Research Paper

Second order permutative conversions with Prawitz's strong validity

Makoto TATSUTA
National Institute of Informatics
The Graduate University for Advanced Studies

ABSTRACT

A clear and complete proof of strong normalization of second order natural deduction with permutative conversions is given by using Prawitz's strong validity. This paper completes Prawitz's original proof.

KEYWORDS

Permutative conversions, strong validity, natural deduction, strong normalization

1 Introduction

Permutative conversions transform a proof with a disjunction or existential quantification elimination rule followed by an elimination rule into a proof with the second rule in the minor deduction of the first rule [14, 21]. Permutative conversions are indispensable for normalizing a proof in a natural deduction system with disjunction or existential quantification. Without permutative conversions, a normal proof fails to have the subformula property, because there may exist an introduction rule of a logical symbol in a minor deduction of a disjunction or existential quantification elimination rule followed by the elimination rule of the same logical symbol, which may break the subformula property.

Strong normalization property is important. First it implies weak normalization property, which proves the subformula property and consistency [14, 21]. In particular, weak normalization of a second order system has been often proved through showing its strong normalization [5, 6]. Secondly, when we consider proof normalization as computation by the proofs-as-programs paradigm [8], strong normalization guarantees termination of programs. Thirdly, it is itself an interesting combinatorial problem in mathematics.

Several papers have studied strong normalization of systems with or without permutative conversions. We summarize them in Table 1. Strong normalization of second order natural deduction with disjunction, existential quantification, and their commutative conversions is proved in [15, 12]. Strong normalization of second order natural deduction with disjunction, first-order existential quantification, and their commutative conversions is proved in [19]. Strong normalization of second order natural deduction with disjunction and existential quantification without their commutative conversions is proved in [5, 6]. Strong normalization of the negative fragment of second order natural deduction is discussed in [4, 7, 11, 20, 21]. Strong normalization of first order natural deduction with disjunction, existential quantification, and their commutative conversions is proved in [10, 20]. Strong normalization of a type theory with Π types, Σ types, and their weak permutative conversions is proved in [18]. Strong normalization of propositional natural deduction with disjunction and commutative conversions is proved in [3, 2, 9].

We will prove strong normalization of second order intuitionistic natural deduction with permutative conversions by using Prawitz's strong validity. This paper completes Prawitz's original proof given in [15].

By Curry-Howard isomorphism [8], a second order logical system corresponds to a functional programming language with polymorphic types and abstract data types. Second order universal quantification gives polymorphic

Received February 12, 2005; Revised July 4, 2005; Accepted July 5, 2005.
tatsuta@nii.ac.jp
DOI : 10.2201/Niipi.2005.2.4.

Table 1 Strong Normalization Results for Permutative Conversions.

Logical systems	Permutative Conversions	Techniques and references
second order	$\vee$, $\exists$, $\exists^2$	strong validity [15] inductive definitions [12]
second order	$\vee$, $\exists$	saturated sets [19]
second order	no	reducibility [5, 6]
first order	$\vee$, $\exists$	strong validity [10, 20]
type theory ITT_0	Σ (weak permutative conversions)	(ad hoc) [18]
first order	$\vee$	CPS translation [3] inductive definitions [2, 9]

types [16]. Second order existential quantification gives abstract data types [13]. Disjunction gives if-then-else statements. Then permutative conversions gives program transformation for if-then-else statements and abstract data types. Strong normalization of a second order system with permutative conversions gives termination of programs written in those programming languages.

In the opinion of one of the leading authorities on normalization, [15] described a correct proof which however needed some supplementary details in order to be complete. Moreover, we will give counterexamples to Theorem 2. 2. 1 in Page 302 of [15], which is a key of his proof. [15] also gave a proof of strong normalization for first order natural deduction with permutative conversions. Several proofs [10, 20, 21] have been written to complete his proof for a first order system. Nonetheless, we have not seen any paper written to complete his proof for a second order system. Until very recently the proof in [12] was written with a completely different idea using inductive definitions of strongly normalizable terms, the proof for a second order system with permutative conversions had been only that given in [15]. The main contribution of this paper is completing Prawitz's original proof for a second order system.

Section 2 gives the definition of second order natural deduction with permutative conversions. Counterexamples to Prawitz's original proof are discussed in Section 3. Section 4 proves the strong normalization by using Prawitz's strong validity.

2 Second order natural deduction NJ^2

In this paper, we call the second order intuitionistic natural deduction with permutative conversions the system NJ^2. It has disjunction, first-order and second-order existential quantification and their permutative conversions. We will give the definition of the system NJ^2.

Below we will give the list of axioms and inference rules for NJ^2 together with a standard assignment of the second order λ-terms by Curry-Howard isomorphism. The system of reductions is also standard and includes permutative conversions for $\vee$, $\exists$, $\exists^2$.

Definition 2.1 (Language) We have the following symbols:

First order variables $x, y, z, \ldots$,

Function symbols $f, g, \ldots$,

Predicate variables $X, Y, \ldots$,

Predicate symbols $q, r, \ldots$.

We suppose each of function symbols, predicate variables, and predicate symbols has a fixed arity. We will sometimes write X^n to denote the arity n of X. A sequence $e_1, \ldots, e_n$ of expressions is often written as $\vec{e}$.

First order terms, formulas, and abstraction terms are defined as follows:

First order terms $t, s, \ldots ::= x | f\vec{t}$,

Formulas $A, B, C, D, \ldots ::= \bot | q\vec{t} | X\vec{t} | A \to B | A \,\&\, B | \forall xA | A \vee B | \exists xA | \forall XA | \exists XA$,

Abstraction terms $T ::= X | q | \lambda\vec{x}.A$.

Each abstraction term has a fixed arity. The arity of $\lambda x_1 \ldots x_n.\ A$ is n.

We have term variables $u^A, v^B, w^C, \ldots$ where u^A and u^B are distinct when A is not B.

We will also call a formula a type.

Definition 2.2 (Substitution) Substitutions $s\ [x := t]$, $A\ [\mathrm{x} := t]$, $T\ [x := t]$, $A\ [X := T]$, and $T_1\ [X := T]$ are defined in a familiar way. Simultaneous substitutions such as $s\ [x_1 := t_1, \ldots, x_n := t_n]$ are also defined in a standard way. They will be sometimes written using the vector notation such as $s\ [\vec{x} := \vec{t}]$.

We suppose that for a formula A, $(\lambda \vec{x}.\ A)\ \vec{t}$ is identical to $A\ [\vec{x} := \vec{t}]$. Note that for a term M, $(\lambda \vec{x}.\ M)\ \vec{t}$ will not be identical to $M\ [\vec{x} := \vec{t}]$.

Terms and their typing rules are defined as follows.

Definition 2.3 (Terms and typing rules)

Assumption

$$u^A : A$$

Inference rules

$$\dfrac{\begin{array}{c}[u^A : A]\\ \vdots \\ M : B\end{array}}{\lambda u^A.\ M : A \to B}\ (\to I) \qquad \dfrac{M : A \to B \quad N : A}{MN : B}\ (\to E)$$

$$\dfrac{M : A \quad N : B}{\langle M, N\rangle : A \,\&\, B}\ (\& I) \qquad \dfrac{M : A \,\&\, B}{Mp_0 : A}\ (\& E1) \qquad \dfrac{M : A \,\&\, B}{Mp_1 : B}\ (\& E2)$$

$$\dfrac{M : A}{\lambda x.M : \forall xA}\ (\forall I) \qquad \dfrac{M : \forall xA}{Mt : A\ [x := t]}\ (\forall E)$$

$$\dfrac{M : A}{\langle 0, M\rangle^{A \vee B} : A \vee B}\ (\vee I1) \qquad \dfrac{M : B}{\langle 1, M\rangle^{A \vee B} : A \vee B}\ (\vee I2) \qquad \dfrac{M : A \vee B \quad \begin{array}{c}[u^A : A]\\ \vdots \\ N : C\end{array} \quad \begin{array}{c}[v^B : B]\\ \vdots \\ L : C\end{array}}{(M, N, L)_{u^A,\, v^B} : C}\ (\vee E)$$

$$\dfrac{M : A\ [x := t]}{\langle t, M\rangle^{\exists xA} : \exists xA}\ (\exists I) \qquad \dfrac{M : \exists xA \quad \begin{array}{c}[u^A : A]\\ \vdots \\ N : C\end{array}}{(M, N)_{x,\, u^A} : C}\ (\exists E) \qquad \dfrac{M : \bot}{Mp_A : A}\ (\bot E)$$

$$\dfrac{M : A}{\lambda X.M : \forall XA}\ (\forall^2 I) \qquad \dfrac{M : \forall XA}{MT : A\ [X := T]}\ (\forall^2 E)$$

$$\dfrac{M : A\ [X := T]}{\langle T, M\rangle^{\exists XA} : \exists XA}\ (\exists^2 I) \qquad \dfrac{M : \exists XA \quad \begin{array}{c}[u^A : A]\\ \vdots \\ N : C\end{array}}{(M, N)_{X,\, u^A} : C}\ (\exists^2 E)$$

The rules $(\forall I)$, $(\exists E)$, $(\forall^2 I)$, and $(\exists^2\ E)$ have a standard condition for variables.
Type superscripts in u^A, $\langle 0, M\rangle^{A \vee B}$, $\langle 1, M\rangle^{A \vee B}$, $\langle t, M\rangle^{\exists xA}$, and $\langle T, M\rangle^{\exists XA}$ will be sometimes omitted to save notation.
We will use M, N, L, K, P, Q to denote terms.

