数理解析研究所講究録 1442 巻 2005 年 97-114

A Galois embedding from polymorphic types into existential types
– Extended Abstract –

Ken-etsu Fujita (藤田 憲悦)
Department of Computer Science,
Gunma University (群馬大学)

Masahito Hasegawa (長谷川 真人)
Research Institute of Mathematical Science,
Kyoto University (京都大学)

Abstract

We show that there exist translations between polymorphic λ-calculus and a subsystem of minimal logic with existential types, which form a Galois connection and moreover a Galois embedding. From a programming point of view, this result means that polymorphic functions can be represented by abstract data types.

1 Introduction

We show that polymorphic types can be interpreted by the use of second order existential types. For this, we prove that there exist translations between polymorphic λ-calculus $\lambda 2$ and subsystem of minimal logic with existential types, which form a Galois connection and moreover a Galois embedding. From a programming point of view, this result means that polymorphic functions can be represented by abstract data types and vice versa.

Peter Selinger [Seli01] has introduced control categories and established an isomorphism between call-by-name and call-by-value $\lambda\mu$-calculi. The isomorphism reveals duality not only on logical connectives $(\wedge, \vee)$ like de Morgan but also on reduction strategies (call-by-name and call-by-value), input-output relations (demand- and data-driven) and inference rules (introduction and elimination).

Philip Wadler [Wad03] introduced the dual calculus in the style of Gentzen's sequent calculus LK, such that the duality explicitly appears on antecedent and succedent in the sequent of the propositional calculus.

Our main interest is a neat connection and proof duality between polymorphic types and existential types. It is logically quite natural like de Morgan's duality, and computationally still interesting, since dual of polymorphic functions with universal type can be regarded as abstract data types with existential type [MP85]. Instead of classical systems like [Pari92], even intuitionistic systems can enjoy that polymorphic types can be interpreted by existential types and vice versa. This interpretation also contains proof duality, such that the universal introduction rule is interpreted by the use of the existential elimination rule, and the universal elimination by the existential introduction. Moreover, we established not only a Galois connection but also a Galois embedding from polymorphic λ-calculus (Girard-Reynolds) into a calculus with existential types.

2 Polymorphic λ-calculus $\lambda 2$

We give the definition of polymorphic λ-calculus *à la* Church as second order intuitionistic logic, denoted by $\lambda 2$. This calculus is also known as the system F. The syntax of types is defined from type variables denoted by X, using $\Rightarrow$ or $\forall$ over type variables. The syntax of $\lambda 2$-terms is defined from individual variables denoted by x, using term-applications, type-applications or λ-abstractions over individual variables or type variables.

Definition 1 (Types)

$$A \quad ::= \quad X \mid A \Rightarrow A \mid \forall X.A$$

Definition 2 (Pseudo-terms)

$$\Lambda 2 \ni M ::= x \mid \lambda x\!:\!A.M \mid MM \mid \lambda X.M \mid MA$$

Definition 3 (Reduction rules) (β) $(\lambda x\!:\!A.M)M_1 \to M[x := M_1]$

(β_t) $(\lambda X.M)A \to M[X := A]$

(η) $\lambda x.Mx \to M$ *if* $x \notin FV(M)$

(η_t) $\lambda X.MX \to M$ *if* $X \notin FV(M)$

A set of free variables in M is denoted by $FV(M)$. The one step reduction relation is denoted by $\to_{\lambda 2}$. We write $\to^+_{\lambda 2}$ or $\to^*_{\lambda 2}$ to denote the transitive closure or the reflexive and transitive closure of $\to_{\lambda 2}$, respectively. We employ the notation $=_{\lambda 2}$ for the symmetric, reflexive and transitive closure of the one step reduction $\to_{\lambda 2}$ defined above. We write $\equiv$ for a syntactical identity modulo renaming of bound variables. Let R be β, β_t, η or η_t. Then we often write $\to_R$ to denote the corresponding subset of $\to_{\lambda 2}$.

The typing judgement of $\lambda 2$ takes the form of $\Gamma \vdash M : A$, where Γ is a set of declarations in the form of $x : A$ with distinct variables as subjects.

Definition 4 (Type assignment rules)

$$\frac{x\!:\!A \in \Gamma}{\Gamma \vdash x : A}$$

$$\frac{\Gamma, x\!:\!A_1 \vdash M : A_2}{\Gamma \vdash \lambda x\!:\!A_1.M : A_1 \Rightarrow A_2}\ (\Rightarrow I) \qquad \frac{\Gamma \vdash M_1 : A_1 \Rightarrow A_2 \quad \Gamma \vdash M_2 : A_1}{\Gamma \vdash M_1 M_2 : A_2}\ (\Rightarrow E)$$

$$\frac{\Gamma \vdash M : A}{\Gamma \vdash \lambda X.M : \forall X.A}\ (\forall I)^\star \qquad \frac{\Gamma \vdash M : \forall X.A}{\Gamma \vdash M A_1 : A[X := A_1]}\ (\forall E)$$

where $(\forall I)^\star$ denotes the eigenvariable condition $X \notin FV(\Gamma)$

3 Minimal logic with second order sum

Next, we introduce the counter calculus $\lambda^\exists$ as minimal logic consisting of negations, conjunctions and second order sums. Such a calculus seems to be logically weak and has never been considered as far as we know. However, $\lambda^\exists$ turns out strong enough to interpret $\lambda 2$ and interesting to investigate polymorphism.

Definition 5 (Types)

$$A ::= \bot \mid X \mid \neg A \mid A \wedge A \mid \exists X.A$$

Definition 6 (Pseudo-terms)

$$\begin{aligned}\Lambda^\exists \ni M \quad ::= \quad & x \mid \lambda x\!:\!A.M \mid MM \\ & \mid \langle M, M\rangle \mid \texttt{let}\ \langle x, x\rangle = M\ \texttt{in}\ M \\ & \mid \langle A, M\rangle_{\exists X.A} \mid \texttt{let}\ \langle X, x\rangle = M\ \texttt{in}\ M\end{aligned}$$

Definition 7 (Reduction rules) (β) $(\lambda x\!:\!A.M)M_1 \to M[x := M_1]$

(η) $\lambda x\!:\!A.Mx \to M$ if $x \notin FV(M)$

$(\texttt{let}_\wedge)$ $\texttt{let}\ \langle x_1, x_2\rangle = \langle M_1, M_2\rangle\ \texttt{in}\ M \ \to\ M[x_1 := M_1, x_2 := M_2]$

$(\texttt{let}_{\wedge_\eta})$ $\texttt{let}\ \langle x_1, x_2\rangle = M_1\ \texttt{in}\ M[z := \langle x_1, x_2\rangle] \ \to\ M[z := M_1]$
if $x_1, x_2 \notin FV(M)$

$(\texttt{let}_\exists)$ $\texttt{let}\ \langle X, x\rangle = \langle A_1, M_2\rangle_{\exists X.A}\ \texttt{in}\ M \ \to\ M[X := A_1, x := M_2]$

$(\texttt{let}_{\exists_\eta})$ $\texttt{let}\ \langle X, x\rangle = M_1\ \texttt{in}\ M[z := \langle X, x\rangle] \ \to\ M[z := M_1]$
if $X, x \notin FV(M)$

A simultaneous substitution for free variables x_1, x_2 or X, x is denoted by $[x_1 := M_1, x_2 := M_2]$ or $[X := A, x := M]$, respectively. We also write $=_{\lambda^\exists}$ for the reflexive, symmetric and transitive closure of the one step reduction $\to_{\lambda^\exists}$ defined above. We may sometimes omit type annotations from terms.

