Draft

Calculus of Recursive Constructions

Name1 Name2 Name3

Affiliation1

Email1

Abstract

Place holder for abstract.

Categories and Subject Descriptors D.3.1 [*Programming Languages*]: Formal Definitions and Theory

Keywords Dependent types, Calculus of Constructions

1. Calculus of Constructions

Our language is based on the *Calculus of Constructions*, a special case of the *Pure Type System*. We give the definition as follows:

(i) A *Calculus of Constructions* (λC) is a triple tuple $(\mathcal{S}, \mathcal{A}, \mathcal{R})$ where

(a) $\mathcal{S} = \{\star, \Box\}$ is a set of *sorts*;

(b) $\mathcal{A} = \{(\star, \Box)\} \subseteq \mathcal{S} \times \mathcal{S}$ is a set of *axioms*;

(c) $\mathcal{R} = \{(\star, \star), (\star, \Box), (\Box, \star), (\Box, \Box)\} \subseteq \mathcal{S} \times \mathcal{S}$ is a set of *rules*.

(ii) *Raw expressions* A and *raw environments* Γ are defined in Figure 1.

A	$::=$	x	(variable)
	$\mid$	$\star$	(star)
	$\mid$	$\Box$	(square)
	$\mid$	$A\,A$	(application)
	$\mid$	$\lambda x : A.\, A$	(abstraction)
	$\mid$	$\Pi x : A.\, A$	(product)
Γ	$::=$	$\varnothing$	(empty)
	$\mid$	$\Gamma, x : A$	(variable binding)

Figure 1. Syntax of λC

We use s, t to range over *sorts*, x, y, z to range over *variables*, and A, B, C, a, b, c to range over *expressions*.

(iii) Π and λ are used to bind variables. Let $\mathrm{FV}(A)$ denote free variable set of A. Let $A[x := B]$ denote the substitution of x in A with B. We use $A \to B$ as a syntactic sugar for $(\Pi\_ : A.\, B)$.

(iv) The β-reduction ($\to_\beta$) is the smallest binary relation on raw expressions satisfying

$$(\lambda x : A.\, M)N \to_\beta M[x := N]$$

which can be used to define the notation $\twoheadrightarrow_\beta$ and $=_\beta$ by convention. Reduction rules are given in Figure 2. Highlighted premises and rules are only for *call-by-value* evaluation.

Values: $v ::= \quad \lambda x : A.\, B \mid \Pi x : A.\, B$

(R-Beta) $$\frac{N \in \mathit{Value}}{(\lambda x : A.\, M)N \longrightarrow M[x := N]}$$

(R-AppL) $$\frac{M \longrightarrow M'}{MN \longrightarrow M'N}$$

(R-AppR) $$\frac{v \in \mathit{Value} \qquad M \longrightarrow M'}{vM \longrightarrow vM'}$$

Figure 2. Reduction rules for λC

(v) Type assignment rules for $(\mathcal{S}, \mathcal{A}, \mathcal{R})$ are given in Figure 3.

(Ax) $$\frac{}{\varnothing \vdash \star : \Box}$$

(Var) $$\frac{\Gamma \vdash A : s}{\Gamma, x : A \vdash x : A} \qquad x \notin \mathrm{dom}(\Gamma)$$

(Weak) $$\frac{\Gamma \vdash b : B \qquad \Gamma \vdash A : s}{\Gamma, x : A \vdash b : B} \qquad x \notin \mathrm{dom}(\Gamma)$$

(App) $$\frac{\Gamma \vdash f : (\Pi x : A.\, B) \qquad \Gamma \vdash a : A}{\Gamma \vdash f a : B[x := a]}$$

(Lam) $$\frac{\Gamma, x : A \vdash b : B \qquad \Gamma \vdash (\Pi x : A.\, B) : t}{\Gamma \vdash (\lambda x : A.\, b) : (\Pi x : A.\, B)} \qquad t \in \{\star, \Box\}$$

(Pi) $$\frac{\Gamma \vdash A : s \qquad \Gamma, x : A \vdash B : t}{\Gamma \vdash (\Pi x : A.\, B) : t} \qquad (s, t) \in \mathcal{R}$$

(Conv) $$\frac{\Gamma \vdash a : A \qquad \Gamma \vdash B : s \qquad A =_\beta B}{\Gamma \vdash a : B}$$

Figure 3. Typing rules for λC

2. Extend with recursive types

2.1 Core language

We extend Calculus of Constructions (λC) with recursive types, namely λC_μ. Differences with λC are highlighted. Figure 4 shows the extended syntax.