Substitutions $M\ [x := t]$, $M\ [u^A := N]$ and $M\ [X := T]$ and their simultaneous substitutions are defined in a standard way.

Definition 2.4 (Reductions) We define the relation $M \to N$ for terms M and N in the following way.

β conversions:

$(\beta \to)$ $\quad (\lambda \alpha.M)R \to M\ [\alpha := R]$ $\qquad$ (α is x, u^A, or X, and R is t, N, or T respectively.)

$(\beta\&1)$ $\langle M, N\rangle p_0 \to M$

$(\beta\&2)$ $\langle M, N\rangle p_1 \to N$

$(\beta\vee 1)$ $(\langle 0, M\rangle, N, L)_{u^A, v^B} \to N\,[u^A := M]$

$(\beta\vee 2)$ $(\langle 1, M\rangle, N, L)_{u^A, v^B} \to L\,[v^B := M]$

$(\beta\exists)$ $(\langle R, M\rangle, N)_{\alpha, u^A} \to N\,[\alpha := R, u^A := M]$ (α is x or X, and R is t or T respectively.)

Permutative conversions:

$(\pi\exists)$ $(M, N)_{\alpha, u^A} R \to (M, NR)_{\alpha, u^A}$ (R is t, L, T, p_0, p_1, or p_C.)

$(\pi\exists\exists)$ $((M, N)_{\alpha, u^A}, L)_{\beta, v^B} \to (M, (N, L)_{\beta, v^B})_{\alpha, u^A}$

$(\pi\exists\vee)$ $((M, N)_{\alpha, u^A}, L_1, L_2)_{u_1^B, u_2^C} \to (M, (N, L_1, L_2\,)_{u_1^B, u_2^C})_{\alpha, u^A}$

$(\pi\vee)$ $(M, N, L)_{u^A, v^B} R \to (M, NR, LR)_{u^A, v^B}$ (R is t, L, T, p_0, p_1, or p_C.)

$(\pi\vee\exists)$ $((M, N, L)_{u_1^A, u_2^B}, K)_{\alpha, v^C} \to (M, (N, K)_{\alpha, v^C}, (L, K)_{\alpha, v^C})_{u_1^A, u_2^B}$

$(\pi\vee\vee)$ $((M, N, L)_{v_1^A, v_2^B}, K_1, K_2)_{u_1^C, u_2^D} \to (M, (N, K_1, K_2)_{u_1^C, u_2^D}, (L, K_1, K_2)_{u_1^C, u_2^D})_{v_1^A, v_2^B}$

where α is x or X and β is y or Y.

Congruence.

$(congr)$ $M \to M'$

if N is a subterm of M, $N \to N'$ holds, and M' is obtained from M by replacing one occurrence of N by N'.

We will say that M reduces to N if $M \to N$ holds. The relation $\to^*$ is defined as the reflexive transitive closure of the relation $\to$. We will write $M \to_\pi N$ if M reduces to N by using only the permutative conversions and the congruence. The relation $\to_\pi^*$ is the reflexive transitive closure of the relation $\to_\pi$.

Remark. (1) Subject reduction property and Church Rosser property hold.

(2) We will not treat $\perp$ reductions according to [15].

A term M is strongly normalizable if there is no infinite reduction sequence

$M \to M_1 \to M_2 \to \ldots$

beginning with M.

Theorem 2.5 (Strong normalization) *Every term of the system NJ^2 is strongly normalizable.*

Section 4 will prove this theorem by using Prawitz's strong validity [15].

3 Counterexamples

The notions such as reducibility [5, 6], saturated sets [1, 17], and strong validity [15], which are defined by induction on types for first order systems, have difficulty when we try to extend them to a second order system in a naive way. Reducibility candidates technique used in [5, 6] solved this kind of problem by using an assignment to second order variables.

In [15], first the notion of strong validity was defined for a first order system, then he tried to extend it to a second order system by using the notion of the assignment defined in Page 300. This would be a key to treat a second order system. However, this notion cannot work because Theorem 2.2.1 in Page 302 of the paper has the counterexamples we will give later in this section.

Page 300 of [15] defines $\mathcal{N}$ as an assignment that assigns a regular set to an occurrence of a second order term in a formula. It says that different occurrences of the same second order term may be assigned different sets, and this is emphasized by the additional explanation given in the footnote. Page 301 defines the notion: a derivation Π is strongly valid relative $\mathcal{N}$. To define it, the definition A.3.2.1 of strong validity given for the first order system is extended to the notion of strong validity relative an assignment for the second order system. The introduction rule consists of the conclusion A and some assumptions of immediate subformulas of A. When the definitions A.3.2.1.1 –3 of strong validity for the introduction rules are extended to the second order system, to define a strongly valid derivation of the conclusion A relative $\mathcal{N}$, he uses strongly valid derivations of immediate subformulas of A relative $\mathcal{N}'$ where $\mathcal{N}'$ is obtained from $\mathcal{N}$ by stating that $\mathcal{N}'$ is to assign to an occurrence of a second order term in the immediate subformulas of A in question the same value that $\mathcal{N}$ assigns to the corresponding occurrence in A. However, this feature causes the following counterexample to the theorem 2.2.1.

Let SN be the set of strongly normalizing derivations. Note that SN is regular.

We summarize facts on his definitions of strong validity. We will use only those from his definitions to construct counterexamples. This interpretation of his book is plausible since at least these facts are clearly stated there, though other parts of his discussions may be ambiguous.

Facts. (1) (By A.3.2.1.2 and Page 301 in [15]) Suppose Π is of the form

$$\dfrac{\begin{array}{c}[A]\\ \vdots\ \Pi_1\\ B\end{array}}{A \to B}\ (\to I)$$

Then Π is strongly valid relative $\mathcal{N}$, if and only if for any derivation Σ of A which is strongly valid relative $\mathcal{N}_1$, the derivation

$$\begin{array}{l}\vdots\ \Sigma\\ A\\ \vdots\ \Pi_1\\ B\end{array}$$

is strongly valid relative $\mathcal{N}_2$, where the assignment $\mathcal{N}_1$ is defined as an assignment that maps an occurrence of a second order term T in A to a regular set N when $\mathcal{N}$ maps the corresponding occurrence of T in $A \to B$ to N, and the assignment $\mathcal{N}_2$ is defined as an assignment that maps an occurrence of a second order term T in B to a regular set N when $\mathcal{N}$ maps the corresponding occurrence of T in $A \to B$ to N.

(2) (By A.2.1.2.1 in [15]) Suppose Π is of the form

$$\dfrac{\begin{array}{c}\vdots\\ A\,[x := t]\end{array}}{(\lambda x.\ A)t}\ (\lambda I)$$

and the occurrence of the second order term $\lambda x.A$ is in the domain of $\mathcal{N}$. Then Π is strongly valid relative $\mathcal{N}$, if and only if Π is in $\mathcal{N}(\lambda x.\ A)$.

Proposition 3.1 *Let P be a 0-place predicate constant. Let Π be the derivation*

$$\dfrac{[P]}{P \to P}$$

Let $\mathcal{N}$ be the assignment that maps the first occurrence of P in $P \to P$ to SN and the second occurrence of P in $P \to P$ to the empty set. Then Π is not strongly valid relative $\mathcal{N}$.

Proof. By the definition of strong validity given in Pages 291 and 301, the claim that Π is strongly valid relative $\mathcal{N}$ is equivalent to the claim that for every derivation Σ of P that is strongly valid relative $\mathcal{N}_1$, the derivation Σ is strongly valid relative $\mathcal{N}_2$. By the definition given in Page 301 extending the definition A.3.2.1.2 to the second order system, $\mathcal{N}_1$ maps the conclusion P of Σ to SN since this occurrence of P comes from the first occurrence of P in $P \to P$, while $\mathcal{N}_2$ maps the conclusion P of Σ to the empty set since this occurrence of P comes from the second occurrence of P in $P \to P$. Hence the claim that Π is strongly valid relative $\mathcal{N}$ is equivalent to the claim that for every derivation Σ of P in SN, the derivation Σ is in the empty set. The latter claim does not hold, so Π is not strongly valid relative $\mathcal{N}$. □

Counterexample 1. Apply the theorem 2.1.1 in [15] to the derivation Π and the assignment $\mathcal{N}$ given in Proposition 3.1. We do not have any individual variables, second order parameters, nor open assumptions in Π. Π should be strongly valid relative $\mathcal{N}$ according to that theorem. On the other hand, Π is not strongly valid relative $\mathcal{N}$ by Proposition 3.1. Hence the theorem 2.1.1 does not hold. □

Page 300 of [15] defines an assignment as a mapping that maps not only a second order variable but also a second order term to a regular set. According to this definition, the second order term $\lambda x.A$ can be assigned some regular set independent of A. This feature causes another counterexample as follows.

Proposition 3.2 *Let P be a 1-place predicate constant,* 0 *be an individual constant, x be an individual variable, and Π be the derivation*

$$\dfrac{\dfrac{[P0]}{(\lambda x.Px)0}}{P0 \to (\lambda x.Px)0}$$

Let the assignment $\mathcal{N}$ be the mapping that maps P to SN and $\lambda x.Px$ to the empty set. Then Π is not strongly valid relative $\mathcal{N}$.

