**, wenn sie bewohnt und transitiv ist und zweitstufige Collection modelliert, also wenn gilt:

$$\forall a \in A \forall R \subseteq a \times A.\, R : a \rightrightarrows A \to \exists b \in A\, R : a \rightrightarrows b$$

Man kann nun die folgenden Aussage betrachten:

wREA $\forall a \exists A \ni a.\ A$ schwach regulär

REA $\forall a \exists A \ni a.\ A$ regulär

Das folgende Lemma ist eine leichte Verallgemeinerung des Resultats in [22], aber bis auf unwesentliche Änderungen, die auf unsere abweichende Definition von $V(S)$ zurückzuführen sind, verläuft der Beweis genauso. Das Lemma sagt aus, dass der Schnitt einer (schwach) regulären Menge mit unserem Modell wieder eine Menge bildet; dies ist nicht trivial, da $x \in V(S)$ ja keine beschränkte Aussage ist.

Lemma 81. *Ist B schwach reguläre Menge, so ist $B \cap V(S)$ eine Menge.*

Beweis. Sei $\kappa = rk(B) \in On$. Betrachte die induktive Definition

$$\Phi = \{(x,a) | a \subseteq S \times x \wedge \forall y \in Bi(a)\, a^{-1}y = {}^{\lhd}a^{-1}y\}$$

mit den zugehörigen

$$V(S)^{\alpha} = \Gamma_{\Phi}(\hat{\bigcup}_{\beta \in \alpha} V(S)^{\beta}),$$

wobei

$$\Gamma_{\Phi}(X) = \{a | \exists x \subseteq X.(x,a) \in \Phi\}$$

Man betrachte nun die leicht veränderte induktive Definition

$$\Phi' := \{(x,y) | (x,y) \in \Phi \wedge y \in B\}$$

mit zugehörigen $J^\alpha = \Gamma_{\Phi'}(\hat{\bigcup}_{\beta\in\alpha} J^\beta)$, wobei

$$\Gamma_{\Phi'}(X) = \{a\in B | \exists x \subseteq X.(x,a)\in\Phi\}$$

Man beachte, dass die J^α Mengen sind (wie man durch Induktion sofort sieht, hierbei geht die Separiertheit der formalen Topologie ein).

Es genügt zu zeigen, dass

$$\forall \alpha \in On\, V(S)^\alpha \cap B \subseteq \hat{\bigcup}_{\nu\in\kappa} J^\nu$$

Denn dann gilt Gleichheit und die linke Seite ist also eine Menge.

Dies soll durch Induktion über α geschehen. Sei die Aussage für $\beta\in\alpha$ also schon gezeigt. Sei $c\in V(S)^\alpha$ und $c\in B$. Insbesondere

$$c \subseteq S \times \hat{\bigcup}_{\beta\in\alpha} (V(S)^\beta \cap B)$$

Denn wegen der Transitivität von B sind die Elemente der Rechtsprojektion von c wieder in B. Nach Induktionsvoraussetzung ist aber

$$V(S)^\beta \cap B \subseteq \hat{\bigcup}_{\nu\in\kappa} J^\nu$$

Also existiert für jedes $x\in c$ ein $e\in S$ und ein $\nu\in\kappa$ mit $x = (e,b)$ für $b\in J^\nu \subseteq B$. Da $\kappa = rk(B) = \bigcap_{b'\in B} rk(b')$, gilt sogar

$$\forall x\in c \exists e\in S \exists b', b\in B. b\in J^{rk(b')} \wedge x = (e,b)$$

Da B schwach regulär ist, kann man die b' in einer Menge in B sammeln (denn $\{(x,b')\in c\times B | \exists e\in S \exists b\in B. b\in J^{rk(b')} \wedge x = (e,b)\}$ ist eine Menge, da die J^ζ Mengen sind), man erhält also ein $d\in B$ mit

$$\forall x\in c \exists e\in S, b\in B, b'\in d. b\in J^{rk(b')} \wedge x = (e,b)$$

Also folgt

$$c \subseteq S \times \hat{\bigcup}_{\gamma\in rk(d)} J^\gamma$$

Und da c die Bedingung über die Abgeschlossenheit bezüglich $\lhd$ erfüllt folgt

$$c\in J^{rk(d)} \subseteq \hat{\bigcup}_{\nu\in\kappa} J^\nu$$

Q.E.D.

Damit können wir die Absolutheit von REA zeigen. Der Beweisaufbau hat leichte Ähnlichkeiten mit [22], wo der zweite Teil des Theorems für Realisierbarkeit mit applikativen Strukturen nachgewiesen wird. Nach Kenntnisstand des Autoren ist die Absolutheit von REA für Heyting-Algebra-bewertete Modelle mit mengenartiger formaler Topologie neu. Der erste Teil des Theorems ist nach dem Wissen des Autoren zwar auch selbst für Realisierbarkeit mit applikativen Strukturen neu, jedoch ist seine Aussage nach den Ergebnissen von [22] keinesfalls erstaunlich und die dortigen Beweise könnten sehr leicht adaptiert werden, um die Aussage für wREA zu erhalten.

Theorem 82. *Sei S eine starke applikative Topologie.*

1. $CZF \vdash (wREA \rightarrow \Vdash wREA)$
2. $CZF \vdash (REA \rightarrow \Vdash REA)$

Beweis.

1. Angenommen wREA. Man setze

$$e := p(p(pke_r)(\lambda xy.pke_r))(\lambda xyz.yz)$$

Wir zeigen, dass e realisiert, dass es für alle a ein C gibt so dass $a \in C$ und

$$\forall x \in C \forall y \in x y \in C \wedge \forall r \forall a \in C. \forall x \in a \exists y \in C \phi(x, y, r) \rightarrow \exists b \in C \forall x \in a \exists y \in b \phi(x, y, r)$$

Hierbei setzt man

$$\phi(x, y, r) :\leftrightarrow ((x, y) \in r \wedge r : a \rightrightarrows C)$$

Rathjen verwendet in seinem Beweis beliebiges ϕ, allerdings bilden die Realisierer von einer solchen Formel nicht unbedingt eine Menge, so dass REA in diesem Fall nicht anwendbar ist. Allerdings ist dies nicht schlimm, da die oben getroffene spezielle Wahl von ϕ die einzige ist, die für den Beweis des Theorems tatsächlich benötigt wird.

Sei also $a \in V(S)$. Sei B eine reguläre Menge, die a, S, $r[S]$ und 2 enthält. Letzteres impliziert wegen der Regularität, dass B abgeschlossen unter Paaren ist.

Sei

$$C := S(\{(k, x) | x \in B \cap V(S)\}) \in V(S)$$

nach dem letzten Lemma. Es wird gezeigt, dass dann e die folgende Aussage realisiert:

$$a \in C \wedge \forall x \in C \forall y \in x y \in C \wedge \forall a \in C. \forall r \forall x \in a \exists y \in C \phi(x, y, r) \rightarrow \exists b \in C \forall x \in a \exists y \in b \phi(x, y, r)$$

Wir zeigen die drei Konjunkte einzeln:

(a) Dies gilt trivialerweise wegen $(k, a) \in C$:

$$lle \trianglelefteq pke_r \Vdash a \in C$$

(b) Sei $(f, x) \in C$, $(g, y) \in x$. Dann ist $x \in B \cap V(S)$. Wegen Transitivität von B und Definition von $V(S)$ also auch $y \in B \cap V(S)$ und somit $(k, y) \in C$. Daher gilt

$$r(le)fg \trianglelefteq pke_r \Vdash y \in C$$

(c) Sei $r \in V(S)$, $(f,a) \in C$. Sei

$$g \Vdash \forall x \in a \exists y \in C \phi(x,y,u)$$

Das bedeutet

$$\forall (h,x) \in a \exists u \in r[S].gh \lhd u \wedge \forall j \in u \exists (i,y) \in C.i = j \wedge j \Vdash \phi(x,y,u)$$

Die schwache Regulärität erlaubt uns, die (i,y) in einem b' zu sammeln, denn für die u aus der Formel gilt $u \in B$ und $i = j \wedge j \Vdash \phi(x,y,u)$ ist äquivalent zur Zugehörigkeit zu einer bestimmten Menge, da ϕ beschränkt ist und somit $[\![\phi]\!]$ eine Menge ist. Also

$$\forall (h,x) \in a \exists u \in r[S].gh \lhd u \wedge \exists b' \in B \forall j \in u \exists (i,y) \in b'.i = j \wedge j \Vdash \phi(x,y,u)$$

Unter Beachtung der Tatsache, dass man $b' \in V(S)$ wählen kann, lässt sich dies umformen zu

$$\forall (h,x) \in a \exists b' \in C \exists u \in r[S] \forall j \in u \exists (i,y) \in b'.gh \lhd u \wedge i = j \wedge j \Vdash \phi(x,y,u) \wedge b' \in V(S)$$

Worauf man nochmals die schwache Regularität anwenden kann. Man erhält die Existenz eines $b'* \in C$, so dass

$$\forall (h,x) \in a \exists b' \in b'* \exists u \in r[S] \forall j \in u \exists (i,y) \in b'.gh \lhd u \wedge i = j \wedge j \Vdash \phi(x,y,u) \wedge b' \in V(S)$$

Ohne Einschränkung sei $b'* \subseteq V(S)$. Man definiere nun

$$b := \{(i,y) | \exists b' \in b' * (i,y) \in b'\} \in V(S)$$

Wir wollen zeigen, dass

$$refg \unlhd \lambda x.gx \Vdash \forall x \in a \exists y \in b \phi(x,y,r)$$

Sei also $(h,x) \in a$. Dann gibt es ein $b' \in b'*$ mit

$$\exists u \in r[S] \forall j \in u \exists (i,y) \in b'.gh \lhd u \wedge i = j \wedge j \Vdash \phi(x,y,u) \wedge b' \in V(S)$$

Insbesondere

$$\exists u \in r[S] \forall j \in u \exists (i,y) \in b.gh \lhd u \wedge i = j \wedge j \Vdash \phi(x,y,u) \wedge b' \in V(S)$$

Also

$$gh \Vdash \exists y \in b \phi(x,y,u)$$

2. Angenommen REA. Es wird behauptet, dass mit

$$e := p(p(pke_r)(\lambda xy.pke_r))(\lambda xy.p(\lambda z.yz)(\lambda z.rz))$$

gilt, dass e realisiert, dass es für jedes a ein C gibt mit:

$$(a \in C \wedge \forall x \in C \forall y \in xy \in C) \wedge \forall r \forall a \in C.\forall x \in a \exists y \in C \phi(x,y,r) \rightarrow$$

$$\exists b \in C.\forall x \in a \exists y \in b \phi(x,y,r) \wedge \forall y \in b \exists x \in a \phi(x,y,r))$$

Die ersten beiden Konjunkte gelten ganz analog zum vorigen Fall wREA. Das dritte ist allerdings komplexer, dennoch wird versucht, die Parallelen zum ersten Teil des Theorems zu Tage treten zu lassen:

Sei $r \in V(S)$, $(f,a) \in C$. Sei

$$g \Vdash \forall x \in a \exists y \in C \phi(x,y,u)$$

Das bedeutet

$$\forall (h,x) \in a \exists u \in r[S].gh \lhd u \wedge \forall j \in u \exists (i,y) \in C.i = j \wedge j \Vdash \phi(x,y,u)$$

Die Regularität erlaubt uns ähnlich wie zuvor, die (ϕ, y) in einem b' zu sammeln. Also

$$\forall (h,x) \in a \exists u \in r[S].gh \lhd u \wedge \exists b' \in B.\forall j \in u \exists (i,y) \in b'$$

$$(i \unlhd phj \wedge j \Vdash \phi(x,y,u)) \wedge \forall (i,y) \in b' \exists j \in u (i \unlhd phj \wedge j \Vdash \phi(x,y,u))$$

Unter Beachtung der Tatsache, dass man $b' \in V(S)$ wählen kann, lässt sich dies umformen zu

$$\forall (h,x) \in a \exists b' \in B \exists u \in r[S].$$

$$\forall j \in u \exists (i,y) \in b' (gh \lhd u \wedge i \unlhd phj \wedge j \Vdash \phi(x,y,u) \wedge b' \in V(S)) \wedge \forall (i,y) \in b' \exists j \in u$$

$$(gh \lhd u \wedge i \unlhd phj \wedge j \Vdash \phi(x,y,u)) \wedge b' \in V(S)$$

Woraufhin man nochmals die schwache Regularität ausnutzen kann. Man erhält die Existenz eines $b'* \in C$, so dass

$$\forall (h,x) \in a \exists b' \in b' * \exists u \in r[S].$$

$$\forall j \in u \exists (i,y) \in b' (gh \lhd u \wedge i \unlhd phj \wedge j \Vdash \phi(x,y,u) \wedge b' \in V(S)) \wedge \forall (i,y) \in b' \exists j \in u$$

$$(gh \lhd u \wedge i \unlhd phj \wedge j \Vdash \phi(x,y,u)) \wedge b' \in V(S)$$

und

$$\forall b' \in b' * \exists (h,x) \in a \exists u \in r[S].$$

$$\forall j \in u \exists (i,y) \in b' (gh \lhd u \wedge i \unlhd phj \wedge j \Vdash \phi(x,y,u) \wedge b' \in V(S)) \wedge \forall (i,y) \in b' \exists j \in u.$$

$$(gh \lhd u \wedge i \unlhd phj \wedge j \Vdash \phi(x,y,u)) \wedge b' \in V(S)$$

Ohne Einschränkung sei $b'* \subseteq V(S)$. Man definiere nun

$$b := \{(i,y) | \exists b' \in b' * (i,y) \in b'\} \in V(S)$$

Wie oben zeigt man, dass

$$l(refg) \unlhd \lambda x.gx \Vdash \forall x \in a \exists y \in b \phi(x,y,r)$$

Wir möchten noch zeigen, dass

$$l(refg) \unlhd \lambda x.rx \Vdash \forall y \in b \exists x \in a \phi(x,y,r)$$

Sei dazu $(i,y)\in b$, also

$$\exists b'\in b' * (i,y)\in b'$$

Für dieses b' gibt es dann ein $(h,x)\in a$ und ein $u\in r[S]$ so dass

$$\forall j\in u\exists(i',y')\in b'.gh \lhd u \wedge i' \unlhd phj \wedge (j \Vdash \phi(x,y',u)) \wedge b'\in V(S)$$

$$\forall(i',y')\in b'\exists j\in u.gh \lhd u \wedge i' \unlhd phj \wedge (j \Vdash \phi(x,y',u)) \wedge b'\in V(S)$$

Insbesondere für eben jenes $(i,y)\in b'$

$$\exists u\in r[S]\exists j\in u(gh \lhd u \wedge i = phj \wedge j \Vdash \phi(x,y,u)) \wedge b'\in V(S)$$

Daher gibt es ein j mit $j \Vdash \phi(x,y,u)$ und $i \unlhd phj$. Also

$$ri \unlhd j \Vdash \phi(x,y,u)$$

Q.E.D.

4.4.2 Absolutheit für natürliche Zahlen

Bekanntermaßen ([26]) können schon viel schwächere Theorien als CZF über primitiv rekursive Relationen natürlicher Zahlen sprechen und diese sind in CZF repräsentiert, d.h. zu jeder solchen Relation gibt es eine Formel $\phi(x,y)$, so dass

$$CZF \vdash \phi(\bar{\bar{n}}, \bar{\bar{m}})$$

genau dann, wenn n und m in der Relation stehen. Dabei ist $\bar{\bar{n}}$ der die metatheoretische natürliche Zahl n bezeichnende Term von CZF, also

$$\bar{\bar{0}} = \emptyset, n \bar{\bar{+}} 1 = \bar{\bar{n}} \cup \{\bar{\bar{n}}\}$$

Wir wollen Aussagen über die Absolutheit dieser Formeln machen und einen kanonischen Realisierer dafür finden. Dies skizziert auch McCarty ([20]), der allerdings eine starke Metatheorie verwenden zu scheint (insbesondere wendet er nicht viel Aufmerksamkeit auf die Unterschiede zwischen metatheoretisch definierten Termen $\bar{\bar{m}}$ und natürlichen Zahlen, über die man in CZF quantifizieren könnte auf, so dass die Aussage, die er eigentlich beweist, viel zu schwach ist, um daraus die Folgerungen zu ziehen, der er ziehen will, etwa die Realisiertheit der Church'schen These in V(Kl)). Deshalb werden die hier wiedergegebenen Argumente völlig neu sein.

