A Relation-algebraic Treatment of the Dedekind Recursion Theorem

Rudolf Berghammer

Institut für Informatik
Christian-Albrechts-Universität zu Kiel

RAMiCS 2020

October 2020

Was beweisbar ist, soll in der Wissenschaft nicht ohne Beweis geglaubt werden.*

Richard Dedekind, 1888
first sentence of the article
„Was sind und was sollen die Zahlen“

*What can be proven should in science not be believed without proof.

Introduction

Definition of **algebraic datatypes** in programming languages (SML):

$$\textbf{datatype}\ nat\ =\ zero \mid succ\ \textbf{of}\ nat;$$

Definition of **functions via pattern matching** over algebraic datatypes (SML, without currying):

$$\begin{aligned}
\textbf{fun}\ \ & add\ \ (zero, y) = y \\
\mid\ \ & add\ (succ(x), y) = succ(add(x, y)); \\
\textbf{fun}\ \ & mult\ \ (zero, y) = zero \\
\mid\ \ & mult\ (succ(x), y) = add(x, mult(x, y));
\end{aligned}$$

Why this works?

- In practise: Since it can be implemented.
- Theoretically: Because of the **recursion theorem of Dedekind**.

Modern Approach: Peano Structures

An algebraic structure (N, z, s) of type $(0, 1)$ is a **Peano structure**, if:

$$(P_3) \quad \forall x, y \in N : s(x) = s(y) \Rightarrow x = y$$
$$(P_4) \quad \forall x \in N : \neg s(x) = z$$
$$(P_5) \quad \forall A \in 2^N : z \in A \wedge (\forall x \in A : s(x) \in A) \Rightarrow A = N$$

In the article „Was sind und was sollen die Zahlen“ (1888) Dedekind

- constructs (not completely formal*) a set-theoretic model of a Peano structure
- shows that for each pair (N_1, z_1, s_1) and (N_2, z_2, s_2) of Peano structures there exists a bijektive function $\Phi : N_1 \to N_2$ such that:

$$\Phi(z_1) = z_2 \qquad \forall x \in N_1 : \Phi(s_1(x)) = s_2(\Phi(x))$$

(Satz 132, nowadays **Dedekind isomorphism theorem**.)

*because of Satz 66, saying that there exists an infinite set.

The Dedekind Recursion Theorem

To define functions – like $\Phi : N_1 \to N_2$ – over Peano structures via recursion, Dedekind shows in his article (as Satz 126) the following result:

Recursion theorem. Given a Peano structure (N, z, s), a set A, an element $c \in A$ and a function $F : A \to A$, there exists precisely one function $f : N \to A$ such that:

$$\text{(IB)} \quad f(z) = c \qquad\qquad \text{(IS)} \quad \forall x \in N : f(s(x)) = F(f(x))$$

Modern proofs (based on Paul Lorenzen, 1939) define the function f as a relation between N and A as follows:

$$f := \bigcap \{ S \in 2^{N \times A} \mid z\, S\, c \wedge \forall x \in N, y \in A : x\, S\, y \Rightarrow s(x)\, S\, F(y) \}$$

It is to verify that f is total, f is univalent, f satisfies (IB) and (IS) and if an arbitrary $g : N \to A$ satisfies (IB) and (IS), then $f = g$.

(heutzutage so genannten) Isomorphiesatz für Peano-Strukturen, welcher in dem gleichen Büchlein zu finden ist.

11.1.4 Satz: Rekursionssatz von R. Dedekind

Es seien (N, a, nf) eine Peano-Struktur, $F : A \to A$ eine Funktion und $c \in A$. Dann gibt es genau eine Funktion $f : N \to A$, welche die folgenden zwei Eigenschaften erfüllt:

$$\text{(IB)} \quad f(a) = c \qquad\qquad \text{(IS)} \quad \forall\, n \in N : f(nf(n)) = F(f(n))$$

