A Predicative Strong Normalisation Proof for a λ-calculus with Interleaving Inductive Types

Andreas Abel[1] and Thorsten Altenkirch[2]

[1] Department of Computer Science,
University of Munich
abel@informatik.uni-muenchen.de
[2] School of Computer Science & Information Technology,
University of Nottingham
txa@cs.nott.ac.uk

Abstract. We present a new strong normalisation proof for a λ-calculus with interleaving strictly positive inductive types λ^μ which avoids the use of impredicative reasoning, i.e., the theorem of Knaster-Tarski. Instead it only uses predicative, i.e., strictly positive inductive definitions on the metalevel. To achieve this we show that every strictly positive operator on types gives rise to an operator on saturated sets which is not only monotone but also (deterministically) set based – a concept introduced by Peter Aczel in the context of intuitionistic set theory. We also extend this to coinductive types using greatest fixpoints of strictly monotone operators on the metalevel.

1 Introduction

We shall investigate a λ-calculus with strictly positive[1] inductive types. I.e., given a type $\sigma(X)$ where X appears only strictly positive we may construct a new type $\mu X.\sigma$ which is generated by the constructor $\mathsf{c} : \sigma(\mu X.\sigma) \to \mu X.\sigma$. Examples are the natural numbers $\mathsf{Nat} = \mu X.1 + X$, lists over a given type τ: $\mathsf{List}^\tau = \mu X.1 + \tau \times X$ or trees branching over τ: $\mathsf{Tree}^\tau = \mu X.1 + (\tau \to X)$. We also allow *interleaving* inductive types, as an example consider arbitrarily but finitely branching trees which can be defined by

$$\mathsf{Fin} = \mu X.\mathsf{List}^X = \mu X.\mu Y.1 + X \times Y$$

We call Fin interleaving because the inductive definition goes through another inductive type – List. A type like $\mathsf{Tree}^{\mathsf{Nat}}$ is nested but not interleaved. [2]

[1] The occurrence of a type variable is *positive* iff it occurs within an even number of left hand sides of $\to$-types, it is strictly positive iff it never occurs on the left hand side of a $\to$-type. We will only use strictly positive occurrences in this paper because positive inductive types cannot be understood predicatively in general.

[2] The use of the term *interleaving* for this situation is due to Ralph Matthes, e.g., see [Mat98]. An alternative would be *mutually*.

Positivity is essential for normalisation, i.e., we do not allow recursive domain equations like $X = X \to X$ which may be represented by the type $\mu X.X \to X$. The difference between positive and strictly positive is more subtle, i.e., $\mu X.(X \to \mathsf{Bool}) \to \mathsf{Bool}$ is an example of a positive but not strictly positive type. This example has been used by Reynolds to show that there are no set-theoretical models of System F [Rey84].

We consider λ^μ as a simply typed programming language corresponding to a subset of Martin-Löf's Type Theory (MLTT) [Mar84]. For our system we show the important property of strong normalisation, following the idea of Tait [Tai67]. To show strong normalisation of the simply typed λ-calculus, he defined a set-valued interpreting function $[\![-]\!]$ on the types. For each type σ the set $[\![\sigma]\!]$ contains the *computable terms* of type σ. Later Girard extended this idea to the impredicative System F under the name *candidates of reducibility* [Gir72]. Our construction is based on a technical alternative to *candidates* called *saturated sets* - this technique has been used by Luo [Luo90] and by the second author [Alt93]. Since in our system a type σ may contain free variables, the interpretation $[\![\sigma]\!]$ is no longer just a saturated set but a monotone operator on saturated sets.

Now we could just adopt the normalisation proof for System F and use Knaster's and Tarski's theorem, stating that every monotone operator on a complete lattice has a least fixed point, to define the interpretation for μ-types. But this construction would require impredicative reasoning and the full proof-theoretical strength of System F. It could not be carried out in a predicative meta theory like MLTT. Should it not be possible to reason about a predicative system like λ^μ in a predicative[3] meta theory, as for instance, MLTT?

Predicative theories allow only *strictly positive* inductive definitions. That means they must be given by an operator $\Phi(P)$ where P only occurs strictly positive, i.e., never on the left hand side of an arrow. Φ defines a set μ which is characterized as the smallest set closed under Φ:

$$\frac{}{\Phi(\mu) \subseteq \mu}\,(\mathrm{intro}) \qquad \frac{\Phi(Q) \subseteq Q}{\mu \subseteq Q}\,(\mathrm{elim})$$

Strictly positive inductive definitions can be understood as defined by well founded derivation trees which may be infinitely branching. Hence, when building a derivation, we only refer to subderivations which are smaller in an intuitive sense. In this way the consistency of predicative theories can be justified, whereas the consistency of impredicative theories is only empiric. Furthermore there are more options to extend a weaker, i.e., predicative theory without getting into inconsistencies.

In this paper we show that indeed the strong normalisation of λ^μ can be proven by predicative means. We manage to define the interpretation $[\![-]\!]$ of the types without Knaster-Tarski, just by strictly positive inductive definitions, using the concept of (deterministically) *set based operators* introduced by Peter

[3] We are using the term *predicative* in the sense of *avoiding circular definitions* — this usage has been popularized by Per Martin-Löf. In the terminology of proof theory our system would be called impredicative since its ordinal is greater than Γ_0.

Aczel in the context of intuitionistic set theory [Acz97]. Intuitively, a set based operator can be understood as a monotone operator Φ which comes with a *urelement* relation $\mathcal{U}$. We require that if $y \in \Phi(P)$ and $x \;\mathcal{U}\; y$ (read x is an urelement of y) then $x \in P$. We also require that the urelements can be used to reconstruct the whole, i.e., $y \in \Phi(\{x \mid x \;\mathcal{U}\; y\})$ for reasonable $y \in \Phi(\mathsf{True})$. For any monotone operator Φ which satisfies the conditions given above the predicate $x \in \Phi(P)$ can be replaced by the conditions $x \in \Phi(\mathsf{True})$ and $\forall y \;\mathcal{U}\; x \to y \in P$ which is strictly positive in P (see proposition 1). We have used this technique in [AA99] to construct a value semantics for the types of the foetus system predicatively.

As an example consider Φ_{List} which can be defined inductively (writing [] for the empty list and :: for cons):

$$\frac{}{[] \in \Phi_{\mathsf{List}}(P)} \qquad \frac{a \in P \qquad l \in \Phi_{\mathsf{List}}(P)}{a :: l \in \Phi_{\mathsf{List}}(P)}$$

The appropriate relation $\mathcal{U}_{\mathsf{List}}$ can be defined inductively as well:

$$\frac{}{a \;\mathcal{U}_{\mathsf{List}}\; a :: l} \qquad \frac{a \;\mathcal{U}_{\mathsf{List}}\; l}{a \;\mathcal{U}_{\mathsf{List}}\; b :: l}$$

It is now straightforward to verify that Φ_{List} is set based by rule induction.

We show that every strictly positive type can be interpreted by a set based operator and that fixpoints of set based operators can be constructed by strictly positive inductive definitions on the meta level. Unsurprisingly, we need additional power on the metalevel which is given by one level of reflection corresponding to the introduction of a Martin-Löf universe. Specifically, this is required when defining the interpretation of types $[\![\sigma]\!]$.

We also extend the construction to coinductive or lazy types (like the type of Streams over τ which is given by $\mathsf{Stream}^{\tau} = \nu X.\tau \times X$). To do so we consider strictly positive definitions of greatest fixpoints as predicatively acceptable. This assumption is based on the work on coinductive types in Type Theory [Coq94]. Intuitively, greatest fixpoints correspond to arbitrary trees, i.e., not necessarily well founded ones.

To be precise: We assume that given a propositional expression $\Phi(P)$ s.t. P appears strictly positive, it is possible to construct the greatest fixpoint ν of Φ, s.t.

$$\frac{}{\nu \subseteq \Phi(\nu)}\,(\text{co-intro}) \qquad \frac{Q \subseteq \Phi(Q)}{Q \subseteq \nu}\,(\text{co-elim})$$

1.1 Related work

Lambda calculi with inductive types have been considered by a number of authors, e.g., see [Hag87,Men88,Dyb91,CM89,Geu92,Loa97,Alt98]. Loader notes that strong normalisation can be shown by using the techniques from System F. This is carried out for monotone inductive types with primitive recursion by Ralph Matthes [Mat98], using an impredicative meta theory. Benl presents a predicative strong normalisation proof for non-interleaving inductive types [Ben98], but this has not been extended to interleaving inductive types or coinductive types.

Jouannaud and Okada [JO97], later with Blanqui [BJO99], also do not treat interleaving inductive types, which they call mutually inductive. Furthermore their normalisation proof is not predicative from our perspective, since they use the theorem of Knaster and Tarski to construct the computability predicates. This requires quantification over all such predicates, which can only be carried out in an impredicative meta theory.

The system we are investigating here is closely related to the proof-theoretical system $\mathsf{ID}^i_{<\omega}$. However, we differ in allowing interleaving inductive definitions which correspond to simultaneously defined sets. It is not clear in the moment whether Buchholz' reduction from ID^c_α to ID^i_α [Buc81], which also justifies positive inductive definitions, can be extended to our system.

1.2 Acknowledgments

Thierry Coquand has pointed out to us that one should use set based operators to prove normalisation predicatively. We would also like to acknowledge discussions with Peter Aczel on set based operators. Helmut Schwichtenberg allowed us to present this work to his group, where we got interesting feedback from him and his colleagues. Ralph Matthes gave a lot of very helpful comments on the draft. We would also like to thank the anonymous referees who invested a lot of time and effort to write reports which helped us to improve the paper.