Die folgenden Formeln sind Repräsentanten der primitiv rekursiver Funktionen:

Definition 83. *Die primitiv rekursiven Formeln* $\phi(\vec{n}, m)$[11] *sind rekursiv definiert*[12]*:*

[11] Für primitiv rekursive Formeln oder Kandidaten für solche sollen die angegebenen Variablen die einzigen freien sein. Die Reihenfolge ist nicht unerheblich, das heißt, eigentlich ist eine primitiv rekursive Formel als syntaktisches Objekt nicht nur eine Formel, sondern eine Formel mit einer totalen Ordnung ihrer Variablen.

[12] Wie stets ist gebundene Umbenennung durchzuführen, um unbeabsichtigte doppelte Quantifizierung über eine Variable zu vermeiden.

1. $\phi(\vec{n}, m) \equiv m = n_i \wedge \vec{n} \in \omega$ *ist eine primitiv rekursive Formel für* $i \in lh(\vec{n})$.
2. $\phi(\vec{n}, m) \equiv m = 0 \wedge \vec{n} \in \omega$ *ist eine primitiv rekursive Formel.*
3. $\phi(n, m) \equiv m = n + 1 \wedge \vec{n} \in \omega$ *ist eine primitiv rekursive Formel.*
4. *Sind* $\phi(n_0, ..., n_N, m), \psi_i(\vec{n'}, m))$ *primitiv rekursive Formeln für* $i = 0...N$, *so ist auch*

$$\phi'(\vec{n'}, m) \equiv \exists v_0...v_N. \bigwedge_{i=0...N} \psi_i(\vec{n'}, v_i) \wedge \phi(v_0, ..., v_N, m)$$

eine primitiv rekursive Formel. Dabei ist die Länge von $\vec{n'}$ *unabhängig von* N.

5. *Sind* $\phi(\vec{n}, m), \psi(n, n', \vec{n}, m)$ *primitiv rekursive Formeln, so auch*

$$\exists F. \forall v(\phi(\vec{n}, v) \rightarrow (0, v) \in F) \wedge \forall i, v, w((i, v) \in F \rightarrow \psi(v, i, \vec{n}, w) \leftrightarrow (i+1, w) \in F) \wedge (n, m) \in F$$

wobei die Reihenfolge der freien Variablen $(n, \vec{n}, m)$ *sein soll.*

Lemma 84. *Sei* $\phi(\vec{n}, m)$ *primitiv rekursiv. Dann sind in CZF herleitbar:*

$$\forall \vec{n} \in \omega \exists ! m \in \omega\ \phi(\vec{n}, m)$$

$$\forall \vec{n}, m.\ \phi(\vec{n}, m) \vee \neg\phi(\vec{n}, m)$$

Beweis. Klar nach Induktion über die Eigenschaft, primitiv rekursiv zu sein unter Beachtung der Diskretheit der natürlichen Zahlen für die Entscheidbarkeit der primitiv rekursiven Formeln. q.e.d.

Wäre die Klausel für die primitive Rekursion auf $F \subseteq \omega \times \omega$ beschränkt worden, hätte man auch ableiten können

$$\forall \vec{n}, m.\ \phi(\vec{n}, m) \rightarrow \vec{n}, m \in \omega$$

Dies hätte aber die folgenden Beweise etwas umständlicher (wenn auch nicht konzeptuell schwieriger) gemacht.

Wir werden im Folgenden verwenden, dass dies eine Repräsentation der primitiv rekursiven Funktionen darstellt, wie man leicht sieht.

Eine Erweiterung der primitiv rekursiven Formeln sind die fast negativen arithmetischen Formeln. Die folgende Definition entspricht der aus [22] (bis auf logische Äquivalenz):

Definition 85. *der* ***ana-Formeln*** *(almost negative arithmetic).*

1. *Sei* $\phi(\vec{n}, m)$ *primitiv rekursiv, so ist dies eine ana-Formel, und auch*

$$\exists n_i \in \omega \phi(\vec{n}, m)$$

ist eine ana-Formel.

2. *Sind* ϕ *und* ψ *ana, so sind auch*

$$\neg\phi$$

$$\phi \wedge \psi$$

$$\phi \rightarrow \psi$$

$$\forall n \in \omega \phi$$

ana-Formeln.

Formeln, die von natürlichen Zahlen handeln, erlauben einen stärkeren Absolutheitsbegriff, nämlich Absolutheit mit einem kanonischen Realisierer, die nun definiert werden soll.

Definition 86. *Sei ϕ eine Formel mit freien Variablen $n_0, ..., n_N$. Dann heißt ϕ* ***natürlich absolut****, falls sich in CZF herleiten lässt: $\exists e \in \nabla$, so dass für alle $n_0 ... n_N \in \omega$ äquivalent sind:*

1. $\phi(n_0, ..., n_N)$
2. $e\underline{n_0}...\underline{n_n} \Vdash \phi[\bar{n_0}, ..., \bar{n_N}]$
3. $\Vdash \phi[\bar{n_0}, ..., \bar{n_N}]$

Die folgende Aussage ist verwandt mit Theorem 8.7 in [22], das allerdings nur von Realisierbarkeit über $V(Kl)$ handelt. Am wichtigsten ist wohl die Aussage über primitiv-rekursive Formeln.

Theorem 87. *Jede Formel aus der Gesamtheit an Formeln, die folgende Eigenschaften erfüllt, ist natürlich absolut:*

- *Alle primitiv rekursiven Formeln gehören zu der Gesamtheit.*
- *Falls MP_{pr} gilt*[13] *oder falls jede Menge, die ein Element von ∇ überdeckt, bewohnt ist, gehören alle existenzquantifizierten primitiv-rekursive Formeln zu der Gesamtheit.*
- *Die Gesamtheit ist bezüglich Konjunktion und Allquantifikation abgeschlossen.*
- *Falls jedes Element von S entweder in ∇ liegt oder von der leeren Menge überdeckt wird, ist die Gesamtheit bezüglich Implikation und Verneinung abgeschlossen.*

Falls die Bedingungen aus 2 und 4 beide erfüllt sind, sind dies genau die ana-Formeln.

Der erste Punkt, dass primitiv rekursive Formeln natürlich absolut sind, ist dabei wohl der wichtigste.

Beweis. Induktion über die Eigenschaft von ϕ, ana-Formel zu sein.

1. Für den Induktionsanfang, dass $\phi(\vec{n}, m)$ primitiv rekursiv ist, konstruieren wir durch Induktion über die Definition der primitive Rekursivität ein solches e:

   (a) Für die Projektionsfunktion $m = n_i \wedge \vec{n} \in \omega$ ist dies

   $$e := \lambda \vec{v} w.p(p(\lambda x.pxe_r)(\lambda x.px_r))e'$$

   wobei e' eine einfach zu konstruierende Zusammensetzung aus pv_ie_r ist. Falls tatsächlich $m = n_i$ ist, so wird die Aussage für die Internalisierungen offenbar von $p(\lambda x.pxe_r)(\lambda x.px_r)$ realisiert, und wenn es

[13] Dies ist das Schema

$$\neg\nexists x \in \omega\phi \to \exists x \in \omega\phi$$

für primitiv rekursive Formeln ϕ. Es handelt sich hierbei um ein sowohl klassisch als auch rekursiv gültiges Prinzip.

davon realisiert ist, ist es natürlich auch irgendwie realisiert. Ist es aber realisiert, so gilt es auch in V:

Dass $(\Vdash \bar{n} = \bar{m}) \rightarrow n = m$ gilt, sieht man beispielsweise durch Induktion über $min(n, m)$. Der Induktionsanfang wird im nächsten Punkt gezeigt. Der Induktionsschritt ergibt sich daraus, dass $(\Vdash \bar{n} = \bar{m})$ impliziert, dass

$$\forall n' \in n \exists m' \in m \Vdash \bar{n'} = \bar{m'} \wedge \forall m' \in m \exists n' \in n \Vdash \bar{n'} = \bar{m'}$$

(b) Für die Nullfunktion $m = 0 \wedge \vec{n} \in \omega$ setze man[14]

$$e := \lambda \vec{v} w.p(\lambda x.k)e'$$

mit gleichem e' wie oben. Falls nämlich $\bar{m} = \bar{0} = \emptyset$, so gilt offenbar

$$\lambda x.k \Vdash \forall x \in \bar{0} \bot$$

da der Quantor leer läuft. Falls dies aber gilt, so gibt es überhaupt einen Realisierer in ∇ für die Formel $\forall x \in \bar{m} \bot$. Existiert aber so einer, dann gibt es ein Element aus ∇, das angewandt auf jeden Grund, warum etwas in $\bar{m}$ liegt, von der leeren Menge überdeckt würde. Dann kann dieser Grund also nicht in ∇ gelegen haben, daher muss $\bar{m} = \bar{0} = \emptyset$ gelten.

(c) Nun zur Nachfolgerfunktion $m = n_i + 1 \wedge \vec{n} \in \omega$. Hier sei

$$e := \lambda \vec{v} w.p(e_+ v_i)e'$$

wobei e' wieder wie zuvor und e_+ wie im Hilfssatz 70 für den Beweis der Realisiertheit des Unendlichkeitsaxioms ist. Der Hilfssatz sagt, dass falls $m = n + 1$, dann folgt

$$m = n + 1 \rightarrow e_+ \underline{n} \Vdash \bar{m} = \bar{n} + 1$$

Dann gibt es natürlich auch irgendeinen Realisierer in ∇. Nun ist noch zu zeigen, dass gilt

$$\exists f \in \nabla f \Vdash \bar{n} = \bar{m} + 1 \rightarrow n = m + 1$$

Aber es gibt ja einen Realisierer aus ∇ für $\overline{m+1} = \bar{m}+1$, nämlich e_+, also gibt es in dieser Situation einen Realisierer aus ∇ für $\overline{m+1} = \bar{n}$. Nach dem ersten Induktionsanfang folgt $n = m + 1$

(d) Nun zur primitiv rekursiven Formel

$$\phi(\vec{n'}, m) \equiv \exists v_0 ... v_N . \bigwedge i = 0 ... N \psi_i(\vec{n'}, v_i) \wedge \phi'(v_0, ..., v_N, m)$$

Wobei e' zu ϕ' und e_i zu ψ_i für alle passenden i nach Induktionsvoraussetzung wie im Theorem gefordert sind. Nach dem Lemma über primitiv rekursive Formeln kann man in CZF herleiten, dass es zu

[14]Die Formel x=0, die ja formal nicht der Sprache von CZF zugehörig ist, sei als $\forall y \in x \bot$ ausgeschrieben.

$\vec{n}\in\omega$ genau ein m gibt mit $\psi_i(\vec{n}, m)$. Sei also deswegen nach Konsistenzsatz und Voraussetzung f_i so, dass

$$\forall \vec{n}, m\in\omega.\psi_i(\vec{n}, m) \to f_i\underline{\vec{n}} \trianglelefteq \underline{m}$$

Dann kann man e wählen als

$$e := \lambda\vec{x}w.p(e_0\vec{x}f_0\vec{x})(p(e_1\vec{x}f_1\vec{x})(...p(e_N\vec{x}f_N\vec{x})(e'\vec{f}\vec{x}w)...))$$

Sei nun $\phi(\vec{n'}, m)$, das heißt (mit dem Lemma über primitiv rekursive Funktionen)

$$\exists v_0...v_N\in\omega.\bigwedge i = 0...N\psi_i(\vec{n'}, v_i) \wedge \phi'(v_0, ..., v_N, m)$$

Für solche $v_0, ..., v_N$ realisiert nach Induktionsvoraussetzung und den Annahmen über $\vec{f}$

$$p(e_0\underline{\vec{n'}}f_0\underline{\vec{n'}})(p(e_1\underline{\vec{n'}}f_1\underline{\vec{n'}})(...p(e_N\underline{\vec{n'}}f_N\underline{\vec{n'}})(e'\vec{f}\vec{x}w)))$$

die Formel

$$\bigwedge i = 0...N\psi_i(\vec{\bar{n'}}, \bar{v_i}) \wedge \phi'(\bar{v_0}, ..., \bar{v_N}, \bar{m})$$

Insbesondere gilt dann

$$e\underline{\vec{n'}m} \Vdash \phi(\vec{\bar{n'}}, \bar{m})$$

Ist dies der Fall, so ist diese Formel natürlich überhaupt durch ein Element von ∇ realisiert. Dann folgt mit Konsistenzsatz und dem Lemma zu primitiv rekursiven Funktionen auch

$$\exists v_0...v_N.\bigwedge i = 0...N\psi_i(\underline{\vec{n'}}, v_i) \wedge \phi'(v_0, ..., v_N, \underline{m})$$

Der Realisierer ist überdeckt von denjenigen Realisierern, zu denen es $v_0, ...\in\bar{\omega}$ gibt, so dass etwas bestimmtes gilt. Aber ∇ ist nicht von der leeren Menge überdeckt, also gilt insbesondere:
Es gibt nicht nicht $(g_i, \bar{v_i})\in\omega$ mit $\nabla \ni g_i \trianglelefteq \underline{v_i}$ so dass realisiert ist

$$\bigwedge i = 0...N\psi_i(\underline{\vec{n'}}, v_i) \wedge \phi'(v_0, ..., v_N, \underline{m})$$

Dies soll abgekürzt werden mit $\neg\neg A$. Angenommen, es gälte A. Nach Induktionsvoraussetzung wäre dann

$$\bigwedge i = 0...N\psi_i(\vec{n'}, v_i) \wedge \phi'(v_0, ..., v_N, m)$$

Also wäre

$$\phi(\vec{n'}, m)$$

Darum gilt

$$\neg\neg\phi(\vec{n'}, m)$$

Denn allgemein folgt aus $\neg\neg A$ und $A \to B$ auch $\neg\neg B$ (denn: Angenommen es sei $\neg B$. Dann $\neg A$. Widerspruch!). Aber nach dem Lemma zu primitiv rekursiven Funktionen folgt

$$\phi(\vec{n'}, m)$$

(e) Der letzte Fall ist die primitive Rekursion. Sei also die Formel $\phi(n, \vec{n}, m)$ gleich

$$\exists F.\forall v(\phi'(\vec{n}, v) \to (0, v) \in F) \wedge \forall i, v, w((i, v) \in F \to \psi(v, i, \vec{n}, w) \leftrightarrow (i{+}1, w) \in F) \wedge (n, m) \in F$$

Wähle nach Induktionsvoraussetzung e_ψ und nach Induktionsvoraussetzung und dem Lemma über primitiv rekursive Funktionen und e_1, e_2, e' und e'' so, dass die Allabschlüsse der folgenden Formeln gelten[15]

$$\phi'(\vec{n}, m) \to e'\underline{\vec{n}} \trianglelefteq \underline{m}$$

$$\psi(\vec{n}, m) \to e''\underline{\vec{n}} \trianglelefteq \underline{m}$$

$$(h \Vdash \phi'(\vec{\bar{n}}, a)) \to \phi'(\vec{n}, m) \to e_1 h \underline{\vec{n}} \Vdash a = \bar{m}$$

$$(h \Vdash \psi(\vec{\bar{n}}, a)) \to \psi(\vec{n}, m) \to e_2 h \underline{\vec{n}} \Vdash a = \bar{m}$$

