Universität München
Centrum für Informations- und
Sprachverarbeitung

Zweitstufige prä-logische Relationen und Repräsentationsunabhängigkeit

Hans Leiß

CIS-Bericht-01-127

21. März 2001

Kurzfassung erscheint in:
S.Abramsky (ed) Proceedings of the 5th International Conference on Typed Lambda Calculi and Applications, May 2–5, 2001, Krakow, Poland. Springer Verlag, LNCS 2044

Zweitstufige prä-logische Relationen und Repräsentationsunabhängigkeit

Hans Leiß

Centrum für Informations- und Sprachverarbeitung
Universität München, Oettingenstr. 67, D-80538 München
leiss@cis.uni-muenchen.de

Zusammenfassung Wir erweitern den von F. Honsell und D. Sannella eingeführten Begriff einer prä-logischen Relation zwischen Modellen des einfach getypten Lambda-Kalküls auf Modelle des zweitstufigen Lambda-Kalküls. Mit prä-logischen Relationen lassen sich für Umgebungsmodelle des zweitstufigen Lambda-Kalküls die Definierbarkeit von Elementen und die Beobachtungsgleichheit einfacher charakterisieren als mit logischen Relationen auf Erweiterungen der Modelle.

Außerdem charakterisieren wir die Repräsentationsunabhängigkeit abstrakter Datentypen und -konstruktoren durch die Existenz einer prälogischen Relation zwischen den repräsentierenden Implementationen. Das verallgemeinert Ergebnisse von J.C. Mitchell auf Sprachen und abstrakte Datentypen mit höherstufigen Konstanten.

1 Einleitung

"Logische" Relationen zwischen Termen oder Elementen von Modellen des einfach getypten λ-Kalküls erlauben es, induktiv über den Typaufbau syntaktische Eigenschaften wie die (starke) Normalisierung oder den Church-Rosser-Satz (W. Tait[Tai67], R. Statman [Sta85]) und semantische Eigenschaften wie die λ-Definierbarkeit von Elementen (G. Plotkin [Plo80], R. Statman [Sta85]) oder die Beobachtungsgleichheit von Modellen (J. Mitchell [Mit91]) zu beweisen.

Im erststufigen, d.h. einfach getypten λ-Kalkül wird eine logische Relation $\mathcal{R} = \{R_\tau \mid \tau \in \mathit{Typ}\}$ durch

$$(f,g) \in R_{(\rho\to\sigma)} \iff \forall a,b : \rho\ ((a,b) \in R_\rho \to (f\cdot a,\ g\cdot b) \in R_\sigma) \qquad (1)$$

induktiv über den Typaufbau aus Relationen R_τ auf den Grundtypen τ erzeugt. Im zweitstufigen λ-Kalkül laubt der Bereich der (semantischen) Typen keinen induktiven Aufbau mehr; trotzdem lassen sich wesentliche Ergebnisse des erststufigen Falls wie die Charakterisierung der λ-Definierbarkeit und der Beobachtungsgleichheit übertragen (vgl. J. Mitchell [MM85],[Mit86]). Der zweitstufige Kalkül dient hier als Modell von Programmiersprachen mit polymorphen Funktionen und abstrakten Datentypen.

Logische Relationen haben schon beim einfach getypten λ-Kalkül einige störende Eigenschaften, z.B. sind sie nicht unter Komposition abgeschlossen und erlauben eine Charakterisierung der Beobachtungsgleichheit nur für Sprachen ohne höherstufige Konstanten. In jüngster Zeit wurde daher von verschiedenen Autoren (vgl. [HS99], [PPST00], [PR00]) vorgeschlagen, allgemeinere *prä-logischen* Relationen zu verwenden, bei denen man in (1) die Richtung $\Leftarrow$ auf (mit korrelierten Parametern) λ-definierbare Funktionen einschränkt. F.Honsell und D. Sannella [HS99] geben verschiedene Charakterisierungen und Anwendungen prä-logischer Relationen, die die Stabilität und Nützlichkeit des Begriffs demonstrieren.

Wir setzen hier diesen Weg fort und verallgemeinern die logischen Relationen des zweitstufigen λ-Kalküls durch analoge Abschwächung der Bedingung an $R_{\forall\alpha\tau}$. Wie im erststufigen Fall lassen sich dann die λ-definierbaren Elemente eines Modells einfach als Durchschnitt aller prä-logischen Prädikate auf dem Modell beschreiben. Daraus ergibt sich eine Darstellung der Beobachtungsäquivalenz durch prä-logische Relationen.

Unser Hauptinteresse gilt aber der Äquivalenz verschiedener Implementierungen eines abstrakten Datentyps α und seiner zugehörigen Operationen $c : \sigma(\alpha)$. Zwei Repräsentationen $(\tau_i, t_i : \sigma[\tau_i/\alpha])$ von $(\alpha, c : \sigma)$ in einem Modell $\mathcal{A}$ sind äquivalent, wenn geeignet definierte Expansionen $\mathcal{A}(\tau_i, t_i)$ von $\mathcal{A}$ bezüglich der Sprache ohne α und c beobachtungsgleich sind. Für Sprachen ohne höherstufige Konstanten hat J. C. Mitchell[Mit86,Mit91] diese Äquivalenz durch die Existenz einer geeigneten logischen Relation zwischen den Expansionen charakterisiert. Programmiersprachen wie Standard ML [MTHM97] erlauben aber nicht nur höherstufige Konstante, sondern auch abstrakte Datentyp*konstruktoren*. (Da diese - anders als abstrakte Datentypen [MP85]- sich nicht durch $\exists$-Typen modellieren lassen, beschränken wir uns auf den zweitstufigen Kalkül mit $\forall$-Typen.) Wir fassen Implementierungen abstrakter Datentypkonstruktoren als Expansionen der Artenstruktur eines Modells des zweitstufigen λ-Kalküls auf. Die Repräsentationsunabhängigkeit für abstrakte Datentypkonstruktoren läßt sich dann als Existenz einer zweitstufigen prä-logischen Relation zwischen den Repräsentationen charakterisieren, auch für Sprachen mit höherstufigen Konstanten.

Die Arbeit ist wie folgt gegliedert: In Abschnitt 2 werden logische und prälogische Relationen definiert und in 2.1 an die Charakterisierung der definierbaren Elemente eines Modells und die Beobachtungsgleichheit zweier Modelle durch prä-logische Relationen erinnert. In Abschnitt 2.2 beschreiben wir die Deklaration abstrakter Datentypen als Expansion von Modellen durch definierbare Typen und Elemente und charakterisieren die Beobachtungsgleichheit zweier Repräsentationen durch die Existenz einer korrelierenden prä-logischen Relation zwischen ihnen.

Abschnitt 3 beschreibt Syntax und Semantik des zweitstufigen λ-Kalküls. Abschnitt 4 definiert zweitstufige prä-logische Relationen und gibt eine Charakterisierung der definierbaren Elemente sowie der Beobachtungsgleichheit zweitstufiger Modelle durch prä-logische Relationen. Abschnitt 4.3 behandelt abstrakte Typkonstruktoren und polymorphe Konstanten und präsentiert ein Kriterium für die Beobachtungsgleichheit zweier Repräsentationen. Abschnitt 5 nennt ei-

nige mögliche Weiterentwicklungen und potentielle Anwendungen zweitstufiger prä-logischer Relationen.

2 Prä-logische Relationen für den erststufigen λ-Kalkül

Sei T die Menge der einfachen Typen $\sigma, \tau ::= \beta \mid (\sigma \to \tau)$ über einer Menge B von Basistypen β. Wir schreiben $\Gamma \vdash t : \tau$ für einen im Kontext $\Gamma : Var \to T$ mit den üblichen Regeln typisierbaren Term, und $\lambda^{\to}_C$ für die Menge der getypten λ-Terme über einer Menge C von getypten Konstanten, $c : \sigma$.

Definition 2.1. *Ein* (extensionales) Modell $\mathcal{A} = (A, \Phi^{\to}, \Psi^{\to}, C^{\mathcal{A}})$ *des einfach getypten λ-Kalküls* $\lambda^{\to}_C$ *besteht aus einer Familie* $A = \langle A_\sigma \rangle_{\sigma \in T}$ *von Mengen, einer Interpretation* $C^{\mathcal{A}}(c) \in A_\sigma$ *der Konstanten* $c : \sigma \in C$*, und Familien* $\langle \Phi^{\to}_{\sigma,\tau} \rangle_{\sigma,\tau \in T}$ *und* $\langle \Psi^{\to}_{\sigma,\tau} \rangle_{\sigma,\tau \in T}$ *von Abbildungen*

$$\Phi^{\to}_{\sigma,\tau} : A_{(\sigma \to \tau)} \to (A_\sigma \to A_\tau) \text{ und } \Psi^{\to}_{\sigma,\tau} : (A_\sigma \to A_\tau) \to A_{(\sigma \to \tau)},$$

wobei $(A_\sigma \to A_\tau) \subseteq \{h \mid h : A_\sigma \to A_\tau\}$ *alle definierbaren Funktionen enthalten, so daß* $\Phi^{\to}_{\sigma,\tau} \circ \Psi^{\to}_{\sigma,\tau} = Id_{(A_\sigma \to A_\tau)}$ *(und* $\Psi^{\to}_{\sigma,\tau} \circ \Phi^{\to}_{\sigma,\tau} = Id_{A_{(\sigma \to \tau)}}$*) für alle* $\sigma, \tau \in T$.

Eine Belegung η über $\mathcal{A}$ *erfüllt den Kontext* Γ, kurz $\eta : \Gamma \to \mathcal{A}$, wenn $\eta(x) \in A_\sigma$ für alle $x : \sigma$ in Γ. Man interpretiert getypte Terme in $\mathcal{A}$ unter $\eta : \Gamma \to \mathcal{A}$ über

$$[\![\Gamma \rhd (r \cdot s)]\!]\eta := \Phi_{\sigma,\tau}([\![\Gamma \rhd r : (\sigma \to \tau)]\!]\eta)([\![\Gamma \rhd s : \sigma]\!]\eta),$$
$$[\![\Gamma \rhd \lambda x t : (\sigma \to \tau)]\!]\eta := \Psi_{\sigma,\tau}(\lambda a \in A_\sigma . [\![\Gamma, x : \sigma \rhd t : \tau]\!]\eta[a/x]).$$

Wir schreiben $[\![t]\!]\eta$ statt $[\![\Gamma \rhd t : \tau]\!]\eta$, wenn Γ und τ aus dem Kontext klar sind.

Definition 2.2. *Ein* Prädikat $\mathcal{R} \subseteq \mathcal{A}$ auf $\mathcal{A}$ *ist eine Familie* $\mathcal{R} = \{R_\sigma \mid \sigma \in T\}$ *mit* $R_\sigma \subseteq A_\sigma$ *für jedes* $\sigma \in T$*. Eine Belegung* $\eta : \Gamma \to \mathcal{A}$ *über* $\mathcal{A}$ respektiert $\mathcal{R}$*, kurz:* $\eta : \Gamma \to \mathcal{R}$*, wenn* $\eta(x) \in R_\sigma$ *für jedes* $x : \sigma \in \Gamma$*. Ein Prädikat* $\mathcal{R} \subseteq \mathcal{A}$ *heißt* prä-logisch*, wenn*

$$[\![\Gamma \rhd t : \tau]\!]\eta \in R_\tau$$

für jeden Term $\Gamma \rhd t : \tau$ *und jede Belegungen* $\eta : \Gamma \to \mathcal{R}$*. Eine* prä-logische Relation *zwischen* $\mathcal{A}$ *und* $\mathcal{B}$ *ist ein prä-logisches Prädikat auf* $\mathcal{A} \times \mathcal{B}$.

Die hier als Definition benutzte Eigenschaft nennen Honsell und Sannella das *Basislemma* für prä-logische Relationen. Zur Definition nehmen sie die folgenden Eigenschaften:

Lemma 2.3. *(Definition 3.2 of [HS99]) Ein Prädikat* $\mathcal{R} \subseteq \mathcal{A}$ *ist genau dann prä-logisch, wenn*

1. $\mathcal{R}$ *ist* algebraisch*, d.h. für alle* $\sigma, \tau \in T$ *und* $c : \sigma \in C$ *ist* $c^{\mathcal{A}} \in R_\sigma$ *und*

$$R_{(\sigma \to \tau)} \subseteq \{f \in A_{(\sigma \to \tau)} \mid f \cdot R_\sigma \subseteq R_\tau\},$$

2. *Für jeden Term* $\Gamma, x:\sigma \vdash t:\tau$ *und jede Belegung* $\eta:\Gamma\to\mathcal{R}$ *gilt:*

$$\forall a\in R_\sigma\ [\![\Gamma, x:\sigma \triangleright t:\tau]\!]\eta[a/x]\in R_\tau \quad\Rightarrow\quad [\![\Gamma\triangleright \lambda x t:(\sigma\to\tau)]\!]\eta\in R_{(\sigma\to\tau)}.$$

Die Definition läßt sich in naheliegender Weise auf Erweiterungen von T um z.B. kartesisches Produkt $(\sigma\times\tau)$ und disjunkte Vereinigung $(\sigma+\tau)$ ausdehnen.

Das Basislemma für logische Relationen (Fundamentalsatz, [Sta85]) besagt, daß jede logische Relation prä-logisch ist.

2.1 Definierbarkeit und Beobachtungsgleichheit

Definition 2.4. *Ein Element* a *eines Modells* $\mathcal{A}$ *von* $\lambda_C^\to$ *heißt* $\lambda_C^\to$-definierbar vom Typ τ, *wenn* $a=[\![t]\!]^{\mathcal{A}}$ *für einen geschlossenen* $\lambda_C^\to$*-Term* $\vdash t:\tau$. *Sei*

$$Def_\tau^{\mathcal{A}} := \{[\![t]\!]^{\mathcal{A}} \mid \triangleright t:\tau,\ t\in\lambda_C^\to\}\ \subseteq A_\tau$$

und $Def^{\mathcal{A}}=\{Def_\tau^{\mathcal{A}}\mid\tau\in T\}$ *die Familie der definierbaren Elemente von* $\mathcal{A}$.

Beachte, daß $Def_\tau^{\mathcal{A}}\subseteq R_\tau$ für jedes prä-logische Prädikat $\mathcal{R}\subseteq\mathcal{A}$.