Definition 8 (Type assignment rules)

$$\frac{x\!:\!A \in \Gamma}{\Gamma \vdash x : A}$$

$$\frac{\Gamma, x{:}A \vdash M : \bot}{\Gamma \vdash \lambda x{:}A.M : \neg A}\ (\neg I) \qquad \frac{\Gamma \vdash M_1 : \neg A \quad \Gamma \vdash M_2 : A}{\Gamma \vdash M_1 M_2 : \bot}\ (\neg E)$$

$$\frac{\Gamma \vdash M_1 : A_1 \quad \Gamma \vdash M_2 : A_2}{\Gamma \vdash \langle M_1, M_2 \rangle : A_1 \wedge A_2}\ (\wedge I)$$

$$\frac{\Gamma \vdash M_1 : A_1 \wedge A_2 \quad \Gamma, x_1{:}A_1, x_2{:}A_2 \vdash M : A}{\Gamma \vdash \mathtt{let}\ \langle x_1, x_2 \rangle = M_1\ \mathtt{in}\ M : A}\ (\wedge E)$$

$$\frac{\Gamma \vdash M : A[X := A_1]}{\Gamma \vdash \langle A_1, M \rangle_{\exists X.A} : \exists X.A}\ (\exists I) \qquad \frac{\Gamma \vdash M_1 : \exists X.A_1 \quad \Gamma, x{:}A_1 \vdash M : A}{\Gamma \vdash \mathtt{let}\ \langle X, x \rangle = M_1\ \mathtt{in}\ M : A}\ (\exists E)^\star$$

where $(\exists E)^\star$ denotes the eigenvariable condition $X \notin FV(\Gamma, A)$

4 CPS-translation and soundness

For a CPS-translation from $\lambda 2$-calclus into $\lambda^{\exists}$-calculus, we define an embedding of types (types for denotations of proof terms), denoted by A^k, and types for continuations, denoted by A^*, which also work for denotation of $\lambda 2$-types.

Definition 9 (Embedding of types)
$A^k = \neg A^*$

Definition 10 (Types for continuations and denotation of types)

(1) $X^* = X$

(2) $(A_1 \Rightarrow A_2)^* = A_1^k \wedge A_2^*$

(3) $(\forall X.A)^* = \exists X.A^*$

The definition above inherits the propositional case from Hofmann-Streicher [HS97] and Selinger [Seli01]. The operator $*$ exactly takes logical duality when one reads $A_1 \Rightarrow A_2$ as $\neg A_1 \vee A_2$. It is remarked that in terms of classical logic, we have $(A_1 \Rightarrow A_2)^k \leftrightarrow (A_2^* \Rightarrow A_1^*)$, which means that a function is interpreted as an inverse function over continuations.

Lemma 1 *We have* $A^*[X := A_1^*] = (A[X := A_1])^*$ *and* $(A[X := A_1])^k = A^k[X := A_1^*]$.

Proof. By induction on the structure of A. □

The definition of denotation of proof terms, denoted by $[\![M]\!]$, is given by induction on the typing derivation of M.

Definition 11 (Denotation of $\lambda 2$-terms)

(i) $[\![x]\!] = x \quad$ *if* $\Gamma \vdash x : A$

(ii) $[\![\lambda x{:}A_1.M]\!] = \lambda k{:}(A_1 \Rightarrow A_2)^*.(\mathtt{let}\ \langle x, c \rangle = k\ \mathtt{in}\ [\![M]\!]c)$
if $\Gamma \vdash \lambda x{:}A_1.M : A_1 \Rightarrow A_2$

(iii) $[\![M_1 M_2]\!] = \lambda a\!:\!A_2^*.[\![M_1]\!]\langle[\![M_2]\!], a\rangle$
if $\Gamma \vdash M_1 M_2 : A_2$

(iv) $[\![\lambda X.M]\!] = \lambda k\!:\!(\forall X.A)^*.(\texttt{let } \langle X, c\rangle = k \texttt{ in } [\![M]\!]c)$
if $\Gamma \vdash \lambda X.M : \forall X.A$

(v) $[\![M A_1]\!] = \lambda k\!:\!(A[X := A_1])^*.[\![M]\!]\langle A_1^*, k\rangle_{\exists X.A^*}$
if $\Gamma \vdash M A_1 : A[X := A_1]$

The definition above interprets each proof term with type A as a functional element with type A^k (space of denotations of type A), which takes, as an argument, a continuation with type A^*. The cases of application say that continuations are in the form of a pair $\langle[\![M]\!], a\rangle$ or $\langle A^*, a\rangle$ consisting of a denotation and a continuation in this order. The cases of λ-abstraction mean that after the interpretation, λ-abstraction is waiting for a first component of a continuation (i.e., a denotation of its argument), and the second component becomes a rest continuation to the result. It should be remarked that $(\forall I)$ and $(\forall E)$ are respectively interpreted by dual $(\exists E)$ and $(\exists I)$, i.e., we call proof duality.

We may simply write $\langle R_1, R_2, \ldots, R_n, M\rangle$ for $\langle R_1, \langle R_2, \ldots, R_n, M\rangle\rangle$, where we let $\langle M\rangle \equiv M$, and R_i is either M or A.

Example 1 *Let $xM_1 \cdots M_n$ be with type A_{m+1} and A be $A_1 \Rightarrow \cdots \Rightarrow A_{m+1}$:*

$$\begin{aligned}
&[\![\lambda x_1\!:\!A_1 \ldots \lambda x_m\!:\!A_m.xM_1 \cdots M_n]\!] \\
&\quad \to_\beta^+ \ \lambda k_1\!:\!A^*.\ \texttt{let } \langle x_1, k_2\rangle = k_1 \texttt{ in} \\
&\qquad\qquad\qquad \texttt{let } \langle x_2, k_3\rangle = k_2 \texttt{ in} \\
&\qquad\qquad\qquad \ldots \\
&\qquad\qquad\qquad \texttt{let } \langle x_m, k_{m+1}\rangle = k_m \texttt{ in } x\langle[\![M_1]\!], \ldots, [\![M_n]\!], k_{m+1}\rangle \\
&\qquad\qquad \textit{where } k_i : A_i^k \wedge (A_{i+1} \Rightarrow \cdots \Rightarrow A_{m+1})^*
\end{aligned}$$

Lemma 2 *We have* $[\![M[x := N]]\!] = [\![M]\!][x := [\![N]\!]]$ *and* $[\![M[X := A]]\!] = [\![M]\!][X := A^*]$.