Sei außerdem

$$e_{()} \Vdash \forall a, b, b'.b = b' \to \langle a, b\rangle = \langle a, b'\rangle$$

Eine mögliche Wahl für e wäre dann der etwas längliche Realisierer

$$e := \lambda v\vec{v}w.pi_0(p(\lambda x.pi_1 i_2)i_3)$$

mit

$$i_0 := \lambda x.p(p\underline{0}(e'\vec{v}))(e_{()}(e_1 x\vec{v}))$$

$$i_1 := \lambda y.p(p(s_N(l(lx)))(e''(r(lx))(l(lx))\vec{v}))(e_{()}(e_2 y\vec{v}))$$

$$i_2 := \lambda y.e_\psi(l(lx))(r(lx))\vec{v}(r(l(y))$$

$$i_3 := p(pvw)e_r$$

Gelte $\phi(n, \vec{n}, m)$ und sei F' so, dass

$$\forall v(\phi'(\vec{n'}, v) \to (0, v) \in F') \wedge \forall i, v, w((i, v) \in F' \to (\psi(v, i, \vec{n}, w) \leftrightarrow (i{+}1, w) \in F')) \wedge (n, m) \in F$$

Definiere

$$F := \{(p i \underline{v}, \langle \bar{i}, \bar{v}\rangle) | (i, v) \in F\}$$

Es ist zu zeigen

$$e \Vdash \forall v(\phi'(\vec{\bar{n}}, v) \to \langle 0, v\rangle \in F) \wedge \forall i, v, w(\langle i, v\rangle \in F \to \psi(v, i, \vec{\bar{n}}, w) \leftrightarrow \langle i{+}1, w\rangle \in F) \wedge (n, m) \in F$$

Zum ersten Konjunkt: Sei m' die Zahl, so dass $\phi'(\vec{n}, m')$ gilt (also auch $e'\vec{n} \trianglelefteq \underline{m'}$), dann ist für

$$v \in V(S), g \Vdash \phi'(\vec{\bar{n}}, v)$$

wegen der Wahl von e_1

$$p(p\underline{0}(e'\vec{v}))(e_{()}(e_1 g\vec{v})) \Vdash \langle 0, v\rangle \in F$$

[15] Die Benennung der (gebundenen) Variablen ist für die folgenden vier Formeln anders als im Folgenden, um ihre Bedeutung besser zu Tage treten zu lassen

Nun zum zweiten Konjunkt (Hinrichtung): Seien $i, v, w \in V(S)$. Man kann ohne Einschränkung annehmen, dass $i, v, w \in \bar{\omega}$, denn äquivalent zu der obigen Aussage ist ja die Aussage, in der i,v und w auf ω beschränkt werden[16]. Seien also

$$i = \bar{i'}, v = \bar{v'}, w = \bar{w'}$$

Sei m' die Zahl, so dass $\psi(v', i', \vec{n}, m')$ gilt. Sei außerdem

$$(g \Vdash \langle i, v \rangle \in F), (g' \Vdash \psi(v, i, \vec{\bar{n}}, w)$$

Dann ist

$$p(l(lg))(r(lg)) \trianglelefteq p\underline{i'}\underline{v'}$$

Es gilt wegen der Wahl von e_2

$$\begin{aligned} p(p(s_N(l(lg)))(e''(r(lg))(l(lg))\vec{v}))(e_{()}(e_2 g'\vec{v})) \\ \trianglelefteq p(p\underline{i'}(e''(\underline{v'}\,\underline{i'}\vec{v})))(e_{()}(e_2 g'\vec{v})) \\ \Vdash \langle i+1, w \rangle \in F \end{aligned}$$

Nun zur Rückrichtung des zweiten Konjunkts: Seien i', v', w' wie oben. Sei

$$(g \Vdash \langle i, v \rangle \in F), (g' \Vdash \langle i+1, w \rangle \in F)$$

Es ist

$$p(l(lg'))(r(lg')) \trianglelefteq p\underline{i+1'}\underline{w'}$$

Nach dem schon mehrmals verwendetem Schluss gilt

$$g \lhd \{g | (i', v') \in F\}$$

$$g' \lhd \{g | (i'+1, w') \in F\}$$

Also reicht es, die Aussage

$$e_\psi(l(lg))(r(lg))\vec{v}(r(l(g')) \Vdash \psi(v, i, \vec{\bar{n}}, w)$$

unter der Bedingung zu zeigen, dass $(i', v') \in F$ und $(i'+1), w' \in F$. Dann aber ist $\psi(v', i', \vec{n}, w')$ im Grundmodell erfüllt, und die Aussage folgt direkt aus der Eigenschaft von ψ und den oben gegebenen Gleichungen über die Denotation der Terme $l(lg))$ etc.

[16]Genauer: Für die Frage, ob es ein konstruierbares $e \in \nabla$ gibt, das die Formel realisiert, genügt es, ein angebbares $e \in \nabla$ zu finden, das die Formel mit dieser leichten Veränderung der Realisierbarkeitsdefinition realisiert. Denn damit zeigt man, dass der Realisierer, den man aus dem für die ursprüngliche Formel mit Veränderung der Definition gefunden hat, verändert werden kann (indem im Term an geeigneter Stelle t durch $\lambda xyz.t$ mit $x, y, z \notin FV(t)$ ersetzt wird), um die Formel, in der i, v, w auf $\bar{\omega}$ beschränkt ist, zu realisieren. Daraus erhält man aber einen Realisierer der äquivalenten Formel. Tatsächlich ist die gemachte Annahme nicht nur für die Frage nach der Existenz eines angebbaren $e \in \nabla$ ohne Einschränkung, sondern sogar das konkrete e wird davon nicht berührt. Dies ist aber weder wichtig noch leicht einzusehen.

2. Es gibt noch einen zweiten Induktionsanfang, nämlich dass die Formel die Gestalt

   $$\exists n\phi(n,\vec{n},m)$$

   hat, wobei ϕ eine primitiv rekursive Formel ist und es ohne Einschränkung ist, anzunehmen, dass die erste Variable existenzquantifiziert wurde[17]. Für eine solche Formel gilt: Es gibt nicht nur ein e_ϕ wie im Theorem, sondern auch ein $e'_\phi \in \nabla$, so dass die folgenden beiden Tatsachen gelten:

   $$\forall\vec{n},m.\phi(\vec{n},m) \rightarrow e'_\phi\underline{n_0}...\underline{n_n} \trianglelefteq l$$

   und

   $$\forall\vec{n},m.\neg\phi(\vec{n},m) \rightarrow e'_\phi\underline{n_0}...\underline{n_n} \trianglelefteq r$$

   wobei eine der beiden Voraussetzungen ja stets erfüllt ist. Dies sieht man direkt aus der soeben gezeigten Absolutheit von ϕ und der Ableitbarkeit von $\phi \vee \neg\phi$ in CZF.

   Die Idee dieses Beweises ist es, den Zeugen der Existenz durch Anwendung eines μ-Operators zu finden: Die kleinste Zahl, so dass e'_ϕ anzeigt, dass ϕ gilt. Setze

   $$\mu := \tau^{fix}[v_1 := \lambda vn\vec{n}m.D(e_\phi n\vec{n}m)n(v(s_N n)\vec{n}m)]$$

   Man wähle dann

   $$e := \lambda\underline{0}\vec{n}m.p(\mu n\vec{n}m)(e_\phi(\mu n\vec{n}m)\vec{n}m)$$

   Gelte dann $\phi(n,\vec{n},m)$ und sei $n \in \omega$ minimal mit dieser Eigenschaft [18]. Dann gilt

   $$D(e_\phi\underline{n'\vec{n}m})\underline{n'}(v(s_N\underline{n'})\underline{\vec{n'}m}) \trianglelefteq (v(\underline{n'+1}\underline{\vec{n'}m})$$

   für $n' \in n$ und

   $$D(e_\phi\underline{n'\vec{n}m})\underline{n'}(v(s_N\underline{n'})\underline{\vec{n'}m}) \trianglelefteq \underline{n'}$$

   für $n' = n$. Nach n Iterationen ergibt sich:

   $$\mu\underline{0\vec{n}m} \trianglelefteq \underline{n}$$

   Also gilt

   $$e\underline{\vec{n}m} \Vdash \exists n\in\omega\phi(n,\vec{\bar{n}},\bar{m})$$

[17] Man kann durch Induktion über die Eigenschaft, eine primitiv-rekursive Formel zu sein, zeigen: Ist $\phi(\vec{n},m)$ eine primitiv-rekursive Formel, so auch $\phi(\vec{n'},m))$ für alle $\vec{n'}$ Permutationen von $\vec{n}$.

[18] dies ist forderbar, da die Menge der n, die diese Eigenschaft erfüllen, eine abtrennbare Teilmenge der natürlichen Zahlen ist und jede bewohnte abtrennbare Teilmenge von ω ein kleinstes Element besitzt, wie man durch Induktion über den Zeugen für die Bewohntheit direkt sieht.

Dann ist dies also auch realisiert. Sei die Aussage umgekehrt realisiert durch ein $f \in \nabla$, so gilt

$$f \lhd \{h | \exists (lh, \bar{n}) \in \bar{\omega} rh \Vdash \phi(\bar{n}, \vec{\bar{n}}, \bar{m})\}$$

Insbesondere

$$f \lhd \{g | g \leq f \wedge \exists h.g \leq h \wedge \exists (lh, \bar{n}) \in \bar{\omega} rh \Vdash \phi(\bar{n}, \vec{\bar{n}}, \bar{m})\}$$

Also

$$f \lhd \{f | \exists (lf, \bar{n}) \in \bar{\omega} rf \Vdash \phi(\bar{n}, \vec{\bar{n}}, \bar{m})\}$$

Falls jede ein Element von ∇ überdeckende Menge bewohnt wäre, so wären wir fertig, denn rf überzeugt. Sonst wissen wir aber zumindest, dass diese Menge nichtleer ist, also gilt

$$\neg\neg\exists n \in \omega phi(n, \vec{n}, m)$$

Falls Markovs Prinzip für primitiv-rekursive Relationen gilt, folgt daraus das Gewünschte.

3. Falls die Formel die Gestalt $\neg\phi$ hat, so ist dies ein Sonderfall des übernächsten Falles.

4. Falls die Formel die Gestalt $\phi(\vec{n}, m) \wedge \psi(\vec{n}, m)$ hat, so wählt man als e einfach

$$e := \lambda \vec{v} w.p(e_\phi \vec{v} w)(e_\psi \vec{v} w)$$

Wobei e_ϕ und e_ψ wie nach Induktionsvoraussetzung sind. Die Behauptung ergibt sich direkt aus der Induktionsvoraussetzung.

5. Angenommen es sei $S = \nabla \cup \{e \in S | e \lhd \emptyset\}$. Falls die Formel die Gestalt $\phi(\vec{n}, m) \to \psi(\vec{n}, m)$ hat, so wählt man als e etwa

$$e := \lambda \vec{v} w.\lambda x.l(p(e_\psi \vec{v} w)x)$$

Wobei e_ψ wie nach Induktionsvoraussetzung ist. Falls dann

$$\phi(\vec{n}, m) \to \psi(\vec{n}, m)$$

und

$$g \Vdash \phi(\vec{\bar{n}}, \bar{m})$$

gelten und $g \in \nabla$, so ist dies realisiert und nach Induktionsvoraussetzung gilt

$$e\underline{\vec{n}m} \unlhd e_\psi \underline{\vec{n}m} \Vdash \psi(\vec{\bar{n}}, \bar{m})$$

Im anderen Fall, wenn $g \lhd \emptyset$, gilt auch

$$e\underline{\vec{n}m} \lhd \emptyset \subseteq [\![\psi(\vec{\bar{n}}, \bar{m})]\!]$$

6. Falls die Formel die Gestalt $\forall n \in \omega \phi(n, \vec{n}, m)$ hat[19], so wählt man als e etwa

$$e := \lambda \vec{v} w . \lambda x . x e_\psi \vec{v} w$$

Wobei e_ψ wie nach Induktionsvoraussetzung ist.

Gilt dann für alle $n \in \omega$ die Formel $\phi(n, \vec{n}, m)$, so also auch für alle $(f, \bar{n}) \in \bar{\omega}$ mit $f \trianglelefteq \underline{n}$ nach Induktionsvoraussetzung

$$e_\psi \underline{n \vec{n} m} \Vdash \phi(\bar{n}, \vec{\bar{n}}, \bar{m})$$

Also ist e wie gewünscht. Ist umgekehrt die Formel realisiert, so ist für alle $n \in \omega$

$$\Vdash \phi(\bar{n}, \vec{\bar{n}}, \bar{m})$$

und somit gilt die Formel nach Induktionsvoraussetzung auch in V.

Q.E.D.

Bemerkung 88. *1. Ein sofortiges Korollar ist: Falls jeder Realisierer aus ∇ stammt oder von der leeren Menge überdeckt wird, so ist MP_{pr} absolut.*

2. Applikative Topologien, die von applikativen Strukturen herrühren, haben die geforderten Eigenschaften, so dass bei ihnen jede ana-Formel absolut ist. Dies verwenden McCarty und Rathjen [20], [22] um die Church'sche These beziehungsweise eine Erweiterung davon in $V(Kl)$ zu realisieren. Die Eigenschaft, dass ein Element aus ∇ überdeckende Mengen bewohnt sind, haben zum Beispiel alle applikativen Topologien, die die Eigenschaft aufweisen, die später als unzerlegbar definiert wird.

4.5 Mengenuniversen

Definition 89. *Ein (Proto-)**Mengenuniversum** sei eine Klasse W zusammen mit einer zweistelligen Relation $\epsilon \subseteq W \times W$. Abbildungen zwischen Mengenuniversen, die ϵ erhalten, werden wie üblich als Homomorphismen von Mengenuniversen bezeichnet und Monomorphismus beziehungsweise Epimorphismus genannt, wenn sie injektiv beziehungsweise surjektiv sind.*

Mengenuniversen sind Strukturen, die Modelle von CZF sein könnten. Typische Beispiele sind V und $V(S)$ wobei $\forall x, y \in V(S). x \epsilon y :\leftrightarrow \Vdash x \in y$.

Die Abbildung $x \mapsto x^\nabla$ ist im allgemeinen kein Homomorphismus, da durchaus ein Element realisierterweise in x sein kann, ohne dass es gleich mit einem Grund aus ∇ darin liegt.

Proposition 90. *$F : x \mapsto x^k$ ist Monomorphismus von V nach $V(S)$.*

Beweis. Sei $x \in y$. Dann gilt

$$\nabla \ni pke_r \Vdash x^k \in y^k$$

Damit ist F Homomorphismus, und offensichtlicherweise Monomorphismus. Q.E.D.

Die Abbildung F erhält aber noch mehr Struktur:

[19] Wieder ist die Positionierung der Variablen ohne Einschränkung.

Theorem 91. *Es gilt für* $x, y \in V$

$$x = y \to \Vdash x^k = y^k$$

$$x \in y \to \Vdash x^k \in y^k$$

Und falls $\forall e \in \nabla . e \lhd p \to \exists f \in p \cap \nabla$ *gilt, so auch*

$$x = y \leftarrow \Vdash x^k = y^k$$

$$x \in y \leftarrow \Vdash x^k \in y^k$$

Sonst zumindest:

$$x \neq y \to \neg\neg \Vdash x^k \neq y^k$$

$$x \notin y \to \neg\neg \Vdash x^k \notin y^k$$

Beweis.