Beweis: Wir zeigen zuerst, dass maximal eine Funktion $f : N \to A$ mit den Eigenschaften (IB) und (IS) existiert. Dazu seien $f_1 : N \to A$ und $f_2 : N \to A$ Funktionen, und es seien die folgenden vier Aussagen wahr:

$$\begin{array}{ll} f_1(a) = c & \forall\, n \in N : f_1(nf(n)) = F(f_1(n)) \\ f_2(a) = c & \forall\, n \in N : f_2(nf(n)) = F(f_2(n)) \end{array}$$

Wir definieren die Teilmenge X von N durch

$$X := \{n \in N \mid f_1(n) = f_2(n)\}.$$

Wegen $f_1(a) = c = f_2(a)$ gilt $a \in X$. Wir zeigen noch $nf(X) \subseteq X$. Aus der Forderung (3) von Definition 11.1.1 folgt dann $X = N$, also $f_1(n) = f_2(n)$ für alle $n \in N$, was $f_1 = f_2$ bedeutet. Zum Beweis von $nf(X) \subseteq X$ sei $n \in nf(X)$ gegeben. Also gibt es ein $m \in X$ mit $n = nf(m)$. Wegen $m \in X$ gilt $f_1(m) = f_2(m)$, und dies impliziert

$$f_1(n) = f_1(nf(m)) = F(f_1(m)) = F(f_2(m)) = f_2(nf(m)) = f_2(n),$$

woraus $n \in X$ nach der Definition von X folgt.

Es bleibt noch die Existenz einer Funktion $f : N \to A$ zu zeigen, die (IB) und (IS) erfüllt. Dazu betrachten wir die Menge von Relationen $\mathcal{R}$, definiert durch

$$\mathcal{R} := \{S \in \mathcal{P}(N \times A) \mid a\, S\, c \wedge \forall\, n \in N, x \in A : n\, S\, x \Rightarrow nf(n)\, S\, F(x)\},$$

und definieren die Relation $R \subseteq N \times A$ durch $R := \bigcap \mathcal{R}$. Man beachte, dass die Menge $\mathcal{R}$, deren beliebiger Durchschnitt als R definiert wird, die Menge $N \times A$ enthält, also logisch und mengentheoretisch keine Schwierigkeiten entstehen. Zuerst zeigen wir, dass R ein Element von $\mathcal{R}$ ist, also die folgenden zwei Eigenschaften gelten:

$$\text{(IBR)} \quad a\, R\, c \qquad\qquad \text{(ISR)} \quad \forall\, n \in N, x \in A : n\, R\, x \Rightarrow nf(n)\, R\, F(x)$$

Nachfolgend ist der Beweis von (IBR) angegeben:

$$\textbf{wahr} \iff \forall\, S \in \mathcal{R} : a\, S\, c \iff a\, (\bigcap \mathcal{R})\, c \iff a\, R\, c$$

Hier werden die Definition von $\mathcal{R}$ und von R verwendet: Zum Beweis von (ISR) seien $n \in N$ und $x \in A$ beliebig vorgegeben. Dann zeigt die folgende Rechnung die Behauptung:

$$\begin{array}{lll} n\, R\, x & \iff & n\, (\bigcap \mathcal{R})\, x \qquad\qquad \text{Definition von } R \\ & \iff & \forall\, S \in \mathcal{R} : n\, S\, x \\ & \Longrightarrow & \forall\, S \in \mathcal{R} : nf(n)\, S\, F(x) \qquad \text{Definition von } \mathcal{R} \\ & \iff & nf(n)\, (\bigcap \mathcal{R})\, F(x) \\ & \iff & nf(n)\, R\, F(x) \qquad\qquad \text{Definition von } R \end{array}$$

Wir zeigen nun im nächsten Beweisteil, dass R eine Funktion von N nach A ist.

Beweis der Totalität: Wir betrachten die folgende Teilmenge X von N:

$$X := \{n \in N \mid \exists\, x \in A : n\, R\, x\}$$

Aus (IBR) folgt $a \in X$. Wir verifizieren noch $nf(X) \subseteq X$, woraus mit der Forderung (3) von Definition 11.1.1 folgt, dass $X = N$ gilt, also R total ist. Zum Beweis von $nf(X) \subseteq X$ sei $n \in nf(X)$ gegeben. Dann gibt es ein $m \in X$ mit $n = nf(m)$. Wegen $m \in X$ existiert ein $x \in A$ mit $m\, R\, x$. Daraus folgt mit (ISR) die Eigenschaft $nf(m)\, R\, F(x)$, also $n\, R\, F(x)$, was $n \in X$ nach sich zieht.