Lemma 2.5. *Sei* $\mathcal{A}$ *ein Modell von* $\lambda_C^\to$ *und* $\mathcal{C}\subseteq\mathcal{A}$ *ein Prädikat auf* $\mathcal{A}$. *Dann gibt es ein kleinstes prä-logisches Prädikat* $\mathcal{R}\subseteq\mathcal{A}$ *mit* $\mathcal{C}\subseteq\mathcal{R}$.

$Def^{\mathcal{A}}$ ist i.a. kein logisches Prädikat, da normalerweise $(Def_\sigma\to Def_\tau)\not\subseteq Def_{\sigma\to\tau}$. Statman [Sta85] hat $Def^{\mathcal{A}}$ als Durchschnitt aller logischen Prädikate auf einer Erweiterung $\mathcal{A}^*\supseteq\mathcal{A}$ von $\mathcal{A}$ um unendlich viele Unbestimmte jeden Typs charakterisiert. Aber $Def^{\mathcal{A}}$ ist ein prä-logisches Prädikat (Example 3.6 in [HS99]):

Satz 2.6 *Sei* $\mathcal{A}$ *ein Modell von* $\lambda_C^\to$. *Das Element* $a\in\mathcal{A}$ *ist genau dann definierbar vom Typ* τ, *wenn* $a\in R_\tau$ *für jedes prä-logische Prädikat* $\mathcal{R}$ *auf* $\mathcal{A}$.

Wir betrachten –wie Mitchell– folgende Version der Beobachtungsgleichheit:

Definition 2.7. *Sei* $BT\subseteq T$ *eine Menge von* Beobachtungstypen *und* $\mathcal{A},\mathcal{B}$ *zwei Modelle von* $\lambda_C^\to$ *mit* $A_\tau=B_\tau$ *für alle* $\tau\in BT$. $\mathcal{A}$ *und* $\mathcal{B}$ *heißen* beobachtungsäquivalent, *kurz* $\mathcal{A}\equiv_{BT}\mathcal{B}$, *falls* $[\![t]\!]^{\mathcal{A}}=[\![t]\!]^{\mathcal{B}}$ *für alle* $\triangleright t:\tau$ *mit* $\tau\in BT$.

Honsell und Sannella[HS99] verwenden eine etwas andere Version, die Ununterscheidbarkeit durch geschlossene Gleichungen zwischen Termen mit BT-Typen.

Satz 2.8 *Es gilt* $\mathcal{A}\equiv_{BT}\mathcal{B}$ *genau dann, wenn es eine prä-logische Relation* $\mathcal{R}$ *zwischen* $\mathcal{A}$ *und* $\mathcal{B}$ *gibt, so daß für jeden Beobachtungstyp* $\tau\in BT$

$$R_\tau\cap\ (Def_\tau^{\mathcal{A}}\times Def_\tau^{\mathcal{B}})\ \subseteq\ Id_{A_\tau}=Id_{B_\tau}.$$

Beweis: $\Rightarrow$: Nach 2.6 ist $Def^{\mathcal{A}\times\mathcal{B}}$ eine prä-logische Relation zwischen $\mathcal{A}$ und $\mathcal{B}$. Wegen $\mathcal{A} \equiv_{BT} \mathcal{B}$ ist $Def^{\mathcal{A}\times\mathcal{B}}_\tau \subseteq Id_{A_\tau} = Id_{B_\tau}$ für jedes $\tau \in BT$.

$\Leftarrow$: Da $\mathcal{R}$ prä-logisch ist, gilt $[\![t]\!]^{\mathcal{A}}\, R_\tau\, [\![t]\!]^{\mathcal{B}}$, also $[\![t]\!]^{\mathcal{A}} = [\![t]\!]^{\mathcal{B}}$ für $t : \tau \in BT$. $\square$

Mit logischen Relationen gilt $\Rightarrow$ nur, wenn C keine höherstufigen Konstanten hat (vgl. Example 8.3 in [HS99]):

Beispiel 2.9 *Sei $\mathcal{N}$ die volle Typhierarchie über $\mathbb{N}$ mit $0^{\mathcal{N}} = 0, 1^{\mathcal{N}} = 1$. Sei $f : (\mathtt{nat} \to \mathtt{nat}) \to \mathtt{nat}$ eine Konstante, und $\mathcal{N}_i$ die Expansion von $\mathcal{N}$ um f_i,*

$$f_1(g) := 0 \textit{ für alle } g, \qquad f_2(g) := \begin{cases} 0, & \textit{falls } g \textit{ berechenbar,} \\ 1 & \textit{sonst.} \end{cases}$$

Dann ist $\mathcal{N}_1 \equiv_{\mathtt{nat}} \mathcal{N}_2$, da bei der Auswertung geschlossener Terme nur berechenbare Funktionen benutzt werden. Ist $\mathcal{R} \subseteq \mathcal{N}_1 \times \mathcal{N}_2$ logisch, *so ist $(g, g) \in R_{\mathtt{nat}\to\mathtt{nat}}$ für jedes g. Für nicht-berechenbares g ist daher auch $(0, 1) = (f_1 g, f_2 g) \in R_{\mathtt{nat}}$. Also gilt die Bedingung aus 2.8 nicht.*

2.2 Abstrakte Datentypen und Repräsentationsunabhängigkeit

Durch die Deklaration eines abstrakten Datentyps,

$$(\textbf{abstype } (\alpha, x : \sigma) \textbf{ with } x : \sigma \triangleright e_1 = e_2 : \rho \textbf{ is } (\tau, t : \sigma[\tau/\alpha]) \textbf{ in } s), \qquad (2)$$

werden ein "neuer" Typ α und ein "neues" Objekt $x : \sigma(\alpha)$ mit "definierender" Eigenschaft $e_1 = e_2$ erklärt, die im Anwendungsterm s durch den Typ τ und den Term t interpretiert werden, wobei α im Typ von s nicht vorkomme. Bei der Auswertung von (2) in einem Modell $\mathcal{A}$ von $\lambda^{\to}_C$ wird α durch A_τ und x durch den Wert von $t : \sigma[\tau/\alpha]$ interpretiert, und s in der so gegebenen Expansion von $\mathcal{A}$ ausgewertet.

Der Datentyp $(\alpha, x : \sigma)$ ist *abstrakt* in s, wenn der Wert von s von der verwendeten Darstellung (τ, t) unabhängig ist; d.h. wenn für je zwei Darstellungen $(\tau_i, t_i : \sigma[\tau_i/\alpha])$, $i = 1, 2$, die die Gleichung $x : \sigma \triangleright e_1 = e_2 : \rho$ erfüllen, gilt:

$$[\![s]\!]^{\mathcal{A}(\tau_1,t_1)} = [\![s]\!]^{\mathcal{A}(\tau_2,t_2)}. \qquad (3)$$

Um die Gleichung $e_1 = e_2$ in einer Expansion $\mathcal{A}(\tau_i, t_i)$ zu erfüllen, wird die Gleichheit auf dem Typ α normalerweise nicht durch die Gleichheit auf A_{τ_i} interpretiert, sondern durch eine geeignete partielle Äquivalenzrelation auf A_{τ_i}:

$$[\![(\textbf{abstype } (\alpha, x_0 : \sigma_0) \textbf{ with } x_0 : \sigma_0 \triangleright e_1 = e_2 : \rho \textbf{ is } (\tau_0, t : \sigma_0[\tau_0/\alpha]) \textbf{ in } s)]\!]^{\mathcal{A}}\eta$$
$$:= \begin{cases} (\textit{let } \mathcal{A}^+ = \mathcal{A}(\tau_0, [\![t]\!]^{\mathcal{A}}\eta) \textit{ in } [\![s]\!]^{\mathcal{A}^+}\eta), & \text{falls es eine prä-logische} \\ & \text{partielle Äquivalenzrelation } \mathcal{E} \subseteq \mathcal{A}^+ \times \mathcal{A}^+ \text{ gibt mit} \\ & ([\![e_1]\!]\eta^{\mathcal{A}^+}, [\![e_2]\!]\eta^{\mathcal{A}^+}) \in E_\rho \text{ und } E_\tau = Id_{A_\tau} \text{ für } \tau \in T, \\ \textit{error}, & \text{sonst.} \end{cases} \qquad (4)$$

Man beachte, daß im ersten Fall eine kleinste solche Relation $\mathcal{E}$ existiert, und daß $\mathcal{A}$ kanonisch in $\mathcal{A}^+/\mathcal{E} \models e_1 = e_2$ eingebettet ist. Da $\mathcal{E}$ prä-logisch ist, gilt $E_{\sigma_0}(x_0, x_0)$ in $\mathcal{A}^+$, und die durch t eingeführten Operationen gehören zu $\mathcal{A}^+/\mathcal{E}$. Da aber α im Typ von s nicht vorkommt, sind die Werte von s in $\mathcal{A}^+$ und in $\mathcal{A}^+/\mathcal{E}$ dieselben, falls die Gleichheit auf α in s nicht benutzt wird, so daß es unnötig ist, $\mathcal{A}^+/\mathcal{E}$ tatsächlich zu konstruieren.

Definition 2.10. *Sei T^+ die Menge der aus den Basistypen von T mit einem neuen Basistyp α aufgebauten Typen, $\sigma_0 \in T^+$ und $C^+ = C, x_0 : \sigma_0$. Sei $\tau_0 \in T$, $a \in A_{\sigma_0[\tau_0/\alpha]}$ und $\mathcal{A}(\tau_0, a) = \mathcal{A}^+ := (A^+, \Phi^+, \Psi^+, (C^+)^{\mathcal{A}^+})$ gegeben durch:*

$$A^+_\sigma := A_{\sigma[\tau_0/\alpha]}, \qquad (\Phi^+)^{\rightarrow}_{\sigma,\tau} := \Phi^{\rightarrow}_{\sigma[\tau_0/\alpha],\tau[\tau_0/\alpha]},$$

$$(C^+)^{\mathcal{A}^+}(c) = \begin{cases} C^{\mathcal{A}}(c), & c : \tau \in C, \\ a, & c : \tau \equiv x_0 : \sigma_0, \end{cases} \qquad (\Psi^+)^{\rightarrow}_{\sigma,\tau} := \Psi^{\rightarrow}_{\sigma[\tau_0/\alpha],\tau[\tau_0/\alpha]}.$$

Das Modell $\mathcal{A}^+$ von $\lambda^{\rightarrow}_{C^+}$ heiße die durch (τ_0, a) definierte Expansion *von $\mathcal{A}$.*

Von nun an konzentrieren wir uns auf die Äquivlenz zweier Repräsentationen und ignorieren die Einschränkung auf Expansionen, die die Spezifikation $e_1 = e_2$ erfüllen. Zwei Expansionen $\mathcal{A}(\tau_1, t_1)$ und $\mathcal{A}(\tau_2, t_2)$ von $\mathcal{A}$ sind *äquivalente Repräsentationen des abstrakten Typs* $(\alpha, x : \sigma)$, wenn (3) für alle Terme s gilt, in deren Typ α nicht vorkommt, d.h. wenn $\mathcal{A}(\tau_1, t_1) \equiv_T \mathcal{A}(\tau_2, t_2)$ gilt.

Wir können also die Äquivenz zweier Repräsentationen von $(\alpha, x : \sigma)$ als Beobachtungsgleichheit $\mathcal{A}(\tau_1, t_1) \equiv_T \mathcal{A}(\tau_2, t_2)$ ansehen. Sie wird nun durch die Existenz einer geeigneten prä-logischen Relation zwischen den Expansionen charakterisiert. Damit auch geschachtelte Deklarationen abstrakter Datentypen erfaßt sind, gehen wir dabei nicht mehr vom gleichen Modell $\mathcal{A}$ aus, sondern von zwei schon korrellierten Modellen $\mathcal{A}\,\mathcal{R}\,\mathcal{B}$:

Satz 2.11 *Seien $\mathcal{A}$ und $\mathcal{B}$ durch eine prä-logische Relation $\mathcal{R}$ korreliert, und seien $\mathcal{A}^+$ und $\mathcal{B}^+$ definierbare Expansionen von $\mathcal{A}$ und $\mathcal{B}$ zu Modellen von $\lambda^{\rightarrow}_{C^+}$. Dann sind folgende Aussagen äquivalent:*

(i) Für jeden geschlossenen $\lambda^{\rightarrow}_{C^+}$-Term $t : \tau$ mit $\tau \in T$ ist $[\![t]\!]^{\mathcal{A}^+}\ R_\tau\ [\![t]\!]^{\mathcal{B}^+}$.
(ii) Es gibt eine prä-logische Relation $\mathcal{R}^+$ mit $\mathcal{A}^+\,\mathcal{R}^+\,\mathcal{B}^+$ und $R^+_\rho = R_\rho$ für $\rho \in T$.