1. Die Aussage über $\in$ ist bereits gezeigt, und die über die Gleichheit ist trivial nach Reflexivität der Gleichheit.

2. Zunächst soll dies für die Gleichheit induktiv gezeigt werden. Sei also $e \Vdash x^k \subseteq y^k$. Dann gilt

$$\forall (k, a^k) \in x^k \; ek \lhd \{h | \exists (lh, b^k) \in y^k \; rh \Vdash a^k = b^k\}$$

   Nach Voraussetzung gibt es für alle a ein $f \in \nabla$, so dass für alle diese b

$$\nabla \ni rf \Vdash a^k = b^k$$

   Nach Induktionsvoraussetznung folgt daraus aber Gleichheit und es ist also $x \subseteq y$. Damit ist die Aussage über $=$ gezeigt, denn die andere Richtung $\supseteq$ verläuft analog.

   Nun folgt schnell der $\in$-Fall, denn $\Vdash x^k \in y^k$ impliziert

$$\exists (k, z^k) \in x^k \Vdash z^k = x^k$$

3. Durch Induktion über $rk(x \cup y)$ zeigt man: Die Aussagen

$$x^k = y^k \to \perp$$

   werden für $x \neq y$ nicht nicht realisiert von dem wegen dem üblichen Argument denotierenden

$$e := \tau^{fix}[v_1 := \lambda vw.p(v(r(lwk)))(v(r(rwk)))]$$

   Dann werden sie insbesondere überhaupt nicht nicht realisiert.

   Dies zeigt man induktiv über $rk(x \cup y)$. Sei $x \neq y$. Angenommen, $f \Vdash x^k = y^k$, dann

$$\forall (k, a^k) \in x \; lfk \lhd \{h | \exists (lh, b^k) \in y^k \; rh \Vdash a^k = b^k\}$$

Also

$$\forall a \in x\, lfk \lhd \{h | \exists b \in y\, rh \Vdash a^k = b^k\}$$

Analog

$$\forall b \in y\, rfk \lhd \{h | \exists a \in x\, rh \Vdash b^k = a^k\}$$

Somit

$$\begin{aligned} ef &\trianglelefteq p(e(r(lfk)))(e(r(rfk))) \\ &\lhd \{p(ei)(ei') | \forall a \in x, b \in y. i \lhd \{h | \exists a' \in x\, h \Vdash a^k = b'^k\} \wedge i' \lhd \{h' | \exists b' \in y\, h' \Vdash b^k = a'^k\}\} \\ &\lhd \{p(eh)(eh') | \forall a \in x, b \in y \exists a' \in x, b' \in y. (h \Vdash a^k = b'^k) \wedge (h' \Vdash b^k = a'^k)\} \end{aligned}$$

Jedes Element dieser Menge wird nicht nicht von $\emptyset$ überdeckt. Denn falls $\neg x \subseteq y$, so sind nach Induktionsvoraussetzung diese h nicht nicht von der leeren Menge überdeckt, da

$$\begin{aligned} &\neg \forall a \in x \exists b' \in y\; a = b' \\ &\Rightarrow \neg\neg \exists a \in x \forall b' \in y\; a \neq b' \\ &\Rightarrow \neg\neg \exists a \in x. \forall b' \in y\; a \neq b' \wedge \exists b' \in y\; h \Vdash a^k = b'^k \\ &\Rightarrow \neg\neg \exists a \in x. \neg\neg h \lhd \emptyset \\ &\Rightarrow \neg\neg h \lhd \emptyset \end{aligned}$$

Analog wäre für $\neg y \subseteq x$ wieder h nicht nicht von der leeren Menge überdeckt. Es gilt aber wegen $x \neq y$ und also $\neg(x \subseteq y \wedge y \subseteq x)$ Man wendet nun folgendes herleitbares logisches Schema an

$$(\neg\phi_0 \to \neg\neg\psi) \to (\neg\phi_1 \to \neg\neg\psi) \to \neg(\phi_0 \wedge \phi_1) \to \neg\neg\psi$$

um das Ergebnis zu erhalten.

Dieses Schema auch gültig, denn man nehme die Aussagen auf der linken Seite an und angenommen es wäre $\neg\psi$. Wäre $\neg\phi_0$, so wäre auch $\neg\neg\psi$, das kann also nicht sein. Somit ist $\neg\neg\phi_0$ und analog $\neg\neg\phi_1$. Wäre ϕ_0, so würde wegen $\neg(\phi_0 \wedge \phi_1)$ folgen, dass $\neg\phi_1$, woraus ein Widerspruch folgen würde. Also ist $\neg\phi_0$, was aber auch einen Widerspruch bedeutet. Damit ist das Schema gezeigt.

Es fehlt noch die Aussage über $\in$. Sei dazu $x \notin y$. Dann realisiert $f := \lambda x. e(rx)$ nicht nicht die Aussage $x^k \in y^k \to \bot$. Denn wäre

$$g \Vdash x^k \in y^k$$

also

$$g \lhd \{h | lh \lhd k \wedge \exists z^k \in y^k rh \Vdash z^k = y^k\}$$

Dann werden für die $e(rh)$ nach dem oben gezeigten nicht nicht von der leeren Menge überdeckt, also auch g und alles ist gezeigt.

Q.E.D.

Diese starke Absolutheitseigenschaft wird auch später noch große Bedeutung erlangen. Unmittelbar folgt durch reine Logik:

Korollar 92. *Für* $x, y \in V$ *gilt*

$$(\neg \Vdash x^k \neq y^k) \to \neg x \neq y$$

$$(\neg \Vdash x^k \notin y^k) \to \neg x \notin y$$

insbesondere

$$(\Vdash x^k = y^k) \to \neg x \neq y$$

$$(\Vdash x^k \in y^k) \to \neg x \notin y$$

und

$$x \neq y \to \Vdash x^k \neq y^k$$

$$x \notin y \to \Vdash x^k \notin y^k$$

Beweis. Für den dritten Fall muss man sich vergegenwärtigen, dass $e \Vdash \perp$ negativ, das heißt äquivalent zu einer verneinten Formel ist, nämlich

$$\neg \exists p \subseteq S \; \neg e \lhd p$$

Damit ist auch $e \Vdash x^k \neq y^k$ negativ und die Aussage folgt direkt aus dem Theorem. Ebenso für $\in$. Q.E.D.

Kapitel 5

Verallgemeinerungen bekannter Modellkonstruktionen

5.1 Heyting-Algebra-bewertete Modelle

In [15] ist beschrieben, wie man in CZF mit einer formalen Topologie Modelle erstellt[1]. In [14] sind Heyting-Algebra bewertete Modelle für IZF ausgeführt; in diesem Kontext ist es nicht nötig, formale Topologien zu verwenden, da in IZF mit dem Potenzmengenaxiom und, in geringerem Maße, mit voller Separation die Mittel zur Verfügung stehen, mit Heyting-Algebren gut umgehen zu können (zum Beispiel sind mengenerzeugte Heyting-Algebren Mengen). Vorrangig an CZF interessiert, folgen wir [15], dessen Definitionen wir in einer äquivalenten Formulierung, die die hier angegebenen Modelle leichter als Verallgemeinerung erkennbar machen, wiedergeben.

Im Gegensatz zu der hier vorgestellten Konstruktion geht Gambino von einer allgemeinen (und nicht einer separierbaren) formalen Topologie aus. Er behauptet und verwendet, dass die Klasse $H(S) = \{a \subseteq S | a = {}^{\triangleleft}a\}$ dann eine Heyting-Algebra darstellt, wobei insbesondere die Heyting-Operationen den folgenden Gleichungen genügen:

$$a \vee b = {}^{\triangleleft}(a \cup b)$$

$$\bigvee p = {}^{\triangleleft}\bigcup p$$

Dass dies nicht der Fall (genauer: nicht herleitbar) ist, sieht man recht schnell. Diese Behauptung wäre nämlich sogar äquivalent zu voller Separation.
Beweis. Es soll gezeigt werden, dass

$$\{x \in A | \psi(a)\}$$

[1] Der enge Zusammenhang zwischen Heyting-Algebren und formalen Topologien rechtfertigt die Bezeichnung Heyting-Algebra-bewertete Modelle, die historisch ist: die Heyting-Algebra Modelle sind Verallgemeinerungen von Forcing mit Booleschen Algebren [8]. Im prädikativen Zusammenhang ist die Verwendung von Heyting-Algebren wohl auch natürlicher.

eine Menge ist, wobei A und ψ beliebig. Betrachte die formale Topologie mit

$$S = A \cup \{A\}, a \leq b \leftrightarrow a = b, a \lhd p \leftrightarrow a \in p \vee \psi(a)$$

Dies ist eine formale Topologie, zu bedenken ist nur das vierte Axiom, die anderen sind unmittelbar einzusehen (auch, dass es überhaupt eine Pomenge ist). Sei also

$$a \lhd p, q$$

Mithin

$$\psi(a) \vee a \in p, q$$

Im letzten Fall ist offenbar auch $a \in {}^{\leq}p \cap {}^{\leq}q$, insbesondere wird a also davon überdeckt. Im ersten Fall ist sowieso $a \lhd {}^{\leq}p \cap {}^{\leq}q$.

Nach Gambinos Behauptung müsste also $(\bigvee\{\{A\}\}) \setminus \{A\} = ({}^{\lhd}\{A\}) \setminus \{A\}$ eine Menge sein. Dies ist aber ja gerade die zu Beginn betrachtete Klasse. Q.E.D.

Die Eigenschaft, dass $H(S)$ eine Heyting-Algebra ist, ist fundamental wichtig für alle folgenden Sätze, von der Proposition 3.2, die aussagt, dass der Wahrheitswert beschränkter Formeln eine Menge ist, bis zum Beweis des auch in diesem Artikel zentralen Konsistenzsatzes. Dieser Beweis geht ohne diese Eigenschaft sogar für die grundlegendsten Axiome wie beschränkte Aussonderung oder sogar das Vereinigungsmengenaxiom (sogar binäre Vereinigung) schief, von den Kollektionsaxiomen ganz zu schweigen. Dies liegt zum guten Teil daran, dass die Bewohner von $V(S)$ ja Mengen sein müssen, aber dennoch die Gründe, warum ein Element in einer Menge liegt, unter $\lhd$ abgeschlossen sein müssen.

Beispiel 93. *Man betrachte etwa die Topologie* $S = \{+, -, \top\}$ *mit* $x \leq y \leftrightarrow x = y \vee y = \top$ *und* $x \lhd p \leftrightarrow x \in {}^{\leq}p \vee (x = \top \wedge + \in p \wedge - \in p \wedge \psi)$ *für irgendeine nicht separierbare (also insbesondere nicht entscheidbare) Formel* ψ. *Dies ist offenbar eine formale Topologie.*

Die Mengen $(+, \emptyset)$ *und* $(-, \emptyset)$ *haben keine Vereinigungsmenge, denn da keine Menge außer der leeren realisierterweise leer ist, müsste diese*

$$S(\{(+, \emptyset), (-, \emptyset)\})$$

sein — dies ist aber keine Menge, beziehungsweise umgekehrt: Wäre dies stets eine Menge, so würde volle Aussonderung gelten.

Die Eigenschaft, dass $H(S)$ eine Heyting-Algebra ist, ist also sehr wichtig und Topologien ohne sie haben für Modelle der Mengenlehre keinen momentan erkennbaren Wert. Insofern ist die in dieser Arbeit getroffene Forderung, die Topologie müsse separabel sein, keine Einschränkung einer allgemeineren Theorie von Gambino, sondern nur eine notwendige technische Korrektur.

Es werde also im Folgenden angenommen, dass Gambino in [15] die gleiche Einschränkung getroffen habe, damit seine Konstruktion, die nun beschrieben wird, sinnvoll ist.

Es sei V^S induktiv definiert als die kleinste Klasse, die abgeschlossen ist unter der Operation

$$\forall f.\ \exists a \subseteq V^S\ (f : a \to H(S)) \to f \in V^S$$

Dann werden rekursiv die Wahrheitswerte $[\![\phi]\!]_S$ von Formeln[2] auf eine äquivalente Weise[3] wie in der folgenden Definition festgelegt.

Definition 94.

$$[\![a = b]\!]_S := \bigwedge\{a(x) \to \bigvee\{b(y) \wedge [\![x = y]\!]_S | y \in b^{-1}[V]\} | x \in a^{-1}[V]\} \wedge$$

$$\bigwedge\{b(x) \to \bigvee\{a(y) \wedge [\![x = y]\!]_S | y \in a^{-1}[V]\} | x \in b^{-1}[V]\}$$

$$[\![a \in b]\!]_S := \bigvee\{b(x) \wedge [\![a = x]\!]_S | x \in b^{-1}[V]\}$$

$$[\![\bot]\!]_S := \bot$$

$$[\![\phi \to \psi]\!]_S := [\![\phi]\!] \to [\![\psi]\!]$$

$$[\![\phi \wedge \psi]\!]_S := [\![\phi]\!] \wedge [\![\psi]\!]$$

$$[\![\phi \vee \psi]\!]_S := [\![\phi]\!] \vee [\![\psi]\!]$$

$$[\![\exists x \phi]\!]_S := \bigvee\{[\![\phi]\!]_S | x \in V(S)\}$$

$$[\![\forall x \phi]\!]_S := \bigwedge\{[\![\phi]\!]_S | x \in V(S)\}$$

Dabei seien die Heyting-Operationen für $\lhd$-abgeschlossene Teilklassen von S auf die natürliche Weise wie für Teilmengen definiert. Es war

$$\bot = \bigvee \emptyset = {}^{\lhd}\emptyset$$

Eine Formel gilt im Heyting-Algebra-bewerteten Modell, falls ihr Wahrheitswert gleich S ist[4].

Nun soll gezeigt, werden, dass in einem solchen Modell genau die Sätze gelten, die auch in $V(S)$ gelten.

Zunächst sieht man, dass das Universum V^S und $V(S)$ auf natürliche Weise isomorph sind, nämlich durch die induktiv definierte Abbildung

$$F(x) = \{(e, F(y)) | e \in x(y)\}$$

von V^S nach $V(S)$. Man beachte, dass die Definition von V^S impliziert, dass Bilder unter F tatsächlich in $V(S)$ liegen, denn erstens handelt es sich offenbar um Mengen, und zweitens sind die Gründe, warum ein Element in einer Bildmenge liegen sollte, abgeschlossen unter $\lhd$, da die $x(y)$ dies sind.

Damit ist nur noch zu zeigen:

Proposition 95. *Für alle Formeln ϕ gilt*

$$(\Vdash \phi) \leftrightarrow ([\![\phi]\!]_S = S)$$

[2] Im vorliegenden Artikel wird die Annahme, die Sprache enthalte Konstanten für jedes $x \in V^S$ getroffen, was zwar wie früher ausgeführt unnötig, aber bei hinreichend großer Metatheorie (hier $CZF_{S,-}$) nicht unnatürlich ist.

[3] Gambino erleichtert seine späteren Beweise, indem er beschränkte Quantoren als syntaktisch neue Objekte sieht und dafür $\in$ nicht als logisches Zeichen verwendet, da $x \in y \leftrightarrow \exists z \in y\, z = x$.

[4] Gambino schreibt dafür $\top$.

Beweis. Allgemein wird für $e \in S$ gezeigt, dass gilt

$$e \Vdash \phi \leftrightarrow e \in [\![\phi]\!]_S$$

Dies geschieht durch Induktion über den Aufbau von ϕ. Bedenkt man, dass stets $lf = rf = f = pff$ gilt, sind die Schritte für die Junktoren und die Quantoren allesamt trivial und benötigen meist nur die charakterisierende Eigenschaft der jeweiligen Heyting-Operation (so wie: $\wedge$ gibt das Minimum zurück), wobei man beachte, dass $a \vee b := {}^{\lhd}(a \cup b)$ und $\bigvee p := {}^{\lhd}\bigcup p$ definiert sind. Nun also zu den Induktionsanfängen:

1. $e \Vdash \bot$ gilt genau dann, wenn $e \lhd \emptyset$, also $e \in {}^{\lhd}\emptyset$.