Beweis der Eindeutigkeit: Hierzu betrachten wir die folgende Teilmenge X von N:

$$X := \{n \in N \mid \forall x, y \in A : n\, R\, x \wedge n\, R\, y \Rightarrow x = y\}$$

Es genügt wiederum, $a \in X$ und $nf(X) \subseteq X$ zu beweisen. Aus der Forderung (3) von Definition 11.1.1 folgt dann $X = N$, und dies impliziert die Eindeutigkeit von R.

Wir beweisen $a \in X$ durch Widerspruch und nehmen $a \notin X$ an. Wegen (IBR) existiert in diesem Fall ein $c' \in A$ mit $c \neq c'$ und $a\, R\, c'$. Wir definieren nun $R' := R \setminus \{(a, c')\}$ und bekommen dadurch $R' \subset R$. Weiterhin haben wir $a\, R'\, c$ und auch, dass für alle $n \in N$ und $x \in X$ wegen $nf(n) \neq a$ (Forderung (1) von Definition 11.1.1) gilt

$$n\, R'\, x \implies n\, R\, x \implies nf(n)\, R\, F(x) \implies nf(n)\, R'\, F(x),$$

was $R' \in \mathcal{R}$ nach sich zieht. Es ist aber $R' \in \mathcal{R}$ und $R' \subset R$ ein Widerspruch zu $R = \bigcap \mathcal{R}$.

Zum Beweis von $nf(X) \subseteq X$ sei ein $n \in nf(X)$ vorgegeben und ein $m \in X$ mit $n = nf(m)$. Wegen $m \in X$ und der schon bewiesenen Totalität von R gibt es genau ein $x \in A$ mit $m\, R\, x$, woraus auch $nf(m)\, R\, F(x)$ folgt. Wir nehmen nun für einen Beweis von $n \in X$ durch Widerspruch an, dass $n \notin X$ gelte, also $nf(m) \notin X$. Wegen $nf(m)\, R\, F(x)$ gibt es dann ein $y \in X$ mit $y \neq F(x)$ und $nf(m)\, R\, y$. Wie oben definieren wir nun eine Relation $R' \subset R$, indem wir setzen $R' := R \setminus \{(nf(m), y)\}$ und zeigen nachfolgend, dass $R' \in \mathcal{R}$ gilt, was ein Widerspruch zu $R = \bigcap \mathcal{R}$ ist.

Es gilt $a\, R'\, c$ aufgrund von (IBR) und $nf(m) \neq a$ (Forderung (1) von Definition 11.1.1). Zum Beweis der zweiten Eigenschaft, die $R' \in \mathcal{R}$ erfordert, seien $p \in N$ und $z \in A$ gegeben. Dann gilt:

$$p\, R'\, z \implies p\, R\, z \implies nf(p)\, R\, F(z) \implies nf(p)\, R'\, F(z)$$

Hier gilt die zweite Implikation wegen (ISR). Die Begründung für die dritte Implikation ist wie folgt: Im Fall $p \neq m$ gilt $nf(p) \neq nf(m)$ aufgrund der Injektivität von nf (Forderung (2) von Definition 11.1.1). Also sind $nf(p)\, R\, F(z)$ und $nf(p)\, R'\, F(z)$ äquivalent, denn es wird nur ein Paar mit erster Komponente $nf(m)$ aus R entfernt. Gilt hingegen $p = m$, so folgt aus $m\, R\, z$, dass $z = x$ gilt (denn x ist das einzige Element mit $m\, R\, x$; siehe oben), und dies impliziert die folgende Eigenschaft:

$$(nf(p), F(z)) = (nf(m), F(z)) = (nf(m), F(x)) \neq (nf(m), y)$$

Das Paar $(nf(p), F(z))$ wird wegen der zweiten Komponente nun nicht aus R entfernt.