Proof. By the definition of strong validity given in Pages 291 and 301, the claim that Π is strongly valid relative $\mathcal{N}$ is equivalent to the claim that for every derivation Σ of $P0$ that is strongly valid relative $\mathcal{N}$, the derivation Π'

$$\dfrac{\dfrac{\Sigma}{P0}}{(\lambda x.Px)0}$$

is strongly valid relative $\mathcal{N}$. Hence the claim that Π is strongly valid relative $\mathcal{N}$ is equivalent to the claim that for every derivation Σ of $P0$ in SN,the derivation Π' is in the empty set. The latter claim does not hold, so Π is not strongly valid relative $\mathcal{N}$. □

Counterexample 2. Apply the theorem 2.1.1 in [15] to the derivation Π and the assignment $\mathcal{N}$ given in Proposition 3.2. We do not have any individual variables, second order parameters, nor open assumptions in Π. Π should be strongly valid relative $\mathcal{N}$ according to that theorem. On the other hand, Π is not strongly valid relative $\mathcal{N}$ by Proposition 3.2. Hence the theorem 2.1.1 does not hold. □

His proof of strong normalization consists of the theorems 2.2.1 and 2.2.2 in Page 302. The theorem 2.2.1 is one of the two main theorems, and his proof of strong normalization does not work without the theorem 2.2.1.

He also gave a proof of strong normalization for a first order system in [15] and several proofs have been written to complete his proof for the first order system. Until now we do not know any paper that completes his proof for the second order system. In the next section, we will complete his proof for the second order system.

4 Strong normalization

Definition 4.1 For a type A, SN_A is defined as the set of strongly normalizable terms of type A. SN is defined as the set of strongly normalizable terms of any type.

For a set S of terms of type A, S is called regular$_A$ if

(1) $S \subset SN_A$,

(2) If $M \in S$ and $M \to N$, then $N \in S$.

For an abstraction term T of arity n, a regular$_T$ set function is a function that maps a sequence $t_1 \ldots t_n$ of first order terms to a regular$_{Tt_1 \ldots t_n}$ set. A set valuation σ is a mapping which maps a predicate variable X^n to (T, F) where T is an abstraction term of arity n and F is a regular$_T$ set function. The valuation $\sigma[X := (T, F)]$ is defined by $(\sigma[X := (T, F)])(X) = (T, F)$ and $(\sigma[X := (T, F)])(Y) = \sigma(Y)$ for $X \not\equiv Y$.

For a formula A and a set valuation σ, $A\sigma$ is defined as $A[\vec{X}:=\vec{T}]$ where the free predicate variables of A are $\vec{X}$, and $\sigma(X_i)=(T_i, F_i)$. Substitutions $t\sigma$, $T\sigma$, and $M\sigma$ are defined in the same way. Note that $t\sigma$ is always t.

Lemma 4.2 *SN_A is regular$_A$.*

Proof. The clauses (1) and (2) in the definition of regular sets hold trivially for SN_A. □

Definition 4.3 For an abstraction term T, the regular$_T$ set function SN_T is defined by $SN_T(\vec{t}) = SN_{T\vec{t}}$.

Definition 4.4 (Strong validity) For a type A and a set valuation σ, we will define the set sv^σ_A of terms of type $A\sigma$ inductively by using strictly positive inductive definition of sv^σ_A inside induction on the construction of A.

- (Var) $u^{A\sigma} \in sv^\sigma_A$.
- (Var2) $M \in sv^\sigma_{X\vec{t}}$ if $\sigma(X)=(T, F)$ and $M \in F(\vec{t})$.
- $(\to I)$ $\lambda u^{A\sigma}. M \in sv^\sigma_{A\to B}$ if for every $N \in sv^\sigma_A$, $M[u^{A\sigma} := N] \in sv^\sigma_B$.
- $(\to E)$ $MN \in sv^\sigma_A$ if for every L, $MN \to L$ implies $L \in sv^\sigma_A$ and $MN : A\sigma$.
- $(\&I)$ $\langle M, N\rangle \in sv^\sigma_{A\&B}$ if $M \in sv^\sigma_A$ and $N \in sv^\sigma_B$.
- $(\&E)$ $Mp_i \in sv^\sigma_A$ if every L, $Mp_i \to L$ implies $L \in sv^\sigma_A$ and $Mp_i : A\sigma$ $(i{=}0,1)$.
- $(\forall I)$ $\lambda x.M \in sv^\sigma_{\forall xA}$ if for every first order term t, $M[x := t] \in sv^\sigma_{A[x:=t]}$.
- $(\forall E)$ $Mt \in sv^\sigma_A$ if for every L, $Mt \to L$ implies $L \in sv^\sigma_A$ and $Mt : A\sigma$.
- $(\vee I1)$ $\langle 0, M\rangle^{(A\vee B)\sigma} \in sv^\sigma_{A\vee B}$ if $M \in sv^\sigma_A$.

- $(\vee I2)$ $\langle 1, M\rangle^{(A\vee B)\sigma} \in sv^{\sigma}_{A\vee B}$ if $M \in sv^{\sigma}_{B}$.
- $(\vee E)$ $(M, N, L)_{u^A,\, v^B} \in sv^{\sigma}_{C}$ if
  - $M \in SN_{A\vee B}$,
  - $N, L \in sv^{\sigma}_{C}$,
  - for every P, $M \to^{*} \mathcal{C}\,[\langle 0, P\rangle^{A\vee B}]$ implies $N\,[\,u^A := P] \in sv^{\sigma}_{C}$,
  - for every P, $M \to^{*} \mathcal{C}\,[\langle 1, P\rangle^{A\vee B}]$ implies $L\,[\,v^B := P] \in sv^{\sigma}_{C}$.
- $(\exists I)$ $\langle t, M\rangle^{(\exists xA)\sigma} \in sv^{\sigma}_{\exists xA}$ if $M \in sv^{\sigma}_{A[x := t]}$.
- $(\exists E)$ $(M, N)_{x,\, u^A} \in sv^{\sigma}_{C}$ if $M \in SN_{\exists xA}$, $N \in sv^{\sigma}_{C}$, and $M \to^{*} \mathcal{C}\,[\langle t, P\rangle^{\exists xA}]$ implies $N\,[x := t, u^A := P] \in sv^{\sigma}_{C}$ for every P and every t.
- $(\forall^2 I)$ $\lambda X^n.M \in sv^{\sigma}_{\forall X^n A}$ if for every abstraction term T of arity n and every regular$_T$ set function F, $M\,[X := T] \in sv^{\sigma[\,X := (T,\, F)]}_{A}$.
- $(\forall^2 E)$ $MT \in sv^{\sigma}_{A}$ if for every L, $MT \to L$ implies $L \in sv^{\sigma}_{A}$ and $MT : A\sigma$.
- $(\exists^2 I)$ $\langle T, M\rangle^{(\exists XA)\sigma} \in sv^{\sigma}_{\exists XA}$ if $M \in sv^{\sigma[\,X := (T,\, F)\,]}_{A}$ for some regular$_T$ set function F.
- $(\exists^2 E)$ $(M, N)_{X,\, u^A} \in sv^{\sigma}_{C}$ if $M \in SN_{\exists XA}$, $N \in sv^{\sigma}_{C}$, and $M \to^{*} \mathcal{C}\,[\langle T, P\rangle^{\exists XA}]$ implies $N\,[X := T, u^A := P] \in sv^{\sigma}_{C}$ for every term P and every abstraction term T.

In the rules $(\vee E)$, $(\exists E)$, and $(\exists^2 E)$, the segment $\mathcal{C}\,[\cdot]$ is defined by

$$\mathcal{C}\,[\cdot] ::= \cdot\,|(M, \mathcal{C}\,[\cdot], N)_{u^A,\, v^B}\,|(M, N, \mathcal{C}\,[\cdot])_{u^A,\, v^B}\,|(M, \mathcal{C}\,[\cdot])_{x,\, u^A}\,|(M, \mathcal{C}\,[\cdot])_{X,\, u^A}$$

If M is in sv^{σ}_{A}, we will say that M is strongly valid with respect to σ. We call sv^{σ}_{A} strong validity, which will be sometimes abbreviated to sv.

Remark. In this definition, sv^{σ}_{A} is defined by induction on A. Inside each definition for A, we can assume sv^{σ}_{B} is already defined for B smaller than A, and moreover we use strictly positive inductive definition of sv^{σ}_{A}. This kind of definition is discussed in detail in [20] and it has shown that the inductive definition for the first order system can be reduced to arithmetical inductive definitions.

Definition 4.5 For $M \in SN$, $|M|$ is defined as the length of the longest reduction sequence beginning with M. $\#M$ is defined as the number of the symbols occurring in M.

Lemma 4.6 *(1) Suppose that $(M, N, L)_{u,v}$ is a term of type C. Assume that*

- *M, N, L are in SN,*
- *$M \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$ implies $N\,[u := P] \in SN$ for every P,*
- *$M \to^{*} \mathcal{C}\,[\langle 1, P\rangle]$ implies $L\,[v := P] \in SN$ for every P.*

Then $(M, N, L)_{u\,,v}$ is in SN.

(2) Let α be x or X and R be t or T respectively. Suppose that $(M, N)_{\alpha,u}$ is a term of type C. Assume that

- *M, N are in SN,*
- *$M \to^{*} \mathcal{C}\,[\langle R, P\rangle]$ implies $N\,[\alpha := R, u := P] \in SN$ for every R and every P.*

Then $(M, N)_{a,\, u}$ is in SN.

Proof. We will show the claims (1) and (2) simultaneously by induction on $(|M|, \#M, |N|+|L|)$.