2. $e \Vdash a = b$ gilt genau dann, wenn

$$\forall (f,x) \in a \; lef \lhd \{h | \exists (lh, y) \in b \; rh \Vdash x = y\} \wedge \forall (f,x) \in b \; lef \lhd \{h | \exists (lh, y) \in a \; rh \Vdash x = y\}$$

Dies ist aber unter Auflösung der Definitionen direkt äquivalent zu

$$e \in (\bigwedge \{a^{-1}(x) \bigvee \{b^{-1}(y) \to [\![x = y]\!] | y \in b^{-1}[V]\} | x \in a[S]\}$$

und

$$\bigwedge \{b^{-1}(x) \bigvee \{a^{-1}(y) \to x = y | y \in a[S]\} | x \in b^{-1}[V]\})$$

Dies zeigt (mit Nebeninduktion über x und y) das Gewünschte.

3. $e \Vdash a \in b$ gilt genau dann, wenn

$$e \lhd \{h | \exists (lh, a') \in b | rh \Vdash a = a'\}$$

Also nach Definitionen wenn

$$e \leq \bigvee \{b^{-1}(x') \wedge [\![x = x']\!] | x' \in b[S]\}$$

Dies ergibt mit Punkt 2 das Gewünschte.

Q.E.D.

5.2 Realisierbarkeitsmodelle

Im Kapitel über applikative Topologien wurde gezeigt, dass applikative Strukturen auf natürliche Weise zu einer starken applikativen Topologie führen, die für ein Realisierbarkeitsmodell genutzt werden kann. Hier soll gezeigt werden, dass dieses mit dem konstruierten Modell ausgehend von der applikativen Topologie übereinstimmt. Zunächst skizzieren wir die Methode der Realisierbarkeitsmodelle, wir orientieren uns dabei an [22], dessen Zugang für CZF eleganter als McCartys Artikel [20], der für IZF entwickelt wurde, ist, behalten uns jedoch kleine und offensichtlich äquivalente Änderungen vor, um den Zusammenhang mit applikativen Topologien stärker zu Tage treten zu lassen.

In dieser Arbeit wurde bei der Definition der applikativen Strukturen auf eine geringe Anzahl an Axiomen Wert gelegt und es wurden Fallunterscheidungen, Paare etc. definiert statt vorausgesetzt. Rathjen begeht den umgekehrten

Weg, indem er in applikativen Strukturen Konstanten $0, s'_N, p'_N, k, s, d', p', p_0, p_1$ für die 0, eine Einbettung der natürlichen Zahlen, die Nachfolgerfunktion, die Vorgängerfunktion, k, s, Fallunterscheidung (nach 0 und 1 statt r und l), Paarung und die erste beziehungsweise zweite zugehörige Projektion mit den entsprechenden natürlichen Axiomen fordert. Statt $p_i a$ schreibt man oft a_i. Sollte eine Unterscheidung nötig sein, so werden diese Strukturen *starke* applikative Strukturen genannt[5].

Wir halten nun eine starke applikative Struktur A mit zugehöriger applikativer Topologie S fest. Wieder wird zunächst die Grundmenge des Modells und danach eine Interpretation der Sätze geliefert.

Definition 96. *Es sei für $\alpha \in On$ induktiv definiert*

$$V(A)_\alpha = \hat{\bigcup}_{\beta\in\alpha} P(A \times V(A)_\beta)$$

Dann sei $V(A) := \hat{\bigcup}_{\alpha\in On} V(A)_\alpha$.

Natürlich ist dieses Universum übereinstimmend mit $V(S)$, wenn man bedenkt, dass die unter $\lhd$ abgeschlossen Teilmengen von S mit den beliebigen Teilmengen von A übereinstimmen.

Induktiv definiert Rathjen die Realisierbarkeitsrelation $\Vdash'$, wobei er beschränkte Quantoren als syntaktisch unterschiedene Objekte ansieht:

Definition 97. *1.* $e \Vdash' \bot$ *gdw* $\bot$

2. $e \Vdash' a \in b$ *gdw* $\exists c.(e_0, c) \in b \wedge e_1 \Vdash' a = c$

3. $e \Vdash' a = b$ *gdw* $\forall f, d.(f, d) \in a \to e_0 f \Vdash' d \in b \wedge (f, d) \in b \to e_1 f \Vdash' d \in a$

4. $e \Vdash' \phi \wedge \psi$ *gdw* $e_0 \Vdash' \phi \wedge e_1 \Vdash' \psi$

5. $e \Vdash' \phi \vee \psi$ *gdw* $(e_0 = 0 \wedge e_1 \Vdash' \phi) \vee (e_0 = 1 \wedge e_1 \Vdash' \psi)$

6. $e \Vdash' \phi \to \psi$ *gdw* $\forall f. f \Vdash' \phi \to ef \Vdash' \psi$

7. $e \Vdash \forall x \in a \phi(x)$ *gdw* $\forall (f, c) \in a \; ef \Vdash' \phi(c)$

8. $e \Vdash' \exists x \in a \phi(x)$ *gdw* $\exists (e_0, c) \in a \; e_1 \Vdash' \phi(c)$

9. $e \Vdash' \forall x \phi(x)$ *gdw* $\forall c \in V(A) \; e \Vdash' \phi(c)$

10. $e \Vdash' \exists x \phi(x)$ *gdw* $\exists c \in V(A) \; e \Vdash' \phi(c)$
Wieder schreibt man $\Vdash' \phi$ *für* $\exists e \in A \; e \Vdash' \phi$.

Die Vorarbeit zur folgenden Proposition wurde bereits geleistet:

Proposition 98. $(\Vdash' \phi) \leftrightarrow (\Vdash \phi)$

[5] obwohl jede applikative Struktur auf angebbare Weise auch eine starke applikative Struktur ist. Die Umkehrung, dass jede starke applikative Struktur eine applikative Struktur ist, ist allerdings noch direkter.

Beweis. Es wird gezeigt, dass jede Formel ϕ nach beiden Definitionen von den selben Elementen von $A = S$ realisiert werden.

Man beachte, dass hier $\nabla = A$ und $\lhd \leftrightarrow \in$. Insbesondere, wenn $e \lhd \{h | \exists c\theta(h)\}$, so $\exists c\theta(e)$ und es impliziert $a \unlhd b$, dass $a \succeq b$ gilt. Formt man damit die geeigneten alternativen Definitionen der Realisierbarkeit der Zeichen um, so erhält man genau die Definitionen von Rathjen (für manche Versionen war dies die Hauptmotivation) bis auf die leichten Unterschiede von $0, 1$ bzw. p_0, p_1 statt r, l.

Allerdings lassen sich diese in jeder Klausel ersetzen (für $x \in y$ und $x = y$ benötigt man natürlich noch eine Induktion über x und y):

1. Für =: Sei

   $$\forall f, d.(f, d) \in a \to e_0 f \Vdash' d \in b \wedge (f, d) \in b \to e_1 f \Vdash' d \in a$$

   Dann gilt für $e' := (\lambda v.p(p_0 v)(p_1 v))e$, dass $le' = e_0$ und $re' = e_1$, also

   $$\forall f, d.(f, d) \in a \to le' f \Vdash' d \in b \wedge (f, d) \in b \to re' f \Vdash' d \in a$$

   Ist umgekehrt die obige Gleichung erfüllt, so gilt für $e'' := (\lambda v.p'(le)(re))e$ aus analogen Gründen:

   $$\forall f, d.(f, d) \in a \to e''_0 f \Vdash' d \in b \wedge (f, d) \in b \to e''_1 f \Vdash' d \in a$$

   Damit ist Lemma 59 anwendbar.

2. Für $\in$, $\wedge$ und $\exists x \in a \phi$ gilt:

   $$e_0 \lhd p \wedge e_1 \lhd q \to l(\lambda v.p(p_0 v)(p_1 v))e \lhd p \wedge r(\lambda v.p(p_0 v)(p_1 v))e \lhd q$$

   $$le \lhd p \wedge re \lhd q \to ((\lambda v.p'(le)(re))e)_0 \lhd p \wedge ((\lambda v.p'(le)(re))e)_1 \lhd q$$

   Also kann man die Realisierer dieser Formeln mittels Elementen von ∇ aufeinander abbilden und das Lemma 59 liefert die gewünschte Aussage.

Hierbei wurde natürlich verwendet, dass die Realisierer einer Formel unter $\lhd$ abgeschlossen sind. Q.E.D.

5.3 Unzerlegbare und unterscheidende applikative Topologien

Es wurde gezeigt, dass Realisierbarkeitsmodelle Spezialfälle der hier präsentierten Modellkonstruktion sind. Eine applikative Topologie, die von einer applikativen Struktur herrührt, hat bestimmte Eigenschaften, und es ist interessant zu erfahren, welche für Realisierbarkeitsmodelle bekannte Ergebnisse bereits aus solchen Eigenschaften, die eben nicht nur applikative Topologien, die von applikativen Strukturen abstammen, haben, folgen.

5.3.1 Definition und Tatsachen

Definition 99. *Eine schwache applikative Topologie S heißt* ***unzerlegbar****, wenn gilt*

$$\forall B \forall b. b \lhd B \to \exists c \in B \; b \trianglelefteq c$$

Stünde statt dem $\trianglelefteq$ ein $=$, so wären unzerlegbare applikative Topologien nicht viel anderes als applikative Strukturen, bei denen s und k zusammenfallen dürften. Es gibt aber dennoch unzerlegbare applikative Topologien, die in keinem Sinne applikative Strukturen sind. Interessante Beispiele werden später geliefert.

Proposition 100. *Jede applikative Topologie, die von einer applikativen Struktur herrührt, ist unzerlegbar.*

Beweis. Dies gilt stets, wenn $\in$ und $\lhd$ übereinstimmen. q.e.d.

Unzerlegbarkeit impliziert eine wichtige Eigenschaft:

Proposition 101. *Jede unzerlegbare schwache applikative Topologie ist eine starke applikative Topologie.*

Beweis. Definiere

$$r(e) := \{\{f\} | f \in S \wedge e \trianglelefteq f\} = \{\{f\} | f \in S \wedge e \in^{\lhd} \{f\}\}$$

Dies ist nach Replacement und beschränkter Kollektion eine Menge. Dann folgt

$$e \lhd p \leftrightarrow \exists q \in r(e) q \subseteq p$$

q.e.d.

Eine andere Eigenschaft, die von applikativen Strukturen herrührende applikative Topologien aufweisen, ist die folgende:

Definition 102. *Man sagt, eine applikative Topologie S* ***unterscheide****, wenn gilt*

$$\forall e. e \lhd \{l, r\} \to e \trianglelefteq l \dot{\vee} e \trianglelefteq r$$

Gilt sogar für alle abtrennbaren[6] $N \subseteq \omega$

$$\forall e. e \lhd \{\underline{n} | n \in N\} \to \exists! n \in \omega e \underline{n}$$

so sagt man, sie ***unterscheide stark****. Hierbei bedeutet $\dot{\vee}$ exklusives oder, also "oder, aber nicht beides".*

Dies ist eine Verstärkung der Forderung, dass $s \neq k$ gelten müsse, wie man sie bei applikativen Strukturen findet. Underscheidung ist eine partielle Verstärkung von Unzerlegbarkeit in einem der wesentlichsten Fälle: Falls ein Element von $\{l, r\}$ überdeckt wird, wird nicht nur gefordert, dass es auch von einem der beiden, sondern dass es von genau einem der beiden überdeckt wird. Nützlich sind die folgenden Zusammenhänge:

[6] also $\forall n \in \omega \; n \in N \vee n \notin N$

Lemma 103. *Für eine applikative Topologie S gilt:*

1. *Falls gilt*

$$\forall e.e \lhd \{s,k\} \to e \unlhd s \dot{\vee} e \unlhd k$$

so unterscheidet S.

2. *Falls S unterscheidet und MP*[7] *gilt, so unterscheidet S stark.*

3. *Falls S stark unterscheidet, so unterscheidet S.*

Beweis.

1. Angenommen, dies gilt und $e \lhd \{l, r\}$. Dann

$$desk \unlhd \{k, s\}$$

Also

$$desk \unlhd s \dot{\vee} desk \unlhd k$$

Im ersten Fall folgt

$$e \lhd \{h | (h \unlhd l \vee h \unlhd r) \wedge dhsk \unlhd s\}$$

Bei Elementen h dieser Menge tritt das zweite Disjunkt $h \unlhd r$ aber nicht ein, denn sonst wäre $dhsk \unlhd k, s$. Also gilt

$$e \lhd \{h | h \unlhd l\} \to e \unlhd l$$

Und $\neg e \unlhd r$, sonst wäre wieder $desk \unlhd k, s$. Analog folgt im zweiten Fall, dass

$$e \unlhd r, \neg e \unlhd l$$

2. S unterscheide. Sei für $N \subseteq \omega$ abtrennbar und

$$e \lhd \{\underline{n} | n \in N\}$$

Es wird behauptet, dass gilt:

$$\neg\neg\exists n \in \omega (n \in N \wedge e \unlhd \underline{n})$$

Denn angenommen dies würde für alle $n \in \omega$ nicht gelten. Seien dann die Terme $d_{=n}$ so, dass

$$d_{=n}\underline{n} \unlhd l, \forall m \neq n \; d_{=n}\underline{m} \unlhd r$$

[7] Markovs Prinzip ist das Schema

$$\forall n \in \omega \phi(n) \vee \neg(\phi(n)) \to \neg\neg\exists n \in \omega \phi(n) \to \exists n \in \omega \phi(n)$$

Es hat eine berechenbarkeitstheoretische Rechtfertigung und wird in der rekursiven Mathematik oft angenommen: Wenn man eine entscheidbare Eigenschaft von natürlichen Zahlen betrachtet und weiß, dass es klassisch gesehen einen Träger gibt, so kann man ihn berechnen, indem man alle Zahlen durchtestet, was funktioniert, da die Eigenschaft entscheidbar ist. Wegen der klassischen Information weiß man, dass das Programm abbrechen wird.

Einen solchen Term erhält man etwa durch geschickte Zusammensetzung aus $d_{\leq}$. Sei $m \in N$. Wäre nun $d_{=m}e \lhd l$, so wäre

$$e \lhd \{\underline{n}|n \in \omega\}, \{h|d_{=m}h \lhd l\}$$

Demnach hätte man

$$e \lhd\ ^{\leq}\{\underline{n}|n \in \omega\} \cap\ ^{\leq}\{h|d_{=m}h \lhd l\} =\ ^{\leq}\{\underline{m}\}$$

Dem ist aber nicht so. Mithin ergibt sich

$$e \lhd \{\underline{n}|n \in \omega\}, \{h|\forall m \in N\ d_{=m}h \lhd r\}$$

Demnach wird e auch von dem Schnitt der $\leq$-Abschlüsse dieser beiden Mengen überdeckt, der aber seinerseits von der leeren Menge überdeckt wird. Dies ist aber mit der Unterscheidung unvereinbar. Also ist

$$\neg\neg\exists n \in \omega(n \in N \wedge e \unlhd \underline{n})$$

gezeigt und mit Markovs Prinzip folgt die gewünschte Existenz. Denn für alle $n \in \omega$ gilt

$$(n \in N \wedge e \unlhd \underline{n}) \vee \neg(n \in N \wedge e \unlhd \underline{n})$$

Denn die Konjunktion von entscheidbaren Aussagen ist entscheidbar. Für $n \in \omega$ ist $n \in N$ offenbar entscheidbar, und $e \unlhd \underline{n}$ ist auch entscheidbar, denn dies gilt genau dann, wenn

$$d_{=n}e \unlhd l$$

Dabei ist „dann“ klar. „Wenn“ sieht man aber auch leicht, denn es folgte

$$\{d_{=n}m|m \in N\} \unlhd l$$

Also folgt $N \subseteq \{n\}$ und damit $e \unlhd \underline{n}$.