1.3 Notational conventions

We are using a vector notation to simplify our notation. If we have a family of expressions $e_1, e_2, \ldots, e_n$ we write $\boldsymbol{e}$ for the whole sequence. We denote the length n of the sequence by $|\boldsymbol{e}|$. Given a fixed e we write $\boldsymbol{e}e$ for $e_1 e, e_2 e, \ldots, e_n e$. Given a sequence of sets $\boldsymbol{S}$ where $|\boldsymbol{S}| = n$ we write $\Pi \boldsymbol{S}$ for $S_1 \times S_2 \times \cdots \times S_n$.

We use set notation to define predicates, i.e., we write $x \in P$ for $P(x)$ and we define new predicates by the notation for set comprehension. However, sets are not first order citizens in our meta theory, i.e., we do not quantify over sets and we do not use power sets. We write relations infix, i.e., we write $x\ R\ y$ for $(x, y) \in R$. We write projections as partial applications, i.e., $R(y) = \{x \mid x\ R\ y\}$.

We will annotate term families by types but to increase readability we will often omit these annotations. We use the convention that all arrow symbols associate to the right. We consider types and terms upto alpha-equivalence and use $\equiv$ to denote this.

2 The Calculus $\boldsymbol{\lambda}^{\boldsymbol{\mu}}$

We already presented this calculus in [Alt98] also allowing positive inductive types. We shall simplify the presentation here by exploiting the fact that we are only interested in strictly positive types, following [Loa97,Abe99]. The choice of type formers presented here is quite canonical and corresponds to bicartesian closed categories which have also initial algebras for all definable endofunctors.

We assume a set of type variables $\mathcal{X}$, we denote elements of $\mathcal{X}$ by X, Y, Z and finite sequences of type variables by $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z}$. The extension of $\boldsymbol{X}$ by Y is denoted by $\boldsymbol{X}, Y$. We define the set of types in which the variables $\boldsymbol{X}$ occur at most strictly positive $\mathsf{Ty}(\boldsymbol{X})$ inductively by the following rules:

$$\frac{}{0, 1 \in \mathsf{Ty}(\boldsymbol{X})}\,(\mathrm{Const}) \qquad \frac{}{X_i \in \mathsf{Ty}(\boldsymbol{X})}\,(\mathrm{Var}) \qquad \frac{\sigma \in \mathsf{Ty}() \qquad \tau \in \mathsf{Ty}(\boldsymbol{X})}{\sigma \to \tau \in \mathsf{Ty}(\boldsymbol{X})}\,(\mathrm{Arr})$$

$$\frac{\sigma, \tau \in \mathsf{Ty}(\boldsymbol{X})}{\sigma + \tau, \sigma \times \tau \in \mathsf{Ty}(\boldsymbol{X})}\,(\mathrm{Sum}),(\mathrm{Prod}) \qquad \frac{\sigma \in \mathsf{Ty}(\boldsymbol{X}, Y)}{\mu Y.\sigma \in \mathsf{Ty}(\boldsymbol{X})}\,(\mathrm{Mu})$$

Closed types are denoted by $\mathsf{Ty} = \mathsf{Ty}()$. If $\sigma \in \mathsf{Ty}(\boldsymbol{X})$ and $\tau_i \in \mathsf{Ty}$ for $1 \leq i \leq |\boldsymbol{X}|$ we write $\sigma(\boldsymbol{\tau}) \in \mathsf{Ty}$ for the result of substituting X_i in σ by τ_i in a capture avoiding way.

Different to System F, we can restrict the typing rules to closed types because we have no term forming rules which introduce new type variables (like Λ in the case of System F). A type context Γ is a finite sequence of assumptions of the form $x : \sigma$ where $x \in \mathcal{V}$ is a term variable and $\sigma \in \mathsf{Ty}$. We require that all the variables in a context are different. We introduce the judgment $\Gamma \vdash t : \sigma$ meaning that t has the type σ in context Γ, where $\sigma \in \mathsf{Ty}$. $\Gamma \vdash t : \sigma$ is given by the usual rules for simply typed λ calculus:

$$\frac{}{\Gamma, x : \sigma, \Delta \vdash x : \sigma}\,\mathrm{var} \qquad \frac{\Gamma, x : \sigma \vdash t : \tau}{\Gamma \vdash \lambda x^\sigma.t : \sigma \to \tau}\,\mathrm{lam} \qquad \frac{\Gamma \vdash t : \sigma \to \tau \quad \Gamma \vdash u : \sigma}{\Gamma \vdash tu : \tau}\,\mathrm{app}$$

Additionally we assume a set of constants $\mathcal{C}$ and a signature given by $\Sigma \subseteq \mathcal{C} \times \mathsf{Ty}$ which is decidable. We introduce the rule

$$\frac{c : \sigma \in \Sigma}{\Gamma \vdash c : \sigma}\,\mathrm{const}$$

For λ^μ we consider the following signature Σ^μ

$$\begin{aligned}
\mathsf{unit} &: 1 \\
\mathsf{pair}^{\sigma_1,\sigma_2} &: \sigma_1 \to \sigma_2 \to (\sigma_1 \times \sigma_2) \\
\pi_i^{\sigma_1,\sigma_2} &: (\sigma_1 \times \sigma_2) \to \sigma_i && i \in \{1, 2\} \\
\mathsf{case}_0^\sigma &: 0 \to \sigma \\
\mathsf{in}_i^{\sigma_1,\sigma_2} &: \sigma_i \to (\sigma_1 + \sigma_2) && i \in \{1, 2\} \\
\mathsf{case}^{\sigma_1,\sigma_2,\rho} &: (\sigma_1 \to \rho) \to (\sigma_2 \to \rho) \to (\sigma_1 + \sigma_2) \to \rho \\
\mathsf{c}^{X.\tau} &: \tau(\mu X.\tau) \to \mu X.\tau \\
\mathsf{It}^{X.\tau,\sigma} &: (\tau(\sigma) \to \sigma) \to (\mu X.\tau) \to \sigma
\end{aligned}$$

where $\sigma, \sigma_i, \rho \in \mathsf{Ty}$ and $\tau \in \mathsf{Ty}(X)$. We will often omit type annotations when they are clear from the context.

We write Tm^σ for the set of terms of type σ:

$$\mathsf{Tm}^\sigma = \{t | \exists \Gamma . \Gamma \vdash t : \sigma\}$$

Since we only allow strictly positive occurrences of type variables every type gives rise to a functor in the sense of category theory. We exploit this by defining the functorial strength of a type $\rho \in \mathsf{Ty}(\boldsymbol{X})$: Given $f_i \in \sigma_i \to \tau_i$ for $1 \leq i \leq n$, where $n = |\boldsymbol{X}|$ we define

$$\rho(\boldsymbol{f}) : \rho(\boldsymbol{\sigma}) \to \rho(\boldsymbol{\tau})$$

by induction over the structure of ρ: [4]

$$\begin{aligned}
C(\boldsymbol{f}) &= \lambda x^C . x \qquad C \in \{0, 1\} \\
X_i(\boldsymbol{f}) &= f_i \qquad 1 \leq i \leq n \\
(\rho_1 \to \rho_2)(\boldsymbol{f}) &= \lambda g^{\rho_1 \to \rho_2(\boldsymbol{\sigma})} . \lambda x^{\rho_1} . \rho_2(\boldsymbol{f})(g x) \\
(\rho_1 \times \rho_2)(\boldsymbol{f}) &= \lambda p^{\rho_1(\boldsymbol{\sigma}) \times \rho_2(\boldsymbol{\sigma})} . \, \mathsf{pair}^{\rho_1(\boldsymbol{\tau}) \times \rho_2(\boldsymbol{\tau})} (\rho_1(\boldsymbol{f})(\pi_1 p))(\rho_2(\boldsymbol{f})(\pi_2 p)) \\
(\rho_1 + \rho_2)(\boldsymbol{f}) &= \mathsf{case}^{\rho_1(\boldsymbol{\sigma}), \rho_2(\boldsymbol{\sigma}), \rho_1(\boldsymbol{\tau}) + \rho_2(\boldsymbol{\tau})} \\
&\qquad (\lambda x^{\rho_1(\boldsymbol{\sigma})} . \, \mathsf{in}_1(\rho_1(\boldsymbol{f}) x))(\lambda y^{\rho_2(\boldsymbol{\sigma})} . \, \mathsf{in}_2(\rho_2(\boldsymbol{f}) y)) \\
(\mu X . \rho)(\boldsymbol{f}) &= \mathsf{It}^{X . \rho(\boldsymbol{\sigma}, X), \mu\alpha} (\lambda x^{\rho(\boldsymbol{\sigma}, \mu\alpha)} . \, \mathsf{c}^{\,\alpha} (\rho(\boldsymbol{f}, \lambda y^{\mu\alpha} . y) x)) \\
&\qquad \text{where } \alpha \text{ abbreviates } X . \rho(\boldsymbol{\tau}, X)
\end{aligned}$$

This operation is motivated by the fact that each ρ gives rise to a (strong) functor. We allow a partial instantiation of ρ which can be defined by instantiating all other places with the identity function $\lambda x^\sigma . x$. The strength is needed in the definition of the β-rule for μ types, which, read as an equation, corresponds to weak initiality of the appropriate $\rho(-)$-algebra.