(1) Assume $(M, N, L)_{u,v} \to K$. We will show $K \in SN$. We will consider cases according to the reduction.

Case $(M, N, L)_{u,v} \to (M', N, L)_{u,v}$.

For $i = 0, 1$, $M' \to^{*} \mathcal{C}\,[\langle i, P\rangle]$ implies $M \to^{*} \mathcal{C}\,[\langle i, P\rangle]$, so the second and the third assumptions hold for $(M', N, L)_{u,v}$. By IH for $|M'| < |M|$, we have $(M', N, L)_{u,v} \in SN$.

Case $(M, N, L)_{u,v} \to (M, N', L)_{u,v}$.

$N'\,[u := P] \in SN$ if $N\,[u := P] \in SN$, since $N[u := P] \to N'\,[u := P]$. By IH for $|N'| < |N|$, we have $(M, N', L)_{u,v} \in SN$.

Case $(M, N, L)_{u,v} \to (M, N, L')_{u,v}$. This case is similar to the previous case.

Case $(\langle 0, M\rangle, N, L)_{u,v} \to N\,[u := M]$.

By letting $\mathcal{C}\,[\cdot] \equiv \cdot$ in the second assumption, $N\,[u := M]$ is in SN.

Case $(\langle 1, M\rangle, N, L)_{u,v} \to L\,[v := M]$. This case is similar to the previous case.

Case $((M_1, M_2, M_3)_{w_1,w_2}, N, L)_{u,v} \to (M_1, (M_2, N, L)_{u,v}, (M_3, N, L)_{u,v})_{w_1,w_2}$.

We have $M_1 \in SN$, since $(M_1, M_2, M_3)_{w_1,w_2} \in SN$.

We will show $(M_2, N, L)_{u,v} \in SN$. First we have $M_2, N, L \in SN$. Suppose $M_2 \to^* \mathcal{C}_1 [\langle 0, P\rangle]$. Then $(M_1, M_2, M_3)_{w_1,w_2} \to^* (M_1, \mathcal{C}_1 [\langle 0, P\rangle], M_3)_{w_1,w_2}$. By letting $\mathcal{C}[\cdot]$ be $(M_1, \mathcal{C}_1 [\cdot], M_3)_{w_1,w_2}$ in the second assumption, we have $N [u := P] \in SN$. Therefore $M_2 \to^* \mathcal{C}_1 [\langle 0, P\rangle]$ implies $N [u := P] \in SN$. Similarly $M_2 \to^* \mathcal{C}_1 [\langle 1, P\rangle]$ implies $L [v := P] \in SN$. Hence, by IH for $|M_2| \le |M|$ and $\#M_2 < \#M$, we have $(M_2, N, L)_{u,v} \in SN$.

We can prove $(M_3, N, L)_{u,v} \in SN$ in a similar way.

We will show that $M_1 \to^* \mathcal{C}_1 [\langle 0, P\rangle]$ implies $(M_2, N, L)_{u,v} [w_1 := P] \in SN$. Assume $M_1 \to^* \mathcal{C}_1 [\langle 0, P\rangle]$. We will show each condition in IH for $(M_2 [w_1 := P], N, L)_{u,v} \in SN$. We have

$$\begin{aligned}(M_1, M_2, M_3)_{w_1,w_2} &\to^* (\mathcal{C}_1 [\langle 0, P\rangle], M_2, M_3)_{w_1,w_2}\\ &\to^*_\pi \mathcal{C}'_1 [(\langle 0, P\rangle, M_2, M_3)_{w_1,w_2}]\\ &\to \mathcal{C}'_1 [M_2 [w_1 := P]].\end{aligned}$$

By the first assumption $(M_1, M_2, M_3)_{w_1,w_2} \in SN$, we have $M_2 [w_1 := P] \in SN$. By the first assumption, we also have $N, L \in SN$. Suppose $M_2 [w_1 := P] \to^* \mathcal{C}_2 [\langle 0, Q\rangle]$. Then we have

$(M_1, M_2, M_3)_{w_1,w_2} \to^* \mathcal{C}'_1 [M_2 [w_1 := P]] \to^* \mathcal{C}'_1 [\mathcal{C}_2[\langle 0,Q\rangle]]$.

By letting $\mathcal{C}[\cdot]$ be $\mathcal{C}'_1 [\mathcal{C}_2 [\cdot]]$ in the second assumption, we have $N [u := Q] \in SN$. Hence $M_2[w_1 := P] \to^* \mathcal{C}_2 [\langle 0, Q\rangle]$ implies $N [u := Q] \in SN$. Similarly $M_2 [w_1 := P] \to^* \mathcal{C}_2 [\langle 1, Q\rangle]$ implies $L [v := Q] \in SN$. By IH for $|M_2 [w_1 := P]| < |(M_1, M_2, M_3)_{w_1,w_2}|$, we have $(M_2 [w_1 := P], N, L)_{u,v} \in SN$, that is, $(M_2, N, L)_{u,v} [w_1 := P] \in SN$.

We can prove that $M_1 \to^* \mathcal{C}_1 [\langle 1, P\rangle]$ implies $(M_3, N, L)_{u,v} [w_2 := P] \in SN$ in the same way.

By IH for $|M_1| \le |(M_1, M_2, M_3)_{w_1,w_2}|$ and $\#M_1 < \#(M_1, M_2, M_3)_{w_1,w_2}$, we can conclude $(M_1, (M_2, N, L)_{u,v}, (M_3, N, L)_{u,v})_{w1,w2} \in SN$.

Case $((M_1, M_2)_{\alpha,w}, N, L)_{u,v} \to (M_1, (M_2, N, L)_{u,v})_{\alpha,w}$ where α is x or X.

We have $M_1 \in SN$, since $(M_1, M_2)_{\alpha,w} \in SN$.

We will show $(M_2, N, L)_{u,v} \in SN$. First we have $M_2, N, L \in SN$ from the first assumption. Suppose $M_2 \to^* \mathcal{C}_1 [\langle 0, P\rangle]$. Then $(M_1, M_2)_{\alpha,w} \to^* (M_1, \mathcal{C}_1 [\langle 0, P\rangle])_{\alpha,w}$. By letting $\mathcal{C}[\cdot]$ be $(M_1, \mathcal{C}_1 [\cdot])_{\alpha,w}$ in the second assumption, we have $N[u := P] \in SN$. Therefore $M_2 \to^* \mathcal{C}_1 [\langle 0, P\rangle]$ implies $N [u := P] \in SN$. Similarly $M_2 \to^* \mathcal{C}_1 [\langle 1, P\rangle]$ implies $L [v := P] \in SN$. Hence, by IH for $|M_2| \le |M|$ and $\#M_2 < \#M$, we have $(M_2, N, L)_{u,v} \in SN$.

We will show that $M_1 \to^* \mathcal{C}_1 [\langle R, P\rangle]$ implies $(M_2, N, L)_{u,v} [\alpha := R, w := P] \in SN$, where R is t if α is x and R is T if α is X. Assume $M_1 \to^* \mathcal{C}_1 [\langle R, P\rangle]$. We will show each condition in IH for $(M_2 [\alpha := R, w := P], N, L)_{u,v} \in SN$. We have

$$\begin{aligned}(M_1, M_2)_{\alpha,w} &\to^* (\mathcal{C}_1 [\langle R, P\rangle], M_2)_{\alpha,w}\\ &\to^*_\pi \mathcal{C}'_1 [(\langle R, P\rangle, M_2)_{\alpha,w}]\\ &\to \mathcal{C}'_1 [M_2 [\alpha := R, w := P]].\end{aligned}$$

By the first assumption $(M_1, M_2)_{\alpha,w} \in SN$, we have $M_2 [\alpha := R, w := P] \in SN$. By the first assumption, we also have $N, L \in SN$. Suppose $M_2 [\alpha := R, w := P] \to^* \mathcal{C}_2 [\langle 0, Q\rangle]$. Then we have

$(M_1, M_2)_{\alpha,w} \to^* \mathcal{C}'_1 [M_2 [\alpha := R, w := P]] \to^* \mathcal{C}'_1 [\mathcal{C}_2 [\langle 0, Q\rangle]]$.

By letting $\mathcal{C}[\cdot]$ be $\mathcal{C}'_1 [\mathcal{C}_2 [\cdot]]$ in the second assumption, we have $N [u := Q] \in SN$. Hence $M_2 [\alpha := R, w := P] \to^* \mathcal{C}_2 [\langle 0, Q\rangle]$ implies $N [u := Q] \in SN$. Similarly $M_2 [\alpha := R, w := P] \to^* \mathcal{C}_2 [\langle 1, Q\rangle]$ implies $L [v := Q] \in SN$. By IH for $|M_2 [\alpha := R, w := P]| < |(M_1, M_2)_{\alpha,w}|$, we have $(M_2 [\alpha := R, w:= P], N, L)_{u,v} \in SN$, that is, $(M_2, N, L)_{u,v} [\alpha := R, w :=P] \in SN$.

By IH (2) for $|M_1| \le |(M_1, M_2)_{\alpha,w}|$ and $\#M_1 < \# (M_1, M_2)_{\alpha,w}$, we can conclude $(M_1, (M_2, N, L)_{u,v})_{\alpha,w} \in SN$.

(2) These claims are proved in a similar way to the claim (1). □

Proposition 4.7 *$sv^\sigma_A \subset SN_{A\sigma}$ holds.*

Proof. We will use induction on the definition of $M \in sv^\sigma_{\mathrm{A}}$ to prove that $M \in SN$.