Damit ist R eine Funktion. In der üblichen Schreibweise haben wir also $R : N \to A$. Die Eigenschaft (IBR) wird zu $R(a) = c$, also (IB), und die Eigenschaft (ISR) wird zu

$$\forall\, n \in N, x \in A : R(n) = x \Rightarrow R(nf(n)) = F(x),$$

woraus durch Spezialisierung von x zu $R(n)$

$$\forall\, n \in N : R(nf(n)) = F(R(n))$$

folgt, also die Eigenschaft (IS) für R. □

Um die Präsentation möglichst einfach zu halten, haben wir den Rekursionssatz nur für einstellige Funktionen formuliert. Er kann aber durchaus auf mehrstellige Funktionen erweitert werden, beispielsweise auf 2-stellige Funktionen wie folgt: Es seien (N, a, nf) eine Peano-Struktur, $F : A \to A$ eine Funktion und $c : B \to A$ ebenfalls eine Funktion. Dann gibt es genau eine Funktion $f : N \times B \to A$, welche die folgenden zwei Eigenschaften erfüllt:

$$(\mathrm{IB}_1) \quad \forall\, x \in B : f(a, x) = c(x) \qquad (\mathrm{IS}_1) \quad \forall\, n \in N, x \in B : f(nf(n), x) = F(f(n, x))$$

Zum Beweis betrachten wir die folgenden Formeln, wobei als Funktion $g : N \to A^B$ verwendet wird:

$$(\mathrm{IB}_2) \quad g(a) = c \qquad (\mathrm{IS}_2) \quad \forall\, n \in N : g(nf(n)) = F \circ g(n)$$

Nach dem Rekursionssatz gibt es genau eine Funktion $g : N \to A^B$, welche die zwei Eigenschaften (IB_2) und (IS_2) erfüllt. Um dabei formal das Muster in der Eigenschaft (IS) des Rekursionssatzes zu erhalten, schreiben wir die Funktionskomposition $F \circ g(n)$ als Funktionsanwendung $G_F(g(n))$, wobei die Funktion $G_F : A^B \to A^B$ für alle $h : B \to A$ durch $G_F(h) = F \circ h$ definiert ist. Aus der Funktion g bekommen wir nun die eindeutig gewünschte Funktion $f : N \times B \to A$, welche (IB_1) und (IS_1) erfüllt, indem wir $f(n, x) = g(n)(x)$ für alle $n \in N$ und $x \in B$ festlegen.

Sowohl in dieser Verallgemeinerung als auch im Original hängt in der Eigenschaft (IS) die Berechnung des Resultats von f zur Eingabe $nf(n)$ nur von dem Resultat von f zur Eingabe n ab. Bei praktischen Anwendungen induktiver/rekursiver Definitionen kommt es aber sehr oft vor, dass sie auch noch von n und/oder x abhängt. In solchen Fällen ist F z.B. eine Funktion von $A \times N$ nach A und die Gleichung $f(nf(n)) = F(f(n))$ des Rekursionssatzes wird zu $f(nf(n)) = F(f(n), n)$. Analog wird die Gleichung $f(nf(n), x) = F(f(n, x))$ der oben erwähnten Verallgemeinerung zu $f(nf(n), x) = F(f(n, x), n)$.

11.2 Eindeutigkeit und Existenz von Peano-Strukturen

Wir haben im letzten Abschnitt angemerkt, dass die algebraische Struktur $(\mathbb{N}, 0, nachf)$ mit der Menge der bisher intuitiv verwendeten natürlichen Zahlen, der Null und der Nachfolger-Funktion $nachf : \mathbb{N} \to \mathbb{N}$, $nachf(n) = n + 1$ eine Peano-Struktur bildet. Man bekommt aber beispielsweise auch eine Peano-Struktur, indem man im Tripel $(\{|\}^*, (), nf)$

Basic Fixpoint Theory

Assumed are standard notions like complete lattice, CPO, monotonic resp. continuous function, chain, direct product of lattices and CPOs.