Since recursive types are introduced and due to the practical concern, we use the *call-by-name* reduction strategy, i.e. iteratively reducing the *left-most outer-most* redex. Figure 5 shows the dynamic semantics with no call-by-value specific premises or rules.

Terms			
E, T	$::=$	x	(variable)
	$\vert$	$\star$	(star)
	$\vert$	$\Box$	(square)
	$\vert$	$E\,E$	(application)
	$\vert$	$\lambda x : T.\, E$	(abstraction)
	$\vert$	$\Pi x : T.\, T$	(product)
	$\vert$	$\mu x : T.\, E$	(recursive type)
	$\vert$	$\mathsf{fold}[T]\; E$	(generalized roll)
	$\vert$	$\mathsf{unfold}\; E$	(generalized unroll)
Environments			
Γ	$::=$	$\varnothing$	(empty)
	$\vert$	$\Gamma, x : T$	(variable binding)
Syntactic sugar			
let $x : T = E_1$ **in** E_2	$::=$	$(\lambda x : T.\, E_2)\; E_1$	

Figure 4. Syntax of λC_μ

values: v	$::=$	$\lambda x : T.\, E$	(abstraction)
	$\vert$	$\Pi x : T_1.\, T_2$	(product)
	$\vert$	$\mathsf{fold}[T]\; E$	(roll)

(R-AppLam) $$\frac{}{(\lambda x : T.\, E_1)E_2 \longrightarrow E_1[x := E_2]}$$

(R-AppL) $$\frac{E_1 \longrightarrow E_1'}{E_1\, E_2 \longrightarrow E_1'\, E_2}$$

(R-Unfold) $$\frac{E \longrightarrow E'}{\mathsf{unfold}\; E \longrightarrow \mathsf{unfold}\; E'}$$

(R-Unfold-Fold) $$\frac{}{\mathsf{unfold}\; (\mathsf{fold}[T]\; E) \longrightarrow E}$$

(R-Mu) $$\frac{}{\mu x : T.\; \longrightarrow T[x := \mu x : T.\,]}$$

Figure 5. Reduction rules for λC

The extended typing rules are shown in Figure 6. Compared with λC, the original *Conv* rule is replaced by the new *Beta* rule where the latter only performs one step of reduction defined in Figure 5.

2.2 Soundness of core language

We show the soundness of the core language by subject reduction and progress theorems.

Theorem 2.1 (Subject Reduction)
If $\Gamma \vdash A : B$ *and* $A \longrightarrow A'$ *then* $\Gamma \vdash A' : B$.

Proof. See Appendix A. □

Theorem 2.2 (Progress)
If $\cdot \vdash A : B$ *then either* A *is a value* v *or there exists* A' *such that* $A \longrightarrow A'$.

Proof. See Appendix A. □

2.3 Examples of typable terms

- Polymorphic identity function: if $\Gamma \vdash e : \tau$, we have

$$\mathsf{unfold}\; ((\lambda\alpha : \star.\, \lambda x : ((\lambda y : \star.\, y)\; \alpha).\, x)\; \tau\; (\mathsf{fold}[(\lambda y : \star.\, y)\; \tau]\; e))$$
$$\longrightarrow \mathsf{unfold}\; (\mathsf{fold}[(\lambda y : \star.\, y)\; \tau]\; e) \longrightarrow e.$$

(Ax) $$\frac{}{\varnothing \vdash \star : \Box}$$

(Var) $$\frac{\Gamma \vdash T : s}{\Gamma, x : T \vdash x : T} \qquad x \notin \mathrm{dom}(\Gamma)$$

(Weak) $$\frac{\Gamma \vdash E : T_2 \qquad \Gamma \vdash T_1 : s}{\Gamma, x : T_1 \vdash E : T_2} \qquad x \notin \mathrm{dom}(\Gamma)$$

(App) $$\frac{\Gamma \vdash E_1 : (\Pi x : T_2.\, T_1) \qquad \Gamma \vdash E_2 : T_2}{\Gamma \vdash E_1 E_2 : T_1[x := E_2]}$$

(Lam) $$\frac{\Gamma, x : T_1 \vdash E : T_2 \qquad \Gamma \vdash (\Pi x : T_1.\, T_2) : t}{\Gamma \vdash (\lambda x : T_1.\, E) : (\Pi x : T_1.\, T_2)} \qquad t \in \{\star, \Box\}$$