We will list cases according to the definition of $M \in sv^\sigma_A$.

Case (Var). $u^{\mathrm{A}\sigma} \in SN$.

Case (Var2). By the clause (1) in the definition of regular sets.

Case ($\to I$). By (Var), $u^{A\sigma} \in sv^\sigma_A$. By letting N be u in the definition of $\lambda u.M \in sv^\sigma_{A\to B}$, we have $M \in sv^\sigma_B$. By IH, M is in SN. Hence $\lambda u.M$ is in SN.

Case ($\to E$). We will show $MN \in SN$. Assume $MN \to L$ and we will show $L \in SN$. By the definition of $MN \in sv^\sigma_A$, we have $L \in sv^{\sigma}_{A}$. By IH, we have $L \in SN$.

Case ($\&I$). By the definition of $\langle M, N\rangle \in sv^{\sigma}_{A\&B}$, we have $M \in sv^{\sigma}_{A}$ and $N \in sv^{\sigma}_{B}$. By IH, M, N are in SN. Hence $\langle M, N\rangle$ is in SN.

Case ($\&E$). This case is similar to the case ($\to E$).

Case ($\forall I$). By letting t be x in the definition of $\lambda x.M \in sv^{\sigma}_{\forall xA}$, we have $M \in sv^{\sigma}_{A}$. By IH, M is in SN. Hence $\lambda\, x.M$ is in SN.

Case ($\forall E$). This case is similar to the case ($\to E$).

Case ($\bigvee I$). This case is similar to the case ($\&I$).

Case ($\bigvee E$). By IH, we have the following : $M, N, L \in SN$, $M \to {}^{*}\mathcal{C}\,[\,\langle 0, P\rangle]$ implies $N\,[\,u := P] \in SN$ for every P, and $M \to {}^{*}\,\mathcal{C}\,[\langle 1, P\rangle]$ implies $L\,[v := P] \in SN$ for every P. By Lemma 4.6 (1), we have $(M, N, L)_{u,\,v} \in SN$.

Case ($\exists I$). By IH for $M \in sv^{\sigma}_{A\,[x\,:=\,t]}$, M is in SN. Hence $\langle t, M\rangle$ is in SN.

Case ($\exists E$). By IH, we have the following : $M, N \in SN$, and $M \to {}^{*}\,\mathcal{C}\,[\langle t, P\rangle]$ implies $N\,[x := t, u := P] \in SN$ for every t and every P. By Lemma 4.6 (2), $(M, N)_{x,\,u}$ is in SN.

Case ($\forall^2 I$). By letting T be X and F be SN_X in the definition of $\lambda X.M \in sv^{\sigma}_{\forall XA}$, we have $M \in sv^{\sigma\,[X\,:=\,(X,\,SN_X)]}_{A}$. By IH, M is in SN. Then $\lambda X.M$ is in SN.

Case ($\forall^2 E$). This case is similarly proved to the case ($\to E$).

Case ($\exists^2 I$). By IH for $M \in sv^{\sigma\,[X\,:=\,(T,\,F)]}_{A}$, M is in SN. Hence $\langle T, M\rangle$ is in SN.

Case ($\exists^2 E$). By IH, we have the following : $M, N \in SN$, and $M \to {}^{*}\mathcal{C}\,[\langle T, P\rangle]$ implies $N\,[X := T, u := P] \in SN$ for every T and every P. From Lemma 4.6 (2), we have $(M, N)_{X,\,u} \in SN$.

Consequently $sv^{\sigma}_{A} \subset SN$ holds. Since sv^{σ}_{A} is a set of terms of type $A\sigma$, we have $sv^{\sigma}_{A} \subset SN_{A\sigma}$ □

Proposition 4.8 *If $M \in sv^{\sigma}_{A}$ and $M \to N$ hold, then N is in sv^{σ}_{A}.*

Proof. Assume $M \in sv^{\sigma}_{A}$ and $M \to N$. We will show $N \in sv^{\sigma}_{A}$ by induction on the definition of $M \in sv^{\sigma}_{A}$.

We will list cases according to the definition of $M \in sv^{\sigma}_{A}$.

Case (Var). We do not have this case.

Case (Var2). The claim holds from the clause (2) in the definition of regular sets.

Case ($\to I$). The reduction is $\lambda u.M \to \lambda u.M'$. Assume $N \in sv^{\sigma}_{A}$. From the definition of $\lambda u.M \in sv^{\sigma}_{A\to B}$, $M\,[u := N]$ is in sv^{σ}_{B}. From IH and $M\,[u := N] \to M'\,[u := N]$, we have $M'\,[u := N]$ in sv^{σ}_{B}. Hence $\lambda u.M'$ is in $sv^{\sigma}_{A\to B}$.

Case ($\to E$). By the definition of sv, $MN \to L$ implies $L \in sv^{\sigma}_{A}$.

Case ($\&I$). The reduction is either $\langle M, N\rangle \to \langle M', N\rangle$ or $\langle M, N\rangle \to \langle M, N'\rangle$. By the definition of sv, M is in sv^{σ}_{A} and N is in sv^{σ}_{B}. By IH, M' is in sv^{σ}_{A} and N' is in sv^{σ}_{B}. Hence we have $\langle M', N\rangle \in sv^{\sigma}_{A\&B}$ and $\langle M, N'\rangle \in sv^{\sigma}_{A\&B}$ by definition.

Case ($\&E$). This case is similarly proved to the case ($\to E$).

Case ($\forall I$). The reduction is $\lambda x.M \to \lambda x.M'$. By IH for $M\,[x := t] \in sv^{\sigma}_{A\,[x\,:=\,t]}$ and $M\,[x := t] \to M'\,[x := t]$, we have $M'\,[x := t] \in sv^{\sigma}_{A\,[x\,:=\,t]}$ for any first order term t. Hence $\lambda x.M'$ is in $sv^{\sigma}_{\forall xA}$.

Case ($\forall E$). This case is similarly proved to the case ($\to E$).

Case ($\bigvee I$). This case is similar to the case ($\&I$).

Case ($\bigvee E$). Suppose $(M, N, L)_{u,\,v} \in sv^{\sigma}_{C}$ and $(M, N, L)_{u,\,v} \to K$. We will consider cases according to the reduction.

Case 1. $(M, N, L)_{u,\,v} \to (M', N, L)_{u,\,v} \equiv K$. M' is in SN since M is in SN. $M' \to {}^{*}\mathcal{C}\,[\langle 0, P\rangle]$ implies $N\,[u := P] \in sv^{\sigma}_{C}$, since $M' \to {}^{*}\mathcal{C}\,[\langle 0, P\rangle]$ implies $M \to {}^{*}\mathcal{C}\,[\langle 0, P\rangle]$. Similarly $M' \to {}^{*}\mathcal{C}\,[\,\langle 1, P\rangle]$ implies $L\,[\,v := P] \in sv^{\sigma}_{C}$. Hence K is in sv^{σ}_{C} by definition.

Case 2. $(M, N, L)_{u,\,v} \to (M, N', L)_{u,\,v} \equiv K$. By IH, N' is in sv^{σ}_{C}. If $M \to {}^{*}\mathcal{C}\,[\langle 0, P\rangle]$, we have $N\,[u := P] \in sv^{\sigma}_{C}$. Then we have $N'\,[u := P] \in sv^{\sigma}_{C}$ from $N\,[u := P] \to N'\,[u := P]$ and IH. Hence K is in sv^{σ}_{C} by definition.

Case 3. $(M, N, L)_{u,\,v} \to (M, N, L')_{u,\,v} \equiv K$. This case is similar to the previous case.

Case 4. $(\langle 0, P\rangle, N, L)_{u,\,v} \to N\,[u := P] \equiv K$. By letting $\mathcal{C}\,[\cdot] \equiv \cdot$ in the third condition of the definition $(\langle 0, P\rangle, N, L)_{u,\,v} \in sv^{\sigma}_{C}$, we have $N\,[u := P] \in sv^{\sigma}_{C}$.

Case 5. $(\langle 1, P\rangle, N, L)_{u,\,v} \to L\,[v := P] \equiv K$. This case is similarly proved to the previous case.

Case 6. $((M_1, M_2, M_3)_{w_1,\,w_2}, N, L)_{u,\,v} \to (M_1, (M_2, N, L)_{u,\,v}, (M_3, N, L)_{u,\,v})_{w_1,\,w_2} \equiv K$.

The assumption $((M_1, M_2, M_3)_{w_1,\,w_2}, N, L)_{u,\,v} \in sv^{\sigma}_{C}$ gives us the following four conditions : $(M_1, M_2, M_3)_{w_1,\,w_2} \in SN$, $N, L \in sv^{\sigma}_{C}$, $(M_1, M_2, M_3)_{w_1,\,w_2} \to {}^{*}\mathcal{C}\,[\langle 0, P\rangle]$ implies $N\,[u := P] \in sv^{\sigma}_{C}$, and $(M_1, M_2, M_3)_{w_1,\,w_2} \to {}^{*}\mathcal{C}\,[\langle 1, P\rangle]$ implies $L\,[v := P] \in sv^{\sigma}_{C}$. We will show each clause in the definition $(M_1, (M_2, N, L)_{u,\,v}, (M_3, N, L)_{u,\,v})_{w_1,\,w_2} \in sv^{\sigma}_{C}$.

First we have $M_1 \in SN$ from the first condition.