We are now ready to define the reduction relation $\rhd_1 \subseteq \mathsf{Tm} \times \mathsf{Tm}$. We first define top level β-reduction by the following axioms

$$\begin{aligned}
(\lambda x . t) u &\rhd_\beta u[x := t] \\
\pi_i(\mathsf{pair}\, t_1 t_2) &\rhd_\beta t_i \qquad i \in \{1, 2\} \\
\mathsf{case}\, t_1 t_2 (\mathsf{in}_i\, u) &\rhd_\beta t_i u \qquad i \in \{1, 2\} \\
\mathsf{It}^{X . \rho}\, t (\mathsf{c}\, u) &\rhd_\beta t(\rho(\mathsf{It}^{X . \rho}\, t) u)
\end{aligned}$$

and then define $\rhd_1 \subseteq \mathsf{Tm} \times \mathsf{Tm}$ as the congruence closure:

$$\frac{t \rhd_\beta u}{t \rhd_1 u} \qquad \frac{t \rhd_1 t'}{t u \rhd_1 t' u} \qquad \frac{u \rhd_1 u'}{t u \rhd_1 t u'} \qquad \frac{t \rhd_1 t'}{\lambda x . t \rhd_1 \lambda x . t'}$$

[4] The case for $\to$ works only because ρ_1 is closed by definition.

We define the set of strongly normalizing terms SN^σ of type σ inductively by the rule:

$$\frac{t \in \mathsf{Tm}^\sigma \qquad \forall t' \in \mathsf{Tm}^\sigma.(t \rhd_1 t') \implies t' \in \mathsf{SN}^\sigma}{t \in \mathsf{SN}^\sigma}$$

Our goal is to give a predicative proof of the strong normalization theorem:

Theorem 1. $\dfrac{t \in \mathsf{Tm}^\sigma}{t \in \mathsf{SN}^\sigma}$

3 Proving Strong Normalisation using Saturated Sets

Even for the simply typed lambda calculus strong normalisation cannot be proven by a mere induction over the term structure, since an application $(\lambda x.t)\ s$ can beta-reduce to a term $t[x := s]$ that neither is a subterm of t nor of s. To strengthen the induction hypothesis, Tait [Tai67] introduced the set of computable terms $[\![\sigma]\!] \subseteq \mathsf{SN}^\sigma$ of type σ. E.g., given $P \subseteq \mathsf{SN}^\sigma$, $Q \subseteq \mathsf{SN}^\tau$ we define

$$P \Rightarrow Q := \{t \in \mathsf{SN}^{\sigma\to\tau} \mid \forall u \in P.\ t\ u \in Q\}$$
$$[\![\sigma \to \tau]\!] := [\![\sigma]\!] \Rightarrow [\![\tau]\!]$$

The new obligation $\mathsf{Tm}^\sigma \subseteq [\![\sigma]\!]$ can be proven by induction over the terms (cf. Prop. 11) and the application case now is trivial.

But how does one extend this to other types, like the type of natural numbers? In [GLT89] it is suggested to interpret Nat by all strongly normalizing terms of this type. However, one has to pay a high price for this when showing the soundness of the eliminator and it is not clear how this technique can be extended to systems like the one presented here. Here we follow a different way and construct the interpretation of all other types *introduction based*, i.e.,

$$\frac{}{0 \in [\![\mathsf{Nat}]\!]} \qquad \frac{t \in [\![\mathsf{Nat}]\!]}{\mathrm{S}\ t \in [\![\mathsf{Nat}]\!]}$$

However, there are a lot of strongly normalizing terms which are not included in this definition. The basic idea is that the computable terms are the ones such that all computation paths end up in $[\![\mathsf{Nat}]\!]$, i.e., we may want to add the following rule

$$\frac{t \in \mathsf{Tm}^{\mathsf{Nat}} \qquad \forall u.t \rhd_1 u \implies u \in [\![\mathsf{Nat}]\!]}{t \in [\![\mathsf{Nat}]\!]}\ (\mathrm{comp})$$

But this is just the definition of $\mathsf{SN}^{\mathsf{Nat}}$! The key technical insight we use is to restrict attention to (strongly normalizing) terms whose canonical computation, which we call *weak head reduction* ($\rhd_{\mathsf{whd}}$), ends up in $[\![\mathsf{Nat}]\!]$ or which are canonically irreducible, such terms we call *void* (Void). Sets of strongly normalizing terms which are closed under canonical computations and which include all void terms we call *saturated* (SAT). In the example we would replace the rule (comp) by the two rules

$$\frac{t \in \mathsf{Void}^{\mathsf{Nat}}}{t \in [\![\mathsf{Nat}]\!]}\,(\mathrm{sat1}) \qquad \frac{t \in \mathsf{SN}^{\mathsf{Nat}} \qquad t \rhd_{\mathsf{whd}} t' \quad t' \in [\![\mathsf{Nat}]\!]}{t \in [\![\mathsf{Nat}]\!]}\,(\mathrm{sat2})$$

We are now going to define the notions Void and $\rhd_{\mathsf{whd}}$ for our calculus.[5] We define *evaluation contexts* as eliminator terms with a hole in the key position

$$E[X] ::= X\ t_1 \mid \pi_j\ X \mid \mathsf{case}\ t_1\ t_2\ X \mid \mathsf{It}\ t_1\ X$$

Weak head reduction $\rhd_{\mathsf{whd}} \subseteq \rhd_1$ is defined as the least relation closed under the β-axioms and under evaluation contexts.

$$\frac{t \rhd_\beta u}{t \rhd_1 u} \qquad \frac{t \rhd_{\mathsf{whd}} u}{E[t] \rhd_{\mathsf{whd}} E[u]}$$

Note that $\rhd_{\mathsf{whd}}$ is deterministic. Furthermore we define the set Void as the least set which includes variables and which is closed under evaluation contexts:

$$\frac{x \in \mathcal{V}}{x \in \mathsf{Void}} \qquad \frac{t \in \mathsf{Void} \qquad E[x] \in \mathsf{SN}}{E[t] \in \mathsf{Void}}$$

We write Void^σ for $\mathsf{Void} \cap \mathsf{Tm}^\sigma$. We verify the syntactic properties which are needed in the proof and which motivate the definition of $\rhd_{\mathsf{whd}}$:

Lemma 1.

1. $$\frac{t \rhd_{\mathsf{whd}} u \qquad t \rhd t'}{u \equiv t' \lor \exists u'.t' \rhd_{\mathsf{whd}} u' \land u \rhd^* u'}$$
2. $$\frac{t \in \mathsf{Void} \qquad E[x] \in \mathsf{SN}}{E[t] \in \mathsf{SN}}$$
3. $$\frac{t \rhd_{\mathsf{whd}} t' \qquad E[t'] \in \mathsf{SN}}{E[t] \in \mathsf{SN}}$$
4. $$\frac{E[t] \rhd_{\mathsf{whd}} t' \qquad t, t', E[x] \in \mathsf{SN}}{E[t] \in \mathsf{SN}}$$

We omit the proof here. Note that the first property is a weak form of standardisation, expressing that weak head reduction can only be postponed but not avoided. This property is needed to show some of the other properties, which in general can be verified by rule induction over the definition of SN. A simple corollary of 2. is that $\mathsf{Void} \subseteq \mathsf{SN}$.

Given a set of strongly normalizing terms $P \subseteq \mathsf{SN}^\sigma$ we define its saturation $P^* \subseteq \mathsf{SN}^\sigma$ as the least set closed under

$$\frac{t \in P}{t \in P^*}\,(\mathrm{emb}) \qquad \frac{t \in \mathsf{Void}^\sigma}{t \in P^*}\,(\mathrm{sat1}) \qquad \frac{t \in \mathsf{SN}^\sigma \quad t \rhd_{\mathsf{whd}} t' \quad t' \in P^*}{t \in P^*}\,(\mathrm{sat2})$$

We say that a set $P \subseteq \mathsf{SN}^\sigma$ is saturated iff $P^* \subseteq P$ and write $P \in \mathsf{SAT}^\sigma$. Obviously, $P^* \in \mathsf{SAT}^\sigma$.

---

[5] Note that the type Nat can be represented as $\mu X.1 + X$, then define $0 = \mathsf{c}^{X.1+X}(\mathsf{in}_1\ \mathsf{unit}) : \mathsf{Nat}$, $\mathrm{S} = \lambda x^{\mathsf{Nat}}.\mathsf{c}^{X.1+X}(\mathsf{in}_2\ x) : \mathsf{Nat} \to \mathsf{Nat}$

4 A Predicative Interpretation of Types

Following Tait, the interpretations $[\![\sigma]\!]$ of all closed types $\sigma \in \mathsf{Ty}$ will be saturated sets. But how about the types with free type variables? We use Girard's approach, who extended Tait's method to System F [Gir72]: Open types are *operators* on saturated sets (Girard actually used his *candidate sets*, which are more restrictive than saturated sets). Transferred to our notation and terminology, he defined the semantics of second-order quantified types as

$$[\![\Pi Y.\sigma(\boldsymbol{X})]\!](\boldsymbol{P}) := \bigcap_{Q \in \mathsf{SAT}} [\![\sigma(\boldsymbol{X}, Y)]\!](\boldsymbol{P}, Q)$$

making splendid use of impredicativity: He quantifies over all saturated sets while defining one. Since we do not quantify over types but use open types only to define recursive types, we can give the interpretation by inductive definitions (i.e., predicatively). Technically, this requires the "urelement" relation $\mathcal{U}$ to be defined simultaneously with the interpretations. Given $\sigma \in \mathsf{Ty}(\boldsymbol{X})$ and closed types $\tau_i \in \mathsf{Ty}$ for $1 \le i \le n = |\boldsymbol{X}|$, we will define

$$\begin{array}{rl} [\![\sigma]\!](\boldsymbol{P}) \subseteq \mathsf{SN}^{\sigma(\tau)} & P_i \subseteq \mathsf{SN}^{\tau_i} \text{ for } 1 \le i \le n \\ \mathcal{U}_i^\sigma \subseteq \mathsf{Tm}^{\tau_i} \times \mathsf{Tm}^{\sigma(\boldsymbol{\tau})} & 1 \le i \le n \end{array}$$

such that the following properties hold:

Saturated If all $P_i \in \mathsf{SAT}^{\tau_i}$ then $[\![\sigma]\!](\boldsymbol{P}) \in \mathsf{SAT}^{\sigma(\boldsymbol{\tau})}$
Monotone $[\![\sigma]\!]$ is monotone in all arguments, i.e.,

$$\frac{\forall 1 \le i \le n.\ P_i \subseteq Q_i}{[\![\sigma]\!](\boldsymbol{P}) \subseteq [\![\sigma]\!](\boldsymbol{Q})}\,(\mathrm{mon})$$

Set based $[\![\sigma]\!]$ is set based by $\mathcal{U}^\sigma$. For all $1 \le i \le n$, $t \in \mathsf{SN}^{\sigma(\boldsymbol{\tau})}$ and $u \in \mathsf{SN}^{\tau_i}$ the interpretation $[\![\sigma]\!]$ satisfies

$$\frac{t \in [\![\sigma]\!](\boldsymbol{P}) \qquad u\,\mathcal{U}_i^\sigma\, t}{u \in P_i}\,(\mathrm{sb1}) \qquad \frac{t \in [\![\sigma]\!](\mathsf{SN}^{\boldsymbol{\tau}})}{t \in [\![\sigma]\!](\boldsymbol{\mathcal{U}}^\sigma(t))}\,(\mathrm{sb2})$$

Note that (sb1) can be read as $t \in [\![\sigma]\!](\boldsymbol{P}) \implies \mathcal{U}_i^\sigma(t) \subseteq P_i$. Informally, this states that the ith component urelements of t must be in the original set of urelements P_i. Likewise, (sb2) states that t must be reconstructible out of the urelements extracted from t.

We require the operators to be *set based* for the following reason: The interpretation $M := [\![\mu X.\sigma]\!](\boldsymbol{P})$ of an inductive type is defined by

$$\frac{t \in [\![\sigma]\!](\boldsymbol{P}, M)}{\mathsf{c}\,t \in M}\,(\mathrm{cons}')$$

However, this cannot be a rule of an inductive definition since M, which we want to define, does not appear strictly positive in the premise. Although X appears strictly positive in the type σ, M cannot be said to appear strictly positive, since it is argument of $[\![\sigma]\!]$, not of σ, and we do not know "what the operator is doing with M". Monotonicity is not strong enough for our purposes, and this is where set-basedness comes in:

Proposition 1. *Every $[\![\sigma]\!](\boldsymbol{P})$ is equivalent to a predicate which is strictly positive in $\boldsymbol{P}$ - that is for $t \in \mathsf{SN}^{\sigma(\boldsymbol{\tau})}$:*

$$t \in [\![\sigma]\!](\boldsymbol{P}) \quad \Longleftrightarrow \quad t \in [\![\sigma]\!](\mathsf{SN}^{\boldsymbol{\tau}}) \;\wedge\; \forall i.\, \mathcal{U}_i^{\sigma}(t) \subseteq P_i$$

Proof.

- $\Rightarrow$ Assuming $t \in [\![\sigma]\!](\boldsymbol{P})$, we obtain $t \in [\![\sigma]\!](\mathsf{SN}^{\boldsymbol{\tau}})$ by (mon) and $\mathcal{U}_i^{\sigma}(t) \subseteq P_i$ for all i by (sb1).
- $\Leftarrow$ Using (sb2), $t \in [\![\sigma]\!](\mathsf{SN}^{\boldsymbol{\tau}})$ entails

$$t \in [\![\sigma]\!](\boldsymbol{\mathcal{U}}^{\sigma}(t))$$

Since by assumption $\boldsymbol{\mathcal{U}}^{\sigma}(t) \subseteq \boldsymbol{P}$ (component wise), we can derive $t \in [\![\sigma]\!](\boldsymbol{P})$ by (mon). □

In the following we give definitions for $[\![\sigma]\!]$ and $\mathcal{U}^{\sigma}$.

(Const),(Var),(Arr) Let $\sigma \in \mathsf{Ty}$ and $X_i, \tau \in \mathsf{Ty}(\boldsymbol{X})$

$$[\![0]\!](\boldsymbol{P}) = \{\}^* \qquad u\,\mathcal{U}_i^0\; t \iff \text{False}$$

$$[\![1]\!](\boldsymbol{P}) = \{\mathsf{unit}\}^* \qquad u\,\mathcal{U}_i^1\; t \iff \text{False}$$

$$[\![X_i]\!](\boldsymbol{P}) = P_i \qquad u\,\mathcal{U}_j^{X_i}\; t \iff i = j \wedge u \equiv t$$

$$[\![\sigma \to \tau]\!](\boldsymbol{P}) = [\![\sigma]\!] \Rightarrow ([\![\tau]\!](\boldsymbol{P})) \qquad u\,\mathcal{U}_i^{\sigma\to\tau}\; t \iff \exists t' \in [\![\sigma]\!].\; u\,\mathcal{U}_i^{\tau}\; t\,t'$$

The following lemma is standard, e.g. see [Alt93] for a proof:

Lemma 2. *Given $P \subseteq \mathsf{SN}^{\sigma}$ and $Q \in \mathsf{SAT}^{\tau}$ we have that $P \Rightarrow Q \in \mathsf{SAT}^{\sigma\to\tau}$.*

Proposition 2. *The interpretations $[\![0]\!], [\![1]\!], [\![X_i]\!], [\![\sigma \to \tau]\!]$ are saturated, monotone and set based.*

Proof. We verify here the (only interesting) case that $[\![\sigma \to \tau]\!]$ is set based:

- **(sb1)** Given $t \in [\![\sigma \to \tau]\!](\boldsymbol{P})$ and $u\,\mathcal{U}_i^{\sigma\to\tau}\; t$ we know that there is a $t' \in [\![\sigma]\!]$ s.t. $u\,\mathcal{U}_i^{\sigma\to\tau}\; tt'$. Since $tt' \in [\![\tau]\!](\boldsymbol{P})$ we can use (sb1) for τ to conclude $u \in P_i$.
- **(sb2)** Given $t \in [\![\sigma \to \tau]\!](\mathbf{SN}^{\boldsymbol{\tau}})$ we have to show that $t \in [\![\sigma \to \tau]\!](\boldsymbol{\mathcal{U}}^{\sigma\to\tau}(t))$: Assume $u \in [\![\sigma]\!]$ we can use the hypothesis to show that $tu \in \mathsf{SN}$ and hence by (sb2) for τ $tu \in [\![\tau]\!](\boldsymbol{\mathcal{U}}^{\tau}(tu))$. Clearly $\mathcal{U}_i^{\tau}(tu) \subseteq \mathcal{U}_i^{\sigma\to\tau} t$ and hence using mon of $[\![\tau]\!]$ we have $tu \in [\![\tau]\!](\boldsymbol{\mathcal{U}}^{\sigma\to\tau}(t))$ as required. □

(Prod) Given $\sigma_1, \sigma_2 \in \mathsf{Ty}(\boldsymbol{X})$ we define

$$[\![\sigma_1 \times \sigma_2]\!](\boldsymbol{P}) = \{\mathsf{pair}\, t_1 t_2 \mid \forall j \in \{1,2\}.\, t_j \in [\![\sigma_j]\!](\boldsymbol{P})\}^* \tag{1}$$

We define $\mathcal{U}_i^{\sigma_1\times\sigma_2}$ inductively by the following rules

$$\frac{j \in \{1,2\} \qquad u\, \mathcal{U}_i^{\sigma_j}\, t_j}{u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, \mathsf{pair}\, t_1 t_2}\,(\text{pair}) \qquad \frac{t \in \mathsf{SN} \quad t \rhd_{\mathsf{whd}} t' \quad u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, t'}{u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, t}\,(\text{clos}^{\times})$$

Proposition 3. *The interpretation* $[\![\sigma_1 \times \sigma_2]\!]$ *of the product is monotone and set based.*

Proof. Since (mon) is obvious in this and all subsequent cases we concentrate on set based:

(sb1) Given $t \in [\![\sigma_1 \times \sigma_2]\!](\boldsymbol{P})$ to show

$$u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, t \implies u \in P_i$$

we exploit that the closure (1) is defined inductively and analyze the cases:

(emb) $t \equiv \mathsf{pair}\ t_1\, t_2$ where $t_j \in [\![\sigma_j]\!](\boldsymbol{P})$. Hence $u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, t$ can only have been derived from $u\, \mathcal{U}_i^{\sigma_j}\, t_j$. Then (sb1) for σ_j implies $u \in P_i$.

(sat1) For $t \in \mathsf{Void}$ the precondition $u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, t$ is never derivable.

(sat2) We have $t \in \mathsf{SN}$ and $t \rhd_{\mathsf{whd}} t'$ and assume $u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, t$ to show $u \in P_i$. Since t has a weak head reduct, it cannot be of the form $\mathsf{pair}\, t_1 t_2$. Thus $u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, t$ can only have been derived by (clos$^\times$) and since $\rhd_{\mathsf{whd}}$ is deterministic we have $u\, \mathcal{U}_i^{\sigma_1\times\sigma_2}\, t'$. Now, the ind.hyp. for t' entails $u \in P_i$.