Beweis: Zur Vereinfachung der Schreibweise betrachten wir den einstelligen Fall, d.h. prä-logische Prädikate $\mathcal{R} \subseteq \mathcal{A}$ und $\mathcal{R}^+ \subseteq \mathcal{A}^+$. (ii) $\Rightarrow$ (i) ist offensichtlich. (i) $\Rightarrow$ (ii): Für $\tau \in T^+$ sei

$$Def^+_\tau = \{[\![t]\!]^{\mathcal{A}^+} \mid t \in \lambda^{\rightarrow}_{C^+},\ \vdash t : \tau\} \qquad \text{und} \qquad C_\tau := \begin{cases} R_\tau, & \tau \in T, \\ Def^+_\tau, & \text{sonst.} \end{cases}$$

Nach Voraussetzung ist $Def^+_\tau \subseteq R_\tau$ für jedes $\tau \in T$. Jedes logische Prädikat $\mathcal{R}^+$ auf $\mathcal{A}^+$ wie in (ii) erfüllt insbesondere die Bedingungen

$$X_\tau \supseteq C_\tau \cup \bigcup \{X_{(\rho\to\tau)} \cdot X_\rho \mid \rho \in T^+\}, \qquad \tau \in T^+. \tag{5}$$

Sei $\mathcal{R}^+ = \{R^+_\tau \mid \tau \in T^+\}$ die kleinste Lösung des Systems (5) in $\mathcal{A}^+$. Dies ist ein prä-logisches Prädikat auf $\mathcal{A}^+$: ist $\eta : \Gamma \to \mathcal{R}^+$ eine Belegung, und $\Gamma \vdash t : \tau$ ein $\lambda^{\to}_{C^+}$-Term, etwa $\Gamma = \{x : \sigma\}$, so ist mit $a = \eta(x) \in R^+_\sigma$

$$[\![\Gamma \triangleright t : \tau]\!]\eta = [\![\triangleright \lambda x : \sigma.t : \sigma \to \tau]\!] \cdot a \in Def^+_{\sigma\to\tau} \cdot R^+_\sigma \subseteq R^+_{\sigma\to\tau} \cdot R^+_\sigma \subseteq R^+_\tau.$$

Man überlegt sich leicht, daß für jedes $\tau \in T^+$

$$R^+_\tau = \bigcup\{Def^+_{\rho_1\to\ldots\to\rho_n\to\tau} \cdot R_{\rho_1} \cdots R_{\rho_n} \mid n \in I\!N, \rho_1, \ldots \rho_n \in T\}.$$

Da für $\boldsymbol{\rho}, \tau \in T$ nach (i) $Def^+_{\boldsymbol{\rho}\to\tau} \subseteq R_{\boldsymbol{\rho}\to\tau}$ und damit $Def^+_{\boldsymbol{\rho}\to\tau} \cdot R_{\boldsymbol{\rho}} \subseteq R_\tau$ gilt, folgt $R^+_\tau \subseteq R_\tau$. Daher ist auch $R^+_\tau = R_\tau$ für $\tau \in T$. □

Der Satz gilt natürlich ebenso für Erweiterungen von $\lambda^{\to}_C$ um Typkonstruktoren, die monoton in ihren Argumenttypen sind, wenn man den Begriff des prälogischen Prädikates entsprechend anpaßt. Wir betrachten drei Fälle:

1. Kartesische Produkte $\sigma \times \tau$: Die Sprache von $\lambda^{\to,\times}_C$ enthalte Konstanten $\pi_i : \sigma_1 \times \sigma_2 \to \sigma_i$ und $\langle\cdot,\cdot\rangle : \sigma_1 \to \sigma_2 \to \sigma_1 \times \sigma_2$ mit den Reduktionsregeln

   $$\pi_i\langle t_1, t_2\rangle \to_\pi t_i, \qquad \text{für } i = 1, 2.$$

   Ein prä-logisches Prädikat $\mathcal{R}$ auf einem Modell $\mathcal{A}$ von $\lambda^{\to,\times}_C$ enthält die Interpretation dieser Konstanten, erfüllt also für $i = 1, 2$

   $$\forall a \in R_{\sigma_1\times\sigma_2}\ \pi_i \cdot a \in R_{\sigma_i} \quad \text{und} \quad \forall a_1 \in R_{\sigma_1} \forall a_2 \in R_{\sigma_2}\ \langle a_1, a_2\rangle \in R_{\sigma_1\times\sigma_2}.$$

   (Daraus *folgt* aber nicht, daß $\pi_i^{\mathcal{A}} \in R_{\sigma_1\times\sigma_2\to\sigma_i}$ und $\langle\cdot,\cdot\rangle^{\mathcal{A}} \in R_{\sigma_1\to\sigma_2\to\sigma_1\times\sigma_2}$.)
2. Disjunkte Vereinigungen $(\sigma + \tau)$: Die Sprache von $\lambda^{\to,+}_C$ enthalte Konstante

   $$inj_i : \sigma_i \to (\sigma_1 + \sigma_2) \quad \text{und} \quad case : (\sigma_1 + \sigma_2) \to (\sigma_1 \to \rho) \to (\sigma_2 \to \rho) \to \rho$$

   mit den Reduktionsregeln

   $$(case\ (inj_i\ s)\ then\ s_1\ else\ s_2) \to_{case} s_i\, s \qquad \text{für } i = 1, 2.$$

   Ein prälogisches Prädikat $\mathcal{R}$ auf einem Modell $\mathcal{A}$ von $\lambda^{\to,+}_C$ erfüllt für $i = 1, 2$ die Bedingungen

   $$\forall a \in R_{\sigma_i}\ inj_i a \in R_{\sigma_1+\sigma_2} \quad \text{und}$$
   $$\forall a \in R_{\sigma_1+\sigma_2} \forall f_1 \in R_{\sigma_1\to\rho}\, \forall f_2 \in R_{\sigma_2\to\rho}\ (case\ a\ then\ f_1\ else\ f_2) \in R_\rho.$$

3. Homogene Listen τ^*: Die Sprache von $\lambda^{\to,^*}_C$ enthalte Konstante $nil : \sigma^*, cons : \sigma \to \sigma^* \to \sigma^*, hd : \sigma^* \to \sigma, tl : \sigma^* \to \sigma^*$ mit den Reduktionsregeln

   $$hd(consst) \to_{hd} s, \quad tl(consst) \to_{cons} t.$$

   Ein prä-logisches Prädikat $\mathcal{R}$ auf einem Modell von $\lambda^{\to,^*}_C$ erfüllt

   $$nil \in R_{\sigma^*} \quad \text{und} \quad \forall a \in R_\sigma\, \forall b \in R_{\sigma^*}\ consab \in R_{\sigma^*},\ hd\, b \in R_{\sigma^*},\ tl\, b \in R_{\sigma^*}.$$

2.3 Ein Kriterium für Repräsentationsunabhängigkeit

Wir vergleichen Satz 2.11 mit einem schwächeren Satz von Mitchell. Eine Konstante $c : \tau \in C^+$ ist *erststufig in* α, wenn $st_\alpha(\tau) \leq 1$, wobei $st_\alpha(\tau) = 0$ falls $\alpha \notin frei(\tau)$ oder $\tau \equiv \alpha$, und $st_\alpha(\rho \to \sigma) = \max\{st_\alpha(\rho) + 1, st_\alpha(\sigma)\}$ sonst.

Satz 2.12 *(cf. [Mit91], Cor.1) Seien $\mathcal{A}$ und $\mathcal{B}$ durch eine logische Relation $\mathcal{R}$ korreliert, und seien $\mathcal{A}^+$ und $\mathcal{B}^+$ definierbare Expansionen von $\mathcal{A}$ und $\mathcal{B}$ zu Modellen von $\lambda^{\to}_{C^+}$. Dann gilt (ii) $\Rightarrow$ (i), und wenn alle Konstanten von C^+ erststufig in α sind*[1]*, auch (i) $\Rightarrow$ (ii).*

(i) Für jeden geschlossenen $\lambda^{\to}_{C^+}$-Term $t : \tau$ mit $\tau \in T$ ist $[\![t]\!]^{\mathcal{A}^+} \; R_\tau \; [\![t]\!]^{\mathcal{B}^+}$.
(ii) Es gibt eine logische Relation $\mathcal{R}^+$ mit $\mathcal{A}^+ \, \mathcal{R}^+ \, \mathcal{B}^+$ und $R^+_\rho = R_\rho$ für alle $\rho \in T$.

Beweis: Wir schreiben wieder einstellige Prädikate statt Relationen.

(ii) $\Rightarrow$ (i): Mit Hilfe des Fundamentallemmas für logische Relationen.

(i) $\Rightarrow$ (ii): Sei $\mathcal{X} = \{X^\infty_\tau \mid \tau\}$ die kleinste Lösung des Systems (5). Nach Satz 2.11 ist $X^\infty_\tau = R_\tau$ für $\tau \in T$. Definiere $\mathcal{R}^+$ durch

$$R^+_\tau := \begin{cases} X^\infty_\tau, & \tau \in T^+ \text{ ein Basistyp}, \\ (R^+_\rho \to R^+_\tau), & \tau \equiv (\rho \to \sigma), \end{cases}$$

wobei $(R^+_\rho \to R^+_\tau) := \{f \in A^+_{(\rho\to\sigma)} \mid f \cdot R^+_\rho \subseteq R^+_\sigma\}$. Die Relation $\mathcal{R}^+$ ist logisch, wenn $c \in R^+_\tau$ für jedes $c : \tau \in C^+$. Da $c \in C_\tau \subseteq X^\infty_\tau$ ist, genügt dazu $X^\infty_\tau \subseteq R^+_\tau$ für alle τ mit $st_\alpha(\tau) \leq 1$. Für $st_\alpha(\tau) = 0$ ist $X^\infty_\tau = R^+_\tau$ und falls $\tau \in T$, auch $R^+_\tau = R_\tau$: Für Grundtypen $\tau \in T$ ist $R^+_\tau = X^\infty_\tau = R_\tau$, und für $(\rho \to \sigma) \in T$ ist induktiv auch $R^+_{(\rho\to\sigma)} = (R^+_\rho \to R^+_\sigma) = (R_\rho \to R_\sigma) = R_{(\rho\to\sigma)} = X^\infty_{(\rho\to\sigma)}$. Außerdem ist $X^\infty_\alpha = R^+_\alpha$. Für $st_\alpha(\tau) = 1$ ist $\tau \equiv (\rho \to \sigma)$ mit $st_\alpha(\rho) = 0$ und $st_\alpha(\sigma) \leq 1$, so daß nach (5) und Induktion

$$X^\infty_{(\rho\to\sigma)} \;\subseteq\; X^\infty_\rho \to X^\infty_\sigma \;=\; R^+_\rho \to X^\infty_\sigma \;\subseteq\; R^+_\rho \to R^+_\sigma \;=\; R^+_{(\rho\to\sigma)}.$$

Also ist $\mathcal{R}^+$ ein logisches Prädikat auf $\mathcal{A}^+$, das $\mathcal{R}$ wie gewünscht fortsetzt. □

Das folgende Lemma liefert in (i) ein 'lokales' Kriterium, um die Beobachtungsgleichheit zweier Implementierungen eines abstrakten Datentyps nachzuweisen:

Lemma 2.13. *(vgl. Lemma 4 in [Mit86]) Seien $\mathcal{A}$ und $\mathcal{B}$ durch eine logische Relation $\mathcal{R}$ korreliert, und seien $\mathcal{A}^+$ und $\mathcal{B}^+$ definierbare Expansionen von $\mathcal{A}$ und $\mathcal{B}$ zu Modellen von $\lambda^{\to}_{C^+}$. Dann sind (ii) und (i) äquivalent:*

(i) Es gibt eine Relation $R^+_\alpha \subseteq \mathcal{A}^+_\alpha \times \mathcal{B}^+_\alpha$, so daß $c^{\mathcal{A}^+} \, R^+_\tau \, c^{\mathcal{B}^+}$ für jedes $c : \tau \in C^+ \setminus C$, wobei $R^+_\tau := R_\tau$ für $\tau \in T$ und $R^+_{(\rho\to\sigma)} = (R^+_\rho \to R^+_\sigma)$.

[1] Mitchell verlangt, daß alle Konstanten von C^+ sogar erststufig sind.

(ii) Es gibt eine logische Relation $\mathcal{R}^+$ mit $\mathcal{A}^+ \mathcal{R}^+ \mathcal{B}^+$ und $R^+_\rho = R_\rho$ für alle $\rho \in T$.

Beispiel 2.14 *Eine (endliche) A-*Multimenge *ist der Graph einer endlichen Funktion $f : A \to \mathbb{N}^+$ von A in die positiven ganzen Zahlen. Wir wollen einen Typ*[2] *der Multimengen in SML mit z.T. höherstufigen Operationen definieren:*

```
signature BAG =
  sig
    type 'a bag
    val empty : 'a bag
    val member : ''a -> ''a bag -> int
    val insert : ''a * int -> ''a bag -> ''a bag
    val map : ('a -> ''b) -> 'a bag -> ''b bag
    val union : ('a -> ''b bag) -> 'a bag -> ''b bag
  end
```

Ein A-bag B repräsentiert die Multimenge $\{(a, n) \mid$ `member` *$a\ B = n > 0, a \in A\}$. Betrachte folgende Implementierungen von Multimengen durch Listen:*

```
structure Bag1 :> BAG =
  struct
    type 'a bag = 'a list
    val empty = []
    fun member a [] = 0
      | member a (b::B) = if a=b then 1 + (member a B)
                          else (member a B)
    fun insert (a,m) B = if m > 0 then a::(insert (a,m-1) B) else B
    fun map f [] = []
      | map f (b::B) = (f b)::(map f B)
    fun union f [] = []
      | union f (b::B) = (f b) @ (union f B)
  end
```

Die Implementierung `Bag1` *liefert die gewünschten Antworten; platzsparender ist es, wenn man sich die Vielfachheiten bei den Elementen merkt:*

```
structure Bag2 :> BAG =
  struct
    type 'a bag = ('a * int) list
    val empty = []
    fun member a [] = 0
      | member a ((b,n)::B) = if a=b then n else (member a B)
    fun insert (a,m) [] = [(a,m)]
      | insert (a,m) ((b,n)::B) = if a=b then (b,n+m)::B
                                  else (b,n)::(insert (a,m) B)
    fun map f [] = []
```

[2] Man nehme hier an, $\alpha = \beta$ sei ein fester Typ von T. In SML wird ein *Typkonstruktor* *bag* $: T \Rightarrow T$ einführt, da `'a` und `''b` Typvariable sind. Dazu siehe Abschnitt 4.3.

```
    | map f ((b,n)::B) = let val c = f b
                            val C = map f B
                        in
                          insert (c,n) C
                        end
fun union f [] = []
  | union f ((b,n)::B) = let fun addAll [] C = C
                               | addAll ((a,m)::A) C
                               = addAll A (insert (a,n*m) C)
                         in
                           addAll (f b) (union f B)
                         end
end
```

Seien $\mathcal{A}_1^+ := \mathcal{A}(\texttt{Bag1})$ *und* $\mathcal{A}_2^+ := \mathcal{A}(\texttt{Bag2})$ *Expansionen des zu Grunde liegenden Modells* $\mathcal{A}$*. Die Beobachtungsgleichheit von* $\mathcal{A}_1^+$ *und* $\mathcal{A}_2^+$ *bezüglich der bag-freien Typen* T *folgt aus Satz 2.12, (ii)* $\Rightarrow$ *(i), und Korollar 2.13, wenn man eine geeignete Relation* $R^+_{\alpha\ bag}$ *(und* $\mathcal{R} = Id_{\mathcal{A}}$*) zu einer logischen Relation* $\mathcal{R}^+$ *fortsetzen kann, die die neuen Konstanten korreliert. Für Elemente* $B_1 : \alpha^*$ *und* $B_2 : (\alpha \times \texttt{int})^*$ *gelte* $(B_1, B_2) \in R^+_{(\alpha\ bag)}$ *genau dann, wenn*