Next we will show $(M_2, N, L)_{u,\,v} \in sv^{\sigma}_{C}$. M_2 is in SN. From the second condition, N, L are in sv^{σ}_{C}. Suppose $M_2 \to^{*} \mathcal{C}_1\,[\langle 0, P\rangle]$. Then $(M_1, M_2, M_3)_{w_1,\,w_2} \to^{*} (M_1, \mathcal{C}_1\,[\langle 0, P\rangle], M_3)_{w_1,\,w_2}$. By letting $\mathcal{C}\,[\cdot]$ be $(M_1, \mathcal{C}_1\,[\cdot], M_3)_{w_1,\,w_2}$ in the third condition, we have $N[u:=P] \in sv^{\sigma}_{C}$. Therefore $M_2 \rightarrow^{*} \mathcal{C}_1[\langle 0, P\rangle]$ implies $N[u:=P] \in sv^{\sigma}_{C}$. Similarly $M_2 \rightarrow^{*} \mathcal{C}_1[\langle 1, P\rangle]$ implies $L[v:=P] \in sv^{\sigma}_{C}$. Hence $(M_2, N, L)_{u,v}$ is in sv^{σ}_{C} by definition.

We can prove $(M_3, N, L)_{u,v} \in sv^{\sigma}_{C}$ in the same way.

We will show that $M_1 \rightarrow^{*} \mathcal{C}_1[\langle 0, P\rangle]$ implies $(M_2, N, L)_{u,v}[w_1:=P]\ sv^{\sigma}_{C}$. Assume $M_1 \rightarrow^{*} \mathcal{C}_1[\langle 0, P\rangle]$. Then we have

$$\begin{aligned}(M_1, M_2, M_3)_{w_1, w_2} &\rightarrow^{*} (\mathcal{C}_1[\langle 0, P\rangle], M_2, M_3)_{w_1, w_2}\\ &\rightarrow^{*}_{\pi} \mathcal{C}'_1[(\langle 0, P\rangle, M_2, M_3)_{w_1, w_2}]\\ &\rightarrow \mathcal{C}'_1[M_2[w_1:=P]].\end{aligned}$$

By the first condition, we have $M_2[w_1:=P] \in SN$. By the second condition, we have $N, L \in sv^{\sigma}_{C}$. Suppose $M_2[w_1:=P] \rightarrow^{*} \mathcal{C}_2[\langle 0, Q\rangle]$. Then we have

$$(M_1, M_2, M_3)_{w_1, w_2} \rightarrow^{*} \mathcal{C}'_1[M_2[w_1:=P]] \rightarrow^{*} \mathcal{C}'_1[\mathcal{C}_2[\langle 0, Q\rangle]].$$

By letting $\mathcal{C}[\cdot]$ be $\mathcal{C}'_1[\mathcal{C}_2[\cdot]]$ in the third condition, we have $N[u:=Q] \in sv^{\sigma}_{C}$. Hence $M_2[w_1:=P] \rightarrow^{*} \mathcal{C}_1[\langle 0, Q\rangle]$ implies $N[u:=Q]\ sv^{\sigma}_{C}$. Similarly we can prove that $M_2[w_1:=P] \rightarrow^{*} \mathcal{C}_1[\langle 1, Q\rangle]$ implies $L[v:=Q] \in sv^{\sigma}_{C}$. Hence by definition we have $(M_2[w_1:=P], N, L)_{u,v} \in sv^{\sigma}_{C}$, that is, $(M_2, N, L)_{u,v}[w_1:=P] \in sv^{\sigma}_{C}$.

We can prove that $M_1 \rightarrow^{*} \mathcal{C}_1[\langle 1, P\rangle]$ implies $(M_3, N, L)_{u,v}[w_2:=P] \in sv^{\sigma}_{C}$ in a similar way.

Therefore we can conclude $(M_1, (M_2, N, L)_{u,v}, (M_3, N, L)_{u,v})_{w_1, w_2} \in sv^{\sigma}_{C}$ by definition.

Case ($\exists I$). The reduction is $\langle t, M\rangle \rightarrow \langle t, M'\rangle$. By the definition, we have $M \in sv^{\sigma}_{A[x:=t]}$. By IH, we have $M' \in sv^{\sigma}_{A[x:=t]}$. Hence $\langle t, M'\rangle$ is in $sv^{\sigma}_{\exists xA}$.

Case ($\exists E$). This case can be proved in a similar way to the case ($\vee E$).

Case ($\forall^2 I$). The reduction is $\lambda X^n.M \rightarrow \lambda X^n.M'$. Assume T is an abstraction term of arity n and F is a regular$_T$ set function. By the definition of $\lambda X.M \in sv^{\sigma}_{\forall XA}$, we have $M[X:=T] \in sv^{\sigma[X:=(T,F)]}_{A}$. By IH and $M[X:=T] \rightarrow M'[X:=T]$, we have $M'[X:=T] \in sv^{\sigma[X:=(T,F)]}_{A}$. Hence $\lambda X.M'$ is in $sv^{\sigma}_{\forall XA}$.

Case ($\forall^2 E$). This case is similar to the case ($\rightarrow E$).

Case ($\exists^2 I$). The reduction is $\langle T, M\rangle \rightarrow \langle T, M'\rangle$. By the definition of $\langle T, M\rangle \in sv^{\sigma}_{\exists XA}$, we have $M \in sv^{\sigma[X:=(T,F)]}_{A}$ for some F. By IH, we have $M' \in sv^{\sigma[X:=(T,F)]}_{A}$. Hence $\langle T, M'\rangle$ is in $sv^{\sigma}_{\exists XA}$.

Case ($\exists^2 E$). This case is proved in a similar way to the case ($\vee E$). □

Theorem 4.9 *sv^{σ}_{A} is a regular $_{A\sigma}$ set.*

Proof. Proposition 4.7 shows the clause (1) in the definition of regular sets. Proposition 4.8 proves the clause (2). □

Definition 4.10 For an abstraction term T and a set valuation σ, the regular $_{T\sigma}$ set function sv^{σ}_{T} is defined by $sv^{\sigma}_{T}(\vec{t}) = sv^{\sigma}_{T\vec{t}}$.

Lemma 4.11 *(1) If $sv^{\sigma[X:=(T\sigma, sv^{\sigma}_{T})]}_{B} = sv^{\sigma}_{B[X:=T]}$ holds for every proper subformula B of A, then $M \in sv^{\sigma[X:=(T\sigma, sv^{\sigma}_{T})]}_{A}$ implies $M \in sv^{\sigma}_{A[X:=T]}$.*

(2) If $sv^{\sigma[X:=(T\sigma, sv^{\sigma}_{T})]}_{B} = sv^{\sigma}_{B[X:=T]}$ holds for every proper subformula B of A, then $M \in sv^{\sigma}_{A[X:=T]}$ implies $M \in sv^{\sigma[X:=(T\sigma, sv^{\sigma}_{T})]}_{A}$.

(3) $sv^{\sigma[X:=(T\sigma, sv^{\sigma}_{T})]}_{A} = sv^{\sigma}_{A[X:=T]}$ holds for every type A.

Proof. Let σ' be $\sigma[X:=(T\sigma, sv^{\sigma}_{T})]$. Let C' be $C[X:=T]$ for every type C. We will say the small type condition to denote the condition that $sv^{\sigma}_{B}[X:=(T\sigma, sv^{\sigma}_{T})] = sv^{\sigma}_{B[X:=T]}$ for every proper subformula B of A. We note $A(\sigma') = A'\sigma$ since the both sides are $A[\vec{Y}:=\vec{T}, X:=T\sigma]$ where $\sigma(Y_i) = (T_i, F_i)$.

(1) We will use induction on the definition of $M \in sv^{\sigma'}_{A}$ to prove $M \in sv^{\sigma}_{A'}$.

Cases will be listed according to the definition of $sv^{\sigma'}_{A}$.

Case (Var). The claim holds since $M \equiv u^{\mathrm{A}(\sigma')}$.

Case (Var2) (1) $A \equiv X\vec{t}$. The assumption is $M \in sv^{\sigma'}_{X\vec{t}}$. By the definition of sv, we have $M \in sv^{\sigma}_{T}(\vec{t})$. So $M \in sv^{\sigma}_{T\vec{t}}$ holds by the definition of sv^{σ}_{T}. The claim $M \in sv^{\sigma}_{(X\vec{t})'}$ is also $M \in sv^{\sigma}_{T\vec{t}}$ by the definition of substitution.

Case (Var2) (2) $A \equiv Y\vec{t}$ and $Y \not\equiv X$. Both of the assumption and the claim are $M \in F(\vec{t})$ by definition where $\sigma(Y) = (T_1, F)$.

Case ($\rightarrow I$) $\lambda u.M \in \mathrm{sv}^{\sigma'}_{C\rightarrow D}$. By the assumption and the definition, for every $N \in sv^{\sigma'}_{C}$, $M[u:=N]$ is in $sv^{\sigma'}_{D}$. By the small type condition, it is equivalent to that for every $N \in sv^{\sigma}_{C'}$, $M[u:=N]$ is in $sv^{\sigma}_{D'}$. Hence we have $\lambda u.M \in sv^{\sigma}_{(C\rightarrow D)'}$.

Case ($\rightarrow E$). By the assumption, $MN \rightarrow L$ implies $L \in sv^{\sigma'}_{A}$. By IH, $MN \rightarrow L$ implies $L \in sv^{\sigma}_{A'}$. Therefore MN is in

$sv^{\sigma}_{A'}$ by definition.