(Pi) $$\frac{\Gamma \vdash T_1 : s \qquad \Gamma, x : T_1 \vdash T_2 : t}{\Gamma \vdash (\Pi x : T_1.\, T_2) : t} \qquad (s, t) \in \mathcal{R}$$

(Mu) $$\frac{\Gamma, x : T \vdash E : T \qquad \Gamma \vdash T : s}{\Gamma \vdash (\mu x : T.\, E) : T} \qquad s \in \{\star, \Box\}$$

(Fold) $$\frac{\Gamma \vdash E : T_2 \qquad \Gamma \vdash T_1 : s \qquad T_1 \longrightarrow T_2}{\Gamma \vdash (\mathsf{fold}[T_1]\; E) : T_1}$$

(Unfold) $$\frac{\Gamma \vdash E : T_1 \qquad \Gamma \vdash T_2 : s \qquad T_1 \longrightarrow T_2}{\Gamma \vdash (\mathsf{unfold}\; E) : T_2}$$

Figure 6. Typing rules for λC_μ

- A polymorphic fixed-point constructor $\mathsf{fix} : (\Pi\alpha : \star.(\alpha \to \alpha) \to \alpha)$ can be defined as follows:

$$\mathsf{fix} = \lambda\alpha : \star.\lambda f : \alpha \to \alpha.$$
$$(\lambda x : (\mu\sigma : \star.\, \sigma \to \alpha).f((\mathsf{unfold}\; x)x))$$
$$(\mathsf{fold}[\mu\sigma : \star.\, \sigma \to \alpha]\; (\lambda x : (\mu\sigma : \star.\, \sigma \to \alpha).f((\mathsf{unfold}\; x)x)))$$

  Note that this is the so called call-by-name fixed point combinator. It is useless in a call-by-value setting, since the expression $\mathsf{fix}\, \alpha\, g$ diverges for any g.

- Using fix, we can build recursive functions. For example, given a "hungry" type $H = \mu\sigma : \star.\, \alpha \to \sigma$, the "hungry" function h where

$$h = \lambda\alpha : \star.\mathsf{fix}\; (\alpha \to H)\; (\lambda f : \alpha \to H.\lambda x : \alpha.\mathsf{fold}[H]\; f)$$

  can take arbitrary number of arguments.

3. Formal Elaboration of Datatypes and Case Analysis

3.1 Extended Language

We extend λC_μ with simple datatypes (polymorphic and recursive[1]) and case analysis [6], namely $\lambda C_{\mu c}$. Differences with λC_μ are highlighted in Figure 7.

An *algebraic data type* D is introduced as a top-level **data** declaration with its *data constructors*. The type of a data constructor K has the form:

$$K : \Pi\overline{x : \kappa}^n.\Pi\overline{y : \iota}.\overline{\tau} \to D\,\overline{x}^n$$

The first n quantified type variables $\overline{x}$ appear in the same order in the return type $D\,\overline{x}$, and $\overline{y}$ stands for existentially quantified type variables. There is a **case** expression to take apart values built with data constructors. The patterns of a case expression are flat (no nested patterns), and bind existential type variables.

The extended typing rules are shown in Figure 8. To save space, we only show the new typing rules.

[1] Polymorphic recursion is not supported yet, since we have difficulty generalizing μ to have higher kind.

Declarations

pgm	$::=$	$\overline{decl}; e$	(Declarations)
$decl$	$::=$	$\mathbf{data}\, D : \overline{\kappa} \to \star\, \mathbf{where}$ $\overline{K : \Pi \overline{x : \kappa}. \Pi \overline{y : \iota}. \overline{\tau} \to D\, \overline{x}}$	(Datatype)

Terms

u	$::=$	$x \mid K$	(Variables and data constructors)
$e, \tau, \sigma, \kappa, \iota$	$::=$	u	(Term atoms)
		$\ldots$	
	$\mid$	$\mathbf{case}\, e\, \mathbf{of}\, \overline{p \Rightarrow e}$	(Case analysis)
p	$::=$	$K\, \overline{y : \iota}\, \overline{x : \tau}$	(Pattern)

Environments

Γ	$::=$	$\varnothing$	(Empty)
	$\mid$	$\Gamma, u : \tau$	(Variable binding)