Fixpoint theorem I. Let $f : A \to A$ be a monotonic function on a CPO $(A, \leq)$. Then f has a least fixpoint, denoted as $\mu(f)$.

Fixpoint theorem II. Let $f : A \to A$ be a monotonic function on a complete lattice $(A, \leq)$. Then $\mu(f) = \mathbf{inf}\{x \in A \mid f(x) \leq x\}$.

A predicate P on a CPO $(A, \leq)$ is **admissible** (for Scott induction), if for all chains $K \subseteq A$ it holds:

$$(\forall x \in K : P(x)) \Rightarrow P(\mathbf{sup}\, K)$$

If $P(x)$ can be specified as $f(x) \leq g(x)$, where $f, g : A \to B$ are continuous functions into a CPO $(B, \leq)$, then P is admissible.

Scott induction. Let $(A, \leq)$ be a CPO and $f : A \to A$ be monotoic. If P is an admissible predicate on $(A, \leq)$ such that

$$\boxed{\text{(IB)} \quad P(\bot)} \qquad \boxed{\text{(IS)} \quad \forall x \in A : P(x) \Rightarrow P(f(x)),}$$

then $P(\mu(f))$ holds.

Similtaneous Scott induction. Let $(A \times B, \leq)$ be the direct product of the CPOs $(A, \leq)$ and $(B, \leq)$ and $f : A \to A$ and $g : B \to B$ be monotonic. If P is an admissible predicate on $(A \times B, \leq)$ such that

$$\boxed{\text{(IB)} \quad P(\bot, \bot)} \qquad \boxed{\text{(IS)} \quad \forall x \in A, y \in B : P(x, y) \Rightarrow P(f(x), g(y)),}$$

then $P(\mu(f), \mu(g))$ holds.

The second induction principle can be reduced to the first one using the **tupling** $[f, g] : A \times B \to A \times B$, where $[f, g](x, y) = (f(x), g(y))$, since $[f, g]$ is monotonic and $\mu([f, g]) = (\mu(f), \mu(g))$.

Heterogeneous Relation Algebra

Constants: $\mathsf{O} : A \leftrightarrow B$, $\mathsf{L} : A \leftrightarrow B$ and $\mathsf{I} : A \leftrightarrow A$.

Operations: $R \cup S$, $R \cap S$, $R;S$, $\overline{R}$ and R^{T}.

Tests: $R \subseteq S$ and $R = S$.

Laws:

- Lattice (Boolean algebra) theory:

$$R \cap S \subseteq R \quad R \subseteq R \cup S \quad \overline{\overline{R}} = R \quad \ldots$$

- Composition and transposition:

$$(R;S)^{\mathsf{T}} = S^{\mathsf{T}};R^{\mathsf{T}} \quad (R \cup S)^{\mathsf{T}} = R^{\mathsf{T}} \cup S^{\mathsf{T}} \quad \ldots$$

- Monotonicity:

$$R \subseteq S \Rightarrow Q;R \subseteq Q;S \quad R \subseteq S \Rightarrow R^{\mathsf{T}} \subseteq S^{\mathsf{T}} \quad \ldots$$

- Dedekind rule:

$$Q;R \cap S \subseteq (Q \cap S;R^{\mathsf{T}});(R \cap Q^{\mathsf{T}};S)$$

$A \leftrightarrow B$ denotes the set of relations with source A and target B.

Relational Peano Structures (N, z, S)

- Relation $z : N \leftrightarrow \mathbf{1}$ (or $z : N \leftrightarrow B$) is a **(relational) point**:

  (1) $\boxed{z;\mathsf{L} = \mathsf{L} \qquad z;z^{\mathsf{T}} \subseteq \mathsf{I} \qquad z^{\mathsf{T}};\mathsf{L} = \mathsf{L}}$

- Relation $S : N \leftrightarrow N$ is **total** and **univalent**:

  (2) $\boxed{S;\mathsf{L} = \mathsf{L} \qquad S^{\mathsf{T}};S \subseteq \mathsf{I}}$

- Relational version of (P_3):

  (3) $\boxed{S;S^{\mathsf{T}} \subseteq \mathsf{I}}$ (S is injective)