(sb2) Given $t \in [\![\sigma_1 \times \sigma_2]\!](\mathsf{SN})$ we show

$$t \in [\![\sigma_1 \times \sigma_2]\!](\boldsymbol{\mathcal{U}}^{\sigma_1\times\sigma_2}(t))$$

by induction over the closure rules:

(emb) $t \equiv \mathsf{pair}\ t_1\, t_2$ where $t_j \in [\![\sigma_j]\!](\mathsf{SN})$. We apply the ind.hyp. to derive $t_j \in [\![\sigma_j]\!](\boldsymbol{\mathcal{U}}^{\sigma_j}(t_j))$. Since $\mathcal{U}_i^{\sigma_j}(t_j) \subseteq \mathcal{U}_i^{\sigma_1\times\sigma_2}(\mathsf{pair}\ t_1\, t_2)$ by (pair) we use (mon) to derive $t_j \in [\![\sigma_j]\!](\boldsymbol{\mathcal{U}}^{\sigma_1\times\sigma_2}(\mathsf{pair}\, t_1 t_2))$ and hence $t \in [\![\sigma_1 \times \sigma_2]\!](\boldsymbol{\mathcal{U}}^{\sigma_1\times\sigma_2}(t))$.

(sat1) Since $[\![\sigma_1 \times \sigma_2]\!]$ is defined as a closure it contains all $t \in \mathsf{Void}$.

(sat2) We have $t \in \mathsf{SN}$, $t \rhd_{\mathsf{whd}} t'$, and the ind.hyp. $t' \in [\![\sigma_1 \times \sigma_2]\!](\boldsymbol{\mathcal{U}}^{\sigma_1\times\sigma_2}(t'))$. (clos$^\times$) implies that $\boldsymbol{\mathcal{U}}^{\sigma_1\times\sigma_2}(t') \subseteq \boldsymbol{\mathcal{U}}^{\sigma_1\times\sigma_2}(t)$ and hence using (mon) we know $t' \in [\![\sigma_1 \times \sigma_2]\!](\boldsymbol{\mathcal{U}}^{\sigma_1\times\sigma_2}(t))$. We use the premises again and apply (sat2) for $[\![\sigma_1 \times \sigma_2]\!]$ to derive $t \in [\![\sigma_1 \times \sigma_2]\!](\boldsymbol{\mathcal{U}}^{\sigma_1\times\sigma_2}(t))$

$\square$

Since we have not used $\times$-specific properties in the case that the last step was (clos$^\times$) we can transfer these parts of the proof to sum and inductive types.

(Sum) Given $\sigma_1, \sigma_2 \in \mathsf{Ty}(\boldsymbol{X})$ we define

$$[\![\sigma_1 + \sigma_2]\!](\boldsymbol{P}) = \{\mathsf{in}_j\, t \mid j \in \{1,2\} \wedge t \in [\![\sigma_j]\!](\boldsymbol{P})\}^*$$

We define $\mathcal{U}_i^{\sigma_1+\sigma_2}$ inductively by the following rules ($j \in \{1,2\}$)

$$\frac{u\,\mathcal{U}_i^{\sigma_j}\ t}{u\,\mathcal{U}_i^{\sigma_1+\sigma_2}\ \mathsf{in}_j\, t}\,(\mathrm{in}_j) \qquad \frac{t \in \mathsf{SN} \quad t \rhd_{\mathsf{whd}} t' \quad u\,\mathcal{U}_i^{\sigma_1+\sigma_2}\ t'}{u\,\mathcal{U}_i^{\sigma_1+\sigma_2}\ t}\,(\mathrm{clos}^+)$$

Proposition 4. *The interpretation* $[\![\sigma_1 + \sigma_2]\!]$ *of the disjoint union is monotone and set based.*

Proof.

(sb1) By induction on $t \in [\![\sigma_1 + \sigma_2]\!](\boldsymbol{P})$:
- **(emb)** $t \equiv \mathsf{in}_j\, s$ and $s \in [\![\sigma_j]\!](\boldsymbol{P})$. Since $u\,\mathcal{U}_i^{\sigma_1+\sigma_2}\ t$ must have been derived from $u\,\mathcal{U}_i^{\sigma_j}\ s$, we may apply the ind.hyp. to conclude $u \in P_i$.
- **(sat1),(sat2)** As before for $\times$.

(sb2) By induction on $t \in [\![\sigma_1 + \sigma_2]\!](\mathsf{SN})$:
- **(emb)** $t \equiv \mathsf{in}_j\, s$ and $s \in [\![\sigma_j]\!](\mathsf{SN})$. By ind.hyp. we have $s \in [\![\sigma_j]\!](\boldsymbol{\mathcal{U}}^{\sigma_j}(s))$. Since $\mathcal{U}_i^{\sigma_j}(s) \subseteq \mathcal{U}_i^{\sigma_1+\sigma_2}(\mathsf{in}_j\, s)$ we can show $s \in [\![\sigma_j]\!](\boldsymbol{\mathcal{U}}^{\sigma_1+\sigma_2}(\mathsf{in}_j\, s))$ using (mon) and hence $t \in [\![\sigma_1 + \sigma_2]\!](\boldsymbol{\mathcal{U}}^{\sigma_1+\sigma_2}(t))$.
- **(sat1),(sat2)** As before for $\times$. □

(Mu) Given $\sigma \in \mathsf{Ty}(\boldsymbol{X}, X)$ where $n = |\boldsymbol{X}|$ we define $[\![\mu X.\sigma]\!](\boldsymbol{P})$ inductively by (sat1), (sat2) and:

$$\frac{t \in [\![\sigma]\!](\boldsymbol{P}, \mathsf{SN}^{\mu X.\sigma}) \quad \forall u.\ u\,\mathcal{U}_{n+1}^{\sigma}\ t \implies u \in [\![\mu X.\sigma]\!](\boldsymbol{P})}{\mathsf{c}\, t \in [\![\mu X.\sigma]\!](\boldsymbol{P})}\,(\mathrm{cons})$$

We could not have used the saturation operator * here instead of (sat1) and (sat2), since saturation and (cons) may have to be interleaved.

Note that $[\![\mu X.\sigma]\!]$ appears only strictly positively in the premises! By Prop. 1 (cons) is equivalent to the rule (cons') given on page 9. We could not have used cons' for the definition because $[\![\mu X.\sigma]\!]$ appears non-positively as an argument to $[\![\sigma]\!]$.

We also define $\mathcal{U}_i^{\mu X.\sigma}$ inductively:

$$\frac{1 \le i \le n \quad u\,\mathcal{U}_i^{\sigma}\ t}{u\,\mathcal{U}_i^{\mu X.\sigma}\ \mathsf{c}\, t}\,(\text{non-rec}) \qquad \frac{u\,\mathcal{U}_i^{\mu X.\sigma}\ t' \quad t'\,\mathcal{U}_{n+1}^{\sigma}\ t}{u\,\mathcal{U}_i^{\mu X.\sigma}\ \mathsf{c}\, t}\,(\text{rec})$$

$$\frac{t \in \mathsf{SN} \quad t \rhd_{\mathsf{whd}} t' \quad u\,\mathcal{U}_i^{\mu X.\sigma}\ t'}{u\,\mathcal{U}_i^{\mu X.\sigma}\ t}\,(\mathrm{clos}^{\mu})$$

Proposition 5. *The interpretation* $[\![\mu X.\sigma]\!]$ *of inductive types is monotone and set based.*

Proof. We omit (mon) since this follows from the fact that least fixpoints preserve monotonicity:

(sb1) We define a family of relations $\boldsymbol{R}$ by

$$u \; R_i \; t \iff (t \in [\![\mu X.\sigma]\!](\boldsymbol{P}) \implies u \in P_i)$$

and show that R_i is closed under the rules defining $\mathcal{U}_i^{\mu X.\sigma}$

(non-rec) Given $u \; \mathcal{U}_i^{\sigma} \; t$ and $\mathsf{c}\, t \in [\![\mu X.\sigma]\!](\boldsymbol{P})$ we show $u \in P_i$. Since from the second assumption we can infer $t \in [\![\sigma]\!](\boldsymbol{P}, [\![\mu X.\sigma]\!](\boldsymbol{P}))$, our goal follows by (sb1) for σ, using the first assumption.

(rec) As before we have $t \in [\![\sigma]\!](\boldsymbol{P}, [\![\mu X.\sigma]\!](\boldsymbol{P}))$. Hence, using (sb1) for σ, the premise $t' \; \mathcal{U}_{n+1}^{\sigma} \; t$ implies $t' \in [\![\mu X.\sigma]\!](\boldsymbol{P})$. Now we use the ind.hyp. $u \; R_i \; t'$ to conclude $u \in P_i$.

(clos$^\mu$) Assuming $t \in \mathsf{SN}$ and $t \rhd_{\mathsf{whd}} t'$ we exploit (sat2) for $[\![\mu X.\sigma]\!](\boldsymbol{P})$.

(sb2) We show that the set

$$Q = \{t \mid t \in [\![\mu X.\sigma]\!](\boldsymbol{\mathcal{U}}^{\mu X.\sigma}(t))\}$$

is closed under the rules defining $[\![\mu X.\sigma]\!](\mathsf{SN}^{\boldsymbol{\tau}})$.