(i) B_1 *und* B_2 *dieselbe Multimenge repräsentieren,*
(ii) B_2 *keine Paare* (a, n) *mit* $n \leq 0$ *und zu jedem* a *höchstens ein* (a, n) *enthält.*

Da $R^+_{\alpha\ bag}$ *nur die gewünschten Repräsentanten derselben Multimengen korreliert, sind die Interpretationen von* `empty`, `member`, `insert`, `map`, `union` *durch* $\mathcal{R}^+$ *korreliert, obwohl z.B. der Typ von* `union` *zweitstufig in* α *bag ist. Wegen*

$$R^+_{(\alpha\to\alpha\ bag)\to\alpha\ bag\to\alpha\ bag} = ((R_\alpha \to R^+_{\alpha\ bag}) \to (R^+_{\alpha\ bag} \to R^+_{\alpha\ bag}))$$

muß man nur zeigen, daß für jedes $f \in (R_\alpha \to R^+_{\alpha\ bag})$ *und* $B \in R^+_{\alpha\ bag}$ *auch* $union \cdot f \cdot B \in R^+_{\alpha\ bag}$ *ist. Durch (ii) werden unerwünschte Repräsentanten von Multimengen ausgeschlossen, was die Definitionen der Operationen vereinfacht. Dies entspricht der partiellen Äquivalenzrelation* $\mathcal{E}$ *aus (4).*

Wenn $\mathcal{R}$ nur eine prä-logische Relation ist, sichert die Bedingung (i) aus 2.13 aber *nicht* die Existenz einer prä-logischen Relation wie in (ii): dazu braucht man nach Theorem 2.11 nämlich $Def^+_{\sigma\to\tau} \subseteq R_{\sigma\to\tau}$ für $(\sigma \to \tau) \in T$. Aber für $f \in (R_\sigma \to R_\tau) \setminus R_{(\sigma\to\tau)}$ und $f = c_2 \circ c_1$ mit Konstanten $c_1 : \sigma \to \rho$ und $c_2 : \rho \to \tau$ für $\rho \notin T$ gilt das nicht.

Obwohl also prä-logische Relationen eine *Charakterisierung* der Beobachtungsgleichheit auch für Sprachen mit höherstufigen Konstanten erlauben, scheint ein *Nachweisen* der Beobachtungsäquivalenz mit ihnen schwieriger: anstatt nur die lokale Bedingung (i) von 2.13 zeigen zu müssen, muß man auch alle neuen Terme von altem Typ betrachten, was auf einen direkten Nachweis der Beobachtungsgleichheit hinauszulaufen scheint.

3 Der zweitstufige λ-Kalkül, $\lambda_C^{\rightarrow,\forall}$

Wir betrachten nun Definierbarkeit und Beobachtungsäquivalenz für den zweitstufigen λ-Kalkül $\lambda_C^{\rightarrow,\forall}$. Die Charakterisierung durch prä-logische Relationen ist hier aufwendiger als bei $\lambda_C^{\rightarrow}$, da diese sich nicht mehr durch Induktion über den Aufbau der Typ*ausdrücke* definieren lassen.

3.1 Konstruktoren und Terme von $\lambda_C^{\rightarrow,\forall}$

Allgemeiner lassen wir nun Ausdrücke zu, mit denen man Typen berechnen kann. Die Klassifizierung C der Konstanten wird in zwei Komponenten aufgespalten, $C = (C_{Art}, C_{Typ})$. Neben $\rightarrow, \forall$ können dadurch weitere Typkonstruktoren als Konstante vorgeben werden.

Wir definieren zuerst eine Oberklasse von Ausdrücken, aus denen die eigentlichen Typen und Terme relativ zu einem Kontext ausgesondert werden.

Definition 3.1. *Die* Arten κ *von* $\lambda_C^{\rightarrow,\forall}$ *sind durch* $\kappa := T \mid (\kappa \Rightarrow \kappa)$ *gegeben. Die Klassifikation* C *der Konstanten wird in zwei Komponenten,* $C = (C_{Art}, C_{Typ})$*, aufgespalten. Durch* C_{Art}*, einer Menge von Annahmen der Form* $c : \kappa$*, wird jeder Konstrukturkonstanten* c *eindeutig eine Art* κ *zugeordnet. Insbesondere enthalte* C_{Art} *die Typkonstruktoren*

$$\rightarrow : \ T \Rightarrow (T \Rightarrow T) \quad \textit{und} \quad \forall : \ (T \Rightarrow T) \Rightarrow T.$$

Ein Konstruktor der Art κ *ist eine mit folgenden Regeln von* $\lambda_{C_{Art}}^{\Rightarrow}$ *herleitbare Sequenz* $\Delta \triangleright \mu : \kappa$*, wobei* Δ *ein Kontext von Artannahmen für Konstruktorvariable ist:*

$$(Mon)\ \frac{\Delta \triangleright \mu : \kappa}{\Delta, \upsilon : \kappa' \triangleright \mu : \kappa}, \quad \upsilon \notin dom(\Delta)$$

$$(Const)\ \Delta \triangleright c : \kappa, \quad \textit{für } c : \kappa \in C_{Art} \qquad (Var)\ \Delta, \upsilon : \kappa \triangleright \upsilon : \kappa$$

$$(\Rightarrow E)\ \frac{\Delta \triangleright \mu : (\kappa_1 \Rightarrow \kappa_2), \quad \Delta \triangleright \nu : \kappa_1}{\Delta \triangleright (\mu \cdot \nu) : \kappa_2} \qquad (\Rightarrow I)\ \frac{\Delta, \upsilon : \kappa_1 \triangleright \mu : \kappa_2}{\Delta \triangleright \lambda\upsilon.\mu : (\kappa_1 \Rightarrow \kappa_2)}.$$

Für $\lambda_{C_{Art}}^{\Rightarrow}$ *nehmen wir eine Reduktionsrelation* $\rightsquigarrow$ *an, die die* α, β, η*-Reduktion umfaßt und die Subjekterhaltungseigenschaft erfüllt, d.h. wenn* $\Delta \vdash \mu : \kappa$ *und* $\mu \rightsquigarrow \nu$*, so ist* $\Delta \vdash \nu : \kappa$*.*

$$(=_1)\ \frac{\Delta \triangleright \mu : \kappa \qquad \mu \rightsquigarrow \nu}{\Delta \triangleright \mu = \nu : \kappa} \qquad (=_2)\ \frac{\Delta \triangleright \mu : \kappa \qquad \mu \rightsquigarrow \nu}{\Delta \triangleright \nu = \mu : \kappa}$$

Ein Typ $\Delta \triangleright \mu : T$ *ist eine Konstruktor der Art* T*. Wir benutzen* τ, σ *für Typen und schreiben* $(\sigma \rightarrow \tau)$ *und* $\forall\upsilon\tau$ *usw. Durch* C_{Typ}*, einer Menge von Annahmen*

der Form $c : \mu$, wird jeder Individuenkonstanten c eindeutig ein geschlossener Konstruktor μ der Art T zugeordnet.

Ein getypter Term *ist eine Sequenz $\Delta\,;\,\Gamma \triangleright t : \tau$, die mit folgenden Regeln*[3] *herleitbar ist, wobei Δ ein Kontext von Artannahmen für Konstruktorvariable und Γ ein Kontext von Typannahmen für Individuenvariable ist:*

$$(mon)\ \frac{\Delta\,;\,\Gamma \triangleright t : \tau \qquad \Delta \triangleright \sigma : T}{\Delta\,;\,\Gamma, x : \sigma \triangleright t : \tau}, \quad x \notin dom(\Gamma)$$

$$(const)\ \frac{\triangleright \tau : T}{\Delta\,;\,\Gamma \triangleright c : \tau}, \quad \text{für } c : \tau \in C_{Typ}$$

$$(var)\ \frac{\Delta \triangleright \tau : T}{\Delta\,;\,\Gamma, x : \tau \triangleright x : \tau}, \quad x \notin dom(\Gamma)$$

$$(\to I)\ \frac{\Delta \triangleright \sigma : T \qquad \Delta\,;\,\Gamma, x : \sigma \triangleright t : \tau}{\Delta\,;\,\Gamma \triangleright (\lambda x : \sigma.t) : (\sigma \to \tau)}$$

$$(\to E)\ \frac{\Delta \triangleright \tau : T \qquad \Delta\,;\,\Gamma \triangleright t : (\sigma \to \tau) \qquad \Delta\,;\,\Gamma \triangleright s : \sigma}{\Delta\,;\,\Gamma \triangleright (t \cdot s) : \tau}$$

$$(\forall I)\ \frac{\Delta \triangleright \mu : (T \Rightarrow T) \qquad \Delta, \alpha : T\,;\,\Gamma \triangleright t : (\mu \cdot \alpha)}{\Delta\,;\,\Gamma \triangleright \lambda \alpha t : \forall \mu}, \quad \text{falls } \alpha \text{ nicht in } \Gamma$$

$$(\forall E)\ \frac{\Delta \triangleright \mu : (T \Rightarrow T) \qquad \Delta \triangleright \tau : T \qquad \Delta\,;\,\Gamma \triangleright t : \forall \mu}{\Delta\,;\,\Gamma \triangleright (t \cdot \tau) : (\mu \cdot \tau)}$$

$$(Typ =)\ \frac{\Delta\,;\,\Gamma \triangleright t : \tau \qquad \Delta \triangleright \tau = \sigma : T}{\Delta\,;\,\Gamma \triangleright t : \sigma}$$

Proposition 3.2. *Ist $\Delta\,;\,\Gamma \vdash t : \sigma$, so ist auch $\Delta \vdash \sigma : T$.*

Beweis: Durch Induktion über die Herleitung. Im Fall (Typ =) benutzt man die Subjekterhaltungseigenschaft von $\lambda^{\Rightarrow}_{C_{Art}}$. □

3.2 Umgebungsmodelle von $\lambda^{\to,\forall}_{C}$

Definition 3.3. *Ein* Modellrahmen $\mathcal{M} = (\mathcal{U}, \mathcal{D}, \Phi, \Psi)$ *für $\lambda^{\to,\forall}_{C}$ besteht aus*

1. *einem extensionalen Modell $\mathcal{U} = (\langle U_\kappa \rangle_{\kappa \in Art}, \Phi^{\Rightarrow}, \Psi^{\Rightarrow}, C^{\mathcal{U}}_{Art}, [\![\cdot]\!]^{\mathcal{U}} \cdot)$ von $\lambda^{\Rightarrow}_{C_{Art}}$ zur Interpretation der Konstruktoren,*
2. *Einer Familie von Individuenbereichen für die Typen, $\mathcal{D} = (\langle D_A \rangle_{A \in U_T}, C^{\mathcal{D}}_{Typ})$, mit Elementen $C^{\mathcal{D}}_{Typ}(c) \in D_{[\![\tau]\!]^{\mathcal{U}}}$ für $c : \tau \in C_{Typ}$,*

[3] Die Annahmen $\Delta \triangleright \sigma : T$ and $\Delta \triangleright \tau : T$ in $(\to I)$ and $(\to E)$ ersparen es, Eigenschaften der Herleitung von Artaussagen nachzuweisen, was wegen $(\forall I)$ and $(=_i)$ umständlich ist.

3. *Abbildungsscharen* $\Phi = (\Phi^{\to}, \Phi^{\forall})$, $\Psi = (\Psi^{\to}, \Psi^{\forall})$ *mit* $\Phi^{\to} = \langle \Phi^{\to}_{A,B} \rangle_{A,B \in U_T}$, $\Phi^{\forall} = \langle \Phi^{\forall}_f \rangle_{f \in U_{(T \Rightarrow T)}}, \Psi^{\to} = \langle \Psi^{\to}_{A,B} \rangle_{A,B \in U_T}$, *und* $\Psi^{\forall} = \langle \Psi^{\forall}_f \rangle_{f \in U_{(T \Rightarrow T)}}$ *wobei*

$$\Phi^{\to}_{A,B} : D_{(A \to B)} \longrightarrow (D_A \to D_B) \qquad \Psi^{\to}_{A,B} : (D_A \to D_B) \longrightarrow D_{(A \to B)}$$
$$\Phi^{\forall}_f : D_{\forall f} \longrightarrow (\Pi A \in U_T . D_{f \cdot A}) \qquad \Psi^{\forall}_f : (\Pi A \in U_T . D_{f \cdot A}) \longrightarrow D_{\forall f},$$

für gewisse Teilmengen

$$\begin{aligned} (D_A \to D_B) &\subseteq \{h \mid h : D_A \to D_B\} \quad \textit{und} \\ (\Pi A \in U_T . D_{f \cdot A}) &\subseteq \Pi A \in U_T . D_{f \cdot A}, \end{aligned}$$

so daß für alle $A, B \in U_T$ *und* $f \in U_{(T \Rightarrow T)}$

$$\Phi^{\to}_{A,B} \circ \Psi^{\to}_{A,B} = Id_{(D_A \to D_A)} \quad \textit{und} \quad \Phi^{\forall}_f \circ \Psi^{\forall}_f = Id_{(\Pi A \in U_T . D_{f \cdot A})}.$$

Ein Modell *von* $\lambda^{\to,\forall}_C$ *besteht aus einem Modellrahmen* $\mathcal{M} = (\mathcal{U}, \mathcal{D}, \Phi, \Psi)$ *und einer Auswertung* $[\![\cdot]\!]^{\mathcal{D}}\cdot$ *von Termen, so daß jeder Term nach folgenden Regeln einen Wert erhält:*

$[\![\Delta\,;\, \Gamma \triangleright x : \tau]\!]\eta = \eta(x)$,

$[\![\Delta\,;\, \Gamma \triangleright c : \tau]\!]\eta = C^{\mathcal{D}}_{Typ}(c)$, *für* $c : \tau \in C_{Typ}$

$[\![\Delta\,;\, \Gamma \triangleright (t \cdot s) : \tau]\!]\eta =$
$\quad \Phi^{\to}_{[\![\Delta \triangleright \sigma]\!]\eta, [\![\Delta \triangleright \tau]\!]\eta}([\![\Delta\,;\, \Gamma \triangleright t : (\sigma \to \tau)]\!]\eta)([\![\Delta\,;\, \Gamma \triangleright s : \sigma]\!]\eta)$

$[\![\Delta\,;\, \Gamma \triangleright \lambda x : \sigma . t : (\sigma \to \tau)]\!]\eta =$
$\quad \Psi^{\to}_{[\![\Delta \triangleright \sigma]\!]\eta, [\![\Delta \triangleright \tau]\!]\eta}(\lambda a \in D_{[\![\Delta \triangleright \sigma : T]\!]\eta} . [\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]\eta[a/x])$

$[\![\Delta\,;\, \Gamma \triangleright (t \cdot \tau) : (\mu \cdot \tau)]\!]\eta = \Psi^{\forall}_{[\![\Delta \triangleright \mu : (T \Rightarrow T)]\!]\eta}([\![\Delta\,;\, \Gamma \triangleright t : \forall \mu]\!]\eta)([\![\Delta \triangleright \tau : T]\!]\eta)$

$[\![\Delta\,;\, \Gamma \triangleright \lambda \alpha t : \forall \mu]\!]\eta =$
$\quad \Psi^{\forall}_{[\![\Delta \triangleright \mu : (T \Rightarrow T)]\!]\eta}(\lambda A \in U_T . [\![\Delta, \alpha : T\,;\, \Gamma \triangleright t : (\mu \cdot \alpha)]\!]\eta[A/\alpha])$

Insbesondere ist $[\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]\eta \in D_{[\![\Delta \triangleright \tau : T]\!]\eta}$. Wenn klar ist, welcher Kontext und Typ gemeint sind, schreiben wir $[\![t]\!]\eta$ statt $[\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]\eta$. Außerdem schreiben wir $c^{\mathcal{U}}$ statt $C^{\mathcal{U}}_{Art}(c)$ und $c^{\mathcal{D}}$ statt $C^{\mathcal{D}}_{Typ}(c)$.