Case ($\vee E$) $(M, N, L)_{u,v} \in sv^{\sigma'}_{C}$. By the assumption and the definition, $M \in SN$, $N, L \in sv^{\sigma'}_{C}$, $M \to {}^{*}\mathcal{C}\,[\langle 0, P\rangle]$ implies $N\,[u := P] \in sv^{\sigma'}_{C}$ for every P, and $M \to^{*} \mathcal{C}\,[\langle 1, \mathrm{P}\rangle]$ implies $L\,[v := P] \in sv^{\sigma'}_{C}$ for every P. By IH, $N, L \in sv^{\sigma}_{C'}$, $M \to {}^{*}\mathcal{C}\,[\langle 0, P\rangle]$ implies $N\,[u := P] \in sv^{\sigma}_{C'}$ for every P, and $M \to {}^{*}\mathcal{C}\,[\langle 1, P\rangle]$ implies $L\,[v := P] \in sv^{\sigma}_{C'}$ for every P. Hence we have $(M, N, L)_{u,v}\ sv^{\sigma}_{C'}$ by definition.

Cases ($\&I$), ($\&E$), ($\vee I$), ($\forall I$), and ($\forall E$) are similarly proved to the previous three cases.

Case ($\forall^2 I$) $\lambda Y.M \in sv^{\sigma'}_{\forall YA}$. By the assumption and the definition, for every abstraction term T_1 and every regular$_{T_1}$ set function F, $M\,[Y := T_1] \in sv^{\sigma'[Y := (T_1, F)]}_{A}$ holds. By combining this with the small type condition, we have $M\,[Y := T_1] \in sv^{\sigma[Y := (T_1, F)]}_{A}$. Hence we have $\lambda Y.M \in sv^{\sigma}_{(\forall YA)'}$ by definition.

Case ($\forall^2 E$) can be proved in the same way as the case ($\to E$).

Case ($\exists^2 I$) $\langle T_1, M\rangle \in sv^{\sigma'}_{\forall YA}$. By the assumption and the definition, we have $M \in sv^{\sigma'[Y := (T_1, F)]}_{A}$ for some regular$_{T_1}$ set function F. By the small type condition, we have $M \in sv^{\sigma'\,[Y := (T_1, F)]}_{A'}$. Hence $\langle T_1, M\rangle \in sv^{\sigma}_{(\exists YA)'}$ holds by definition.

Case ($\exists^2 E$) $(M, N)_{Y,u} \in sv^{\sigma}_{C}{}'$. By the assumption and the definition, M is in SN, N is in $sv^{\sigma'}_{C}$, and M $\to {}^{*}\mathcal{C}\,[\langle T_1, P\rangle]$ implies $N\,[Y := T_1, u := P] \in sv^{\sigma'}_{C}$ for every T_1 and every P. By IH, N is in $sv^{\sigma}{}_{C'}$, and $M \to {}^{*}\mathcal{C}\,[\langle T_1, P\rangle]$ implies $N\,[Y := T_1, u := P] \in sv^{\sigma}_{C'}$ for every T_1 and every P. Hence we have $(M, N)_{Y,u} \in sv^{\sigma}_{C'}$ by definition.

Cases ($\exists I$) and ($\exists E$) can be proved similarly to the previous two cases.

(2) We will show that if we have $M \in sv^{\sigma}_{C'}$ then $C \equiv A\,[X := T]$ implies $M \in sv^{\sigma[X := (T\sigma, sv^{\sigma}_{T})]}_{A}$, by induction on the definition of $M \in sv^{\sigma}_{C}$.

Cases will be listed according to the definition of $M \in sv^{\sigma}_{C}$ except the case (Subst).

Case (Subst) $C \equiv T\vec{t}$, $A \equiv X\vec{t}$, and $M \in sv^{\sigma}_{C}$. By the definition of sv^{σ}_{T}, we have $sv^{\sigma}_{C} = sv^{\sigma}_{T}\,(\vec{t})$. By the definition of sv, $M \in sv^{\sigma'}_{X\vec{t}}$ holds.

Case (Var2) (1) $C \equiv Y\vec{s}\,[\vec{x} := \vec{t}]$, $A \equiv X\vec{t}$, and $T \equiv \lambda\vec{x}.Y\vec{s}$, and $M \equiv sv^{\sigma}_{C}$. This case is included in Case (Subst).

Case (Var2) (2) $C \equiv A \equiv Y\vec{t}$, $X \not\equiv Y$, and $M \in sv^{\sigma}_{C}$. Let $\sigma\,(Y) = (T_0, F)$. We have $M \in F\,(\vec{t})$ by the definition of sv. So $M \in sv^{\sigma'}_{A}$ holds by the definition of sv.

Case ($\to I$) (1) $C \equiv B_1\,[\vec{x} := \vec{t}] \to B_2\,[\vec{x} := \vec{t}]$, $A \equiv X\vec{t}$, $T \equiv \lambda\vec{x}.B_1 \to B_2$, and $\lambda u^{B_1\,[\vec{x} := \vec{t}]\sigma}.\ M \in sv^{\sigma}_{B_1\,[\vec{x} := \vec{t}] \to B_2\,[\vec{x} := \vec{t}]}$. This case is included in Case (Subst).

Case ($\to I$) (2) $C \equiv A'_1 \to A'_2$ and $A \equiv A_1 \to A_2$, and $\lambda u^{A'_1\sigma}.\ M \in sv^{\sigma}_{A'_1 \to A'_2}$. Assume $N \in sv^{\sigma'}_{A_1}$. By the small type condition for A_1, N is in $sv^{\sigma}_{A'_1}$. By the definition of sv, we have $M\,[u^{A_1'\sigma} := N] \in sv^{\sigma}_{A'_2}$. By the small type condition for A_2, $M\,[u^{A'_1\sigma} := N]$ is in $sv^{\sigma'}_{A_2}$. Since $A_1\,(\sigma') \equiv A'_1\sigma$, we have $M\,[u^{A_1\sigma'} := N]$ is in $sv^{\sigma'}_{A_2}$. By the definition of sv, $\lambda u^{A_1\sigma'}.\ M \in sv^{\sigma'}_{A_1 \to A_2}$.

Case ($\to E$) $MN \in sv^{\sigma}_{A'}$. By the definition of sv, we have $MN : A'\sigma$, so we have $MN : A\,(\sigma')$. Assume $MN \to L$. By the definition of sv, we have $L \in sv^{\sigma}_{A'}$. By IH, L is in $sv^{\sigma'}_{A}$. By the definition of sv, we have $MN \in sv^{\sigma'}_{A}$.

Case ($\forall^2 I$) (1) $C \equiv \forall Y\,(B\,[\vec{x} := \vec{t}])$, $A \equiv X\vec{t}$, $T \equiv \lambda\vec{x}.\forall YB$, and $\lambda Y.M \in sv^{\sigma}_{C}$. This case is included in Case (Subst).

Case ($\forall^2 I$) (2) $C \equiv \forall YB'$, $A \equiv \forall YB$, and $\lambda Y.M \in sv^{\sigma}_{\forall YB'}$. We can suppose Y is fresh by renaming bound variables. By the definition of sv, $M\,[Y := T_1]$ is in $sv^{\sigma\,[Y := (T_1, F_1)]}_{B'}$ for every abstraction term T_1 and every regular$_{T_1}$ set function F_1. By the small type condition for B, $M\,[Y := T_1]$ is in $sv^{\sigma'[Y := (T_1, F_1)]}_{B}$. By the definition of sv, $\lambda Y.M \in sv^{\sigma'}_{\forall YB}$.

Case ($\forall^2 E$) $MT \in sv^{\sigma}_{A'}$. By the definition of sv, we have $MT : A'\sigma$, so we have $MT : A\,(\sigma')$. Assume $MT \to L$. By the definition of sv, we have $L \in sv^{\sigma}_{A'}$, By IH, L is in $sv^{\sigma'}_{A}$. By the definition of sv, we have $MT \in sv^{\sigma'}_{A}$.

Other cases can be proved similarly.

(3) We will use induction on A to prove $sv^{\sigma'}_{A} = sv^{\sigma}_{A'}$. We will prove the claim for A. Then the induction hypothesis is that the claim holds for every proper subformula B of A. Suppose $M \in sv^{\sigma'}_{A}$. By IH and (1), we have $M \in sv^{\sigma}_{A'}$. On the other hand, by IH and (2), $M \in sv^{\sigma}_{A'}$ implies $M \in sv^{\sigma'}_{A}$. Therefore we can conclude $sv^{\sigma'}_{A} = sv^{\sigma}_{A'}$. □

Lemma 4.12 *(1) If M is in $sv^{\sigma}_{A \to B}$ and N is in sv^{σ}_{A}, then MN is in sv^{σ}_{B}.*

(2) If M is in $sv^{\sigma}_{A\&B}$, then Mp_0 is in sv^{σ}_{A} and Mp_1 is in sv^{σ}_{B}.

(3) If M is in $sv^{\sigma}_{\forall xA}$ and t is a first order term, then Mt is in $sv^{\sigma}_{A[x := t]}$.

(4) If M is in $sv^{\sigma}_{\forall X^n A}$ and T is an abstraction term of arity n, then $M\,(T\sigma)$ is in $sv^{\sigma}_{A[X := T]}$.

Proof. (1) We will use induction on $(|M|, \#M, |N|)$. Assume $MN \to L$. We will show $L \in sv^{\sigma}_{B}$. Cases will be listed according to the reduction.