- Relational version of (P_4):

  (4) $\boxed{S;z = \mathsf{O}}$

- Relational version of (P_5):

  $$\forall v \in [N \leftrightarrow \mathbf{1}] : z \subseteq v \wedge S^{\mathsf{T}};v \subseteq v \Rightarrow v = \mathsf{L}$$

  Due to the fixpoint theorem II this is equivalent to:

  (5) $\boxed{\mu(g) = \mathsf{L}, \text{ where } g : [N \leftrightarrow \mathbf{1}] \to [N \leftrightarrow \mathbf{1}], g(v) = z \cup S^{\mathsf{T}};v}$

Relational Version of the Recursion Theorem

We assume a relational Peano structure (N, z, S), a point $c : A \leftrightarrow \mathbf{1}$ and a total and univalent relation $F : A \leftrightarrow A$.

For each univalent and total relation $f : N \leftrightarrow A$ then the relational versions of the formulae (IB) and (IS) of the recursion theorem are $z;c^{\mathsf{T}} \subseteq f$ and $S;f = f;F$ and these are equivalent to:

$$\text{(D)} \qquad \boxed{z;c^{\mathsf{T}} \cup S^{\mathsf{T}};f;F \subseteq f}$$

Theorem I. Consider the following $\subseteq$-monotonic function:

$$h : [N \leftrightarrow A] \to [N \leftrightarrow A] \qquad\qquad h(X) = z;c^{\mathsf{T}} \cup S^{\mathsf{T}};X;F$$

Then we have:

(a) $\mu(h)$ satisfies (D).

(b) $\mu(h)$ is total and univalent.

(c) If $R : N \leftrightarrow A$ satisfies (D) and is total and univalent, then $R = \mu(h)$.

Proof. (a) is trivial.

(b) Totality of $\mu(h)$: Scott induction with the following predicate on the direct product of the lattices $([N \leftrightarrow \mathbf{1}], \subseteq)$ and $([N \leftrightarrow A], \subseteq)$:

$$P(v, X) :\Leftrightarrow v \subseteq X;\mathsf{L}$$

Admissibility of P: Obvious.

Induction base: $P(\mathsf{O}, \mathsf{O})$ is trivial.

Induction step: Assume $v : N \leftrightarrow \mathbf{1}$ and $X : N \leftrightarrow A$ such that $P(v, X)$ is true. With the function g from (5) then $P(g(v), h(X))$ is shown by:

$$\begin{aligned} g(v) &= z \cup S^{\mathsf{T}};v && \text{definition } g \\ &\subseteq z \cup S^{\mathsf{T}};X;\mathsf{L} && P(v, X) \\ &= z \cup S^{\mathsf{T}};X;F;\mathsf{L} && F \text{ total} \\ &= z;c^{\mathsf{T}};\mathsf{L} \cup S^{\mathsf{T}};X;F;\mathsf{L} && z, c \text{ points} \\ &= h(X);\mathsf{L} && \text{distr., definition } h \end{aligned}$$

From (5) and $P(\mu(g), \mu(h))$ it follows $\mathsf{L} = \mu(g) \subseteq \mu(h);\mathsf{L}$.

Univalence of $\mu(h)$: Scott induction with the following predicate on $([N \leftrightarrow A], \subseteq)$:

$$P(X) :\Leftrightarrow X^{\mathsf{T}};X \subseteq \mathsf{I}$$

Admissibility of P: Assume $\mathcal{K} \subseteq [N \leftrightarrow A]$ to be a chain such that $P(X)$ is true for all $X \in \mathcal{K}$. Then $P(\bigcup \mathcal{K})$ is shown by:

$$\begin{aligned}
(\bigcup \mathcal{K})^{\mathsf{T}};(\bigcup \mathcal{K}) &= (\bigcup\{R^{\mathsf{T}} \mid R \in \mathcal{K}\});(\bigcup \mathcal{K}) && \text{transp. distr.}\\
&= \bigcup\{R^{\mathsf{T}};(\bigcup \mathcal{K}) \mid R \in \mathcal{K}\} && \text{comp. distr.}\\
&= \bigcup\{\bigcup\{R^{\mathsf{T}};S \mid S \in \mathcal{K}\} \mid R \in \mathcal{K}\} && \text{comp. distr.}\\
&\subseteq \bigcup\{\mathsf{I} \mid R \in \mathcal{K}\} && \text{see below}\\
&= \mathsf{I}
\end{aligned}$$