Außerdem kann man entscheiden, ob $d_{=n}e \unlhd l$ gilt, denn

$$d_{=n}e \lhd \{d_{=n}\underline{m}|m \in N\} \lhd \{r, l\}$$

Da die Topologie unterscheidet, tritt genau einer der Fälle $\unlhd l$ und $\unlhd r$ ein, insbesondere ist der Eintritt eines der Fälle entscheidbar.

Die Eindeutigkeit ist klar, denn wäre $e \unlhd \underline{n}, \underline{m}$, so wäre $d_{=}e \unlhd l, r$.

3. Dies zeigt man genauso wie Fall 1, nur mit $de\underline{01}$ statt $desk$.

Q.E.D.

Unterscheidende oder unzerlegbare applikative Topologien haben einige interessante Eigenschaften. Zum Beispiel zeigen sie ein Verhalten, dass von Realisieren mit applikativen Strukturen her bekannt ist: Nämlich den vollkommenen Verlust der Information über Realisierer (dies entspricht dem konstruktiven Inhalt) bei der Verneinung.

Lemma 104. *Ist S unzerlegbar oder unterscheidet S, so gilt $f \Vdash \neg\Phi$ genau dann, wenn es kein $e \in S$ gibt, das Φ realisiert.*

Beweis. „Dann“ ist klar. Zu „nur dann“ bemerkt man, dass in beiden Fällen kein Element der applikativen Topologie von der leeren Menge überdeckt wird. Wenn f also $\neg\Phi$ realisiert, ist für jeden Realisierer $e \Vdash \Phi$ das denotierende ef ein Realisierer von $\perp$ – davon gibt es jedoch keinen. Q.E.D.

Eine weitere interessante Eigenschaft dieser besonderen applikativen Topologien findet man bei der Realisierung der Schemata der Unzerlegbarkeit und dem stärkeren Schema der ω-Unzerlegbarkeit:

UZ $\forall x(\phi(x) \vee \psi(x)) \rightarrow \forall x\phi(x) \vee \forall x\psi(x)$ für alle Formeln ϕ und ψ

ω-UZ $\forall x \exists n \in \omega \phi(x, n) \rightarrow \exists n \in \omega \forall x \phi(x, n)$ für alle Formeln ϕ

Die folgende Proposition ist nach Kenntnisstand des Autors auch für den Spezialfall der Realisierbarkeitsmodelle eine Verallgemeinerung bisher getroffener Aussagen zu Realisierbarkeitstheorie:

Theorem 105. *1. Sei S unzerlegbar. Dann ist Unzerlegbarkeit und ω-Unzerlegbarkeit absolut. Außerdem ist das folgende Schema der Unabhängigkeit der Voraussetzung (Independance of Premises, **IP**) absolut:*

$$(\neg\phi \rightarrow \exists x\psi) \rightarrow \exists x(\neg\phi \rightarrow \psi)$$

für geschlossene ϕ.

2. S unterscheide. Dann realisiert S Unzerlegbarkeit und ω-Unzerlegbarkeit und sogar allgemein Unzerlegbarkeit in diskrete Mengen:

$$\forall a.(\forall y, y' \in a\, y = y \vee y \neq y) \rightarrow \forall x \exists y \in a \phi(x, y) \rightarrow \exists y \in a \forall x \phi(x, y)$$

Beweis.

1. UZ Der Realisierer sei skk. Denn angenommen, für jedes $x \in V(S)$ gelte $f \Vdash \phi(x) \vee \psi(x)$, also

$$\forall x \in V(S) f \lhd \{h | (lh \trianglelefteq l \wedge rh \Vdash \phi(x)) \vee (lh \trianglelefteq r \wedge rh \Vdash \psi(x))\}$$

Dann ist

$$\forall x \in V(S).(lf \trianglelefteq l \wedge rf \Vdash \phi(x)) \vee (lf \trianglelefteq r \wedge rf \Vdash \psi(x))$$

Dies erfüllt nicht die formalen Anforderungen für die Anwendung von UZ. Es gibt aber eine surjektive Abbildung $F : V \twoheadrightarrow V(S)$, definiert durch

$$F(x) := S(\{(e, y) | (e, y) \in x \wedge y \in V(S)\})$$

Damit erhält man

$$\forall x.(lf \trianglelefteq l \wedge rf \Vdash \phi(F(x))) \vee (lf \trianglelefteq r \wedge rf \Vdash \psi(F(x)))$$

Nun wendet man UZ im Hintergrund an und erhält dass

$$\forall x(lf \trianglelefteq l \wedge rf \Vdash \phi(F(x))) \vee \forall x(lf \trianglelefteq r \wedge rf \Vdash \psi(F(x)))$$

Da F surjektiv ist, folgt daraus die Aussage für alle $x \in V(S)$.

ω-UZ Der Realisierer sei skk. Denn angenommen für alle $x \in V(S)$ gelte

$$\exists (lf, \bar{n}) \in \bar{\omega}\; rf \Vdash \phi(x,n)$$

Dann gilt wegen $\omega - UZ$ im Hintergrund, dass dieses $lf \trianglelefteq \underline{n}$ stets auf das selbe n deuten muss (wieder wird der selbe Trick mit der Klassenfunktion F angewandt).

IP Ein möglicher Realisierer wäre wieder $\lambda xy.xk$. Gelte nämlich

$$e \Vdash \neg\phi \to \exists x \psi(x)$$

so bedeutet das, dass falls es keinen Realisierer von ϕ gibt, ef für alle f ein Realisierer von $\exists x\psi(x)$ ist, es also ein a gibt, so dass $\psi(a)$ von ef realisiert wird. Also $\forall f \exists a ef \Vdash \psi(a)$. Wir haben

$$\neg(\exists f\; f \Vdash \phi) \to \exists a\; (\lambda xy.xk)e \Vdash \psi(a)$$

IP im Hintergrund impliziert nun die Behauptung. Hier wurde das vorige Lemma, dass Realisierer einer verneinten Aussage keinerlei Information mehr enthalten, voll ausgenutzt.

2. Es muss nur die Aussage gezeigt werden, die offenbar die stärkste ist. Sei also $a \in V(S)$ und

$$e \Vdash \forall y, y' \in a\; y = y \vee y \neq y$$

Sei außerdem

$$f \Vdash \forall x \exists y \in a \phi(x,y)$$

Wir zeigen

$$\begin{aligned}(\lambda xy.p(ly)(e_\phi(ry)(x(ly)(ly))))ef \\ \trianglelefteq p(lf)(e_\phi(rf)(e(lf)(lf))) \\ \Vdash \exists y \in a \forall x \phi(x,y)\end{aligned}$$

Wobei $e_\phi \Vdash \phi(z) \to z = z' \to \phi(z')$.

Der Grund, weswegen für $x \in V(S)$ das $y \in a$ mit ϕ in a liegt, kann nicht von x abhängen. Es genügt also zu zeigen:

$$(h,y) \in a \to (h',y') \in a \to i \trianglelefteq h, h' \to ehh' \Vdash y = y'$$

In dieser Situation gilt unter Anwendung der Unterscheidung:

$$(l(ehh') \trianglelefteq l \wedge r(ehh') \Vdash y = y') \vee (l(ehh') \trianglelefteq r \wedge r(ehh') \Vdash y \neq y')$$

Wir zeigen, dass das zweite Disjunkt unmöglich ist. Nach Unterscheidbarkeit wäre unter der Annahme, dass es zuträfe, nämlich auch $\neg(l(eii) \trianglelefteq l)$, also

$$r(eii) \trianglelefteq y \neq y$$

Damit wäre nach Konsistenzsatz

$$r(eii) \triangleleft \emptyset \triangleleft \{r\}, \{l\}$$

Also Widerspruch.

Q.E.D.

5.3.2 Auswahlprinzipien

Das Auswahlaxiom der klassischen Mengenlehre impliziert das ausgeschlossene Dritte (für beschränkte Formeln) und ist allein schon deshalb für konstruktive Mengenlehren ungeeignet, ganz abgesehen davon, dass auch philosophische Bedenken bestehen. Für viele Anwendungen genügen jedoch schwächere Prinzipien, von denen hier drei bedeutende vorgestellt werden sollen.

$AC^{\omega,\omega}$ ist ein auch in ZF (ohne AC) gültiges Schema, das besagt, dass jede totale Relation auf natürlichen Zahlen eine Funktion enthält. Dies genügt etwa, um zu zeigen, dass die Cauchy-reellen Zahlen und die Dedekind-reellen Zahlen übereinstimmen [1].

$AC^{\omega,\omega}$ $\forall x \in \omega \exists y \in \omega \phi(x,y) \to \exists f : \omega \to \omega\ \forall i \in \omega \phi(i, f(i))$

Viel häufiger, vor allem in der konstruktiven Analysis, verwendet man allerdings das stärkere Schema Dependant Choice, das erlaubt, ω-viele Auswahlen zu treffen, die auch von den vorhergehenden abhängen dürfen.

DC $\forall a \forall x_0 \in a. \forall x \in a \exists y \in a \phi(x,y) \to \exists f : \omega \to x. f(0) = x_0 \wedge \forall n \in \omega \phi(f(n), f(n+1))$

Eine leichte Verallgemeinerung ist das relativierte DC, bei der die Zugehörigkeit von x zu der Menge a durch die Zugehörigkeit zu einer beliebigen Klasse $\{y|\psi(y)\}$ ersetzt wird:

RDC $\forall x_0 \in \{y|\psi(y)\}. \forall x \in \{y|\psi(y)\} \exists y \in \{y|\psi(y)\} \phi(x,y) \to \exists f : \omega \to \{y|\psi(y)\}.$
$f(0) = x_0 \wedge \forall n \in \omega \phi(f(n), f(n+1))$

Noch stärker (Beweise hiervon finden sich in [1]) ist Aczels Präsentationsaxiom [3], das seine Motivation aus der Interpretation der konstruktiven Mengenlehre in Martin-Löfscher Typentheorie bezieht. Dieses Axiom sagt aus, dass jede Menge surjektives Bild einer Menge ist, auf der das Auswahlaxiom gilt (solche Mengen nennt man Basen):

PA $\forall a \exists B. \exists f : B \twoheadrightarrow a \wedge \forall r : B \rightrightarrows C\ \exists f : B \to C\ f \subseteq r$

Dieses letzte und stärkste Axiom bleibt beim Übergang von V nach $V(S)$ oft erhalten:

Theorem 106. *Gelte PA und sei S unzerlegbar. Dann gilt $\Vdash PA$.*

Der folgende Beweis verallgemeinert den Absolutheitsbeweis aus [22] für Realisierbarkeit mit Kleenes erstem Modell. Dort geht nämlich ganz wesentlich die Voraussetzung ein, dass $S = \omega$, die hier nicht benötigt wird. Auch in [20] wird diese Voraussetzung an wesentlicher Stelle verwendet, außerdem wird dort sogar AC im Hintergrund vorausgesetzt. Insofern ist dieses Resultat also selbst eingeschränkt auf von applikativen Strukturen herrührende applikative Topologien eine echte Verallgemeinerung der vorhandenen Ergebnisse.

Beweis. Mit Strong Collection ist die Eigenschaft von einem B, eine Basis zu sein, äquivalent zu

$$\forall x \in B \exists y \phi(x,y) \to \exists f : B \to V\ \forall x \in B\ \phi(x, f(x))$$

für beliebige Formeln ϕ, denn mit Kollektion über

$$\psi(a,b) \equiv \exists y.b = (a,y) \wedge \phi(a,y)$$

kann man die y in der Rechtsprojektion der Kollektionsmenge sammeln und $\phi(x,y)$ ist äquivalent dazu, dass (x,y) in dieser Kollektionsmenge liegt.

Man zeigt also für ein beliebiges ϕ: Für alle $a \in V(S)$ gibt es ein $B \in V(S)$ und ein $f \in V(S)$ unabhängig von ϕ (dies wäre nicht unbedingt nötig), so dass die folgenden Aussagen mit Realisierern unabhängig von a (aber eventuell abhängig von ϕ) realisiert sind:

1. $\forall b \in B \exists c \in a \; (b,c) \in f$
2. $\forall c \in a \exists b \in B \; (b,c) \in f$
3. $\forall b,c,c'. \, (b,c) \in f \wedge (b,c') \in f \to c = c'$
4. $\forall b \in B \exists c \phi(b,c) \to \exists f. \forall b \in B \exists c(\phi(b,c) \wedge (b,c) \in f) \wedge \forall b \in B \forall c,c'((b,c) \in f \wedge (b,c') \in f \to c = c')$

Die vierte Aussage impliziert das Gewünschte.

Sei also $a \in V(S)$ gegeben. Sei nach PA $f' : B' \twoheadrightarrow a$ die Surjektion einer Basis auf a. Sei nun

$$B^* := \{(e, \langle e^k, x^k \rangle) | x \in B', \exists y f'(x) = (e,y)\}$$

Dies ist nach dem vorgegangenen Abschnitt bijektives Bild von B' und also wieder Basis. Man definiere

$$B := S(B^*) \in V(S)$$

$$f := S(\{(e, \langle \langle e^k, u^k \rangle, x \rangle) | u \in B', f'(u) = (e,x)\})$$

Nun sind die vier Aussagen zu zeigen.

1. Hierfür ist $\lambda x.pxe_r$ ein Realisierer. Sei $(e, \langle e', x^k \rangle) \in B$, so gilt nach Unzerlegbarkeit $e \trianglelefteq e'$ und $f'(x) = (e',y)$ mit $(e',y) \in a$. Also

   $$(e', \langle \langle e'^k, x^k \rangle, y \rangle) \in f$$

2. Hierfür ist $\lambda x.pxe_r$ ein Realisierer. Sei $(e,y) \in a$, dann ist dies Bild von einem $x \in B'$ unter f'. Es ist dann $(e, \langle e^k, x^k \rangle) \in B$ und $(e, \langle \langle e^k, x^k \rangle, y \rangle) \in f$.