Proposition 1 (Soundness)

(i) *If we have $\Gamma \vdash_{\lambda 2} M : A$, then $\Gamma^k \vdash_{\lambda\exists} [\![M]\!] : A^k$.*

(ii) *For well-typed $M_1, M_2 \in \Lambda 2$, if we have $M_1 \to_{\lambda 2} M_2$ then $[\![M_1]\!] \to_{\lambda\exists}^+ [\![M_2]\!]$.*

Proof. If we have $\Gamma \vdash M : A$, then $\Gamma^k \vdash [\![M]\!] : A^k$ by induction on the derivation together with Definition 11. We show two cases of (1) $\lambda X.M$ and (2) MA.
(1) Suppose the following figure of $\lambda 2$, where X is never free in the context Γ.

$$\frac{M : A}{\lambda X.M : \forall X.A}\ (\forall I)^*$$

Then we have the proof figure of $\lambda^{\exists}$, where the eigenvariable condition of $(\exists E)$ can be guaranteed by that of $(\forall I)$.

$$\dfrac{\dfrac{[k:\exists X.A^*] \qquad \dfrac{[\![M]\!]:A^k \quad [c:A^*]}{[\![M]\!]c:\bot}}{\mathtt{let}\ \langle X,c\rangle = k\ \mathtt{in}\ [\![M]\!]c:\bot}(\exists E)^*}{\lambda k{:}(\exists X.A^*).(\mathtt{let}\ \langle X,c\rangle = k\ \mathtt{in}\ [\![M]\!]c):(\forall X.A)^k}$$

(2) Suppose that

$$\dfrac{M:\forall X.A}{MA_1:A[X:=A_1]}(\forall E)$$

Then we have the following proof figure:

$$\dfrac{\dfrac{[\![M]\!]:(\forall X.A)^k \qquad \dfrac{[a:(A[X:=A_1])^* = A^*[X=A_1^*]]}{\langle A_1^*,a\rangle_{\exists X.A^*}:\exists X.A^*}(\exists I)}{[\![M]\!]\langle A_1^*,a\rangle_{\exists X.A^*}:\bot}}{\lambda a{:}(A[X:=A_1])^*.[\![M]\!]\langle A_1^*,a\rangle_{\exists X.A^*}:(A[X:=A_1])^k}$$

The other cases for $(\Rightarrow I)$ and $(\Rightarrow E)$ are the same as above.

Next, we can prove that if we have $M_1 \to_{\lambda 2} M_2$ then $[\![M_1]\!] \to^+_{\lambda^{\exists}} [\![M_2]\!]$ by induction on the derivation of well-typed terms. We show the cases of (3) (β_t) where $\lambda X.M : \forall X.A$ and (4) (η_t).

(3) $[\![(\lambda X.M)A_1]\!]$

$$\begin{array}{ll}
= & \lambda a{:}(A[X:=A_1])^*.(\lambda k{:}(\exists X.A^*).(\mathtt{let}\ \langle X,c\rangle = k\ \mathtt{in}\ [\![M]\!]c))\langle A_1^*,a\rangle \\
\to_\beta & \lambda a{:}(A[X:=A_1])^*.(\mathtt{let}\ \langle X,c\rangle = \langle A_1^*,a\rangle\ \mathtt{in}\ [\![M]\!]c) \\
\to_{\mathtt{let}_\exists} & \lambda a{:}(A[X:=A_1])^*.[\![M]\!][X:=A_1^*]a \\
= & \lambda a{:}(A[X:=A_1])^*.[\![M[X:=A_1]]\!]a \quad \text{from Lemma 1} \\
\to_\eta & [\![M[X:=A_1]]\!]
\end{array}$$

(4) $[\![\lambda X.MX]\!]$

$$\begin{array}{ll}
= & \lambda k{:}(\forall X.A)^*.(\mathtt{let}\ \langle X,c\rangle = k\ \mathtt{in}\ (\lambda a{:}(A[X:=X])^*.[\![M]\!]\langle X,a\rangle)c) \\
\to_\beta & \lambda k{:}(\forall X.A)^*.(\mathtt{let}\ \langle X,c\rangle = k\ \mathtt{in}\ [\![M]\!]\langle X,c\rangle) \\
\to_{\mathtt{let}_{\exists_\eta}} & \lambda k{:}(\forall X.A)^*.[\![M]\!]k \\
\to_\eta & [\![M]\!]
\end{array}$$

□

5 Inverse translation and Galois embedding

We introduce a generation rule of $\mathcal{R}$ *à la* [SF93], which describes the image of the CPS-translation closed under the reduction rules. We write $R \in \mathcal{R}, \mathcal{R}^*$ for both $R \in \mathcal{R}$ and $R \in \mathcal{R}^*$, and $R_1, \ldots, R_n \in \mathcal{R}$ for $R_i \in \mathcal{R}$ $(1 \le i \le n)$.

Definition 12 (Inductive Generation of $\mathcal{R}$)

$$x \in \mathcal{R}, \mathcal{R}^* \qquad\qquad A^* \in \mathcal{R}^*$$

$$\frac{R \in \mathcal{R} \qquad R_1, \ldots, R_n \in \mathcal{R}^* \qquad a \notin FV(RR_1 \ldots R_n) \quad n \geq 0}{\lambda a.R\langle R_1, \ldots, R_n, a\rangle \in \mathcal{R}, \mathcal{R}^*}$$

$$\frac{\lambda a.W, R_1 \in \mathcal{R} \qquad R_2, \ldots, R_n \in \mathcal{R}^* \qquad b \notin FV(R_1 \ldots R_n W) \quad n \geq 0}{\lambda b.(\texttt{let } \langle x, a\rangle = \langle R_1, \ldots, R_n, b\rangle \texttt{ in } W) \in \mathcal{R}, \mathcal{R}^*}$$

$$\frac{\lambda a.W \in \mathcal{R} \qquad A_1^*, R_2, \ldots, R_n \in \mathcal{R}^* \qquad b \notin FV(R_2 \ldots R_n W) \quad n \geq 0}{\lambda b.(\texttt{let } \langle X, a\rangle = \langle A_1^*, R_2, \ldots, R_n, b\rangle \texttt{ in } W) \in \mathcal{R}, \mathcal{R}^*}$$

From the inductive definition above, $R \in \mathcal{R}$ is in the form of either x or $\lambda a.W$ for some W. It is important that terms with the pattern of $\lambda a.W \in \mathcal{R}$ have the form such that the continuation variable a appears exactly once in W (linear continuation), since our source calculus is intuitionistic.

Lemma 3 (Subject reduction property w.r.t. $\mathcal{R}$) *The category $\mathcal{R}$ is closed under the reduction rules of $\lambda^{\exists}$.*

Proof. Substitutions associated to the reduction rules are closed with respect to $\mathcal{R}$. □

Typing rules for $R \in \mathcal{R}$ are defined in terms of those for $\lambda^{\exists}$ as follows, denoted by $\vdash_{\lambda^{\exists}_{\mathcal{R}}}$. Here, we write R or $\lambda a.W$ for denotations with type A^k, and C_a for continuations with type A^*, where C_a contains exactly one occurrence of the continuation variable a at the tail position:

$$C_a ::= a \mid \langle R, C_a\rangle \mid \langle A^*, C_a\rangle_{\exists X.A^*}$$

$$R ::= x \mid \lambda a.RC_a \mid \lambda a.\texttt{let } \langle x, a\rangle = C_a \texttt{ in } W \mid \lambda a.\texttt{let } \langle X, a\rangle = C_a \texttt{ in } W$$

where we write W for $R \equiv \lambda a.W$.