Given an arbitrary $R \in \mathcal{K}$ we have

$$\bigcup\{R^{\mathsf{T}};S \mid S \in \mathcal{K}\} \subseteq \mathsf{I},$$

since $\mathcal{K}$ is a chain of univalent relations and for all $S \in \mathcal{K}$ we have

$$R^{\mathsf{T}};S \subseteq \begin{cases} S^{\mathsf{T}};S \subseteq \mathsf{I} & \text{if } R \subseteq S \\ R^{\mathsf{T}};R \subseteq \mathsf{I} & \text{if } S \subseteq R. \end{cases}$$

Induction base: $P(\mathsf{O})$ is trivial.

Induction step: Assume $X : N \leftrightarrow A$ such that $P(X)$ holds. Then $P(h(X))$ is shown by:

$$\begin{aligned} h(X)^{\mathsf{T}};h(X) &= (z;c^{\mathsf{T}} \cup S^{\mathsf{T}};X;F)^{\mathsf{T}};(z;c^{\mathsf{T}} \cup S^{\mathsf{T}};X;F) \\ &= (c;z^{\mathsf{T}} \cup F^{\mathsf{T}};X^{\mathsf{T}};S);(z;c^{\mathsf{T}} \cup S^{\mathsf{T}};X;F) \\ &= c;z^{\mathsf{T}};z;c^{\mathsf{T}} \cup c;z^{\mathsf{T}};S^{\mathsf{T}};X;F \cup F^{\mathsf{T}};X^{\mathsf{T}};S;z;c^{\mathsf{T}} \cup F^{\mathsf{T}};X^{\mathsf{T}};S;S^{\mathsf{T}};X;F \\ &\subseteq \mathsf{I} \end{aligned}$$

Here

$$c;z^{\mathsf{T}};z;c^{\mathsf{T}} \subseteq c;\mathsf{L};c^{\mathsf{T}} = c;c^{\mathsf{T}} \subseteq \mathsf{I}$$

uses that c is a point,

$$c;z^{\mathsf{T}};S^{\mathsf{T}};X;F = c;(S;z)^{\mathsf{T}};X;F = c;\mathsf{O};X;F = \mathsf{O}$$

uses (4),

$$F^{\mathsf{T}};X^{\mathsf{T}};S;z;c^{\mathsf{T}} = F^{\mathsf{T}};X^{\mathsf{T}};\mathsf{O};c^{\mathsf{T}} = \mathsf{O}$$

uses again (4) and

$$F^{\mathsf{T}};X^{\mathsf{T}};S;S^{\mathsf{T}};X;F \subseteq F^{\mathsf{T}};X^{\mathsf{T}};X;F \subseteq F^{\mathsf{T}};F \subseteq \mathsf{I}$$

uses that S is injective, $P(X)$ holds and F is univalent.

(c) Let $R : N \leftrightarrow A$ be total, univalent such that (D) holds, i.e., $h(R) \subseteq R$. We use Scott induction with the following predicate on $([N \leftrightarrow A], \subseteq)$:

$$P(X) :\Leftrightarrow X \subseteq R$$

Admissibility of P: Obvious.

Induction base: $P(\mathsf{O})$ is trivial.