3. Hierfür ist ein Realisierer $\lambda xy.e_t(rx)(e_s(ry))$. Seien $b,c,c' \in V(S)$. Sei

   $$e \Vdash (b,c) \in f \wedge e' \Vdash (b,c') \in f$$

   Da ganz allgemein gilt

   $$(h \Vdash z \in S(Z)) \to h \lhd \{j | \exists (lj, z') \in Z rj \Vdash z = z'\}$$

   folgt:

   $$e \lhd \{j | \exists (lj, z') \in f \; rj \Vdash (b,c) = z'\} =: Q$$

   $$e' \lhd \{j | \exists (lj, z') \in f \; rj \Vdash (b,c') = z'\} =: Q'$$

   Insbesondere gilt

   $$\lambda xy.e_t(rx)(e_s(ry))ef \trianglelefteq e_t(re)(re_se') \Vdash (b,c) = (b,c')$$

4. Dies ist der aufwändigste der vier Teile. Sei

$$e \Vdash \forall b \in B \exists c \phi(b,c)$$

Dies impliziert (und ist sogar äquivalent zu):

$$\forall (f, \langle f^k, x^k \rangle) \in B^* \exists u \forall j \in u \exists y \in V(S). ef \lhd u \wedge j \Vdash \phi(\langle f^k, x^k \rangle, y)$$

Wegen Unzerlegbarkeit der schwachen applikativen Topologie folgt

$$\forall (f, \langle f^k, x^k \rangle) \in B^* \exists y \in V(S) ef \Vdash \phi(\langle f^k, x^k \rangle, y)$$

Da B^* eine Basis ist, erhält man daraus eine Funktion $F' : B^* \to V(S)$ mit

$$\forall (f, \langle f^k, x^k \rangle) \in B^* ef \Vdash \phi(\langle f^k, x^k \rangle, F'(f, \langle f^k, x^k \rangle))$$

Man internalisiere diese Funktion zu

$$F^* := \{(f, \langle x, y \rangle) | F'(f,x) = y, (f,x) \in B^*\}$$

$$F := S(\{(f, \langle x, y \rangle) | F'(f,x) = y, (f,x) \in B^*\})$$

Nun existiert offenbar für jedes $(f', \langle f^k, x^k \rangle) \in B$ ein $(f, \langle f^k, x^k \rangle) \in B^*$ mit $f' \unlhd f$ (wegen Unzerlegbarkeit), und für dieses gibt es ein $y \in V(S)$, so dass

$$pfe_r \Vdash \langle \langle f^k, x^k \rangle, y \rangle \in F$$

und

$$ef \Vdash \phi(\langle f^k, x^k \rangle, y)$$

Es bleibt noch zu zeigen, dass die Funktionalität von F realisiert ist. Sei dazu

$$f \Vdash \langle z, y \rangle \in F, f' \Vdash \langle z, y' \rangle \in F$$

Nach der vorherigen allgemeinen Aussage über die Realisierer der Zugehörigkeit eines Elements zu einer Menge, die durch die $x \mapsto S(x)$-Operation erhalten wurde, werden die f und f' überdeckt von Elementen — seien also o.E. solche Elemente — so dass es Elemente gibt, die das folgende erfüllen:

$$(g, \langle \langle g^k, x^k \rangle, F'(g, \langle g^k, x^k \rangle) \rangle) \in F^* \wedge rf \Vdash \langle \langle g^k, x^k \rangle, F'(g, \langle g^k, x^k \rangle) \rangle = \langle z, y \langle \wedge lf \unlhd g$$

$$(g', \langle \langle g'^k, x'^k \rangle, F'(g', \langle g'^k, x'^k \rangle) \rangle) \in F^* \wedge rf \Vdash \langle \langle g'^k \rangle, x'^k, F'(g', \langle g'^k, x'^k \rangle) \rangle = \langle z, y' \rangle \wedge lf \unlhd g$$

Daraus kann man, unter Beachtung, dass in CZF zwei Paare beweisbarerweise nur dann gleich sein können, wenn auch die Komponenten gleich sind, folgern, dass $x^k = x'^k$ und $g^k = g'^k$— nach den Eigenschaften der ^{k}-Einbettung folgt also $x = x'$ und $g = g'$. Darum ist auch

$$F'(g, \langle g^k, x^k \rangle) = F'(g', \langle g'^k, x'^k \rangle)$$

Q.E.D.

Gleiches gilt für DC und RDC:

Theorem 107. *Sei S unzerlegbar.*

1. *Gilt DC, so gilt $\Vdash DC$.*
2. *Gilt sogar RDC, so gilt $\Vdash RDC$.*

Beweis. Dieser Beweis orientiert sich eng an [22] und unterscheidet sich nur in einigen leichten Vereinfachungen sowie dem Wechsel zu applikative Topologien geschuldete Änderungen. Dort ist die Behauptung zwar nur für Kl formuliert, der Beweis lässt sich allerdings hier problemlos verallgemeinern.

1. Angenommen

$$e \Vdash \forall x \in a \exists y \in a \phi(x, y)$$

dann folgt unter Berücksichtigung der Unzerlegbarkeit

$$\forall (f, x) \in a \exists (g, y) \in a. l(ef) \trianglelefteq g \wedge r(ef) \Vdash \phi(x, y)$$

Dann gilt für alle $(f', x') \in a$ wegen DC im Hintergrund: Es gibt

$$F_0 : \omega \to S, F_1 : \omega \to a[S]$$

mit

$$\forall n \in \omega l(e(F_0(n)) \trianglelefteq F_0(n+1) \wedge r(e(F_0(n))) \Vdash \phi(F_1(n), F_1(n+1))$$

und

$$F_0(0) = f', F_1(0) = x'$$

Nun internalisiert man

$$F := S(\{(p\underline{n}F_0(n), [\![\bar{n}, F_1(n)]\!])|n \in \omega\})$$

Man muss zeigen, dass es einen Realisierer gibt, den man erhält, indem man einen in ∇ denotierenden Wert, der nur von ϕ abhängig sein darf, auf e anwendet, und der realisiert:

$$F : \omega \to a \wedge \forall n \in \omega \forall x, y \in a. [\![n, x]\!] \in F \wedge [\![n+1, y]\!] \in F \to \phi(x, y)$$

Dies folgt wie in [22]. Da hier nicht mit Kl realisiert wird, ist nur nicht ganz klar, ob es einen Term $e \in \nabla$ gibt, so dass gilt

$$\forall n \in \omega \forall f, g \in S. enf \trianglelefteq f^n g$$

wobei $f^n g$ die n-fache Anwendung von f auf g sein soll. So einen Term gibt es aber, nämlich zum Beispiel

$$\tau^{fix}[v_0 := \lambda vxyz.d(lx)g(y(v(rx)yz))]$$

2. Den zweiten Teil erhält man wie in [22] aus dem ersten, indem man RDC auflöst als DC plus das Schema

$$\forall x(\phi(x) \to \exists y.\phi(y) \wedge \psi(x,y)) \to \exists z.b \in z \wedge \forall x \in z\ \exists y \in z.\phi(y) \wedge \psi(x,y)$$

Dass dieses absolut ist, kann leicht gezeigt werden.

Q.E.D.

Das dritte betrachtete Auswahlprinzip zu realisieren benötigt nicht Unzerlegbarkeit, sondern Unterscheidung. Dann wird es aber auch unabhängig von der Hintergrundtheorie realisiert. Für Realisierbarkeit mit applikativen Strukturen hat dies schon [20] gezeigt, dessen Beweis kann allerdings nicht einfach übernommen werden, da unterscheidende applikative Topologien dazu eine zu deutliche Verallgemeinerung von applikativen Strukturen darstellen.

Theorem 108. *S unterscheide. Dann ist $AC^{\omega,\omega}$ realisiert.*

Beweis. Sei

$$e \Vdash \forall x \in \omega \exists y \in \omega \phi(x,y)$$

Dann gilt insbesondere

$$\forall n \in \omega\ e\underline{n} \lhd \{h | \exists (lh, \bar{m}) \in \omega\ rh \Vdash \phi(\bar{n}, \bar{m})\}$$

Also

$$\forall n \in \omega\ e\underline{n} \lhd \{h | \exists m \in \omega . lh = \underline{m} \wedge rh \Vdash \phi(\bar{n}, \bar{m})\}$$

Es folgt, da $\bar{m}$ aus lh wegen der Unterscheidung eindeutig bestimmt ist, dass für alle $n \in \omega$ gilt:

$$l(e\underline{n}) \lhd \{h | \exists m \in \omega . h = \underline{m} \wedge r(e\underline{n}) \Vdash \phi(\bar{n}, \bar{m})\},$$

also gibt es stets ein $m \in \omega$ mit

$$l(e\underline{n}) \unlhd \underline{m} \wedge r(e\underline{n}) \Vdash \phi(\bar{n}, \bar{m})$$

Man betrachte die Mengen

$$F^* := \{(n, \langle \bar{n}, \bar{m} \rangle) | l(e\underline{n} \unlhd \underline{m}, n, m \in \omega\}$$

$$F := S(F^*)$$

Dann gilt

$$\lambda x.p(l(ex))(p(pxe_r)(r(ex))) \Vdash \forall n \in \omega \exists m \in \omega \langle n, m \rangle \in F \wedge \phi(n,m)$$

Analog zu den vorhergehenden Beweisen von Funktionalität gilt

$$\Vdash \forall n, m, m'. \langle n, m \rangle \in F \wedge \langle n, m' \rangle \in F \to m = m'$$

Q.E.D.

Kapitel 6

Konkrete Modelle

Die in dieser Arbeit vorgestellte Maschinerie ist sehr reichhaltig und erlaubt, eine fast unüberschaubare Vielfalt von Modellen zu konstruieren, insbesondere Realisierbarkeitsmodelle und Heyting-Algebra-bewertete Modelle. Es gibt aber auch Aussagen, deren Konsistenz man mit applikativen Topologien zeigen kann, bei denen es sich um keines von beidem handelt, und bei denen es auch schwer vorstellbar wäre, dass man sie mit einer der beiden Spezialfälle zeigen könnte, oder zumindest unklar, wie. Dies zeigt, dass die Verallgemeinerung mehr als nur den ästhetischen Reiz hat, zwei bisher unvereinte Konzepte als Spezialfälle des Gleichen zu erkennen und daraus eine erhöhte Ökonomie der Beweise möglich zu machen, da man vieles nun nicht mehr doppelt beweisen muss. Hier werden nur einige Beispiele gegeben, obwohl der Autor von der Existenz vieler weiterer überzeugt ist.

Alle in diesem Kapitel getroffenen Aussagen über CZF lassen sich leicht auf andere konstruktive Theorien wie IZF übertragen.

6.1 Das Halteproblem

Die Lösbarkeit des Halteproblems sei die Aussage

$$\forall e \in \omega . \exists n, q \in \omega T(e, n, q) \vee \neg \exists n, q \in \omega T(e, n, q),$$

wobei T die primitiv-rekursive Formel ist, die genau dann gilt, wenn das Programm mit Nummer e nach n Schritten das Ergebnis p liefert. Die Formel sagt also aus: Jedes Programm hält an oder nicht. Turing [28] bewies (im Wesentlichen) die Unlösbarkeit des Halteproblems in der rekursiven Mathematik. Sein Beweis zeigt, dass sie der Chruchschen These (die dort wahr ist) widerspricht, nach der es insbesondere zu jeder Aussage der Form $\forall e \in \omega \phi \vee \psi$ eine rekursive Funktion geben müsste, die zu jedem e ein Disjunktionsglied anzeigt, das für e erfüllt ist.

In $V(Kl)$, das in vielerlei Hinsicht als geeignetes Modell für rekursive Mathematik oder die Mathematik der Schule der russischen Konstruktivisten um Markov erscheint, gilt die Church'sche These [22], entsprechend ist dort das Halteproblem unlösbar. In Modellen mit klassischer Logik ist die Lösbarkeit des Halteproblems natürlich eine Trivialität. Unser Ziel ist es, ausgehend von Modellen, in denen das Halteproblem lösbar ist, Zwischenstufen zu konstruieren, also Modelle, in denen das Halteproblem zwar nicht lösbar ist, die Unlösbarkeit des Halteproblems jedoch auch kein Satz ist und in denen gilt: Das Halteproblem ist nicht unlösbar. Damit wäre zum Beispiel gezeigt, dass die Nichtunlösbarkeit des Halteproblems nicht seine Lösbarkeit impliziert.

Man nehme also die Lösbarkeit des Halteproblems im Hintergrund an. Sei $t : \omega \to \{0,1\} \times \omega \times \omega$ so, dass

$$t(e) = (1, n, q) \to T(e, n, q), t(e) = (0, n, q) \to \neg \exists n', q \in \omega T(e, n', q)$$

Sei $Kl[t]$ (lies: Kl adjungiert t) die applikative Struktur der Indizes der partiell rekursiven Funktionen in t. Falls also S' die kleinste Klasse partieller Funktionen von endlichen Potenzen von ω auf ω ist, die t, die Nachfolgerfunktion, die Projektionen, die Nullfunktion und die Pseudovorgängerfunktion $x \mapsto max(0, x-1)$ enthält und abgeschlossen gegenüber Komposition und Minimumsbildung[1] ist, so enthält $Kl[t]$ Indizes für alle Funktionen von S', deren Definitionsbereiche Teilmengen von ω sind. Es handelt sich bekanntlich um aufzählbare Mengen, seien also $Kl[t]$ und ω wie auf übliche Weise identifiziert, so dass die Bezeichnung $e \circ f$ sinnvoll ist.

Sei S disjunkte Vereinigung von $Kl[t]$ und Kl also etwa

$$S = \{0\} \times Kl[t] \dot{\cup} \{1\} \times Kl$$

Die Verknüpfung $\circ$ sei innerhalb von $Kl[t]$ bzw. Kl definiert wie in diesen beiden Strukturen. Kl ist offenbar auf natürliche Weise eine Substruktur von $Kl[t]$, wird also mit $\circ$ ein Element von Kl mit einem von $Kl[t]$ (in beliebiger Reihenfolge) verknüpft, so soll dies gleich dem Ergebnis der Verknüpfung in $Kl[t]$ sein, nachdem das Element von Kl via einer (fest gewählten) Einbettung von Kl nach $Kl[t]$ geschickt wurde. Formal ausgedrückt: Sei $F : Kl \to Kl[t]$ Monomorphismus applikativer Strukturen fest gewählt, so sei

$$(0, e) \circ (0, f) \simeq \{e\} f$$

$$(1, e) \circ (0, f) \simeq e \circ F(f)$$

$$(0, e) \circ (1, f) \simeq F(e) \circ f$$

$$(1, e) \circ (1, f) \simeq e \circ f$$

Dabei bedeutet $\simeq$ wie üblich: Ist eine Seite definiert, sind sie es beide und der Wert stimmt überein.

Würde man jetzt s und k als s und k aus $Kl[t]$wählen, so würde man eine applikative Struktur erhalten, mit der man wohl die Lösbarkeit des Halteproblems realisieren könnte (und auch $AC^{\omega,\omega}$, und DC oder sogar PA, falls diese im Hintergrund gelten), aber nicht ein Modell konstruieren könnte, das die doppelte Verneinung, aber nicht die Lösbarkeit des Halteproblems selbst realisiert. Darum wählt man s und k als die s und k von Kl, so dass die entstehende Struktur sicherlich keine applikative mehr ist.

Man setzt $e \leq f \leftrightarrow e = f \vee F(f) = e$. Man wählt $\lhd$ minimal als

$$e \lhd p \leftrightarrow \exists f \in pe \leq f$$

Als ∇ wählt man Kl, also genauer $\{1\} \times Kl$.

[1] also dem μ-Operator: $\mu x.f(x) = y \leftrightarrow f(y) = 0 \wedge \forall y' < y\, f(y') > 0$

Man sieht schnell, dass dies eine (starke) applikative Topologie ergibt: Jedes einzelne Axiom ist recht offensichtlich erfüllt. Außerdem ist S unzerlegbar und unterscheidet.

Proposition 109. *Für das durch S bestimmte Modell gilt*

1. $\nVdash \forall e\in\omega.\exists n,q\in\omega\, T(e,n,q) \vee \neg\exists n,q\in\omega\, T(e,n,q)$
2. $\nVdash \neg\forall e\in\omega.\exists n,q\in\omega\, T(e,n,q) \vee \neg\exists n,q\in\omega\, T(e,n,q)$
3. $\Vdash \neg\neg\forall e\in\omega.\exists n,q\in\omega\, T(e,n,q) \vee \neg\exists n,q\in\omega\, T(e,n,q)$

Beweis.

1. Angenommen, diese Formel würde durch $f\in\nabla = Kl$ realisiert. Nach Anwendung der Unzerlegbarkeit und Unterscheidung erhält man

   $$\forall e.(l(fe) \trianglelefteq l \wedge \Vdash \exists n,q\in\omega T(e,n,q)) \vee (l(fe) \trianglelefteq r \wedge \Vdash \neg\exists n,p\in\omega T(e,n,q))$$

   Auf Grund der Absolutheitsresultate aus dem Abschnitt „Absolutheit in den natürlichen Zahlen“ (4.4.2) folgt: $(\lambda x.l(fx))e$ ist l, falls die partiell rekursive Funktion mit Nummer e abbricht, und falls sie nicht abbricht, so ist es r (denn dann ist das erste Disjunkt falsch). Da $e\in Kl$ liegen würde, ist dies ein Widerspruch.