Figure 7. Syntax of $\lambda C_{\mu c}$ (e for terms; τ, σ for types; κ, ι for kinds)

$$\boxed{\Gamma \vdash pgm : \tau}$$

(Pgm)
$$\frac{\overline{\Gamma_0 \vdash decl : \Gamma_d} \qquad \Gamma = \Gamma_0, \overline{\Gamma_d} \qquad \Gamma \vdash e : \tau}{\Gamma_0 \vdash \overline{decl}; e : \tau}$$

$$\boxed{\Gamma \vdash decl : \Gamma'}$$

(Data)
$$\frac{\Gamma \vdash \kappa : \Box \qquad \overline{\Gamma, D : \kappa \vdash \tau : \star}}{\Gamma \vdash (\mathbf{data}\, D : \kappa\, \mathbf{where}\, \overline{K : \tau}) : (D : \kappa, \overline{K : \tau})}$$

$$\boxed{\Gamma \vdash e : \tau}$$

(Case)
$$\frac{\Gamma \vdash e_1 : \sigma \qquad \overline{\Gamma \vdash_p p \Rightarrow e_2 : \sigma \to \tau}}{\Gamma \vdash \mathbf{case}\, e_1\, \mathbf{of}\, \overline{p \Rightarrow e_2} : \tau}$$

$$\boxed{\Gamma \vdash_p p \Rightarrow e : D \to \tau}$$

(Alt)
$$\frac{K : \Pi \overline{a : \kappa}. \Pi \overline{y : \iota}. \overline{\sigma} \to D\, \overline{a} \in \Gamma \qquad \theta = [\overline{a := v}] \qquad \Gamma, \overline{y : \iota}, \overline{x : \theta(\sigma)} \vdash e : \tau}{\Gamma \vdash_p K\, \overline{y : \iota}\, \overline{x : \theta(\sigma)} \Rightarrow e : D\, \overline{v} \to \tau}$$

Figure 8. Typing rules for $\lambda C_\mu c$

3.2 Translation Overview

We use a type-directed translation [3]. The typing relations have the form:

$$\Gamma \vdash e : \tau \rightsquigarrow E$$

It states that λC_μ expression E is the translation of $\lambda C_{\mu c}$ expression e of type τ. Figure 9 shows the translation rules, which are the typing rules of the previous section extended with the resulting expression E. In the translation, *We require that applications of type functions D to be saturated.*

3.3 Examples of Simple Datatypes

- Encoding of natural numbers

$$\begin{array}{l} \mathbf{data}\, \mathsf{Nat} : \star\, \mathbf{where} \\ \quad \mathsf{zero} : \mathsf{Nat} \\ \quad \mathsf{suc} : \mathsf{Nat} \to \mathsf{Nat} \end{array}$$

Nat, zero and suc are encoded as follows:

$$\begin{array}{l} \mathbf{let}\, \mathsf{Nat} : \star = \mu X : \star.\, \Pi b : \star.\, b \to (X \to b) \to b\, \mathbf{in} \\ \mathbf{let}\, \mathsf{zero} : \mathsf{Nat} = \mathsf{fold}[\mathsf{Nat}]\, (\lambda(b : \star)(z : b)(f : \mathsf{Nat} \to b).\, z)\, \mathbf{in} \\ \mathbf{let}\, \mathsf{suc} : \mathsf{Nat} \to \mathsf{Nat} = \lambda(n : \mathsf{Nat}).\, \mathsf{fold}[\mathsf{Nat}]\, (\lambda(b : \star)(z : b) \\ \quad (f : \mathsf{Nat} \to b).\, f\, n)\, \mathbf{in} \end{array}$$

- Encoding of polymorphic lists

$$\begin{array}{l} \mathbf{data}\, \mathsf{List} : \star \to \star\, \mathbf{where} \\ \quad \mathsf{nil} : \Pi a : \star.\, \mathsf{List}\, a \\ \quad \mathsf{cons} : \Pi a : \star.\, a \to \mathsf{List}\, a \to \mathsf{List}\, a \end{array}$$