4 Prä-logische Relationen für den zweitstufigen λ-Kalkül

Im Folgenden sei $\mathcal{A} = (\mathcal{U}, \mathcal{D}, \Phi, \Psi, [\![\cdot]\!]^{\mathcal{D}}\cdot)$ ein Umgebungsmodell von $\lambda^{\to,\forall}_C$.

Definition 4.1. *Ein* Prädikat $\mathcal{R} = (\mathcal{R}_{Art}, \mathcal{R}_{Typ})$ auf $\mathcal{A}$ *besteht aus einer Familie* $\mathcal{R}_{Art} = \{R_\kappa \mid \kappa \in Art\}$ *mit* $R_\kappa \subseteq \mathcal{U}_\kappa$ *für jedes* $\kappa \in Art$ *und einer Familie* $\mathcal{R}_{Typ} = \{R_A \mid A \in R_T\}$ *mit* $R_A \subseteq D_A$ *für jedes* $A \in R_T$.

Eine Belegung $\eta : \Delta; \Gamma \to \mathcal{A}$ respektiert *das Prädikat* $\mathcal{R}$, *kurz:* $\eta : \Delta; \Gamma \to \mathcal{R}$, *wenn* $\eta(v) \in R_\kappa$ *für jedes* $v : \kappa \in \Delta$ *und* $\eta(x) \in R_{[\![\Delta \triangleright \tau:T]\!]\eta}$ *für jedes* $x : \tau \in \Gamma$.

Das Prädikat $\mathcal{R} \subseteq \mathcal{A}$ *ist* algebraisch, *falls* $\mathcal{R}_{Art}$ *algebraisch ist und*

a) für alle $c : \tau \in C_{Typ}$ *ist* $c^{\mathcal{D}} \in R_A$ *für* $A = [\![\triangleright \tau : T]\!]^{\mathcal{U}}$,
b) für alle $A, B \in R_T$ *ist* $R_{(A \to B)} \subseteq \{h \in D_{(A \to B)} \mid h \cdot R_A \subseteq R_B\}$,
c) für alle $f \in R_{(T \Rightarrow T)}$ *ist* $R_{\forall f} \subseteq \{h \in D_{\forall f} \mid \forall A \in R_T \; h \cdot A \in R_{f \cdot A}\}$.

Ein algebraisches Prädikat $\mathcal{R}$ *heißt* logisch, *wenn in b) und c) auch* $\supseteq$ *gilt.*

Definition 4.2. *Ein Prädikat* $\mathcal{R} = (\mathcal{R}_{Art}, \mathcal{R}_{Typ})$ *auf* $\mathcal{A}$ *ist* prä-logisch, *wenn*

(i) $\mathcal{R}_{Art}$ *ein prä-logischen Prädikat auf* $\mathcal{U}$ *ist, und*
(ii) $\mathcal{R}_{Typ}$ *'ein prä-logisches Prädikat auf* $\mathcal{D}$*' ist, d.h.*

$$[\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]\eta \in R_{[\![\Delta \triangleright \tau:T]\!]\eta}$$

für jeden Term $\Delta\,;\, \Gamma \vdash t : \tau$ *und jede Belegung* $\eta : \Delta\,; \Gamma \to \mathcal{R}$.

Eine algebraische (logische, prä-logische) Relation $\mathcal{R}$ *zwischen* $\mathcal{A}_1, \ldots, \mathcal{A}_n$ *ist ein algebraisches (logisches, prä-logisches) Prädikat* $\mathcal{R} \subseteq \mathcal{A}_1 \times \ldots \times \mathcal{A}_n$.

4.1 Grundeigenschaften zweitstufiger prä-logischer Relastionen

Das folgende 'Basislemma für zweitstufige logische Relationen' besagt, daß zweitstufige logische Relationen prä-logisch sind.

Satz 4.3 *([MM85], Theorem 2) Sei* $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$ *eine logische Relation zwischen den Umgebungsmodellen* $\mathcal{A}$ *und* $\mathcal{B}$ *von* $\lambda_C^{\to,\forall}$. *Dann gilt für jeden Term* $\Delta\,;\, \Gamma \vdash t : \sigma$ *und jede Belegung* $\eta : \Delta; \Gamma \to \mathcal{R}$

$$[\![\Delta \triangleright \sigma : T]\!]\eta \in R_T \quad \textit{und} \quad [\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]\eta \in R_{[\![\Delta \triangleright \sigma:T]\!]\eta}.$$

Wie im erststufigen Fall kann Definition 4.2 als Basislemma für Relationen mit folgender Eigenschaft angesehen werden:

Lemma 4.4. *Ein Prädikat* $\mathcal{R} \subseteq \mathcal{A}$ *ist genau dann prä-logisch, wenn gilt:*

1. $\mathcal{R}_{Art}$ *ist prä-logisch und* $\mathcal{R}$ *ist algebraisch,*
2. *für alle Terme* $\Delta\,;\, \Gamma, x : \sigma \vdash t : \tau$ *und jede Belegung* $\eta : \Delta; \Gamma \to \mathcal{R}$ *mit*

$$\forall a \in R_{[\![\sigma]\!]\eta}\, [\![\Delta\,;\, \Gamma, x : \sigma \triangleright t : \tau]\!]\eta[a/x] \in R_{[\![\tau]\!]\eta}$$

gilt $[\![\Delta\,;\, \Gamma \triangleright \lambda x : \sigma\, t : (\sigma \to \tau)]\!]\eta \in R_{[\![\sigma \to \tau]\!]\eta}$,

3. für alle Terme $\Delta, \alpha : T \,;\, \Gamma \vdash t : \tau$ *und Belegungen* $\eta : \Delta; \Gamma \to \mathcal{R}$ *mit*

$$\forall A \in R_T \; [\![\Delta, \alpha : T \,;\, \Gamma \triangleright t : \tau]\!]\eta[A/\alpha] \in R_{[\![\Delta,\alpha:T \,\triangleright\, \tau:T]\!]\eta[A/\alpha]}$$

gilt $[\![\Delta \,;\, \Gamma \triangleright \lambda\alpha\, t : \forall\alpha\, \tau]\!]\eta \in R_{[\![\forall\alpha\tau]\!]\eta}$.

Beweis: $\Rightarrow$: Sei $\mathcal{R}$ prä-logisch. Dann ist natürlich $\mathcal{R}_{Art}$ prä-logisch und (nach Lemma 2.3) algebraisch. Daß $\mathcal{R}_{Typ}$ algebraisch ist, d.h. daß a), b), c) aus Definition 4.1 gelten, zeigen wir an c): Sind $f \in R_{(T \Rightarrow T)}$, $h \in R_{\forall f}$ und $A \in R_T$, und ist $\Delta = v : (T \Rightarrow T), \alpha : T$ und $\Gamma = x : \forall v$, so gilt wegen $\Delta \,;\, \Gamma \vdash x \cdot \alpha : v \cdot \alpha$

$$h \cdot A = [\![\Delta \,;\, \Gamma \triangleright x \cdot \alpha : v \cdot \alpha]\!]\eta \in R_{[\![\Delta \,\triangleright\, v\cdot\alpha:T]\!]\eta} = R_{fA}$$

für alle Belegungen η mit $\eta(v) = f$, $\eta(\alpha) = A$, und $\eta(x) = h$. Daß $\mathcal{R}$ auch die Bedingungen (iii) und (iv) an definierbare Funktionen erfüllt, geht bei (ii) über $\Delta \,;\, \Gamma \vdash \lambda x : \sigma\, t : (\sigma \to \tau)$ und bei (iv) entsprechend über $\Delta \,;\, \Gamma \vdash \lambda\alpha t : \forall\alpha\tau$.

$\Leftarrow$: Bedingung (i) aus Definition 4.2 ist klar, und für (ii) reichen die Voraussetzungen gerade, um die Behauptung $[\![\Delta \,;\, \Gamma \triangleright t : \tau]\!]\eta \in R_{[\![\tau]\!]\eta}$ durch Induktion über die Herleitung von $\Delta \,;\, \Gamma \vdash t : \tau$ zu beweisen. □

Im Unterschied zu logischen Relationen ist die Klasse der erststufigen (zweistelligen) prä-logischen Relationen unter Komposition abgeschlossen. Für zweitstufige Relationen $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$ und $\mathcal{B} \subseteq \mathcal{B} \times \mathcal{C}$ definiere $\mathcal{R} \circ \mathcal{S}$ durch [4]

$$\begin{aligned}
(\mathcal{R} \circ \mathcal{S})_{Art} &= \{(R \circ S)_\kappa \mid \kappa \in Art\}, \quad \text{mit } (R \circ S)_\kappa := R_\kappa \circ S_\kappa, \\
(\mathcal{R} \circ \mathcal{S})_{Typ} &= \{(R \circ S)_{(A,C)} \mid (A, C) \in (R \circ S)_T\}, \quad \text{mit} \\
(R \circ S)_{(A,C)} &= \bigcup\{R_{(A,B)} \circ S_{(B,C)} \mid B \in U^{\mathcal{B}}_T, (A, B) \in R_T, (B, C) \in S_T\}.
\end{aligned}$$

Man prüft dann leicht folgende Aussage nach:

Proposition 4.5. *Seien* $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$ *und* $\mathcal{S} \subseteq \mathcal{B} \times \mathcal{C}$ *prä-logische Relationen zwischen Modellen von* $\lambda^{\to,\forall}_C$. *Sei* $\eta = (\eta^{\mathcal{A}}, \eta^{\mathcal{C}}) : \Delta; \Gamma \to \mathcal{R} \circ \mathcal{S}$ *und es gebe eine Belegung* $\eta^{\mathcal{B}} : \Delta; \Gamma \to \mathcal{B}$ *mit* $(\eta^{\mathcal{A}}, \eta^{\mathcal{B}}) : \Delta; \Gamma \to \mathcal{R}$ *und* $(\eta^{\mathcal{B}}, \eta^{\mathcal{C}}) : \Delta; \Gamma \to \mathcal{S}$. *Dann ist*

$$[\![\Delta \,;\, \Gamma \triangleright t : \tau]\!]\eta \in (R \circ S)_{[\![\Delta \,\triangleright\, \tau:T]\!]\eta}$$

für jeden Term $\Delta \,;\, \Gamma \vdash t : \tau$.

Das bedeutet aber nicht ganz, daß $\mathcal{R} \circ \mathcal{S}$ eine prä-logische Relation ist: zwar gibt es für jedes $\eta : \Delta; \Gamma \to \mathcal{R} \circ \mathcal{S}$ ein $\eta^{\mathcal{B}}_{Art} : \Delta \to \mathcal{B}$ so daß $(\eta^{\mathcal{A}}, \eta^{\mathcal{B}}_{Art}) : \Delta \to \mathcal{R}_{Art}$ und $(\eta^{\mathcal{B}}_{Art}, \eta^{\mathcal{C}}) : \Delta \to \mathcal{S}_{Art}$ ist. Aber es braucht keine Fortsetzung $\eta^{\mathcal{B}} = \eta^{\mathcal{B}}_{Art} \cup \eta^{\mathcal{B}}_{Typ}$ wie in der Proposition zu geben: ist $\eta(x : \sigma) = (a, c) \in (R \circ S)_{(A,C)}$ für $(A, C) = [\![\Delta \triangleright \sigma : T]\!]\eta$, so gibt es *irgend ein* B mit $(A, B) \in R_T, (B, C) \in S_T$,

[4] Nimmt man in der Definition von $(R \circ S)_{(A,C)}$ statt der Vereinigung den Durchschnitt, so brauchen die Individuenkonstanten nicht durch $\mathcal{R} \circ \mathcal{S}$ korreliert zu sein.

und $(a,b) \in R_{(A,B)}, (b,c) \in S_{(B,C)}$, aber B kann von (a,c), nicht bloß von (A,C) abhängen, und kann von $[\![\sigma]\!]\eta^{\mathcal{B}}_{Art}$ verschieden sein.