(cons) We assume

$$t \in [\![\sigma]\!](\mathsf{SN}^{\boldsymbol{\tau}}, Q) \tag{2}$$

which by using (sb2) for σ (and $Q \subseteq \mathsf{SN}$) entails

$$t \in [\![\sigma]\!](\boldsymbol{\mathcal{U}}^{\sigma}(t)) \tag{3}$$

Using (cons'), to show that $\mathsf{c}\, t \in Q$ it suffices to show

$$t \in [\![\sigma]\!](\boldsymbol{\mathcal{U}}^{\mu X.\sigma}(\mathsf{c}\, t), [\![\mu X.\sigma]\!](\boldsymbol{\mathcal{U}}^{\mu X.\sigma}(\mathsf{c}\, t)))$$

We derive this from 3 using (mon), which leaves us two subgoals

1. For $1 \leq i \leq n$ prove that $\mathcal{U}_i^{\sigma}(t) \subseteq \mathcal{U}_i^{\mu X.\sigma}(\mathsf{c}\, t)$, which is an immediate consequence from (non-rec).
2. To show $\mathcal{U}_{n+1}^{\sigma}(t) \subseteq [\![\mu X.\sigma]\!](\boldsymbol{\mathcal{U}}^{\mu X.\sigma}(\mathsf{c}\, t))$ assume

$$t' \; \mathcal{U}_{n+1}^{\sigma} \; t \tag{4}$$

Under this assumption we have that $\mathcal{U}_i^{\mu X.\sigma}(t') \subseteq \mathcal{U}_i^{\mu X.\sigma}(\mathsf{c}\, t)$ by (rec). Using (sb1) for σ on 2 and 4 we have that $t' \in Q$, i.e.,

$$t' \in [\![\mu X.\sigma]\!](\boldsymbol{\mathcal{U}}^{\mu X.\sigma}(t'))$$

and hence using (mon) $t' \in [\![\mu X.\sigma]\!](\boldsymbol{\mathcal{U}}^{\mu X.\sigma}(\mathsf{c}\, t))$.

(sat1),(sat2) As for $\times$. □

Having defined the interpretation for all types we show that the interpretation is compatible with substitution:

Proposition 6. *Given* $\tau \in \mathsf{Ty}(\boldsymbol{X})$ *and* $\sigma_i \in \mathsf{Ty}$ *for* $1 \leq i \leq |\boldsymbol{X}|$ *we have*

$$[\![\tau]\!]([\![\boldsymbol{\sigma}]\!]) = [\![\tau(\boldsymbol{\sigma})]\!]$$

Proof. Straightforward induction on $\tau \in \mathsf{Ty}(\boldsymbol{X})$. □

5 Strong Normalisation

We have to show that all constructions are sound wrt. our semantics. The verification for simple types is standard (see [Alt93]) and summarized by the following proposition:

Proposition 7. *Given* $\sigma, \tau \in \mathsf{Ty}$ *the following implications hold*

$$\frac{t \in [\![\sigma \to \tau]\!] \qquad u \in [\![\sigma]\!]}{t u \in [\![\tau]\!]}\ \textit{(sem-app)} \qquad \frac{\forall u \in [\![\sigma]\!]. t[x := u] \in [\![\tau]\!]}{\lambda x.t \in [\![\sigma \to \tau]\!]}\ \textit{(sem-lam)}$$

The difficult case is (sem-lam), since $\Rightarrow$ is defined *elimination based*. In contrast, the semantics for all other type constructors introduced so far is *constructor based*, hence the soundness of constructors is trivial:

Proposition 8.

$$\begin{aligned} \mathsf{unit} &\in [\![1]\!] \\ \mathsf{pair}^{\sigma_1,\sigma_2} &\in [\![\sigma_1 \to \sigma_2 \to (\sigma_1 \times \sigma_2)]\!] \\ \mathsf{in}_i^{\sigma_1,\sigma_2} &\in [\![\sigma_i \to (\sigma_1 + \sigma_2)]\!] \qquad\qquad i \in \{1,2\} \\ \mathsf{c}^{X.\tau} &\in [\![\tau(\mu X.\tau) \to \mu X.\tau]\!] \end{aligned}$$

To show the soundness of eliminators we have to exploit the saturatedness. We postpone the case for It since its soundness has to be shown mutually with the soundness of strength.

Proposition 9.

$$\begin{aligned} \pi_i^{\sigma_1,\sigma_2} &\in [\![(\sigma_1 \times \sigma_2) \to \sigma_i]\!] \qquad\qquad i \in \{1,2\} \\ \mathsf{case}_0^{\sigma} &\in [\![0 \to \sigma]\!] \\ \mathsf{case}^{\sigma_1,\sigma_2,\rho} &\in [\![(\sigma_1 \to \rho) \to (\sigma_2 \to \rho) \to (\sigma_1 + \sigma_2) \to \rho]\!] \end{aligned}$$

Proof. We show soundness for the binary case to illustrate the idea: Given $t_i \in [\![\sigma_i \to \rho]\!]$ and

$$u \in [\![\sigma_1 + \sigma_2]\!] \tag{5}$$

we prove $t \equiv \mathsf{case}\ t_1 t_2 u \in [\![\rho]\!]$ by induction over the rules used to derive (5):

(sat1) If $u \in \mathsf{Void}$ then $\mathsf{case}\ t_1 t_2 u \in \mathsf{Void} \subseteq [\![\rho]\!]$, using (sat1) for ρ.

(sat2) Given $u \in \mathsf{SN}$, $u \rhd_{\mathsf{whd}} u'$ with $u' \in [\![\sigma_1 + \sigma_2]\!]$. Now by ind.hyp. we have that $\mathsf{case}\ t_1 t_2 u' \in [\![\rho]\!]$ and we observe that $t \rhd_{\mathsf{whd}} \mathsf{case}\ t_1 t_2 u'$. Using Lemma 1 we can show $t \in \mathsf{SN}$ and hence by (sat2) $t \in [\![\rho]\!]$.

(emb) $u \equiv \mathsf{in}_i\, u'$ with $u' \in [\![\sigma_i]\!]$. Using Lemma 1 we derive that $t \in \mathsf{SN}$. We have $t \rhd_{\mathsf{whd}} t_i u'$ and from the premises we know $t_i u' \in [\![\rho]\!]$. Hence by (sat2) $t \in [\![\rho]\!]$. □

We are now ready to establish the soundness of It and strength:

Proposition 10. *Given $\rho \in \mathsf{Ty}(\boldsymbol{X})$, let $n = |\boldsymbol{X}|$:*

1. *Assume $\sigma_i, \tau_i \in \mathsf{Ty}$, $P_i \in \mathsf{SAT}^{\sigma_i}$, $Q_i \in \mathsf{SAT}^{\tau_i}$ and $f_i \in P_i \Rightarrow Q_i$ for $1 \leq i \leq n$, we have that*
$$\rho(\boldsymbol{f}) \in [\![\rho]\!](\boldsymbol{P}) \Rightarrow [\![\rho]\!](\boldsymbol{Q})$$
2. *If $n > 1$ assume $\tau_i \in \mathsf{Ty}$ and $P_i \in \mathsf{SAT}^{\tau_i}$ for $1 \leq i < n$. Let $\sigma \in \mathsf{Ty}$ and $Q \in \mathsf{SAT}^{\sigma}$, it holds that*
$$\mathsf{It}^{X.\rho(\boldsymbol{\tau},X),\sigma} \in ([\![\rho]\!](\boldsymbol{P}, Q) \Rightarrow Q) \Rightarrow [\![\mu X.\rho]\!](\boldsymbol{P}) \Rightarrow Q$$

Proof. We show both properties by mutual induction on $\rho \in \mathsf{Ty}(\boldsymbol{X})$:

1. For all cases but (Mu) the property follows from the ind.hyp. 1. and Prop. 7, 8 and 9. For (Mu) we also have to use the 2nd part of the ind.hyp.
2. Assume $f \in [\![\rho]\!](\boldsymbol{P}, Q) \Rightarrow Q$ we define
$$S = \{t \mid \mathsf{It}\, f t \in Q\}$$
Note that $\mathsf{It}\, f \in S \Rightarrow Q$ by definition. We show that S is closed under the rules defining $[\![\mu X.\rho]\!]$:
(sat1) If $t \in \mathsf{Void}$ then $\mathsf{It}\, f t \in \mathsf{Void} \subseteq Q$ using (sat1) for Q.
(sat2) We have $t \in \mathsf{SN}$, $t \rhd_{\mathsf{whd}} t'$ and $t' \in S$, i.e., $\mathsf{It}\, f t' \in Q$. From these assumptions we infer $\mathsf{It}\, f t \rhd_{\mathsf{whd}} \mathsf{It}\, f t'$. Using Lemma 1 we can show $\mathsf{It}\, f t \in \mathsf{SN}$ and hence, exploiting the saturatedness of Q, by (sat2) $\mathsf{It}\, f t \in Q$, that is $t \in S$. As a byproduct we have shown $S \in \mathsf{SAT}$.
(cons) For this rule from the assumption $t \in [\![\rho]\!](\boldsymbol{P}, S)$ we have to show $\mathsf{c}\, t \in S$, or, by definition of S, $\mathsf{It}\, f(\mathsf{c}\, t) \in Q$. Using the first part of the ind.hyp. and the saturatedness of S shown above, we establish[6]
$$\rho(\boldsymbol{\tau}, \mathsf{It}\, f) \in [\![\rho]\!](\boldsymbol{P}, S) \Rightarrow [\![\rho]\!](\boldsymbol{P}, Q)$$
Now using our assumptions we can further establish
$$f(\rho(\mathsf{It}\, f)\, t) \in Q$$
We observe that $\mathsf{It}\, f(\mathsf{c}\, t) \rhd_{\mathsf{whd}} f(\rho(\mathsf{It}\, f)\, t)$ and using Lemma 1 we can show $\mathsf{It}\, f(\mathsf{c}\, t) \in \mathsf{SN}$. Hence by (sat2) $\mathsf{It}\, f(\mathsf{c}\, t) \in Q$.
By minimality of $[\![\mu X.\rho]\!]$ we have that $[\![\mu X.\rho]\!](\boldsymbol{P}) \subseteq S$ and hence
$$\mathsf{It}\, f \in [\![\mu X.\rho]\!](\boldsymbol{P}) \Rightarrow Q$$

□

Proposition 11 (Soundness). *Given $\Gamma = x_1 : \sigma_1, \ldots, x_n : \sigma_n$ and $u_i \in [\![\sigma_i]\!]$ for $1 \leq i \leq n$ it follows that*
$$\Gamma \vdash t : \tau \implies t[\boldsymbol{x} := \boldsymbol{u}] \in [\![\tau]\!]$$

Proof. By induction over the derivation of $\Gamma \vdash t : \tau$ using Prop. 7–10. □

Theorem 1 is now a simple corollary:

Proof. Given $\Gamma \vdash t : \tau$ by (sat1) we know $x_i \in [\![\sigma_n]\!]$ and hence by Prop. 11 $t[\boldsymbol{x} = \boldsymbol{x}] \in [\![\tau]\!] \subseteq \mathsf{SN}^{\tau}$. □

[6] $\rho(\mathsf{It}\, f)$ is an abbreviation of $\rho(\boldsymbol{\lambda x^{\tau}.x}, \mathsf{It}\, f)$, cf. the definition of strength in Sect. 2.