List, nil and cons are encoded as follows:

$$\begin{array}{l} \mathbf{let}\, \mathsf{List} : \star \to \star = \lambda a : \star.\, \mu X : \star.\, \Pi b : \star.\, b \to (a \to X \to b) \to b\, \mathbf{in} \\ \mathbf{let}\, \mathsf{nil} : \Pi a : \star.\, \mathsf{List}\, a = \lambda a : \star. \\ \quad \mathsf{fold}[\mathsf{List}\, a]\, (\lambda(b : \star)(z : b)(f : a \to \mathsf{List}\, a \to b).\, z)\, \mathbf{in} \\ \mathbf{let}\, \mathsf{cons} : \Pi a : \star.\, a \to \mathsf{List}\, a \to \mathsf{List}\, a = \lambda(a : \star)(x : a)(xs : \mathsf{List}\, a). \\ \quad \mathsf{fold}[\mathsf{List}\, a]\, (\lambda(b : \star)(z : b)(f : a \to \mathsf{List}\, a \to b).\, f\, x\, xs)\, \mathbf{in} \end{array}$$

$\boxed{\Gamma \vdash e : \tau \leadsto E}$

(Ax)
$$\frac{}{\varnothing \vdash \star : \Box \leadsto \star}$$

(Var)
$$\frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau \leadsto x}$$

(App)
$$\frac{\Gamma \vdash e_1 : (\Pi x : \tau_2 .\, \tau_1) \leadsto E_1 \qquad \Gamma \vdash e_2 : \tau_2 \leadsto E_2}{\Gamma \vdash e_1 e_2 : \tau_1[x := e_2] \leadsto E_1 E_2}$$

(Lam)
$$\frac{\Gamma, x : \tau_1 \vdash e : \tau_2 \leadsto E \qquad \Gamma \vdash (\Pi x : \tau_1 .\, \tau_2) : t}{\Gamma \vdash (\lambda x : \tau_1 .\, e) : (\Pi x : \tau_1 .\, \tau_2) \leadsto \lambda x : \tau_1 .\, E} \qquad t \in \{\star, \Box\}$$

(Pi)
$$\frac{\Gamma \vdash \tau_1 : s \qquad \Gamma, x : \tau_1 \vdash \tau_2 : t}{\Gamma \vdash (\Pi x : \tau_1 .\, \tau_2) : t \leadsto \Pi x : \tau_1 .\, \tau_2} \qquad (s, t) \in \mathcal{R}$$

(Mu)
$$\frac{\Gamma, x : \tau \vdash e : \tau \leadsto E \qquad \Gamma \vdash \tau : s}{\Gamma \vdash (\mu x : \tau .\, e) : \tau \leadsto \mu x : \tau .\, E} \qquad s \in \{\star, \Box\}$$

(Fold)
$$\frac{\Gamma \vdash e : \tau_2 \leadsto E \qquad \Gamma \vdash \tau_1 : s \qquad \tau_1 \longrightarrow \tau_2}{\Gamma \vdash (\mathsf{fold}[\tau_1]\, e) : \tau_1 \leadsto \mathsf{fold}[\tau_1]\, E}$$

(Unfold)
$$\frac{\Gamma \vdash e : \tau_1 \leadsto E \qquad \Gamma \vdash \tau_2 : s \qquad \tau_1 \longrightarrow \tau_2}{\Gamma \vdash (\mathsf{unfold}\, e) : \tau_2 \leadsto \mathsf{unfold}\, E}$$

(Case)
$$\frac{\Gamma \vdash e_1 : \sigma \leadsto E_1 \qquad \overline{\Gamma \vdash_p p \Rightarrow e_2 : \sigma \to \tau \leadsto E_2}}{\Gamma \vdash \mathbf{case}\, e_1\, \mathbf{of}\, \overline{p \Rightarrow e_2} : \tau \leadsto (\mathsf{unfold}\, E_1)\, \tau\, \overline{E_2}}$$

$\boxed{\Gamma \vdash_p p \Rightarrow e : D \to \tau \leadsto E}$

(Alt)
$$\frac{\begin{array}{c} \qquad\qquad\qquad\qquad \theta = [\overline{a := \upsilon}] \\ K : \Pi \overline{a : \kappa} . \Pi \overline{y : \iota} . \overline{\sigma} \to D\, \overline{a} \in \Gamma \qquad \Gamma, \overline{y : \iota}, \overline{x : \theta(\sigma)} \vdash e : \tau \leadsto E \end{array}}{\Gamma \vdash_p K\, \overline{y : \iota}\, \overline{x : \theta(\sigma)} \Rightarrow e : D\, \overline{\upsilon} \to \tau \leadsto \lambda(\overline{y : \iota})(\overline{x : \theta(\sigma)}).E}$$