Falls allerdings für jedes $(A,C) \in (R \circ S)_T$ die Relationen $R_{(A,B)} \circ S_{(B,C)}$ für alle B mit $(A,B) \in R_T$ und $(B,C) \in S_T$ übereinstimmen, kann man $\eta^{\mathcal{B}}_{Art}$ durch eine geeignete Belegung $\eta^{\mathcal{B}}_{Typ}$ fortsetzen. Also gilt noch der folgende Spezialfall, der vielleicht ausreicht, um zweitstufige prä-logische Relationen in der Verifikation schrittweiser Verfeinerungen bei der Programmentwicklung (cf. [HLST00]) anzuwenden:

Korollar 4.6 *Sind $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$ und $\mathcal{S} \subseteq \mathcal{B} \times \mathcal{A}$ prä-logisch und ist R_T (oder die Inverse von S_T) eine Funktion, so ist $\mathcal{R} \circ \mathcal{S}$ prä-logisch.*

Aus dem gleichen Grund ist die Projektion einer prä-logischen Relation $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$ auf die erste Komponente dann eine prä-logische Relation auf $\mathcal{A}$, wenn $\mathcal{R}$ funktional ist, aber nicht im allgemeinen.

Proposition 4.7. *Sei $\{\mathcal{R}_i \mid i \in I\}$ eine Familie prä-logischer Prädikate auf $\mathcal{A}$. Dann ist $\bigcap\{\mathcal{R}_i \mid i \in I\}$ ein prä-logisches Prädikat.*

Proof. Ist $\Delta\,;\Gamma \triangleright t : \tau$ und $\eta : \Delta;\Gamma \to \bigcap\{\mathcal{R}_i \mid i \in I\}$, dann ist für jedes $i \in I$ $[\![\Delta \triangleright \tau : T]\!]\eta \in R_{i,T}$ und $[\![\Delta\,;\,\Gamma \triangleright t : \tau]\!]\eta \in R_{i,[\![\Delta \triangleright \tau:T]\!]\eta}$, da $\eta : \Delta;\Gamma \to \mathcal{R}_i$ und $\mathcal{R}_i$ prä-logisch ist. Daraus folgt die Behauptung.

Bemerkung 4.8 *Nach Proposition 7.1 of [HS99] ist jede erststufige prä-logische Relation $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$ die Komposition dreier logischer Relationen, $embed_A \subseteq \mathcal{A} \times \mathcal{A}[X]$, $\mathcal{R}[X] \subseteq \mathcal{A}[X] \times \mathcal{B}[X]$, und $embed_B^{-1} \subseteq \mathcal{B}[X] \times \mathcal{B}$, wobei X eine Menge von Unbestimmten ist. Da die Einbettungsrelationen funktional sind, läßt sich mit Korollar 4.6 erwarten, daß dieses Resultat auch im zweitstufigen Fall gilt. Die Details müssen aber noch überprüft werden.*

4.2 Definierbarkeit und Beobachtungsgleichheit für $\lambda_C^{\to,\forall}$

Definition 4.9. *Sei $A \in \mathcal{U}_T$. Ein Element $a \in D_A$ heißt* definierbar (vom Typ A)*, wenn es einen geschlossenen Term $\vdash t : \tau$ von $\lambda_C^{\to,\forall}$ mit $A = [\![\triangleright \tau : T]\!]^{\mathcal{A}}$ und $a = [\![; \triangleright t : \tau]\!]^{\mathcal{A}}$ gibt. Die Menge der definierbaren Elemente vom Typ A bezeichnen wir mit*

$$Def_A^{\mathcal{A}} := \{[\![; \triangleright t : \tau]\!]^{\mathcal{A}} \mid ; \vdash t : \tau,\ A = [\![\triangleright \tau : T]\!]^{\mathcal{A}}\}.$$

Den Index $\mathcal{A}$ schreiben wir nur, wenn er nicht aus dem Kontext hervorgeht.

Mitchell und Meyer ([MM85], Theorem 4) haben die Menge der definierbaren Elemente eines Modells $\mathcal{A}$ von $\lambda_C^{\to,\forall}$ als Durchschnitt aller logischen Relationen auf einer Erweiterung $\mathcal{A}^*$ von $\mathcal{A}$ um unendlich viele Unbestimmte jeden Typs charakterisiert. Eine einfachere Charakterisierung liefert

Satz 4.10 *Ein Element a von $\mathcal{A}$ ist genau dann definierbar vom Typ $A \in \mathcal{U}_T$, wenn für jedes prä-logische Prädikat $\mathcal{R} \subseteq \mathcal{A}$ sowohl $A \in R_T$ als auch $a \in R_A$.*

Beweis: $\Rightarrow$: Es gibt einen Term $; \vdash t : \tau$ mit $A = [\![\triangleright \tau : T]\!]$ und $a = [\![; \triangleright t : \tau]\!] \in D_A$. Für jedes prä-logische Prädikat $\mathcal{R}$ auf $\mathcal{A}$ ist

$$[\![; \vdash t : \tau]\!] \in R_{[\![\triangleright \tau:T]\!]},$$

nach Definition und $A = [\![\triangleright \tau : T]\!] \in R_T$ wegen $\vdash \tau : T$, nach Satz 2.6.

$\Leftarrow$: Wir zeigen, daß $Def = (Def_{Art}, Def_{Typ})$ ein prä-logisches Prädikat auf $\mathcal{A}$ ist. Dann ist $A \in Def_T$, also $A = [\![\triangleright \sigma : T]\!]$ für einen Typ $\vdash \sigma : T$, und zu $a \in Def_A$ gibt es einen Term $; \vdash t : \tau$ mit $a = [\![; \triangleright t : \tau]\!]$ und $[\![\triangleright \tau : T]\!] = A$. Also ist a definierbar vom Typ A.

Nach Satz 2.6 ist $Def_{Art} = \{Def_\kappa \mid \kappa \in Art\}$ mit $Def_\kappa = \{[\![\mu]\!] \mid \vdash \mu : \kappa\}$ prä-logisch, da $\mathcal{U}$ ein Umgebungsmodell von $\lambda^{\vec{\Rightarrow}}_{C_{Art}}$ ist.

Für Def_{Typ} sei $\Delta ; \Gamma \vdash t : \tau$ und $\eta : \Delta ; \Gamma \to Def$. Zu jedem $v_i : \kappa_i \in \Delta$ und jedem $x_j : \tau_j \in \Gamma$ gibt es $\vdash \mu_i : \kappa$ und $; \vdash t_j : \tau_j$ mit $\eta(v_i) = [\![\mu_i]\!] \in Def_\kappa$ und $\eta(x_j) = [\![; \triangleright t_j : \tau_j]\!] \in Def_{[\![\triangleright \tau_j:T]\!]}$. Mit dem Substitutionslemma für $\lambda^{\rightarrow,\forall}_C$ (vgl. [BMM90]) erhält man

$$\begin{aligned}
[\![\Delta ; \Gamma \triangleright t : \tau]\!]\eta &= [\![\Delta ; \Gamma \triangleright t : \tau]\!][[\![\triangleright \mu_1 : \kappa_1]\!]/v_1, \ldots, [\![; \triangleright t_1 : \tau_i]\!]/x_1, \ldots] \\
&= [\![; \triangleright (t : \tau)[\mu_1/v_1, \ldots, t_1/x_1, \ldots]]\!] \\
&\in Def_{[\![\triangleright \tau[\mu_1/v_1,\ldots,t_1/x_1,\ldots]:T]\!]} \;=\; Def_{[\![\Delta \triangleright \tau:T]\!]\eta}.
\end{aligned}$$

Daher ist Def das kleinste prä-logische Prädikat auf $\mathcal{A}$. □

Definition 4.11. *Sei BT eine Menge von geschlossenen Typen und $\mathcal{A}, \mathcal{B}$ zwei Modelle von $\lambda^{\rightarrow,\forall}_C$ mit $D^{\mathcal{A}}_{[\![\triangleright \tau:T]\!]} = D^{\mathcal{B}}_{[\![\triangleright \tau:T]\!]}$ für alle $\tau \in BT$. $\mathcal{A}$ und $\mathcal{B}$ heißen* beobachtungsäquivalent*, kurz $\mathcal{A} \equiv_{BT} \mathcal{B}$, falls $[\![; \triangleright t : \tau]\!]^{\mathcal{A}} = [\![; \triangleright t : \tau]\!]^{\mathcal{B}}$ für alle geschlossenen Terme $; \vdash t : \tau$ mit $\tau \in BT$.*

Die Beobachtungsgleichheit läßt sich wie im erststufigen Fall durch die Existenz einer geeigneten prä-logischen Relation charakterisieren:

Satz 4.12 *Es gilt $\mathcal{A} \equiv_{BT} \mathcal{B}$ genau dann, wenn es eine prä-logische Relation $\mathcal{R}$ zwischen $\mathcal{A}$ und $\mathcal{B}$ gibt, so daß*

$$R_{(A,B)} \cap (Def^{\mathcal{A}}_A \times Def^{\mathcal{B}}_B) \;\subseteq\; Id_{A,B} \subseteq D^{\mathcal{A}}_A \times D^{\mathcal{B}}_B$$

für jeden Beobachtungstyp $\triangleright \tau : T \in BT$, wobei $(A, B) = [\![\triangleright \tau : T]\!]^{\mathcal{A}\times\mathcal{B}}$.

Beweis: $\Leftarrow$ Sei $; \vdash t : \tau$. Dann ist $\vdash \tau : T$, und da $\mathcal{R}$ prä-logisch ist, gilt $(A, B) \in R_T$ für $(A, B) = [\![\triangleright \tau : T]\!]^{\mathcal{A}\times\mathcal{B}}$ und $(a, b) \in R_{A,B}$ für $(a, b) = [\![\triangleright t : \tau]\!]^{\mathcal{A}\times\mathcal{B}}$. Ist $\tau : T \in BT$, so folgt $a = b$ aus der Voraussetzung.

$\Rightarrow$: Wähle $\mathcal{R} := Def^{\mathcal{A}\times\mathcal{B}}$, was nach Satz 4.10 eine prä-logische Relation ist. Sei $\triangleright\, \tau : T \in BT$ und $(A,B) = [\![\triangleright\, \tau : T]\!]^{\mathcal{A}\times\mathcal{B}}$. Zu $(a,b) \in Def^{\mathcal{A}\times\mathcal{B}}_{(A,B)}$ gibt es einen Term $; \vdash s : \sigma$ mit

$$(a,b) = [\![; \triangleright\, s : \sigma]\!]^{\mathcal{A}\times\mathcal{B}} \quad \text{und} \quad (A,B) = [\![\triangleright\, \sigma : T]\!]^{\mathcal{A}\times\mathcal{B}}.$$

Wegen $\mathcal{A} \equiv_{BT} \mathcal{B}$ ist $a = b$. Die prä-logische Relation $\mathcal{R} := Def^{\mathcal{A}\times\mathcal{B}}$ erfüllt die Behauptung. □

4.3 Abstrakte Konstruktoren und Repräsentationsunabhängigkeit

Damit sich der abstrakte Datentyps der Multimengen in $\lambda^{\rightarrow}_{C}$ darstellen ließ, haben wir in Beispiel 2.14 vereinfachend angenommen, daß durch die Datentypdeklaration ein neuer *Typ*, $\alpha\ bag$, und Konstante $x : \sigma$ von einfachem Typ in α eingeführt wurde. Eigentlich wollen wir aber wie in

$$(\textbf{abstype}\ (bag : T \Rightarrow T, x : \sigma)\ \textbf{with}\ e = e'\ \textbf{is}\ (\lambda\alpha : T.\tau, t : \sigma[\lambda\alpha : T.\tau/bag])\ \textbf{in}\ s)$$

einen *Typkonstruktor bag* und Konstante x von *polymorphem* Typ σ deklarieren. Das können wir im Rahmen von $\lambda^{\rightarrow,\forall}_{C}$ grob gesagt wie folgt: wir erweitern ein Modell $\mathcal{A} = (\mathcal{U}, \mathcal{D}, \Phi, \Psi, C^{\mathcal{A}}, [\![\cdot]\!]^{\mathcal{D}}\cdot)$ zu einem Modell $\mathcal{A}^{+}$, indem wir zuerst eine Unbekannte, *bag*, an die Artenstruktur $\mathcal{U}$ adjungieren: (vgl. Definition 6.1)

$$\mathcal{U}^{+} = \mathcal{U}[bag : T \Rightarrow T] = \{U^{+}_{\kappa} \mid \kappa \in Art\},\ \text{mit}\ U^{+}_{\kappa} := U_{(T\Rightarrow T)\Rightarrow\kappa} \cdot bag.$$

Dadurch erhalten wir für $A \in U_T$ neue Typen $(A\ bag), ((A\ bag)\ bag) \in U^{+}_{T}$, und man kann neue Konstante von polymorphem Typ einführen, z.B.

$$empty : \forall\alpha.(\alpha\ bag) \quad \text{oder} \quad member : \forall\alpha(\alpha \to ((\alpha\ bag) \to int)).$$

Nun interpretieren wir *bag* durch einen definierbaren Konstruktor, z.B. die Listenbildung $\lambda\alpha.\alpha^{*} : T \Rightarrow T$, nehmen als Individuenbereiche der neuen Typen die Bereiche der Typen unter dieser Interpretation, d.h.

$$D^{+}_{A\ bag} := D_{[\![\lambda\alpha.\alpha^{*}\cdot A]\!]} = D_{A^{*}} = (D_A)^{*},$$

und als Interpretation der neuen Konstanten die Werte ihrer definierenden Terme dieser Typen, z.B.

$$[\![empty : \forall\alpha.(\alpha\ bag)]\!]^{+} := [] \in D_{[\![\forall\alpha.\alpha^{*}]\!]} = D^{+}_{[\![\forall\alpha(\alpha\ bag)]\!]}.$$

Beachte, daß ein Prädikat $\mathcal{R}$ auf $\mathcal{A}^{+}$ *verschiedene* Prädikate $R_{A\ bag}, R_{A^{*}} \subseteq D_{A\ bag} = D_{A^{*}}$ enthält, da die Typen $A\ bag$ und A^{*} verschieden sind.

Definition 4.13. *Sei $v_0 : \kappa_0 \vdash \sigma_0 : T$ und $C^{+} := C_{Art}, v_0 : \kappa_0\,; C_{Typ}, x_0 : \sigma_0$ eine Erweiterung von C um neue 'Konstante' v_0, x_0. Sei $\mathcal{A} = (\mathcal{U}, \mathcal{D}, \Phi, \Psi, [\![\cdot]\!]\cdot)$*

ein Umgebungsmodell von $\lambda_C^{\rightarrow,\forall}$, $\vdash \mu_0 : \kappa_0$ *ein geschlossener Konstruktor von* $\lambda_{C_{Art}}^{\Rightarrow}$ *mit Wert* $k_0 = [\![\triangleright \mu_0 : \kappa_0]\!]$, *und* $A = [\![\sigma_0[\mu_0/v_0]]\!] \in U_T$ *und* $a \in D_A$.