6 Coinductive Types

We shall sketch in this section how to extend our construction to coinductive types, i.e., introduce a type constructor ν to introduce terminal coalgebras. We will use greatest fixpoints of strictly positive operators.

6.1 Extending the Calculus

The calculus $\lambda^{\mu\nu}$ is given by the following extensions of λ^{μ}:

Type constructor: $$\frac{\rho \in \mathsf{Ty}(\boldsymbol{X}, Y)}{\nu Y.\rho \in \mathsf{Ty}(\boldsymbol{X})}\,(\mathrm{Nu})$$

Constants: $$\mathsf{d}^{X.\rho} : (\nu X.\rho) \to \rho(\nu X.\rho)$$
$$\mathsf{Co}^{X.\rho,\sigma} : (\sigma \to \rho(\sigma)) \to \sigma \to \nu X.\rho$$

Strength: $(\nu X.\rho)(\boldsymbol{f}) = \mathsf{Co}^{X.\rho(\boldsymbol{\tau},X),\nu\alpha}(\lambda x^{\nu\alpha}.\,\rho(\boldsymbol{f}, \lambda y^{\nu\alpha}.y)(d^{\alpha}\,x))$
where α stands for $X.\rho(\boldsymbol{\sigma}, X)$

β axiom: $\mathsf{d}(\mathsf{Co}^{X.\rho,\sigma}\,ft) \rhd \rho(\mathsf{Co}\,f)(ft)$

Evaluation context: $E[X] ::= \cdots \mid \mathsf{d}X$

We interpret $\rhd_{\mathsf{whd}}$ and Void wrt. to the extended definition of $E[X]$. We note that Lemma 1 remains true under this extension and we now understand Theorem 1 wrt. the extended calculus.

6.2 Extending the Interpretation

Given $\rho \in \mathsf{Ty}(\boldsymbol{X}, X)$ where $n = |\boldsymbol{X}|$ we define $[\![\nu X.\rho]\!](\boldsymbol{P})$ (predicatively) as the greatest fixpoint of the following rules:

$$\frac{t \in [\![\nu X.\rho]\!](\boldsymbol{P})}{\mathsf{d}t \in [\![\rho]\!](\boldsymbol{P}, \mathsf{SN}^{\nu X.\rho})}\,(\mathrm{destr1}) \qquad \frac{t \in [\![\nu X.\rho]\!](\boldsymbol{P}) \qquad u\,\mathcal{U}^{\rho}_{n+1}\,\mathsf{d}t}{u \in [\![\nu X.\rho]\!](\boldsymbol{P})}\,(\mathrm{destr2})$$

Note that, dually to the inductive case, the rules are supposed to match the (co-ind) scheme, i.e., we define the greatest fixpoint of the operator

$$\Phi(Q) = \{t \mid \mathsf{d}t \in [\![\rho]\!](\boldsymbol{P}, \mathsf{SN}^{\nu X.\rho}) \wedge \forall u.(u\,\mathcal{U}^{\rho}_{n+1}\,\mathsf{d}t) \to u \in Q\}$$

Using Prop. 1 we can show that (destr1) and (destr2) are equivalent to

$$\frac{t \in [\![\nu X.\rho]\!](\boldsymbol{P})}{\mathsf{d}t \in [\![\rho]\!](\boldsymbol{P}, [\![\nu X.\rho]\!](\boldsymbol{P}))}\,(\mathrm{destr}')$$

We define $\mathcal{U}^{\nu X.\rho}_i$ **inductively (!)**, i.e., as a least not a greatest fixpoint:

$$\frac{1 \le i \le n \quad u\,\mathcal{U}^{\rho}_i\,\mathsf{d}t}{u\,\mathcal{U}^{\mu X.\rho}_i\,t}\,(\text{non-rec}) \qquad \frac{u\,\mathcal{U}^{\nu X.\rho}_i\,t' \quad t'\,\mathcal{U}^{\rho}_{n+1}\,\mathsf{d}t}{u\,\mathcal{U}^{\nu X.\rho}_i\,t}(\mathrm{rec})$$

Note that different to the μ types we have not explicitely closed the interpretation under (sat1) and (sat2). However, we can show:

Proposition 12. *The interpretation $[\![\nu X.\rho]\!]$ of coinductive types is saturated.*

Proof. We show that

$$[\![\nu X.\rho]\!](\boldsymbol{P})^* \subseteq [\![\nu X.\rho]\!](\boldsymbol{P})$$

by verifying that $[\![\nu X.\rho]\!](\boldsymbol{P})^*$ is closed under (destr') (and hence equivalently under (destr1) and (destr2)) by induction over $t \in [\![\nu X.\rho]\!](\boldsymbol{P})^*$:

(sat1) If $t \in \mathsf{Void}$ then $\mathsf{d}t \in \mathsf{Void} \subseteq [\![\rho]\!](\boldsymbol{P}, [\![\nu X.\rho]\!](\boldsymbol{P})^*)$ by (sat1) for ρ.
(sat2) Given $t \in \mathsf{SN}, t \rhd_{\mathsf{whd}} t'$, by ind.hyp we assume that

$$\mathsf{d}t' \in [\![\rho]\!](\boldsymbol{P}, [\![\nu X.\rho]\!](\boldsymbol{P})^*).$$

Since $\mathsf{d}t \in \mathsf{SN}$ by Lemma 1 and $\mathsf{d}t \rhd_{\mathsf{whd}} \mathsf{d}t'$ we can use (sat2) for ρ.
(emb) Given $t \in [\![\nu X.\rho]\!](\boldsymbol{P})$ we know that

$$\begin{aligned}\mathsf{d}t \in& [\![\rho]\!](\boldsymbol{P}, [\![\nu X.\rho]\!](\boldsymbol{P}))\\ \subseteq& [\![\rho]\!](\boldsymbol{P}, [\![\nu X.\rho]\!](\boldsymbol{P})^*)\end{aligned}$$

using (mon) and $[\![\nu X.\rho]\!](\boldsymbol{P}) \subseteq [\![\nu X.\rho]\!](\boldsymbol{P})^*$

To show (sb2) we need an auxiliary relation $\leq\, \subseteq \mathsf{Tm}^{(\nu X.\rho)(\boldsymbol{\tau})} \times \mathsf{Tm}^{(\nu X.\rho)(\boldsymbol{\tau})}$ which is inductively defined by

$$\frac{t \in [\![\nu X.\rho]\!](\mathbf{SN}^{\boldsymbol{\tau}})}{t \leq t}\,(\text{refl}) \qquad \frac{t'' \leq t' \qquad t'\ \mathcal{U}^{\rho}_{n+1}\ \mathsf{d}t}{t'' \leq t}\,(\text{trans})$$

Intuitively, $\leq$ is a generalization of the prefix relation on streams.

Lemma 3. $\dfrac{t' \leq t}{t' \in [\![\nu X.\rho]\!](\boldsymbol{\mathcal{U}}^{\nu X.\rho}(t))}$

Proof. Given a fixed $t \in [\![\nu X.\rho]\!](\mathbf{SN}^{\boldsymbol{\tau}})$ we show that the set $\leq(t)$ is closed under (destr') for $[\![\nu X.\rho]\!](\boldsymbol{\mathcal{U}}^{\nu X.\rho}(t))$ and hence by (co-elim)[7] the rule holds.

We have to show $s \leq t$ (i.e., $s \in \leq(t)$) implies

$$\mathsf{d}s \in [\![\rho]\!](\boldsymbol{\mathcal{U}}^{\nu X.\rho}(t), \leq(t))$$

We show this by induction over $s \leq t$:

(refl) We have to show

$$\mathsf{d}t \in [\![\rho]\!](\boldsymbol{\mathcal{U}}^{\nu X.\rho}(t), \leq(t))$$

By (sb2) for ρ we know $\mathsf{d}t \in [\![\rho]\!](\boldsymbol{\mathcal{U}}^{\rho}(\mathsf{d}t))$. For $1 \leq i \leq n$ (non-rec) implies that $\mathcal{U}^{\rho}_i(\mathsf{d}t) \subseteq \mathcal{U}^{\nu X.\rho}_i(t)$, and using (trans) and (refl) it is easy to see that $\mathcal{U}^{\rho}_{n+1}(\mathsf{d}t) \subseteq \leq(t)$. Hence by (mon) for $[\![\rho]\!]$ we have $\mathsf{d}t \in [\![\rho]\!](\boldsymbol{\mathcal{U}}^{\nu X.\rho}(t), \leq(t))$.

[7] See introduction, page 3.