$\boxed{\Gamma \vdash decl : \Gamma' \leadsto E}$

(Data)
$$\frac{\Gamma \vdash \overline{\kappa} \to \star : \Box \qquad \overline{\Gamma, D : \overline{\kappa} \to \star \vdash \sigma : \star}}{\Gamma \vdash (\mathbf{data}\, D : \overline{\kappa} \to \star\, \mathbf{where}\, \overline{K : \sigma}) : (D : \overline{\kappa} \to \star, \overline{K : \sigma}) \leadsto E}$$

$$\begin{array}{lcl}
\sigma & ::= & \Pi \overline{a : \kappa} . \Pi \overline{y : \iota} . \overline{\tau} \to D\, \overline{a} \\
E & ::= & \mathbf{let}\, D : \overline{\kappa} \to \star = \lambda \overline{a : \kappa} . \mu X . \Pi b : \star . \\
 & & \quad \overline{(\Pi \overline{y : \iota} . \tau [D\, \overline{a} := X] \to b)} \to b\, \mathbf{in} \\
 & & \mathbf{let}\, K_i^{i \in 1..n} : \sigma = \lambda \overline{(a : \kappa)} . \lambda \overline{(y : \iota)} . \lambda \overline{(x : \tau)} . \\
 & & \quad \mathsf{fold}[D\, \overline{a}]\, (\lambda (b : \star) \overline{(c : \Pi \overline{y : \iota} . \overline{\tau} \to b)} . c_i\, \overline{y}\, \overline{x})\, \mathbf{in}
\end{array}$$

$\boxed{\Gamma \vdash pgm : \tau \leadsto E}$

(Pgm)
$$\frac{\overline{\Gamma_0 \vdash decl : \Gamma_d \leadsto E_1} \qquad \Gamma = \Gamma_0, \overline{\Gamma_d} \qquad \Gamma \vdash e : \tau \leadsto E}{\Gamma_0 \vdash \overline{decl}; e : A \leadsto \overline{E_1} \oplus E}$$

Figure 9. Type-directed translation from $\lambda C_\mu c$ to λC_μ

Using fix, we can define a recursive function length as follows:

$$\begin{array}{l}
\mathsf{length} : \Pi a : \star .\, \mathsf{List}\, a \to \mathsf{Nat} \\
\mathsf{length} = \lambda a : \star .\, \mathsf{fix}\, (\mathsf{List}\, a \to \mathsf{Nat}) \\
\qquad (\lambda (f : \mathsf{List}\, a \to \mathsf{Nat})(l : \mathsf{List}\, a). \\
\qquad (\mathsf{unfold}\, l)\, \mathsf{Nat}\, \mathsf{zero}\, (\lambda (x : a)(xs : \mathsf{List}\, a).\, \mathsf{suc}\, (f\, xs)))\, \mathbf{in}
\end{array}$$

- Encoding of a datatype with existential types

$$\begin{array}{l}
\mathbf{data}\, D : \star \to \star\, \mathbf{where} \\
\qquad K : \Pi a : \star .\, \Pi b : \star .\, a \to b \to (b \to \mathsf{Nat}) \to D\, a
\end{array}$$

Acknowledgments

Acknowledgments, if needed.

References

[1] H. Geuvers. The church-scott representation of inductive and coinductive data. Types, 2014.

[2] S. P. Jones and E. Meijer. Henk: a typed intermediate language. *TIC*, 97, 1997.

[3] A. Middelkoop, A. Dijkstra, and S. D. Swierstra. A lean specification for gadts: system f with first-class equality proofs. *Higher-Order and Symbolic Computation*, 23(2):145–166, 2010.

[4] J.-W. Roorda and J. Jeuring. Pure type systems for functional programming. 2007.

[5] M. H. Sørensen and P. Urzyczyn. *Lectures on the Curry-Howard isomorphism*, volume 149. Elsevier, 2006.

[6] M. Sulzmann, M. M. Chakravarty, S. P. Jones, and K. Donnelly. System f with type equality coercions. In *Proceedings of the 2007 ACM SIGPLAN international workshop on Types in languages design and implementation*, pages 53–66. ACM, 2007.