Definition 13 (Typing rules for $\mathcal{R}$)

$$\frac{x : A^k \in \Gamma^k}{\Gamma^k \vdash x : A^k} \qquad \frac{}{\Gamma^k, a : A^* \vdash a : A^*}$$

$$\frac{\Gamma^k \vdash R : A^k \quad \Gamma^k, a : A_1^* \vdash C_a : B^*}{\Gamma^k, a : A_1^* \vdash \langle R, C_a\rangle : (A \Rightarrow B)^*} (\wedge I) \qquad \frac{\Gamma^k, a : A_1^* \vdash C_a : A^*[X := B^*]}{\Gamma^k, a : A_1^* \vdash \langle B^*, C_a\rangle_{\exists X.A^*} : (\forall X.A)^*} (\exists I)$$

$$\frac{\Gamma^k \vdash R : A^k \quad \Gamma^k, a : A_1^* \vdash C_a : A^*}{\Gamma^k \vdash \lambda a : A_1^*.RC_a : A_1^k} (\neg EI)$$

$$\frac{\Gamma^k, x\!:\!A^k \vdash \lambda b\!:\!B^*.W : B^k \quad \Gamma^k, a\!:\!A_1^* \vdash C_a : (A \Rightarrow B)^*}{\Gamma^k \vdash \lambda a\!:\!A_1^*.\mathtt{let}\ \langle x, b\rangle = C_a\ \mathtt{in}\ W : A_1^k}\ (\wedge E)$$

$$\frac{\Gamma^k \vdash \lambda b\!:\!B^*.W : B^k \quad \Gamma^k, a\!:\!A_1^* \vdash C_a : (\forall X.B)^*}{\Gamma^k \vdash \lambda a\!:\!A_1^*.\mathtt{let}\ \langle X, b\rangle = C_a\ \mathtt{in}\ W : A_1^k}\ (\exists E)^\star$$

where $(\exists E)^\star$ denotes the eigenvariable condition $X \notin FV(\Gamma)$.

Lemma 4 (Subject reduction property w.r.t. types) *If we have $R_1 : A^k$ and $C_1 : B^*$, respectively, together with $R_1 \to_{\lambda^\exists}^* R_2$ and $C_1 \to_{\lambda^\exists}^* C_2$, then we also have $R_2 : A^k$ and $C_2 : B^*$.*

Proof. The calculus $\lambda^\exists$ has the subject reduction property. □

Following the patterns of $\lambda a.W \in \mathcal{R}$, we now give the definition of the inverse translation $\sharp$ as $(\lambda a.W)^\sharp = W^\sharp$.

Definition 14 (Inverse translation $\sharp$ for $\mathcal{R}$) (i) $x^\sharp = x$; $\quad (A^*)^\sharp = A$

(ii) $(R\langle R_1, \ldots, R_n, a\rangle)^\sharp = R^\sharp R_1^\sharp \ldots R_n^\sharp$

(iii)
- $(\mathtt{let}\ \langle x, c\rangle = \langle R_1, \ldots, R_n, a\rangle\ \mathtt{in}\ W)^\sharp = (\lambda x.W^\sharp)R_1^\sharp \ldots R_n^\sharp$
- $(\mathtt{let}\ \langle X, c\rangle = \langle R_1, \ldots, R_n, a\rangle\ \mathtt{in}\ W)^\sharp = (\lambda X.W^\sharp)R_1^\sharp \ldots R_n^\sharp$

Proposition 2 (Completeness1) (1) *If we have $\Gamma^k \vdash_{\lambda^\exists_\mathcal{R}} R : A^k$, then $\Gamma \vdash_{\lambda 2} R^\sharp : A$.*

(2) *If we have $\Gamma^k, a\!:\!A^* \vdash_{\lambda^\exists_\mathcal{R}} C_a : B^*$, then $\Gamma, x\!:\!B \vdash_{\lambda 2} (\lambda a.xC_a)^\sharp : A$.*

Proof. By simultaneous induction on the derivations. □

Let (η_a^-) be an η-expansion: $R \to \lambda a\!:\!A^*.Ra$ where $a \notin FV(R)$ and $R \in \mathcal{R}$. Then the set of well-typed $\mathcal{R}$ becomes the image of the CPS-translation closed under the reduction rules, called *Univ*.

Definition 15 (Universe of the CPS-translation)

$$Univ \stackrel{\text{def}}{=} \{P \in \Lambda^\exists \mid [\![M]\!] \to_{\lambda^\exists \eta_a^-}^* P \text{ for some well-typed } M \in \Lambda 2\}$$

Lemma 5 *Univ is generated by $\mathcal{R}$, i.e., Univ $\subseteq \mathcal{R}$.*

Proof. For well typed $M \in \Lambda 2$, we have $[\![M]\!] \in \mathcal{R}$, and moreover $\mathcal{R}$ is closed under (η_a^-) and the reduction rules by Lemma 3. □

Lemma 6 *For any $P \in Univ$, we have some Γ and A such that $\Gamma^k \vdash_{\lambda^\exists} P : A^k$.*

Proof. From the definition of *Univ*, Proposition 1 and Lemma 4. □

Proposition 3 (1) *Let $M \in \Lambda 2$ be a well-typed term. Then we have that $[\![M]\!]^\sharp \equiv M$.*

(2) *Let $P \in \mathcal{R}$ be well-typed. Then we have that $[\![P^\sharp]\!] \to^*_{\beta\eta_a^-} P$.*

(3) *If $P \in \mathcal{R}$ is a normal form of $\lambda^\exists$, then $P^\sharp$ is a normal form of $\lambda 2$.*

Proof.

(1) By induction on the structure of well-typed $M \in \Lambda 2$.

(2) By case analysis on $P \in \mathit{Univ}$, following the definition of $\sharp$.

(3) Following the cases of (i), (ii) and (iii) of the definition of $\sharp$.

- Case of (ii):
  Let P be $\lambda a{:}A^*.R\langle R_1,\dots,R_n,a\rangle$. Since P is a normal form of $\lambda^\exists$, we have $R \equiv x$ and R_i is also in normal with $n \geq 1$, to say, R_i^{nf}. Then we have normal $P^\sharp = x(R_1^{nf})^\sharp \dots (R_n^{nf})^\sharp$.
- Case of (iv) with $n = 0$:
  Let P be $\lambda a{:}A^*.(\texttt{let}\ \langle x,c\rangle = a\ \texttt{in}\ W)$. Since P is in normal, so is W without ($\texttt{let}_{\wedge_\eta}$) nor ($\texttt{let}_{\exists_\eta}$) redexes, to say, W^{nf}. Then we have normal $P^\sharp = \lambda x.(W^{nf})^\sharp$.