(trans) Given

$$t' \, \mathcal{U}^{\rho}_{n+1} \; \mathsf{d}t \tag{6}$$

and as ind.hyp. $\mathsf{d}t'' \in [\![\rho]\!](\boldsymbol{\mathcal{U}}^{\nu X.\rho}(t'), \leq(t'))$ we have to show

$$\mathsf{d}t'' \in [\![\rho]\!](\boldsymbol{\mathcal{U}}^{\nu X.\rho}(t), \leq(t))$$

Using (rec) and (6) we know that $\mathcal{U}^{\nu X.\rho}_i(t') \subseteq \mathcal{U}^{\nu X.\rho}_i(t)$. Using (trans) and (6) we know $\leq(t') \subseteq \leq(t)$ and hence by applying (mon) for $[\![\rho]\!]$ for the ind.hyp. we have $\mathsf{d}t'' \in [\![\rho]\!](\boldsymbol{\mathcal{U}}^{\nu X.\rho}(t), \leq(t))$.

Proposition 13. *$[\![\nu X.\rho]\!]$ is monotone and set based.*

Proof.

(sb1) We show that

$$u \; R_i \; t :\iff t \in [\![\nu X.\rho]\!](\boldsymbol{P}) \implies u \in P_i$$

is closed under the rules defining $\mathcal{U}^{\nu X.\rho}_i$

(non-rec) We have $\mathsf{d}t \in [\![\rho]\!](\boldsymbol{P}, [\![\mu X.\rho]\!](\boldsymbol{P}))$ and hence by (sb1) for ρ the premise $u \, \mathcal{U}^{\rho}_i \, t$ implies $u \in P_i$.

(rec) As before we have $\mathsf{d}t \in [\![\rho]\!](\boldsymbol{P}, [\![\nu X.\rho]\!](\boldsymbol{P}))$. Hence, using (sb1) for ρ, the first premise $t' \, \mathcal{U}^{\rho}_{n+1} \; \mathsf{d}t$ implies $t' \in [\![\nu X.\rho]\!](\boldsymbol{P})$. Now we use the second premise $t' \; R_i \; u$ to conclude $u \in P_i$.

(sb2) Follows from Lemma 3 for $t \leq t$.

6.3 Extending Soundness

The soundness of d follows directly from the definition of ν:

Proposition 14.

$$\mathsf{d}^{X.\rho} \in [\![(\nu X.\rho) \to \rho(\nu X.\rho)]\!]$$

We have to extend Prop. 10 by a case for Co:

Proposition 15. *Prop. 10 extended by:*

3. *If $n > 1$ assume $\tau_i \in \mathsf{Ty}$ and $P_i \in \mathsf{SAT}^{\tau_i}$ for $1 \leq i < n$. Let $\sigma \in \mathsf{Ty}$ and $Q \in \mathsf{SAT}^{\sigma}$; it holds that*

$$\mathsf{Co}^{X.\rho(\boldsymbol{\tau},X),\sigma} \in (Q \Rightarrow [\![\rho]\!](\boldsymbol{P}, Q)) \Rightarrow Q \Rightarrow [\![\nu X.\rho]\!](\boldsymbol{P})$$

Proof. We have to extend 1. by the case for ν but the reasoning is the same as for μ. Let us consider 3.: Assuming $f \in Q \Rightarrow [\![\rho]\!](\boldsymbol{P}, Q)$ we show that

$$S = \{\mathsf{Co}^{X.\rho(\boldsymbol{\tau},X)} \, f t \mid t \in Q\}$$

is closed under (destr').

This entails $S \subseteq [\![\nu X.\rho]\!](\boldsymbol{P})$, since $[\![\nu X.\rho]\!](\boldsymbol{P})$ is defined as the greatest fixpoint of the rule (destr'), and thus our claim follows.

The definition of S implies that $\mathsf{Co}\, f \in Q \Rightarrow S$ (writing Co for $\mathsf{Co}^{X.\rho(\boldsymbol{\tau},X)}$). Assuming $t \in Q$ we have to show that $\mathsf{d}(\mathsf{Co}\, ft) \in [\![\rho]\!](\boldsymbol{P}, Q)$. We use (sat2) since $\mathsf{d}(\mathsf{Co}\, ft) \rhd_{\mathsf{whd}} \rho(\mathsf{Co}\, f)(ft)$. By ind.hyp. we know that $\rho(\mathsf{Co}\, f) \in \rho(\boldsymbol{P}, Q) \Rightarrow \rho(\boldsymbol{P}, S)$, which suffices to show that the reduct is in $\rho(\boldsymbol{P}, S)$. We finish by observing that an application of Lemma 1 shows that $\mathsf{d}(\mathsf{Co}\, ft) \in \mathsf{SN}$. □

Prop. 11 can be extended to the new cases using Prop. 14 and 15 and hence Theorem 1 can be extended to $\lambda^{\mu\nu}$.

7 Conclusions and Further Work

It is straightforward to extend the construction presented here to primitive recursion

$$\mathsf{Re}^{X.\tau,\sigma} : (\tau((\mu X.\tau) \times \sigma) \to \sigma) \to (\mu X.\tau) \to \sigma$$

and corecursion

$$\mathsf{CR}^{X.\tau,\sigma} : (\sigma \to \tau((\nu X.\tau) + \sigma)) \to \sigma \to \nu X.\tau,$$

which we have to omit here due to lack of space.

It may be argued that a syntactic approach to strong normalisation a la Benl [Ben98] may also be extended to a system as general as ours. However, we believe that the semantic approach using set based operators will allow further generalizations such as a functorial calculus (e.g., see [JBM98]) and heterogenous datatypes as discussed in [AR99].

References

[AA99] Andreas Abel and Thorsten Altenkirch. A predicative analysis of structural recursion. Submitted to the Journal of Functional Programming, December 1999.

[Abe99] Andreas Abel. A semantic analysis of structural recursion. Master's thesis, Ludwig-Maximilians-University Munich, 1999. http://www.informatik.uni-muenchen.de/~abel/publications/.

[Acz97] Peter Aczel. Notes on constructive set theory. Available from the WWW, 1997.

[Alt93] Thorsten Altenkirch. *Constructions, Inductive Types and Strong Normalization.* PhD thesis, University of Edinburgh, November 1993.

[Alt98] Thorsten Altenkirch. Logical relations and inductive/coinductive types. 1998.

[AR99] Thorsten Altenkirch and Bernhard Reus. Monadic presentations of lambda terms using generalized inductive types. In *Computer Science Logic 99*, 1999.

[Ben98] Holger Benl. Starke Normalisierung für die Heyting-Arithmetik mit induktiven Typen. Master's thesis, Ludwig-Maximillians-Universität, München, 1998.

[BJO99] Frédéric Blanqui, Jean-Pierre Jouannaud, and Mitsuhiro Okada. Inductive data type systems. To appear in Theoretical Computer Science, 1999.

[Buc81] Wilfried Buchholz. The $\omega_{\mu+1}$-rule. In *Iterated Inductive Definitions and Subsystems of Analysis: Recent Proof-Theoretical Studies*, volume 897 of *Lecture Notes in Mathematics*, pages 188–233. 1981.

[CM89] Thierry Coquand and Christine Mohring. Inductively defined types. In P. Löf and G. Mints, editors, *LNCS 389*, volume 417 of *Lecture Notes in Computer Science*, pages 50–66. Springer-Verlag, 1989.

[Coq94] Infinite objects in type theory. LNCS, pages 62–78, Berlin, 1994. Springer-Verlag.

[Dyb91] Peter Dybjer. Inductive sets and families in Martin-Löf's type theory and their set-theoretic semantics. Technical Report Report 62, Programming Methodology Group, Chalmers University, 1991.

[Geu92] Herman Geuvers. Inductive and coinductive types with iteration and recursion. In *Workshop on Types for Proofs and Programs, Båstad*, pages 193–217, 1992.

[Gir72] J. Y. Girard. *Interprétation fonctionelle et élimination des coupures dans l'arithétique d'ordre supérieur*. PhD thesis, Université Paris VII, 1972.

[GLT89] J.-Y. Girard, Y. Lafont, and P. Taylor. *Proofs and Types*. Cambridge University Press, 1989.

[Hag87] Tatsuya Hagino. *A Categorical Programming Language*. PhD thesis, University of Edinburgh, September 1987.

[JBM98] C.B. Jay, G. Bellè, and E. Moggi. Functorial ML. *Journal of Functional Programming*, 8(6):573–619, 1998.

[JO97] J. P. Jouannaud and M. Okada. Abstract data type systems. *Theoretical Computer Science*, 173, 1997.

[Loa97] Ralph Loader. Equational theories for inductive types. *Annals of Pure and Applied Logic*, 84:175–217, 1997.

[Luo90] Zhaohui Luo. *An Extended Calculus of Constructions*. PhD thesis, University of Edinburgh, 1990.

[Mar84] Per Martin-Löf. *Intuitionistic Type Theory*. Bibliopolis, 1984.

[Mat98] Ralph Matthes. *Extensions of System F by Iteration And Primitive Recursion on Monotone Inductive Types*. PhD thesis, University of Munich, 1998.

[Men88] Nax P. Mendler. *Inductive Definition in Type Theory*. PhD thesis, Cornell University, 1988.

[Rey84] John C. Reynolds. Polymorphism is not set-theoretic. In Gilles Kahn, David B. MacQueen, and Gordon D. Plotkin, editors, *Semantics of Data Types*, volume 173 of *Lecture Notes in Computer Science*, pages 145–156, Berlin, 1984. Springer-Verlag.

[Tai67] W. W. Tait. Intensional interpretations of functionals of finite type I. *Journal of Symbolic Logic*, 32(2):198–212, June 1967.