A. Appendix

Lemma A.1 (Substitutions)
Assume we have

$$\Gamma, x : A \vdash B : C \qquad (1)$$
$$\Gamma \vdash D : A, \qquad (2)$$

then

$$\Gamma[x := D] \vdash B[x := D] : C[x := D].$$

Proof. This is trivial by induction on the typing derivation of (1) by typing rules in Fig.6. We only discuss two cases for example. Let E^* denote $E[x := D]$. Consider following cases

- The last applied rule to obtain (1) is *Var*. There are 2 sub-cases:
  1. It is derived by
  $$\frac{\Gamma \vdash A : s}{\Gamma, x : A \vdash x : A},$$
  then we have $(B : C) \equiv (x : A)$. And $\Gamma \vdash (x : A)^* \equiv (D : A)$ which holds by (2).
  2. It is derived by
  $$\frac{\Gamma, x : A \vdash E : s}{\Gamma, x : A, y : E \vdash y : E},$$
  then we need to show $\Gamma^*, y : E^* \vdash y : E^*$. And it directly follows the induction hypothesis, i.e. $\Gamma^* \vdash E^* : s$.
- The last applied rule to obtain (1) is *App*, i.e.
$$\frac{\Gamma, x : A \vdash B_1 : (\Pi y : C_1.\, C_2) \qquad \Gamma, x : A \vdash B_2 : C_1}{\Gamma, x : A \vdash (B_1 B_2) : C_2[y := B_2]}.$$
By the induction hypothesis, we can obtain $\Gamma^* \vdash B_1^* : (\Pi y : C_1^*.C_2^*)$ and $\Gamma^* \vdash B_2^* : C_1^*$. Thus, $\Gamma^* \vdash (B_1^* B_2^*) : (C_2^*[y := B_2^*])$, i.e. $\Gamma^* \vdash (B_1 B_2)^* : (C_2[y := B_2])^*$.

□

Theorem A.2 (Subject Reduction)
If $\Gamma \vdash A : B$ and $A \longrightarrow A'$ then $\Gamma \vdash A' : B'$ for some B' such that either $B \equiv B'$ or $B \longrightarrow B'$.

Proof. Let $\mathcal{D}$ be the derivation of $\Gamma \vdash A : B$. The proof is by induction on dynamic semantics shown in Fig.5.

case *R-AppLam*: $\dfrac{}{(\lambda x : A.\, M)N \longrightarrow M[x := N]}$.
Derivation $\mathcal{D}$ has the following form

$$\frac{\dfrac{\Gamma, x : A \vdash M : A'}{\Gamma \vdash (\lambda x : A.M) : (\Pi x : A.A')}\,\textit{Lam} \qquad \Gamma \vdash N : A}{\Gamma \vdash (\lambda x : A.M)N : A'}\,\textit{App}$$

Thus, by Lemma A.1 we can obtain $\Gamma \vdash M[x := N] : A'$.

case *R-AppL*: $\dfrac{M \longrightarrow M'}{MN \longrightarrow M'N}$.
Derivation $\mathcal{D}$ has the following form

$$\frac{\Gamma \vdash M : (\Pi x : A.A') \qquad \Gamma \vdash N : A}{\Gamma \vdash MN : A'}\,\textit{App}$$

By the induction hypothesis we have $\Gamma \vdash M' : (\Pi x : A.A')$. Hence,

$$\frac{\Gamma \vdash M' : (\Pi x : A.A') \qquad \Gamma \vdash N : A}{\Gamma \vdash M'N : A'}\,\textit{App}$$

case *R-Unfold*: $\dfrac{M \longrightarrow M'}{\mathsf{unfold}\, M \longrightarrow \mathsf{unfold}\, M'}$.
Derivation $\mathcal{D}$ has the following form

$$\frac{\Gamma \vdash M : \mu x.A}{\Gamma \vdash (\mathsf{unfold}\, M) : A[x := \mu x.A]}\,\textit{Unfold}$$

By the induction hypothesis we have $\Gamma \vdash M' : \mu x.A$. Hence,

$$\frac{\Gamma \vdash M' : \mu x.A}{\Gamma \vdash (\mathsf{unfold}\, M') : A[x := \mu x.A]}\,\textit{Unfold}$$

case *R-Unfold-Fold*: $\dfrac{}{\mathsf{unfold}\,(\mathsf{fold}[\mu x : A.\,]\, M) \longrightarrow M}$.
Derivation $\mathcal{D}$ has the following form

$$\frac{\dfrac{\Gamma \vdash M : (A[x := \mu x.A])}{\Gamma \vdash (\mathsf{fold}[\mu x : A.\,]\, M) : \mu x.A}\,\textit{Fold}}{\Gamma \vdash \mathsf{unfold}\,(\mathsf{fold}[\mu x : A.\,]\, M) : (A[x := \mu x.A])}\,\textit{Unfold}$$

case *R-Mu*: $\dfrac{}{\mu x : M.\; \longrightarrow M[x := \mu x : M.\,]}$.
Derivation $\mathcal{D}$ has the following form

$$\frac{\Gamma, x : s \vdash M : s}{\Gamma \vdash (\mu x : M.\,) : s}\,\textit{Mu}$$