□

Proposition 4 *We have $\mathit{Univ} = \mathcal{R}$ with respect to well-typed terms.*

Proof. We have $\mathit{Univ} \subseteq \mathcal{R}$ from Lemma 5. Let $P \in \mathcal{R}$ be well-typed. Then $P^\sharp \in \Lambda 2$ is well-typed from Proposition 2. Proposition 3 implies that $[\![P^\sharp]\!] \to^*_{\beta\eta_a^-} P$, and hence $P \in \mathit{Univ}$. Therefore we have $\mathcal{R} \subseteq \mathit{Univ}$. □

Lemma 7 $(W[a := \langle\langle R_1,\dots,R_m,b\rangle\rangle])^\sharp = W^\sharp R_1^\sharp,\dots,R_n^\sharp$ *provided $a \in FV(W)$.*

Proof. Following the case analysis on the definition $\sharp$. We show one case of $W = (\texttt{let}\ \langle x,c\rangle = C_a\ \texttt{in}\ W')$, where $C_a = \langle S_1,\dots,S_n,a\rangle$. Let θ be $[a := \langle R_1,\dots,R_n,b\rangle]$. We have $W\theta = (\texttt{let}\ \langle x,c\rangle = \langle S_1,\dots,S_n,R_1,\dots,R_m,b\rangle\ \texttt{in}\ W')$, and then we have $(W\theta)^\sharp = (\lambda x.(W')^\sharp)S_1^\sharp \dots S_n^\sharp R_1^\sharp \dots R_m^\sharp = (W)^\sharp R_1^\sharp \dots R_m^\sharp$. □

Proposition 5 (Completeness2) *Let $P, Q \in \mathit{Univ}$.*

(1) *If $P \to_\beta Q$ then $P^\sharp \equiv Q^\sharp$.*

(2) *If $P \to_\eta Q$ then $P^\sharp \equiv Q^\sharp$.*

(3) *If $P \to_{\texttt{let}_\wedge} Q$ then $P^\sharp \to_\beta Q^\sharp$.*

(4) *If $P \to_{\texttt{let}_\exists} Q$ then $P^\sharp \to_{\beta_t} Q^\sharp$.*

(5) *If $P \to_{\texttt{let}_{\wedge_\eta}} Q$ then $P^\sharp \to_\eta Q^\sharp$.*

(6) *If* $P \to_{\mathtt{let}\exists_\eta} Q$ *then* $P^\sharp \to_{\eta_t} Q^\sharp$.

Proof. By induction on the structure of P, following the case analysis on the definition $\sharp$. The cases (1,2) are straightforward. We show some of the cases;
(4):
Let P be $\lambda a.\mathtt{let}\ \langle X, c\rangle = \langle A^*, R_1, \ldots, R_n, a\rangle\ \mathtt{in}\ W$.

$$\begin{array}{rcl} P^\sharp & = & (\lambda X.W^\sharp)AR_1^\sharp \ldots R_n^\sharp \\ & \to_{\beta_t} & W^\sharp[X := A]R_1^\sharp \ldots R_n^\sharp \\ & = & (W[X := A])^\sharp R_1^\sharp \ldots R_n^\sharp = (W[X := A][c := \langle R_1, \ldots, R_n, a\rangle])^\sharp \end{array}$$

(6): Let P be $\lambda a.\mathtt{let}\ \langle X, c\rangle = a\ \mathtt{in}\ R\langle R_1, \ldots, R_n, X, c\rangle$ where $X, c \notin FV(RR_1 \ldots R_n)$.

$$P^\sharp = \lambda X.R^\sharp R_1^\sharp \ldots R_n^\sharp X \to_{\eta_t} R^\sharp R_1^\sharp \ldots R_n^\sharp$$

Let Q be $\lambda a.\mathtt{let}\ \langle X, c\rangle = a\ \mathtt{in}\ \mathtt{let}\ \langle Y, b\rangle = \langle R_1, \ldots, R_n, X, c\rangle\ \mathtt{in}\ W$ where $X, c \notin FV(R_1 \ldots R_n W)$.

$$Q^\sharp = \lambda X.(\lambda Y.W^\sharp)R_1^\sharp \ldots R_n^\sharp X \to_{\eta_t} (\lambda Y.W^\sharp)R_1^\sharp \ldots R_n^\sharp$$

□

Theorem 1 (i) $\Gamma \vdash_{\lambda 2} M : A$ *if and only if* $\Gamma^k \vdash_{\lambda\exists} [\![M]\!] : A^k$.

(ii) $P \in Univ$ *if and only if* $\Gamma \vdash_{\lambda 2} P^\sharp : A$ *for some* Γ, A.

(iii) *Let* M_1, M_2 *be well-typed* $\lambda 2$*-terms.*
$M_1 =_{\lambda 2} M_2$ *if and only if* $[\![M_1]\!] =_{\lambda\exists} [\![M_2]\!]$.
In particular, $M_1 \to_{\lambda 2} M_2$ *if and only if* $[\![M_1]\!] \to_\beta \to_{\mathtt{let}} \to_\eta [\![M_2]\!]$.

(iv) *Let* $P_1, P_2 \in Univ$. $P_1 =_{\lambda\exists} P_2$ *if and only if* $P_1^\sharp =_{\lambda 2} P_2^\sharp$.

Proof. (i,ii) From Propositions 1 and 2. (iii, iv) From Propositions 1 and 5. □

Theorem 2 *The inverse translation* $\sharp : Univ \to \Lambda 2$ *is bijective, in the following sense:*

(1) *If we have* $P_1^\sharp =_{\lambda 2} P_2^\sharp$ *then* $P_1 =_{\lambda\exists} P_2$ *for* $P_1, P_2 \in Univ$.

(2) *For any well-typed* $M \in \Lambda 2$*, we have some* $P \in Univ$ *such that* $P^\sharp \equiv M$.

Proof. Let M be a well-typed term of $\Lambda 2$. Then we can take P as $[\![M]\!]$, so that we have $P^\sharp \equiv M$. □

Definition 16 (Galois connection) Let $\to_S^*$ and $\to_T^*$ be pre-orders on S and T respectively, and $f : S \to T$ and $g : T \to S$ be maps. Two maps f and g form a Galois connection between S to T whenever $f(M) \to_T^* P$ if and only if $M \to_S^* g(P)$, see also [SW97].

It is known that the definition above is equivalent to the following clauses:

(i) $M \rightarrow_S^* g(f(M))$

(ii) $f(g(P)) \rightarrow_T^* P$

(iii) $M_1 \rightarrow_S^* M_2$ implies $f(M_1) \rightarrow_T^* f(M_2)$

(iv) $P_1 \rightarrow_T^* P_2$ implies $g(P_1) \rightarrow_S^* g(P_2)$

Definition 17 (Galois embedding) Two maps f and g form a Galois embedding into T if they form a Galois connection and $g(f(M)) \equiv M$.

Theorem 3 *The translations* $[\![\ ]\!]$ *and* $\sharp$ *form a Galois connection between* $\lambda 2$ *and Univ, and moreover, they establish a Galois embedding into Univ.*

Proof. From Propositions 1, 3, and 5. □

It is remarked that a Galois embedding is the dual notion of a reflection: f and g form a reflection in S if they form a Galois connection and $f(g(P)) \equiv P$. In fact, let $M \rightarrow^- N$ (expansion) be $N \rightarrow M$ (reduction). Then $\rightarrow^{-*}$ is a pre-order, and $\langle \sharp, [\![\ ]\!], \rightarrow_{\lambda^\exists}^{-*}, \rightarrow_{\lambda 2}^{-*} \rangle$ forms a reflection.