Induction step: Assume $X : N \leftrightarrow A$ such that $P(X)$ holds. Then $P(h(X))$ is shown by:

$$\begin{aligned} h(X) &= z;c^{\mathsf{T}} \cup S^{\mathsf{T}};X;F && \text{definition } h \\ &\subseteq z;c^{\mathsf{T}} \cup S^{\mathsf{T}};R;F && P(X) \\ &= h(R) && \text{definition } h \\ &\subseteq R && \text{assumption} \end{aligned}$$

Totality of $\mu(h)$, Dedekind rule, $\mu(h) \subseteq R$ and univalence of R imply:

$$R = \mu(h);\mathsf{L} \cap R \subseteq (\mu(h) \cap R;\mathsf{L}^{\mathsf{T}});(\mathsf{L} \cap \mu(h)^{\mathsf{T}};R) \subseteq \mu(h);R^{\mathsf{T}};R \subseteq \mu(h)$$

Relational Version of the Isomorphism Theorem

Using Scott induction and relation algebra also the following relational version of the Dedekind isomorphism iheorem easily can be shown.

Theorem II. Let (N_1, z_1, S_1) and (N_2, z_2, S_2) be relational Peano structures. Consider the following instance of the function h of Theorem I:

$$h : [N_1 \leftrightarrow N_2] \to [N_1 \leftrightarrow N_2] \qquad h(X) = z_1;{z_2}^{\mathsf{T}} \cup {S_1}^{\mathsf{T}};X;S_2$$

Then $\mu(h)$ is surjektive and injektive.

Hence, $\mu(h)$ is a bijective function with the following properties:

$$z_1;{z_2}^{\mathsf{T}} \subseteq \mu(h) \qquad S_1;\mu(h) = \mu(h);S_2$$

This means that $\mu(h) : N_1 \leftrightarrow N_2$ is a **(relational) isomorphism** between the relational structures (N_1, z_1, S_1) and (N_2, z_2, S_2).

Generalisation: Additional Arguments

$$\begin{aligned}\textbf{fun } add \quad (zero, y) &= y \\ \mid add\ (succ(x), y) &= succ(add(x, y));\end{aligned}$$

Unary version obtained via currying, $add' = \textbf{curry}(add)$:

$$\begin{aligned}\textbf{fun } add' \quad (zero) &= (\textbf{fn } y \Rightarrow y) \\ \mid add'\ (succ(x)) &= succ \circ add'(x);\end{aligned}$$

Recursion theorem I. Given a Peano structure (N, z, s), sets A and B, a function $c : B \to A$ and a function $F : A \to A$, there exists precisely one function $f : N \times B \to A$ such that:

(IB) $\boxed{\forall b \in B : f(z, b) = c(b)}$

(IS) $\boxed{\forall x \in N, b \in B : f(s(x), b) = F(f(x, b))}$

Proof. Reduction to the original recursion theorem to obtain the Curry version $f' : N \to B^A$ of f. Then $f := \textbf{uncurry}(f')$ shows the claim.

A relational version of the recursion theorem I can be found in the paper.

Generalisation: Additional Dependency

Computation of the sum $sum(x) = 0 + 1 + \ldots + x$:

$$\begin{aligned} \textbf{fun } sum \quad (zero) &= zero \\ \mid sum\ (succ(x)) &= add(sum(x), succ(x)); \end{aligned}$$

In such a situation again the original Dedekind recursion theorem is not applicable and a generalisation is required.

Recursion theorem II. Given a Peano structure (N, z, s), a set A, an element $c \in A$ and a function $F : A \times N \to A$, there exists precisely one function $f : N \to A$ such that:

(IB) $f(z) = c$

(IS) $\forall x \in N : f(s(x)) = F(f(x), x)$

A relational version of this theorem can be found in the paper.

Conclusion

The usual partial order can be defined as reflexive-transitive closure s^*.

Relation-algebraic formulation and proofs of basic properties of the arithmetic operartions and the partial order. Use of theorem provers for that.

- **Isabelle/HOL:** Use of heterogeneous relation algebra may lead to difficulties.
- **Coq:** There exists a library for heterogeneous relation algebra. Library for fixpoint theory **???**

References:

- Richard Dedekind, Was sind und was sollen die Zahlen, Teubner Verlag, Braunschweig, 1888.
- Edmund Landau, Grundlagen der Analysis, Akademische Verlagsgesellschaft, Leipzig, 1930.
- Paul Lorenzen, Die Definition durch vollständige Induktion, Monatshefte für Mathematik und Physik 47, 356-358, 1939.