Hence, by Lemma A.1 we have $\dfrac{\Gamma, x : s \vdash M : s \qquad \Gamma \vdash \mu x : M.\, : s}{\Gamma \vdash (M[x := \mu x : M.\,]) : s}$.

□

Theorem A.3 (Progress)
If $\cdot \vdash A : B$ then either A is a value v or there exists A' such that $A \longrightarrow A'$.

Proof. We can give the proof by induction on the derivation of $\cdot \vdash A : B$ by typing rules in Fig.6:

case *Var*: $\dfrac{\cdot \vdash A : s}{\cdot, x : A \vdash x : A}$.
This case cannot be reached. Proof is by contradiction. If we have $\cdot \vdash x : A$ then x is assigned with type A from a context "$\cdot$" without A, which is not possible.

case *Weak*: $\dfrac{\cdot \vdash b : B \qquad \cdot \vdash A : s}{\cdot, x : A \vdash b : B}$.
The result is trivial by induction hypothesis.

case *App*: $\dfrac{\cdot \vdash M : (\Pi x : A.B) \qquad \cdot \vdash N : A}{\cdot \vdash MN : B}$.
By induction hypothesis on $\cdot \vdash M : (\Pi x : A.B)$, there are two possible cases.
1. $M = v$ is a value. Hence $v = \lambda x : A.M'$ where $\cdot \vdash M' : B$. Then $MN = vN = (\lambda x : A.M')N = M'[x := N]$. By the substitution lemma, $\cdot \vdash (M'[x := N]) : B$ which is just $\cdot \vdash MN : B$.
2. $M \longrightarrow M'$. The result is obvious by the operational semantic $\dfrac{M \longrightarrow M'}{MN \longrightarrow M'N}\,\textit{R-AppL}$.

case *Lam*: $\dfrac{\cdots}{\cdot \vdash (\lambda x : A.M) : (\Pi x : A.B)}$.
The result is trivial if let $v = \lambda x : A.M$.

case *Pi*: $\dfrac{\cdot \vdash A : s \qquad \cdot, x : A \vdash B : t}{\cdot \vdash (\Pi x : A.\, B) : t}$.
The result is trivial if let $v = \Pi x : A.\, B$.

case *Mu*: $\dfrac{\cdots}{\cdot \vdash (\mu x : A.\,) : s}$.
The result is trivial since we always have such reduction $\mu x : A.\; \longrightarrow A[x := \mu x : A.\,]$.

case *Fold*: $\dfrac{\cdots}{\cdot \vdash (\mathsf{fold}[\mu x.A]\, M) : \mu x.A}$.
The result is trivial if let $v = \mathsf{fold}[\mu x.A]\, M$.

case *Unfold*: $\dfrac{\cdot \vdash a : \mu x : A. \qquad \cdot \vdash A[x := \mu x : A.\,] : s}{\cdot \vdash (\mathsf{unfold}\, a) : A[x := \mu x : A.\,]}$.

By induction hypothesis on $\cdot \vdash a : \mu x : A.$, there are two possible cases.

1. $a = v$ is a value. Hence $a = \mathsf{fold}[\mu x : A.\,]\, b$ where $\cdot \vdash b : (A[x := \mu x : A.\,])$. Then by the *R-Unfold-Fold* rule, $\mathsf{unfold}\, a = \mathsf{unfold}\, (\mathsf{fold}[\mu x : A.\,]\, b) = b$. Thus $\cdot \vdash (\mathsf{unfold}\, a) : A[x := \mu x : A.\,]$.
2. $a \longrightarrow a'$. The result is obvious by the reduction rule $\dfrac{M \longrightarrow M'}{\mathsf{unfold}\, M \underset{\cdots}{\longrightarrow} \mathsf{unfold}\, M'}$ *R-Unfold* .

case *Beta*: $\dfrac{}{\cdot \vdash (\mathsf{beta}\, a) : B}$.

The result is trivial since we always have such reduction $\mathsf{beta}\, a \longrightarrow a$.

□