Let $\sharp Univ$ be $\{P^\sharp \mid P \in Univ\}$. Let $[\![\sharp Univ]\!]$ be $\{[\![M]\!] \mid M \in \sharp Univ\}$.

Corollary 1 (Kernel of $\Lambda 2$) *For any* $P \in [\![\sharp Univ]\!]$, *we have* $P \equiv [\![P^\sharp]\!]$.

Proof. Let $\Lambda 2$ be a set of well-typed $\lambda 2$-terms. From the theorem above, we have $\sharp Univ = \Lambda 2$ and $[\![\sharp Univ]\!] = [\![\Lambda 2]\!]$. Hence, any $P \in [\![\Lambda 2]\!]$ is in the form $P \equiv [\![M]\!]$ for some $M \in \Lambda 2$, such that $[\![P^\sharp]\!] \equiv [\![[\![M]\!]^\sharp]\!] \equiv [\![M]\!] \equiv P$. □

Corollary 2 (Normalization of $\Lambda 2$) *The weak normalization of* $\lambda 2$ *is inherited from that of* $\lambda^\exists$ $(\lambda^\exists_{\mathcal{R}})$. Moreover, the strong normalization of $\lambda 2$ is implied by that of $\lambda^\exists$ $(\lambda^\exists_{\mathcal{R}})$.

Proof. The weak normalization of $\lambda 2$ is implied by Theorem 3 ($[\![\ ]\!]$ and $\sharp$ form a Galois connection) together with Proposition 3. The strong normalization of $\lambda 2$ is implied by Proposition 1 (soundness). □

Corollary 3 (Church-Rosser of $\Lambda 2$) *The Church-Rosser property of* $\lambda 2$ *is inherited from that of* $\mathcal{R}$.

Proof. The Church-Rosser property of $\lambda 2$ is implied by Theorem 3. □

We remark that the system $\lambda^\exists$ can be regarded logically as a subsystem of F, in the sense that the connectives $\wedge$ and $\exists$ together with the reduction rules can be coded by universal types of F [GTL89]. Our result, in turn, means that universal types can be interpreted by the use of existential types. Moreover, proof duality appears in the proof such that $(\forall I) \leftrightarrow (\exists E)$ and $(\forall E) \leftrightarrow (\exists I)$.

6 Proof duality between polymorphic functions and abstract data types

We discuss the proof duality in detail. If we have $\Gamma \vdash_{\lambda 2} A$ in $\lambda 2$, then classical logic has $A^* \vdash \Gamma^*$, turning assumptions into conclusions and vice versa. In terms of intuitionistic logic, we can expect that $\neg\Gamma^*, A^* \vdash \bot$. In fact, we have $\neg\Gamma^*, a\!:\!A^* \vdash_{\lambda^\exists} \underline{\underline{M}} : \bot$ if $\Gamma \vdash_{\lambda 2} M : A$, under the following definition.

Definition 18 (Modified CPS-translation)

(i) $\underline{\underline{x}} = xa$

(ii) $\underline{\underline{\lambda x\!:\!A_1.M}} = \mathtt{let}\ \langle x, a\rangle = a\ \mathtt{in}\ \underline{\underline{M}}$

(iii) $\underline{\underline{M_1 M_2}} = \underline{\underline{M_1}}[a := \langle \lambda a\!:\!A_1^*.\underline{\underline{M_2}}, a\rangle]$ for $M_2 : A_1$

(iv) $\underline{\underline{\lambda X.M}} = \mathtt{let}\ \langle X, a\rangle = a\ \mathtt{in}\ \underline{\underline{M}}$

(v) $\underline{\underline{MA_1}} = \underline{\underline{M}}[a := \langle A_1^*, a\rangle]$

Lemma 8 *Let $M \in \Lambda 2$ be a well-typed term.*

(1) *We have $[\![M]\!]a \to^*_{\beta\eta_a^-} \underline{\underline{M}}$ and $[\![M]\!] \to^*_{\beta\eta_a^-} \lambda a.\underline{\underline{M}}$.*

(2) $[\![M]\!]^\sharp = (\underline{\underline{M}})^\sharp \equiv M$

(3) *If M is a normal form of $\lambda 2$, then $\underline{\underline{M}}$ is a normal form of $\lambda^\exists$ without (η_a). The form of normal $\underline{\underline{M}}$ without (η_a) is described by NF as follows:*

$$
\begin{array}{rcl}
NF & ::= & xa \\
 & & \mid \mathtt{let}\ \langle \chi, a\rangle = k\ \mathtt{in}\ \mathtt{let}\ \langle \chi, a\rangle = k\ \mathtt{in}\ \ldots \\
 & & \ \ \mathtt{let}\ \langle \chi, a\rangle = k\ \mathtt{in}\ x\langle Nf, \ldots, Nf, a\rangle
\end{array}
$$

where $Nf ::= A^* \mid \lambda a.NF$, and we write χ for either x or X.

Proof. By induction on the structure of M, and Proposition 3. □

The notion of path is defined as in Prawitz [Pra65], together with inference rules.

Definition 19 (Path) A sequence consisting of formulae and inference rules $A_1(R_1)A_2(R_2)\ldots A_{n-1}(R_{n-1})A_n$ is defined as a path in the deduction Π of $\lambda 2$ or $\lambda^\exists$, as follows:

(i) A_1 is a top-formula in Π;

(ii) A_i $(i < n)$ is not the minor premiss of an application of $(\Rightarrow E)$ or $(\neg E)$, and either

1) A_i is not a major premiss of $(\wedge E)$ or $(\exists E)$, and A_{i+1} is the formula occurrence immediately below A_i by an application of (R_i), or

2) A_i is the major premiss of an application of $(\wedge E)$ or $(\exists E)$, and A_{i+1} is the assumption discharged in Π by $(\wedge E)$ or $(\exists E)$, to say, (R_i);

(iii) A_n is either a minor premiss of $(\Rightarrow E)$ or $(\neg E)$, or the end-formula of Π.

We write (I) for either $(\Rightarrow I)$ or $(\forall I)$, and (E) for either $(\Rightarrow E)$ or $(\forall E)$. We also define inference rule correspondence as follows: $(\Rightarrow I)^* = (\wedge E)$, $(\Rightarrow E)^* = (\wedge I)$, $(\forall I)^* = (\exists E)$, $(\forall E)^* = (\exists I)$.