Sei $\mathcal{A}(\mu_0, a) = \mathcal{A}^+ = (\mathcal{U}^+, \mathcal{D}^+, \Phi^+, \Psi^+, [\![\cdot]\!]^+)$ *wie folgt definiert:* $\mathcal{U}^+ = \mathcal{U}[v_0 : \kappa_0]$ *ist die Erweiterung von* $\mathcal{U}$ *um eine Unbestimmte* $v_0 : \kappa_0$ *(vgl. Definition 6.1). Jedes* $k \in U_\kappa^+$ *kann mit einem Element von* $U_{(\kappa_0 \Rightarrow \kappa)}$ *identifiziert werden*[5] *und bestimmt daher ein* $k(k_0) \in U_\kappa$, *sodaß sich* $\mathcal{D}^+, \Phi^+, \Psi^+, ([\![\cdot]\!]\cdot)^+$ *ergeben aus*

$$
\begin{array}{llll}
D_A^+ & := D_{A(k_0)}, & & \\
x_0^{\mathcal{D}^+} & := a & c^{\mathcal{D}^+} & := c^{\mathcal{D}} \text{ für } c : \sigma \in C_{Typ}, \\
(\Phi^+)_{A,B}^{\rightarrow} & := \Phi_{A(k_0),B(k_0)}^{\rightarrow}, & (\Psi^+)_{A,B}^{\rightarrow} & := \Psi_{A(k_0),B(k_0)}^{\rightarrow}, \\
(\Phi^+)_f^{\forall} & := \Phi_{f(k_0)}^{\forall} & (\Psi^+)_f^{\forall} & := \Psi_{f(k_0)}^{\forall}
\end{array}
$$

und $[\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]^{\mathcal{D}^+}\eta := [\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]^{\mathcal{D}}\eta_{k_0}$, *wobei* $\eta_{k_0}(v) := \eta(v)(k_0) \in U_\kappa$ *für* $v : \kappa \in \Delta$ *und* $\eta_{k_0}(x) := \eta(x) \in D_{A(k_0)}$ *für* $x : \sigma \in \Gamma$ *und* $A = [\![\Delta \triangleright \sigma : T]\!] \in U_T^+$.

Wir wollen nun eine Verallgemeinerung der Charakterisierung aus Satz 2.11 auf abstrakte Konstruktoren zeigen. (Hier liegt auch der Grund, warum wir nicht in $\lambda_C^{\rightarrow,\forall,\exists}$ arbeiten, d.h. wie Mitchell und Plotkin [MP85] den Typkonstruktor $\exists : (T \Rightarrow T) \Rightarrow T$ benutzen, um abstrakte *Typen* zu modellieren: wir bräuchten nun auch Existenzquantoren höherer Arten.) Zur Vereinfachung geben wir nur die einstellige Version an.

Satz 4.14 *Seien* $\mathcal{R}$ *eine prä-logische Relation auf dem Modell* $\mathcal{A}$ *von* $\lambda_C^{\rightarrow,\forall}$, *so daß* $\mathcal{R}_{Art}$ *eine logische Relation ist, deren Elemente mit Parametern aus* R_T *definierbar sind. Für jede definierbare Expansion* $\mathcal{A}^+ = \mathcal{A}(\mu_0, a)$ *von* $\mathcal{A}$ *zu einem Umgebungsmodell von* $\lambda_{C^+}^{\rightarrow,\forall}$ *sind folgende Aussagen äquivalent:*

(i) Für alle $A \in R_T$ *ist* $Def_A^+ \subseteq R_A$.
(ii) Es gibt ein prä-logisches Prädikat $\mathcal{R}^+ \subseteq \mathcal{A}^+$ *mit* $R_T \subseteq R_T^+$ *und* $R_A^+ = R_A$ *für alle* $A \in R_T$.

Beweis: (ii) $\Rightarrow$ (i): Für $A \in R_T \subseteq R_T^+$ ist $Def_A^+ \subseteq R_A^+$, da $\mathcal{R}^+$ prä-logisch ist, also $Def_A^+ \subseteq R_A$ wegen $R_A^+ = R_A$.

(i) $\Rightarrow$ (ii): Wir bilden zunächst $\mathcal{U}^+ = \mathcal{U}[v_0 : \kappa_0] = \{\mathcal{U}_\kappa^+ \mid \kappa \in Art\}$, wobei

$$U_\kappa^+ = \{[v_0 : \kappa_0 \triangleright \mu : \kappa] \mid \mu \in \lambda_{C_{Art},\mathcal{U}}^{\Rightarrow},\ v_0 : \kappa_0 \vdash \mu : \kappa\},$$

aus den Äquivalenzklassen von Konstruktoren besteht, die mit Konstanten für Elemente von $\mathcal{U}$ definierbar sind. Jedes Element von $\mathcal{U}_\kappa$ läßt sich in der Form $[k \cdot v_0]$ mit einem eindeutig bestimmten $k \in U_{(\kappa_0 \Rightarrow \kappa)}$ schreiben. Da v_0 als neue Konstruktorkonstante gedacht ist, setzen wir $\mathcal{R}_{Art}^+ \subseteq \mathcal{U}^+$ durch

$$\mathcal{R}_{Art}^+ := \{R_\kappa^+ \mid \kappa \in Art\}, \qquad \text{mit} \quad R_\kappa^+ := R_{(\kappa_0 \Rightarrow \kappa)} \cdot v_0 \text{ für } \kappa \in Art.$$

[5] Hier brauchen wir, daß $\mathcal{U}$ ein extensionales Modell von $\lambda_{C_{Art}}^{\Rightarrow}$ ist.

Für $\mathcal{R}^+_{Typ} = \{R^+_A \mid A \in R^+_T\}$ sei R^+_A die Menge der Elemente von D^+_A, die mit *Typ*parametern aus R_T und Individuenparametern aus $\mathcal{R}_{Typ}$ in $\lambda^{\rightarrow,\forall}_{C^+}$ definierbar sind, d.h. für $A \in R^+_T$ sei (mit $\eta = (\eta_{Art}; \eta_{Typ})$)

$$\begin{aligned} R^+_A := \{\ [\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]\eta \mid \Delta\,;\, \Gamma \vdash t : \tau \text{ ein Term von } \lambda^{\rightarrow,\forall}_{C^+} \\ \eta_{Art} : \Delta \to R_T,\ A = [\![\Delta \triangleright \tau : T]\!]\eta_{Art}, \\ \text{für alle } x : \sigma \in \Gamma \text{ ist } \sigma \text{ ein Typ von } \lambda^{\rightarrow,\forall}_{C}, \\ \eta_{Typ} : \Gamma \to \mathcal{R}_{Typ}\ \}. \end{aligned} \tag{6}$$

Beh 1 $\mathcal{R}^+ := (\mathcal{R}^+_{Art}, \mathcal{R}^+_{Typ})$ ist ein prä-logisches Prädikat auf $\mathcal{A}^+$.

Beweis: (Skizze) Nach Lemma 6.2 ist $\mathcal{R}^+_{Art} \subseteq \mathcal{U}^+$ ein prä-logisches Prädikat. Für $\mathcal{R}_{Typ}$ benutzt man Lemma 4.4. Daß $\mathcal{R}^+$ algebraisch ist, folgt daraus, daß Typen $A \in R^+_T$ als $\mu \cdot v_0$ für ein $\mu \in R_{(\kappa_0 \Rightarrow T)}$ darstellbar sind, und μ (nach Annahme über $\mathcal{R}$) durch einen $\lambda^{\Rightarrow}_{C_{Art}}$-Term mit Parametern aus R_T definierbar ist.

Um (ii) und (iii) aus Lemma 4.4 zu zeigen, d.h. daß die mit Parametern aus $\mathcal{R}^+$ definierbaren Funktionen, die aus $\mathcal{R}^+$ nicht herausführen, schon in $\mathcal{R}^+$ liegen, ersetzt man Parameter von $\mathcal{R}^+$ durch ihre definierenden $\lambda^{\rightarrow,\forall}_{C^+}$-Terme mit Parametern aus $\mathcal{R}_{Typ}$ und benutzt das Substitutionslemma (cf. Lemma 10 of [BMM90]) für $\lambda^{\rightarrow,\forall}_{C}$. △

Beh 2 Für $A \in R_T$ ist $A \in R^+_T$ und $R^+_A = R_A$.

Beweis: Sei $A \in R_T$. Dann ist $A = [\![\alpha : T; \triangleright (\lambda v\, \alpha) \cdot v_0 : T]\!][A/\alpha] \in R_{(\kappa \Rightarrow T)} \cdot v_0 = R^+_T$. Zum Nachweis von $R_A \subseteq R^+_A$ sei η eine Belegung mit $\eta(\alpha : T) = A$ und $\eta(x : \alpha) = a \in R_A$. Nach Definition von R^+_A ist dann

$$a = [\![\alpha : T; x : \alpha \triangleright x : \alpha]\!]\eta\ \in R^+_A,$$

also $R_A \subseteq R^+_A$. Um $R^+_A \subseteq R_A$ zu zeigen, sei $a = [\![\Delta\,;\, \Gamma \triangleright t : \tau]\!]\eta \in R^+_A$ mit den in (6) angegebenen Eigenschaften von $\Delta\,;\, \Gamma \triangleright t : \tau$ und η. Dann hat Δ die Form $\alpha_1 : T, \ldots, \alpha_n : T$, und mit $\Gamma = x_1 : \sigma_1, \ldots, x_m : \sigma_m$ ist

$$\bar{t} : \bar{\tau} := \lambda\alpha_1 \ldots \lambda\alpha_n \lambda x_1 : \sigma_1 \ldots \lambda x_m : \sigma_m.\ t : \forall\alpha_1 \ldots \forall\alpha_n(\sigma_1 \to \ldots \to \sigma_m \to \tau).$$

ein geschlossener $\lambda^{\rightarrow,\forall}_{C^+}$-Term mit Typ $\bar{A} := [\![\triangleright \bar{\tau} : T]\!] \in R_T$. Nach (i) ist daher

$$[\![; \triangleright \bar{t} : \bar{\tau}]\!] \in Def^+_{\bar{A}} \subseteq R_{\bar{A}},$$

Seien $A_i = \eta(\alpha_i)$, $b_j = \eta(x_j)$ und $B_j = [\![\Delta \triangleright \sigma_j : T]\!]\eta$. Nach Voraussetzung über η und da $\mathcal{R}$ prä-logisch ist, sind $A_i, B_j \in R_T$ und $b_j \in R_{B_j}$. Daher ist

$$\begin{aligned} a &= [\![; \triangleright \bar{t} : \bar{\tau}]\!] \cdot A_1 \cdots A_n \cdot b_1 \cdots b_m \in R_{\bar{A}} \cdot A_1 \cdots A_n \cdot b_1 \cdots b_m \\ &\subseteq R_{B_1 \to \ldots \to B_m \to A} \cdot R_{B_1} \cdots R_{B_m} \subseteq R_A. \end{aligned}$$

□

Mitchell gibt für den Kalkül $\lambda^{\rightarrow,\forall,\exists}_{C}$, mit Typkonstruktur $\exists : (T \Rightarrow T) \Rightarrow T$, ohne Beweis folgendes Kriterium für die Beobachtungsgleichheit zweier Repräsentationen eines abstrakten Datentyps an, mit einer *logischen* Relation $\mathcal{R}^+$ in (ii):

Satz 4.15 *([Mit86], Theorem 7) Sei $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{B}$ eine logische Relation zwischen Modellen von $\lambda_C^{\to,\forall,\exists}$ und $A_0 \in U_T^{\mathcal{A}}$, $B_0 \in U_T^{\mathcal{B}}$. Seien $(f,g) \in R_{(T \Rightarrow T)}$, so daß $(\exists f, \exists g) \in R_T$, und seien $c \in D^{\mathcal{A}}_{f \cdot A_0}$, $d \in D^{\mathcal{B}}_{g \cdot B_0}$. Dann sind äquivalent:*

(i) $(\Phi^{\exists}_{f,A_0}(c), \Phi^{\exists}_{g,B_0}(d)) \in R_{(\exists f, \exists g)}$

(ii) Es gibt eine logische Relation $\mathcal{R}^+ \subseteq \mathcal{A}^+(A_0) \times \mathcal{B}^+(B_0)$ *mit* $(c,d) \in R^+_{(f \cdot v_0, g \cdot v_0)}$ *und* $R^+_{(A,B)} = R_{(A,B)}$ *für alle* $(A,B) \in R_T$.

Hierin ist $\Phi^{\exists}_{f,A_0} : D_{f \cdot A_0} \to D_{\exists f}$ die Einbettung von $D_{f \cdot A_0}$ in die Summe $D_{\exists f}$ aller $D_{f \cdot A}$, $A \in U_T^{\mathcal{A}}$, –also $\Phi^{\exists}_{f,A}(c)$ die Implementierung $(A, c : f \cdot A)$ eines abstrakten Datentyps $(\alpha, x : \sigma)$– und da für $\Psi^{\exists}_{f,A} : D_{\forall \alpha (f \cdot \alpha \to A)} \to D_{(\exists f \to A)}$ die Bedingung $\Psi^{\exists}_{f,A}(\tilde{f}) \cdot \tilde{c} = \tilde{f} \cdot A \cdot c$ für $\tilde{c} = \Phi^{\exists}_{f,A}(c)$ erfüllt ist, wird durch

$$(\tilde{c}, \tilde{d}) \in R_{(\exists f, \exists g)} : \Longleftrightarrow \ \forall (A,B) \in R_T \ \forall (\tilde{f}, \tilde{g}) \in R_{(\forall \alpha (f \cdot \alpha \to A), \forall \alpha (g \cdot \alpha \to B))} \\ (\Psi^{\exists}_{f,A}(\tilde{f}) \cdot \tilde{c}, \Psi^{\exists}_{g,B}(\tilde{g}) \cdot \tilde{d}) \in R_{(A,B)}$$

die Beobachtungsgleichheit von Implementierungen formuliert.