2. Dies folgt aus Punkt 3 und Konsistenz.

3. Dies wird etwa von k realisiert. Da es kein Element von S gibt, das von $\emptyset$ überdeckt wird und $kxy\downarrow$, ist die zu zeigende Aussage äquivalent zu

   $$\neg\neg\exists x\in S.x \Vdash \forall e\in\omega.\exists n,q\in\omega T(e,n,q) \vee \neg\exists n,q\in\omega T(e,n,q)$$

   Es soll sogar gezeigt werden, dass es ein solches $x\in S$ gibt, es wird allerdings natürlich nicht in Kl liegen können, sondern Element von $Kl[t]$ sein. Sei nämlich f so, dass

   $$\forall e.\exists n,q\in\omega\, T(e,n,q) \to fe \trianglelefteq pl(p\underline{n}(p\underline{q}(e_T\underline{enq})))$$

   $$\forall e.\neg\exists n,q\in\omega\, T(e,n,q) \to fe \trianglelefteq prk$$

   Dabei sei e_T ein Zeuge für die natürliche Absolutheit von T, die Existenz eines solchen f ist klar nach Wahl von $Kl[t]$[2].

   Sei nun $(e',\bar{e})\in\bar{\omega}$, ohne Einschränkung $e' = (0,\underline{e})$, denn die einzige andere Möglichkeit wäre $(1,\underline{e})$, für die das Folgende erst recht zutrifft. Falls $T(e,n',q')$ für passende n' und q' gilt, so folgt nach Obigem

   $$fe \Vdash \exists n,p\in\omega T(e,n,p)$$

   Falls das Programm mit Nummer e aber nicht anhält, so gibt es gar kein $g \Vdash \exists n,p\in\omega T(e,n,p)$, nach Absolutheit. Also ist dann auch

   $$fe \Vdash \neg\exists n,p\in\omega T(e,n,p)$$

   Wegen unserer Voraussetzung gibt es nur die beiden Fälle, die Aussage ist also bewiesen.

[2]Es ist zwar $t\notin Kl[t]$, aber es sind natürlich Funktionen in $Kl[t]$, die den einzelnen Komponenten von t entsprechen.

Q.E.D.

Es wurde hier also ein Modell präsentiert, in dem weder gilt, dass das Halteproblem lösbar, noch, dass es unlösbar ist. Es gilt allerdings, dass es immerhin nicht unlösbar ist.

6.2 Doppelte Verneinungen

Die Möglichkeit, in Modellen aus applikativen Topologien die doppelte Verneinung von Formeln zu realisieren, ohne die Formel selbst zu realisieren, indem man nur Realisierer aus $S \setminus \nabla$ zulässt, ist natürlich auch auf viele andere Formeln außer dem Halteproblem anwendbar. Mit Realisierbarkeitsmodellen aus applikativen Strukturen ist dies aber nicht so einfach:

Bemerkung 110. *Sei ZF konsistent. Stammt S von einer applikativen Struktur und ist ϕ eine Formel mit*

$$CZF \vdash\Vdash \neg\neg\phi,$$

so ist

$$CZF \nvdash\nVdash \phi$$

Beweis. Gilt die Voraussetzung, so lässt sich die Behauptung erst recht aus klassischer Mengenlehre ZF ableiten, dies ist aber äquivalent dazu, dass es nicht keinen Realisierer von ϕ gibt, also lässt sich dann in ZF ableiten, dass ϕ realisiert ist. Also lässt sich aus CZF nicht das Gegenteil herleiten. Q.E.D.

In $V(Kl)$ ist das ausgeschlossene Dritte bekanntlich falsch, im Sinne, dass es Formeln $\phi(x)$ gibt mit $\Vdash \neg(\forall x.\phi(x) \vee \neg\phi(x))$. Denn es sind einige Sachen realisiert, die dem ausgeschlossenen Dritten widersprechen, wie beispielsweise die Existenz von

$$\omega_0 := \{(k, \bar{n}) | n \in \omega\},$$

realisierterweise einer Obermenge der natürlichen Zahlen, so dass jede Funktion von ihr nach ω konstant ist [20]. Insofern ist also nicht nur das ausgeschlossene Dritte nicht realisiert, sondern auch seine doppelte Verneinung nicht. In klassischen Modellen gilt andererseits natürlich sowohl das ausgeschlossene Dritte als auch seine doppelte Verneinung. Unser Ziel ist es nun, ein Modell zu konstruieren, in dem die doppelte Verneinung des ausgeschlossenen Dritten gilt, also für alle Formeln

$$\Vdash \forall x \neg\neg(\phi(x) \vee \neg\phi(x))$$

aber nicht das ausgeschlossene Dritte selbst, also für mindestens eine Formel

$$\nVdash \forall x(\phi(x) \vee \neg\phi(x))$$

Dazu gehen wir davon aus, dass in unserer Hintergrundtheorie die doppelte Verneinung des ausgeschlossenen Dritten gilt. Wir wählen $S := Kl \dot{\cup} \{\omega\}$ mit $\nabla = Kl$. Es sei $\circ$ auf Kl definiert wie üblich, und

$$a = \omega \vee b = \omega \to a \circ b = \omega$$

Auf Kl sei $\leq$ als Gleichheit definiert, und ω sei kleiner als alle Elemente von S. Es sei definiert

$$x \lhd p \leftrightarrow \exists y \in p\, x \leq y$$

Damit ist S unzerlegbar, unterscheidet aber nicht. Offensichtlich ist es eine applikative Topologie. $b \Vdash \neg\phi$ ist äquivalent zu $\forall a \in S\, a \nVdash \phi$ bzw $\neg\exists a \in S\, a \Vdash \phi$, denn kein Element von S wird von der leeren Menge überdeckt.

S realisiert das ausgeschlossene Dritte nicht. Zum Beispiel realisiert es, dass ω_0 Obermenge der natürlichen Zahlen ist, aber nicht, dass $\omega_0 = \bar{\omega}$ gilt. Dennoch ist auch

$$\nVdash \exists n \in \omega_0 n \notin \bar{\omega}$$

Denn für jedes $(e, \bar{n}) \in \omega_0$ gibt es ja einen Realisierer, der zeigt, dass dieses $\bar{n}$ eine natürliche Zahl ist (nämlich $\underline{n}$ — diese Realisierer sind nur nicht aus den e effektiv zu erhalten).

Allerdings realisiert S die doppelte Verneinung des ausgeschlossenen Dritten, denn es gilt ja

$$\neg\neg(\omega \Vdash \phi \vee \omega \nVdash \phi)$$

Also

$$\neg\neg\omega \Vdash (\phi \vee \neg\phi)$$

Da ω alles realisiert, was nur irgendwie realisiert wird, ist dies äquivalent zu

$$\neg\neg\exists a \in S\, a \Vdash (\phi \vee \neg\phi)$$

Nach dem Obigen ist dies aber äquivalent zu

$$\neg\omega \Vdash \neg(\phi \vee \neg\phi),$$

also zu

$$\neg\exists a \in S a \Vdash \neg(\phi \vee \neg\phi)$$

und somit wieder zu

$$\omega \Vdash \neg\neg(\phi \vee \neg\phi)$$

Kapitel 7

Konklusion

In dieser Arbeit wurde für eine Vielzahl konstruktiver oder intuitionistischer Mengenlehren, insbesondere für die Standardsysteme CZF und IZF, eine Möglichkeit vorgestellt, wie man die bekannten Modellkonstruktionen Realisierbarkeitsmodelle und Heyting-Algebra bewertete Modelle zu einer gemeinsamen Verallgemeinerung führen kann. Beides sind wichtige Methoden, die schon vielfach die Feststellung von beweistheoretischen und logischen Eigenschaften dieser Theorien ermöglicht haben und verwendet wurden, um Konsistenzresultate zu erzielen oder durch die Erforschung von natürlichen Modellen (wie $V(Kl)$) Inspiration betreffend mathematischer Prinzipien zu erlangen.

Es wurde eine algebraische Struktur, von der dieses Modell der Mengenlehre abhängt, definiert und gezeigt, wie sie als Verallgemeinerung der zu den den bereits vorhandenen Modellkonstruktionen zugeordneten Strukturen (Heyting-Algebren beziehungsweise separierbaren formalen Topologien und applikativen Strukturen) gesehen werden kann. Von ihr ausgehend konnte man ein Modell der Mengenlehre definieren, so dass sich sowohl die Heyting-Algebra-bewertete Konstruktion als auch die Realisierbarkeitsmodelle ergaben, wenn man die entsprechende Struktur als zu Grunde liegende hernimmt.

Es ist stets befriedigend, zwei unterschiedliche mathematische Konzepte wie diese beiden Modellkonstruktionen als Spezialfälle einer einzigen zu Grunde liegenden Struktur zu erkennen, einerseits aus ästhetischem, andererseits aber auch aus pragmatischem Anliegen. So wird etwa die Darstellung der Theorie der Modelle konstruktiver Mengenlehre stark vereinfacht, da man viele Beweise nicht mehr doppelt führen muss und oft treten tiefe Eigenschaften erst nach einer derartigen Abstraktion und Generalisierung wirklich an die sichtbare Oberfläche, so dass man hoffen kann, auch über die Spezialfälle fundamentalere Einsichten zu gewinnen.

Es wurden die wesentlichen Eigenschaften der beiden Modellkonstruktionen, wie der Konsistenzsatz oder die Eigenschaft, dass die Realisierer einer beschränkten Formel eine Menge bilden, so mit einem einzigen Beweis, der für die Verallgemeinerung gilt, nachgewiesen und dabei auch einige Resultate gezeigt, die bisher nur für einen der beiden Spezialfälle bekannt waren, oder in manchen Fällen nach Wissensstand des Autoren für keinen der beiden.

Häufig kann man nach einer solchen Generalisierung aber auch darauf hoffen, dass nicht nur die bereits bekannten Spezialfälle interessante Erkenntnisse liefern, sondern auch die durch die Verallgemeinerung neu eröffneten Wege, die mit keinem der ursprünglich bekannten übereinstimmen, es wert sind, begangen zu werden. Das letzte Kapitel sollte illustrieren, dass eine derartige Hoffnung auch in diesem Fall nicht ganz unbegründet ist. Auch dafür lohnt es sich, Eigenschaften für alle Modelle aus applikativen Topologien und nicht nur für beide Spezialfälle herzuleiten.

Wie zu erwarten ist, wurden manche Eigenschaften eines der Spezialfälle nicht von allen Modellen aus applikativen Topologien geteilt, aber es wurde für einige Eigenschaften gezeigt, dass sie doch für deutlich mehr als nur die bekannten Spezialfälle gelten, so dass man sich ihrer für eine Reihe neuer Modelle auch bedienen kann.

Eine weitere Beschäftigung mit dieser Modellkonstruktion bestünde einerseits darin, weitere allgemeine Aussagen über die gebildeten Modelle zu finden, und andererseits in der Suche nach weiteren konkreten Anwendungen, die im letzten Kapitel nur angedeutet wurden. Aber es ist auch eine weitere Verallgemeinerung denkbar, nämlich dass man auf die Bedingung, dass der Träger von S eine Menge ist, verzichten könnte. So könnte man hoffen, die Verallgemeinerung etwa auf die in [23] verwendete Modellkonstruktion ausdehnen zu können. Die Ausdehnung der Methode auf *Klassen* S macht es überhaupt denkbar, eine nichtgenerische Interpretation der Quantoren anzudenken. Dies würde allerdings eine stärkere Struktur erfordern, so dass ein derartiges Vorgehen innerhalb des Umfangs dieser Arbeit nur angedacht, nicht aber ausgeführt werden konnte.

Literaturverzeichnis

[1] ACZEL, P, RATHJEN, M., *Notes on Constructive Set Theory.* Institut Mittag–Leffler Preprint 40, 2000/01

[2] ACZEL, P., The type theoretic interpretation of constructive set theory: Inductive definitions. In: R.B. et. al. Marcus eds., *Logic, Methodology and Philosophy of Science VII.* North–Holland, Amsterdam, 1986, pp. 17–49

[3] ACZEL, P., The Type Theoretic Interpretation of Constructive Set Theory: Choice Principles, in: Troelstra, A. S., van Dalen, D. (eds.), The L.E.J. Brouwer Centenary Symposium, (North–Holland, Amsterdam, 1982

[4] ACZEL, P., A note on interpreting intuitionistic higher order logic. Private Communication, undated

[5] ACZEL, P., The type theoretic interpretation of constructive set theory. In: A. Macintyre, L. Pacholski, J. Paris, eds., *Logic Colloquium '77.* North–Holland, Amsterdam, 1978, pp. 55–66

[6] BARENDREGT, D.C., The Lambda-Calculus. of *Studies in Logic and the Foundation of Mathematics*, Volume 103. North–Holland, Amsterdam, 1981

[7] BARWISE, J., ED., Handbook of Mathematical Logic. (North–Holland, Amsterdam, 1977

[8] BELL, J.L., Boolean-valued Models and Independence Proofs in Set Theory. Clarendon Press, 1977

[9] BATTILOTTI, G., SAMBIN, G. A uniform presentation of sup-lattices, quantales and frames by means of infinitary preordered sets, pretopologies and formal topologies. *Technical Report 19.* Department of Mathematics, University of Padua, 1993

[10] COHEN, C.J., Set Theory and the Continuum Hypothesis. W.A. Benjamin Inc., Ney York, 1966

[11] CROSILLA, L., HAJIME ISHIHARA, AND SCHUSTER, P. On constructing completions. *J. Symbolic Logic,* 2005

[12] EBBINGHAUS, H.D., FLUM, J., THOMAS, W., Einführung in die mathematische Logik. Spektrum akademischer Verlag, Berlin, 1996

[13] FEFERMAN, S., A language and axioms for explicit mathematics. In: J.N. Crossley ed., *Algebra and Logic.* Lecture Notes in Mathematics 450, Springer, Berlin, 1975, pp. 87–139

[14] Fourman, M.P., Mulvey, C.J., Scott, D.S., eds., Applications of Sheaves. volume 753 of *Lecture Notes in Mathematics*. Springer, 1979

[15] Gambino, N., Heyting-valued interpretations for Constructive Set Theory. *Ann. Pure Appl. Logic* 137 (2006), 164–188

[16] Gambino, N., A note on Subset Collection. Private Communication, 2006

[17] Kuhnen, K., Set Theory. North–Holland, Amsterdam, 1980

[18] Link, G, Collegium Logicum — Logische Grundlagen der Philosophie. Mskr. PLW-Seminar, LMU

[19] Lubarsky, R., Independence results around constructive ZF. *Ann. Pure Appl. Logic* 132 (2005), 209–225

[20] McCarty, D.C., D. C. McCarty. Realizability and Recursive Mathematics. PhD thesis, Oxford University, 1984

[21] McCarty, D.C., Incompleteness and Intuitionististic Logic. Talk at the University of Munich, Munich, 2006

[22] Rathjen, M., Realizability for Constructive Zermelo-Fraenkel Set Theory. Available from the author's web page

[23] Rathjen, M., Constructive Set Theory and Brouwerian Principles. *J. Universal Computer Science,* 2005

[24] Rathjen, M., CZF has the Disjunction and Numerical Existence Property. Available from the author's web page

[25] Sambin, S., Some points in formal topology. *Theoretical Computer Science*, 305(1-3), 2003, pp. 347–408

[26] Shoenfield, J.R. Mathematical Logic. Addison-Wesley Publishing Co., 1967

[27] Thiel, K., Constructive Finiteness. Talk at the *Leeds Logic Seminar*, Leeds, 2005

[28] Turing, A., On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, Series 2, 42 (1936), pp. 230–265

[29] Troelstra, A.S., van Dalen, D., Constructivism in Mathematics. North-Holland, 1988

[30] Ziegler, A., Refinement is equivalent to Fullness. Typoscript, 2006

[31] Ziegler, A., Some Reflections about the Principle of Image Collection. In: A. Beckman et. al. eds., *Logical Approaches to Computational Barriers*. University of Swansea Report Series, Swansea, 2006, pp. 282–288