Theorem 4 (Proof duality) *Let Π be a normal deduction of $\Gamma \vdash_{\lambda 2} M : A$, and let π be a path $A_1(E_1)A_2(E_2)\ldots A_i(E_i)A_{i+1}(I_{i+1})\ldots A_{n-1}(I_{n-1})A_n$ in the normal deduction. Then, in the deduction of $\neg\Gamma^*, a : A^* \vdash_{\lambda\exists} \underline{\underline{M}} : \bot$, there exists a path π^*, as follows:*

$$\pi^* = A_n^*(I_{n-1})^*A_{n-1}^* \cdots (I_{i+1})^*A_{i+1}^*\ (E_i)^*A_i^* \ldots (E_2)^*A_2^*(E_1)^*A_1^*.$$

Proof. By induction on the normal derivation of $\Gamma \vdash_{\lambda 2} M : A$. We show here some of the cases:

(0) Case of $n = 1$:

For $x : A$, we have the following deduction:

$$\frac{x : \neg A^* \quad a : A^*}{xa : \bot}\ (\neg E)$$

which means that the corresponding path ends with the minor premiss of $(\neg E)$, just before $\bot$.

(1) A_n $(n = i + 1)$ is derived by an elimination rule.

Case of $(\Rightarrow E)$:

From a normal deduction Π, $(B \Rightarrow A_n)$ cannot be derived by an introduction rule:

$$\frac{\begin{array}{c}\Pi_1\\ M_1 : B \Rightarrow A_n\end{array} \quad \begin{array}{c}\Pi_2\\ M_2 : B\end{array}}{M_1M_2 : A_n}\ (\Rightarrow E)$$

Then we have a path π_1^d from $(B \Rightarrow A_n)^*$, corresponding to the path π_1 to $(B \Rightarrow A_n)$:

$$\begin{array}{c}a : (B \Rightarrow A_n)^*\\ \Sigma_1\\ \underline{\underline{M_1}} : \bot\end{array} \qquad \begin{array}{c}a : B^*\\ \Sigma_2\\ \underline{\underline{M_2}} : \bot\end{array}$$

The figure below says that we have a path $\pi^d = (A_n)^*(\Rightarrow E)^*(B \Rightarrow A_n)^*\pi_1^d$, corresponding to the path $\pi = \pi_1(B \Rightarrow A_n)(\Rightarrow E)(A_n)$:

$$\dfrac{\dfrac{\begin{matrix}[a : B^*] \\ \Sigma_2 \\ \underline{\underline{M_2}} : \bot\end{matrix}}{\lambda a.\underline{\underline{M_2}} : \neg B^*}\ (\neg I) \quad a : A_n^*}{\langle \lambda a.\underline{\underline{M_2}}, a\rangle : \neg B^* \wedge A_n^*}\ (\wedge I)$$
$$\begin{matrix}\Sigma_1 \\ \underline{\underline{M_1}}[a := \langle \lambda a.\underline{\underline{M_2}}, a\rangle] : \bot\end{matrix}$$

Case of $(\exists E)$:

From a normal deduction of Π, $\forall X.A_n$ cannot be derived from an introduction rule:

$$\dfrac{\begin{matrix}\Pi_1 \\ M : \forall X.A_n\end{matrix}}{MB : A_n[X := B]}\ (\forall E)$$

Then we have a path π_1^d from $(\forall X.A_n)^*$, corresponding to the path π_1 to $\forall X.A_n$, as follows:

$$\begin{matrix}a : (\forall X.A_n)^* \\ \Sigma_1 \\ \underline{\underline{M}} : \bot\end{matrix}$$

The following figure shows that we have a path $\pi^d = (A_n[X := B])^*(\forall E)^*(\forall X.A_n)^*\pi_1^d$, corresponding to the path $\pi = \pi_1(\forall X.A_n)(\forall E)(A_n[X := B])$:

$$\dfrac{a : (A_n[X := B])^*}{\langle B^*, a\rangle : \exists X.A_n^*}\ (\exists I)$$
$$\begin{matrix}\Sigma_1 \\ \underline{\underline{M}}[a := \langle B^*, a\rangle] : \bot\end{matrix}$$

(2) A_n $(n = i + 2)$ is derived by an introduction rule.

Case of $(\Rightarrow I)$:

$$\dfrac{\dfrac{\begin{matrix}[x : B] \\ \Pi_1\end{matrix}}{M : A_{n-1}}\ (E)}{\lambda x.M : B \Rightarrow A_{n-1}}\ (\Rightarrow I)$$

Then we have the path π_1^d from A_{n-1}^*, corresponding to the path π_1 to A_{n-1}:

$$\begin{matrix}x : \neg B^* \quad a : A_{n-1}^* \\ \Sigma_1 \\ \underline{\underline{M}} : \bot\end{matrix}$$

Now we have the following figure, so that there exists a path $\pi^d = (B \Rightarrow A_{n-1})^*(\Rightarrow I)^*(A_{n-1}^*)\pi_1^d$, corresponding to the path $\pi = \pi_1(A_{n-1})(\Rightarrow I)(B \Rightarrow A_{n-1})$:

$$\dfrac{a' : \neg B^* \wedge A^*_{n-1} \qquad \begin{array}{c}[x : \neg B^*] \quad [a : A^*_{n-1}] \\ \Sigma_1 \\ \underline{\underline{M}} : \bot\end{array}}{\texttt{let } \langle x, a\rangle = a' \texttt{ in } \underline{\underline{M}} : \bot} (\wedge E)$$

Case of $(\forall I)$:

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1 \\ A_{n-2}\end{array}}{M : A_{n-1}} (E)}{\lambda X.M : \forall X.A_{n-1}} (\forall I)$$

Then we have the path π_1^d from A^*_{n-1}, corresponding to the path π_1 to A_{n-1}, as follows:

$$\begin{array}{c} a : A^*_{n-1} \\ \Sigma_1 \\ \underline{\underline{M}} : \bot \end{array}$$

Now we have the path $\pi^d = (\forall X.A_{n-1})^*(\forall I)^*(A_{n-1})^*\pi_d^1$, corresponding to the path $\pi(A_{n-1})(\forall I)(\forall X.A_{n-1})$ to $\forall X.A_{n-1}$:

$$\dfrac{a' : \exists X.A^*_{n-1} \qquad \begin{array}{c}[a : A^*_{n-1}] \\ \Sigma_1 \\ \underline{\underline{M}} : \bot\end{array}}{\texttt{let } \langle X, a\rangle = a' \texttt{ in } \underline{\underline{M}} : \bot} (\exists E)$$

(3) A_n $(n > i+2)$ is derived by an introduction rule.

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1 \\ A_{n-2}\end{array}}{A_{n-1}} (I_{n-2})}{M : A_n} (I_{n-1})$$

Case I_{n-1} of $(\Rightarrow I)$:

$$\dfrac{\dfrac{\begin{array}{c}[x : A] \\ \Pi_1 \\ A_{n-2}\end{array}}{M : A_{n-1}} (I_{n-2})}{\lambda x.M : A \Rightarrow A_{n-1}} (\Rightarrow I)$$

From the induction hypothesis, there exists the following deduction

$$\dfrac{a : A^*_{n-1} \qquad \begin{array}{c} x : \neg A^* \\ \vdots \\ \bot \end{array}}{\underline{\underline{M}} : \bot} (I_{n-1})^*$$

where we have a path π_1^d from A_{n-1}^*, corresponding to the path π_1 to A_{n-1}. Then in the following deduction:

$$\dfrac{a' : \neg A^* \wedge A_{n-1}^* \qquad \dfrac{[a : A_{n-1}^*] \qquad \begin{array}{c}[x : \neg A^*] \\ \vdots \\ \bot\end{array}}{\underline{\underline{M}} : \bot}\,(I_{n-1})^*}{\mathtt{let}\ \langle x, a\rangle = a'\ \mathtt{in}\ \underline{\underline{M}} : \bot}\,(\Rightarrow I)^*$$

we obtain the path $\pi^d = (A \Rightarrow A_{n-1})^*(\Rightarrow I)^*(A_{n-1})^*\pi_1^d$, corresponding to the path $\pi = \pi_1(A_{n-1})(\Rightarrow I)(A \Rightarrow A_{n-1})$ to $(A \Rightarrow A_{n-1})$.