Die Erweiterung $\mathcal{A}^+(A_0)$ von $\mathcal{A}$ entsteht aus $\mathcal{A}$ nach Mitchell wie folgt: man bildet $\mathcal{U}^+$, indem man einen neuen Typ $v_0 : T$ zu $U_T^{\mathcal{A}}$ hinzunimmt und zu

$$[v_0 : \kappa_0 \triangleright \mu : \kappa] \in U_\kappa^{\mathcal{A}^+(A_0)}$$

die Konstruktoren $\nu \in U_{(T \Rightarrow \kappa)}$ miteinander identifiziert, die $\nu \cdot A_0 = \mu \cdot A_0$ liefern. Die Terme werden durch eine Interpretation $\mathcal{D}^+$ interpretiert, die man wie oben aus $D_{v_0} := D_{A_0}$ durch Übertragung von $\mathcal{D}$ erhält.

Einen Beweis für (i) $\Rightarrow$ (ii) dieses Kriteriums sehe ich nicht. Zunächst ist nicht klar, wie bei der von Mitchell angedeuteten Konstruktion $\mathcal{R}^+$ konstruiert wird. Da C_{Art} höherstufige Konstante $\forall, \exists$ hat, wird durch $R_T^+ := R_T \cup \{(f \cdot v_0, g \cdot v_0)\}$ und $R^+_{(\kappa \Rightarrow \rho)} := (R_\kappa^+ \Rightarrow R_\rho^+)$ i.a. keine logische Relation erzeugt. Daher liegt nahe, wie in Lemma 6.2 $R_\kappa^+ := R_{(T \Rightarrow \kappa)} \cdot v_0$ zu wählen. Da Mitchell aber v_0 *nicht* als Unbestimmte behandelt, erhält man zwar $R^+_{(\kappa \Rightarrow \rho)} \subseteq (R_\kappa^+ \Rightarrow R_\rho^+)$, soweit ich sehe aber nicht die Umkehrung. Immerhin könnte man eine logische Relation $\mathcal{R}^+_{Art}$ durch Lemma 6.2 definieren; da v_0 eine Konstante ist, erhält man $(f \cdot v_0, g \cdot v_0) \in R_T^+$ aus der Annahme $(f,g) \in R_{(T \Rightarrow T)}$. Außerdem sind aber auch in C_{Typ} höherstufige Konstanten erlaubt. Daher kann man m.M. $\mathcal{R}^+_{Typ}$ nicht durch Modifizieren des *prä*-logischen Prädikats aus Satz 4.14 konstruieren.

Insgesamt scheint mir die Behauptung von Satz 4.15 eher zweifelhaft, daß die Beobachtungsgleichheit (i) zweier Implementierungen (A_0, c) und (B_0, d) zu der lokalen Bedingung (ii) einer logischen Korrelation der Operationen c und d auf den neuen Typen $f \cdot v_0$ und $g \cdot v_0$ äquivalent sei.

5 Schluß

Wir haben prä-logische Relationen für den zweitstufigen λ-Kalkül definiert und damit die definierbaren Elemente und die Beobachtungsgleichheit von Modellen in einfacher Weise charakterisiert. Von der Klasse aller prä-logischen Relationen haben wir die Abgeschlossenheit unter Durchschnitten und eine eingeschränkte Form der Abgeschlossenheit unter dem Relationenprodukt gezeigt.

Wir vermuten, daß sich die Darstellung prä-logischer Relationen mittels logischer Relationen nach [HS99] vom erststufigen auf den zweitstufigen Fall verallgemeinern läßt (vgl. Bemerkung 4.8).

Weiter scheint eine kategorientheoretische Verallgemeinerung zweitstufiger prälogischer Relationen, im Sinne der 'lax logical relations' von [PPST00], nützlich für Anwendungen auf kategorientheoretische Modelle und für Repräsentationsunabhängigkeitsfragen bei imperativen Sprachen.

Schließlich wäre für die Repräsentationsunabhängigkeit nicht nur eine Behandlung der $\exists$-Typen, sondern auch die der abhängigen Typen von Interesse, sowie die Berücksichtigung von Gleichungen für die Konstanten des abstrakten Datentyps. Allgemeinere Konstruktionen wie

(**abstype** *Context* **with** *Specification* **is** *Representation* **in** *Scope*)

behandeln zu können wäre nützlich zum Nachweis der Äquivalenz verschiedener SML-Strukturen als Implementierungen einer SML-Signatur, insbesondere wenn höherstufige Funktoren erlaubt sind (vgl. Abschnitt 4 in Leroy[Ler95]).

Bei der Spezifikations- und Implementationsverfeinerung in der Programmentwicklung, wie sie von Hannay[Han99] mit zweitstufigen logischen Relationen untersucht wurde, könnten prä-logische Relationen eine Ausdehnung auf Sprachen mit höherstufigen Konstanten erlauben.

Danksagung: Ich danke Furio Honsell für den Hinweis auf [HS99].

6 Anhang: Adjunktion von Unbestimmten

Definition 6.1. *Sei* $\mathcal{A} = (A, \Phi, \Psi, C^{\mathcal{A}}) \models \lambda^{\rightarrow}_{C}$ *extensional und* $\tau \in T$. *Erweitere* $\lambda^{\rightarrow}_{C}$ *zu* $\lambda^{\rightarrow}_{C,\mathcal{A}}$*-Termen, in denen für jedes* $a \in A_\sigma$ *eine Konstante* $\underline{a} : \sigma$ *erlaubt ist. Auf den* $\lambda^{\rightarrow}_{C,A}$*-Termen vom Typ* σ *in der freien Variable* $x : \tau$ *betrachte*

$$s(x) =_{\mathcal{A}} t(x) : \Longleftrightarrow \forall a \in A_\tau \ [\![s]\!][a/x] = [\![t]\!][a/x] \in A_\sigma .$$

Jede Äquivalenzklasse $[s : \sigma]$ *von* $=_{\mathcal{A}}$ *läßt sich in der Form* $[\underline{f} \cdot x]$ *mit* $f \in A_{\tau\to\sigma}$ *darstellen. Da* $\mathcal{A}$ *extensional ist, ist* $f = [\![\lambda x\, s]\!]$ *eindeutig und* $a \mapsto [\underline{a}]$ *injektiv.*

Die Erweiterung $\mathcal{A}[x : \tau] = (A', \Phi', \Psi', C')$ von $\mathcal{A}$ um die Unbestimmte $x : \tau$ *sei definiert durch*

$$A'_\sigma = A[x : \tau]_\sigma := \{[s] \mid s \in \lambda^{\rightarrow}_{C,A},\ x : \tau \vdash s : \sigma\}$$

$$\Phi'_{\rho,\sigma}([\underline{f} \cdot x])([\underline{g} \cdot x]) := [\underline{\Phi_{\tau\to\rho,\tau\to\sigma}(S_{\tau,\rho,\sigma} \cdot f)(g)} \cdot x]$$
$$\Psi'_{\rho,\sigma}(\lambda[\underline{g} \cdot x].[\underline{h(g)} \cdot x]) := [\underline{\Psi_{\tau\to\rho,\tau\to\sigma}(h)} \cdot x]$$
$$C'(c) := [\underline{C^{\mathcal{A}}(c)}] \quad \textit{für } c : \sigma \in C,$$

wobei $S_{\tau,\rho,\sigma} := \lambda f \lambda g \lambda x (f x (g x)) : (\tau \to \rho \to \sigma) \to (\tau \to \rho) \to (\tau \to \sigma)$.
Wir schreiben kurz $f \cdot' x$ *statt* $[\underline{f} \cdot x]$ *und entsprechend* $A[x : \tau]_\sigma = A_{\tau\to\sigma} \cdot' x$.

Lemma 6.2. *Sei* $\mathcal{A} \models \lambda^{\to}_{C}$ *extensional und* $\mathcal{R} \subseteq \mathcal{A}$ *ein logisches Prädikat. Es gibt ein logisches Prädikat* $\mathcal{S}$ *auf* $\mathcal{A}[x : \tau]$ *mit* $[x] \in S_\tau$ *und* $R_\sigma \subseteq S_\sigma$ *für alle Typen* σ. *Ist* $R_\tau \neq \emptyset$, *so ist* $S_\sigma \cap A_\sigma = R_\sigma$.

Beweis: Definiere $\mathcal{S}$ durch $S_\sigma = R_{\tau\to\sigma} \cdot' x$. Damit ist einerseits $R_\sigma \subseteq S_\sigma$, da

$$b \in R_\sigma \quad \Rightarrow \quad \lambda x.b \in R_{\tau\to\sigma} \quad \Rightarrow \quad b = (\lambda x.b) \cdot' x \ \in R_{\tau\to\sigma} \cdot' x = S_\sigma.$$

Insbesondere ist für $c : \sigma \in C$ daher $c^{\mathcal{A}[x:\tau]} = c^{\mathcal{A}} \in R_\sigma \subseteq S_\sigma$. Außerdem ist $x = (\lambda x\, x) \cdot' x \in R_{\tau\to\tau} \cdot' x = S_\tau$. Ist $f \cdot' x \in S_\sigma \cap A_\sigma$, so gibt es $b \in A_\sigma$ mit $f \cdot a = b$ für alle $a \in A_\tau$. Falls $R_\tau \neq \emptyset$ ist, folgt $b \in f \cdot R_\tau \subseteq R_{\tau\to\sigma} \cdot R_\tau \subseteq R_\sigma$.
Weiter ist $S_{\rho\to\sigma} \subseteq \{h \in A[x : \tau]_{\rho\to\sigma} \mid h \cdot' S_\rho \subseteq S_\sigma\}$: Ist $h \in S_{\rho\to\sigma}$ und $r \in S_\rho$, so gibt es $f \in R_{\tau\to\rho\to\sigma}$ und $g \in R_{\tau\to\rho}$ mit

$$h \cdot' r = (f \cdot' x) \cdot' (g \cdot' x) = \lambda x (f x (g x)) \cdot' x \in R_{\tau\to\sigma} \cdot' x = S_\sigma.$$

Ist $h \cdot' S_\rho \subseteq S_\sigma$ und $h = f \cdot' x$ für ein $f \in A_{\tau\to\rho\to\sigma}$, so ist

$$(f \cdot' x) \cdot' (R_{\tau\to\rho} \cdot' x) \subseteq R_{\tau\to\sigma} \cdot' x. \tag{7}$$

Um $h \in S_{\rho\to\tau}$ zu zeigen, zeigen wir $f \in R_{\tau\to\rho\to\sigma}$. Da $\mathcal{R}$ logisch ist, genügt dafür $f \cdot R_\tau \cdot R_\rho \subseteq R_\sigma$. Zu $b \in R_\rho$ ist $g = \lambda y.b \in R_{\tau\to\rho}$, und nach (7) ist $\lambda x (f x (g x)) \cdot' x = (f \cdot' x) \cdot' (g \cdot' x) \in R_{\tau\to\sigma} \cdot' x$. Da $\mathcal{A}$ extensional ist, folgt $\lambda x (f x (g x)) \in R_{\tau\to\sigma}$, und zu $a \in R_\tau$ ist $f a (g a) = f a b \in R_\sigma$. Also ist $\mathcal{S} \subseteq \mathcal{A}[x : \tau]$ ein logisches Prädikat. □

Das Lemma gilt anscheinend nicht für prä-logische Relationen.

Literatur

[BMM90] Kim B. Bruce, Albert R. Meyer, and John C. Mitchell. The semantics of second-order lambda calculus. *Information and Computation*, 85:76–134, 1990.

[Han99] Jo Erskine Hannay, *Specification refinement with system F*, In Proc. CSL'99, LNCS 1683, Springer Verlag, 1999, pp. 530–545.

[HLST00] Furio Honsell, John Longley, Donald Sannella, and Andrzej Tarlecki, *Constructive data refinement in typed lambda calculus*, 3rd Intl. Conf. on Foundations of Software Science and Computation Structures. European Joint Conferences on Theory and Practice of Software (ETAPS'2000), LNCS 1784, Springer Verlag, 2000, pp. 149–164.

[HS99] Furio Honsell and Donald Sannella. Pre-logical relations. In *Proc. Computer Science Logic, CSL'99*, LNCS. Springer Verlag, 1999.

[Ler95] Xavier Leroy. Applicative functors and fully transparent higher-order modules. In *Proc. of the 22nd Annual ACM Symposium on Principles of Programming Languages*, pages 142–153. ACM, 1995.

[Mit86] John C. Mitchell. Representation independence and data abstraction. In *Proceedings of the 13th ACM Symposium on Principles of Programming Languages*, pages 263–276, January 1986.

[Mit91] John C. Mitchell. On the equivalence of data representations. In V. Lifschitz, editor, *Artificial Intelligence and Mathematical Theory of Computation: Papers in Honour of John C. McCarthy*, pages 305–330. Academic Press, 1991.

[MM85] John C. Mitchell and Albert Meyer. Second-order logical relations. In *Logics of Programs*, volume 193 of *Lecture Notes in Computer Science*, pages 225–236, Berlin, 1985. Springer Verlag.

[MP85] John C. Mitchell and Gordon D. Plotkin. Abstract types have existential type. In *12-th ACM Symposium on Principles of Programming Languages*, pages 37–51, 1985.

[MTHM97] Robin Milner, Mads Tofte, Robert Harper, and David MacQueen. *The Definition of Standard ML (Revised)*. The MIT Press, Cambridge, MA, 1997.

[Plo80] Gordon D. Plotkin. Lambda definability in the full type hierarchy. In *To H.B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, pages 363–373. Academic Press, 1980.

[PPST00] Gordon Plotkin, John Power, Don Sannella, and Robert Tennent. Lax logical relations. In *ICALP 2000*, 2000. to appear.

[PR00] John Power and Edmund Robinson. Logical relations and data abstraction. In P. Clote and H. Schwichtenberg, editors, *Computer Science Logic. 14th International Workshop, CSL 2000. Fischbachau, Germany, August 21-26, 2000*, volume 1862 of *LNCS*, pages 497–511, Berlin, Heidelberg, 2000. Springer Verlag.

[Sta85] R. Statman. Logical relations and the typed lambda calculus. *Information and Control*, 65:85–97, 1985.

[Tai67] W.W. Tait. Intensional interpretation of functionals of finite type. *Journal of Symbolic Logic*, 32:198–212, 1967.