Case I_{n-1} of $(\forall I)$:

$$\dfrac{\dfrac{\begin{array}{c}\Pi_1 \\ A_{n-2}\end{array}}{M : A_{n-1}}\,(I_{n-2})}{\lambda X.M : \forall X.A_{n-1}}\,(\forall I)$$

Then in the following deduction:

$$\dfrac{a : A_{n-1}^* \qquad \begin{array}{c}\vdots \\ \bot\end{array}}{\underline{\underline{M}} : \bot}\,(I_{n-2})^*$$

we have a path π_1^d from A_{n-1}^*, corresponding to the path π_1 to A_{n-1}. Now the following deduction gives the path $\pi^d = (\forall X.A_{n-1})^*(\forall I)^*(A_{n-1})^*\pi_1^d$, corresponding to the path $\pi = \pi_1(A_{n-1})(\forall I)(\forall X.A_{n-1})$:

$$\dfrac{a' : \exists X.A_{n-1}^* \qquad \dfrac{[a : A_{n-1}^*] \qquad \begin{array}{c}\vdots \\ \bot\end{array}}{\underline{\underline{M}} : \bot}\,(I_{n-2})^*}{\mathtt{let}\ \langle X, a\rangle = a'\ \mathtt{in}\ \underline{\underline{M}} : \bot}\,(\forall I)^*$$

□

It is remarked that from the theorem above, inference rules in a path of normal deductions of $\lambda 2$ are reversely applied in the corresponding path of $\lambda^{\exists}$, under the correspondence between $(\forall I)$ and $(\exists E)$; $(\forall E)$ and $(\exists I)$; etc. Moreover, together with lemma 8, normal forms have the following shape:

$$\begin{array}{lll} NF & ::= & xa \\ & & \mid \mathtt{let}\ \langle \chi, a_1\rangle = a\ \mathtt{in}\ \mathtt{let}\ \langle \chi, a_2\rangle = a_1\ \mathtt{in}\ \ldots \\ & & \ \ \mathtt{let}\ \langle \chi, a_n\rangle = a_{n-1}\ \mathtt{in}\ x\langle Nf, \ldots, Nf, a_n\rangle \end{array}$$

where $Nf ::= A^* \mid \lambda a.NF$.

7 Concluding remarks

It is remarked that $\lambda^{\exists}$ can be regarded as a subsystem of $\lambda 2$, in the sense that $\wedge$ and $\exists$ with reduction rules can be impredicatively coded in $\lambda 2$. We have established a Galois embedding from polymorphic $\lambda 2$ into $\lambda^{\exists}$, in which proof duality appears such that polymorphic functions with $\forall$-type can be interpreted by abstract data types with $\exists$-type [MP85] and vice versa. Moreover, inference rules in a path of normal deductions of $\lambda 2$ are reversely applied in the corresponding dual paths of $\lambda^{\exists}$, under the correspondence between $(\forall I)$ and $(\exists E)$; $(\forall E)$ and $(\exists I)$; etc. The involved CPS-translation is similar to that of [Plot75], [HS97], [Seli01] or [Fuji03]. However, relating to extensionality, the case of conjunction-elimination is essentially distinct from them, and this point is important for the completeness. Although none of two through [Plot75], [HS97] and ours in this paper are $\beta\eta$-equal, we remark that they are isomorphic to each other in the simply typed case, from the work on answer type polymorphism by Thielecke [Thie04]. Our definition of the CPS-translation can work even for polymorphic $\lambda\mu$-calculus (second order classical logic) [Pari92].

Acknowledgements The first auther is grateful to Thierry Coquand, Peter Dybjer, Ryu Hasegawa, Per Martin-Löf and Masahiko Sato for helpful discussions and useful comments. This research has been supported by Grants-in-Aid for Scientific Research (C)(2)14540119, Japan Society for the Promotion of Science and by the Kayamori Foundation of Informational Science Advancement.

References

[Coq86] Th. Coquand: An analysis of Girard's paradox, *Proc. the Annual IEEE Symposium on Logic in Computer Science*, pp. 227–236, 1986.

[Fuji03] K. Fujita: A sound and complete CSP-translation for $\lambda\mu$-Calculus, Lecture Notes in Computer Science 2701, pp. 120–134, 2003.

[Fuji05] K. Fujita: Galois embedding from polymorphic types into existentail types, Lecture Notes in Computer Science 3461, pp. 194–208, 2005.

[GTL89] J-Y. Girard, P. Taylor, and Y. Lafont: *Proofs and Types*, Cambridge University Press, 1989.

[HS97] M. Hofmann and T. Streicher: Continuation models are universal for $\lambda\mu$-calculus, *Proc. the 12th Annual IEEE Symposium on Logic in Computer Science*, pp. 387–395, 1997.

[MP85] J. C. Mitchell and G. D. Plotkin: Abstract types have existential type, *Proc. the 12th Annual ACM Symposium on Principles of Programming Languages*, pp. 37–51, 1985.

[Pari92] M. Parigot: $\lambda\mu$-Calculus: An Algorithmic Interpretation of Classical Natural Deduction, Lecture Notes in Computer Science 624, pp. 190–201, 1992.

[Plot75] G. Plotkin: Call-by-Name, Call-by-Value and the λ-Calculus, *Theoretical Computer Science*, Vol. 1, pp. 125–159, 1975.

[Pra65] D. Prawitz: *NATURAL DEDUCTION, A Proof Theoretical Study*, ALMQVIST&WIKSELL, Stockholm, 1965.

[Seli01] P. Selinger: Control Categories and Duality: on the Categorical Semantics of the Lambda-Mu Calculus, *Math. Struct. in Compu. Science*, Vol. 11, pp. 207–260, 2001.

[SF93] A. Sabry and M. Felleisen: Reasoning about Programs in Continuation-Passing Style, *LISP AND SYMBOLIC COMPUTATION: An International Journal*, Vol. 6, pp. 289–360, 1993.

[SW97] A. Sabry and Ph. Wadler: A reflection on call-by-value, *ACM Transactions on Programming Languages and Systems*, Vol. 19, No. 6, pp. 916–941, 1997.

[Thie04] H. Thielecke: Answer type polymorphism in call-by-name continuation passing, Lecture Notes in Computer Science 2986, pp. 279–293, 2004.

[Wad03] Ph. Wadler: Call-by-value is dual to call-by-name, *International Conference on Functional Programming*, August 25-29, Uppsala, 2003.