Case $MN \to M'N$. By Proposition 4.8, M' is in $sv^{\sigma}_{A \to B}$. By IH for $|M'| < |M|$, we have $M'N \in sv^{\sigma}_{B}$.

Case $MN \to MN'$. This case is similar to the previous case.

Case $(\lambda u.M)\,N \to M\,[u := N]$. By the definition of $\lambda u.M \in sv^{\sigma}_{A \to B}$, we have $M\,[u := N] \in sv^{\sigma}_{B}$.

Case $(M_1, M_2, M_3)_{u,v}N \to (M_1, M_2N, M_3N)_{u,v}$. Let M be $(M_1, M_2, M_3)_{u,v}$. From the assumption $M \in sv^{\sigma}_{A \to B}$, the following four conditions hold : $M_1 \in SN$, $M_2, M_3 \in sv^{\sigma}_{A\to B}$, $M_1 \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$ implies $M_2\,[u := P] \in sv^{\sigma}_{A\to B}$, and $M_1 \to^{*} \mathcal{C}\,[\langle 1, P\rangle]$ implies $M_3\,[v := P] \in sv^{\sigma}_{A\to B}$. We will show each clause in the definition of $(M_1, M_2N, M_3N)_{u,v} \in sv^{\sigma}_{A\to B}$.

M_1 is in SN by the first condition.

By the second condition, M_2 is in $sv^{\sigma}_{A\to B}$. By IH for $|M_2| \le |M|$ and $\#M_2 < \#M$, we have $M_2N \in sv^{\sigma}_{B}$.

Similarly we have $M_3N \in sv^{\sigma}_{B}$.

Assume $M_1 \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$ and we will show $(M_2N)\,[u := P] \in sv^{\sigma}_{B}$. we have

$$\begin{aligned}(M_1, M_2, M_3)_{u,v} &\to^{*} (\mathcal{C}\,[\langle 0, P\rangle], M_2, M_3)_{u,v}\\ &\to^{*}_{\pi} \mathcal{C}'\,[(\langle 0, P\rangle, M_2, M_3)_{u,v}]\\ &\to \mathcal{C}'\,[M_2\,[u := P]].\end{aligned}$$

By Proposition 4.8, $\mathcal{C}'\,[M_2\,[u := P]]$ is in $sv^{\sigma}_{A\to B}$. By the definition of sv, $M_2\,[u := P]$ is in $sv^{\sigma}_{A\to B}$. From the above, we also have $|M_2\,[u := P]| < |(M_1, M_2, M_3)_{u,v}|$. By IH for $|M_2\,[u := P]| < |(M_1, M_2, M_3)_{u,v}|$, we have $M_2\,[u := P]\,N \in sv^{\sigma}_{B}$, that is, $(M_2N)\,[u := P] \in sv^{\sigma}_{B}$. Hence $M_1 \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$ implies $(M_2N)\,[u := P] \in sv^{\sigma}_{B}$.

Similarly $M_1 \to^{*} \mathcal{C}\,[\langle 1, P\rangle]$ implies $(M_3N)\,[v := P] \in sv^{\sigma}_{B}$.

Hence we have $(M_1, M_2N, M_3N)_{u,v} \in sv^{\sigma}_{A\to B}$, since each clause in its definition has been shown.

Case $(M_1, M_2)_{\alpha,u}\,N \to (M_1, M_2N)_{\alpha,u}$ where α is x or X. This case can be proved in a similar manner to the previous case.

We have proved that $MN \to L$ implies $L \in sv^{\sigma}_{B}$ for every L. Therefore $MN \in sv^{\sigma}_{B}$ holds by definition.

(2) This claim can be proved similarly to the claim (1).

(3) This claim can be proved in the same way as the claim (4).

(4) We will use induction on $(|M|, \#M)$. Assume $M\,(T\sigma) \to N$. We will show $N \in sv^{\sigma}_{A\,[X := T\,]}$. Cases will be listed according to the reduction.

Case $M\,(T\sigma) \to M'\,(T\sigma)$. By Proposition 4.8, M' is in $sv^{\sigma}_{\forall XA}$. By IH for $|M'| < |M|$, we have $M'\,(T\sigma) \in sv^{\sigma}_{A\,[X := T]}$.

Case $(\lambda X.M)\,(T\sigma) \to M\,[X := T\sigma]$. By letting T be $T\sigma$ and F be sv^{σ}_{T} in the definition of $\lambda X.M \in sv^{\sigma}_{\forall XA}$, we have $M\,[X := T\sigma] \in sv_{A}^{\sigma[X := (T\sigma,\, sv^{\sigma}_{T})]}$. By Lemma 4.11 (3), we have $M\,[X := T\sigma] \in sv^{\sigma}_{A\,[X := T]}$.

Case $(M_1, M_2, M_3)_{u,v}\,(T\sigma) \to (M_1, M_2\,(T\sigma), M_3\,(T\sigma))_{u,v}$. From the definition of $(M_1, M_2, M_3)_{u,v} \in sv^{\sigma}_{\forall XA}$, the following four conditions hold : M_1 is in SN, M_2, M_3 are in $sv^{\sigma}_{\forall XA}$, $M_1 \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$ implies $M_2\,[u := P] \in sv^{\sigma}_{\forall XA}$, and $M_1 \to^{*} \mathcal{C}\,[\langle 1, P\rangle]$ implies $M_3\,[v := P] \in sv^{\sigma}_{\forall XA}$. We will show each clause in the definition of $(M_1, M_2\,(T\sigma), M_3\,(T\sigma))_{u,v} \in sv^{\sigma}_{A\,[X := T]}$.

M_1 is in SN by the first condition.

M_2 is in $sv^{\sigma}_{\forall XA}$ by the second condition. By IH for $|M_2| \le |(M_1, M_2, M_3)_{u,v}|$ and $\#M_2 < \#(M_1, M_2, M_3)_{u,v}$, we have $M_2(T\sigma) \in sv^{\sigma}_{A\,[X := T]}$.

Similarly we have $M_3\,(T\sigma) \in sv^{\sigma}_{A\,[X := T]}$.

Assume $M_1 \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$. Then we have

$$\begin{aligned}(M_1, M_2, M_3)_{u,v} &\to^{*} (\mathcal{C}\;[\langle 0, P\rangle], M_2, M_3)_{u,v}\\ &\to^{*}_{\pi} \mathcal{C}'\,[(\langle 0, P\rangle, M_2, M_3)_{u,v}]\\ &\to \mathcal{C}'\,[M_2\,[u := P]].\end{aligned}$$

By Proposition 4.8, we have $\mathcal{C}'\,[M_2\,[u := P]] \in sv^{\sigma}_{\forall XA}$. By the definition of sv, we have $M_2\,[u := P] \in sv^{\sigma}_{\forall XA}$. From the above, $|M_2\,[u := P]| < |(M_1, M_2, M_3)_{u,v}|$ holds. By IH for $M_2\,[u := P]$, we have $M_2\,[u := P]\,(T\sigma) \in sv^{\sigma}_{A\,[X := T]}$, that is, $(M_2\,(T\sigma))\,[u := P] \in sv^{\sigma}_{A\,[X := T]}$. Hence $M_1 \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$ implies $(M_2\,(T\sigma))\,[u := P] \in sv^{\sigma}_{A\,[X := T]}$.

Similarly $M_1 \to^{*} \mathcal{C}\,[\langle 1, P\rangle]$ implies $(M_3\,(T\sigma))\,[v := P] \in sv^{\sigma}_{A\,[X := T]}$.

We have shown each condition in the definition, so we can conclude $(M_1, M_2\,(T\sigma), M_3\,(T\sigma))_{u,v} \in sv^{\sigma}_{A\,[X := T]}$.

Case $(M_1, M_2)_{\alpha,u}\,(T\sigma) \to (M_1, M_2\,(T\sigma))_{\alpha,u}$ where α is x or X. This case can be proved in the same way as the previous case.

We have proved that $M\,(T\sigma) \to N$ implies $N \in sv^{\sigma}_{A\,[X := T]}$ for every N. Hence $M\,(T\sigma)$ is in $sv^{\sigma}_{A\,[X := T]}$ by definition.

□

Definition 4.13 A first order valuation is a mapping that maps a first order variable to a first order term. A valuation is a mapping that maps a term variable u^A to a term of type A.

For a first order valuation τ and a term M, $M\tau$ is defined as $M\,[x_1 := \tau\,(x_1), \ldots, x_n := \tau\,(x_n)]$ where all the free first order variables in M are $x_1, \ldots, x_n$. For a first order term t, a formula A, and an abstraction term T, $t\tau$, $A\tau$, and $T\tau$ are defined in the same way as for $M\tau$.

For a valuation ρ and a term M, $M\rho$ is defined as $M\,[u_1 := \rho\,(u_1), \ldots, u_n = \rho\,(u_n)]$ where all the free term variables in M are $u_1, \ldots, u_n$.

For a set valuation σ and a term M, $M\sigma$ is defined as $M\,[X_1 : = T_1,..., X_n : = T_n]$ where the free predicate variables in M are $X_1,..., X_n$ and $\sigma\,(X_i) = (T_i, F_i)$.

The valuation $\rho\,[u^A : = M]$ is defined by $(\rho\,[u^A : = M])\,(u^A) = M$ and $(\rho\,[u^A : = M])\,(v^B) = \rho\,(v^B)$ if $u^A \not\equiv v^B$. The first order valuation $\tau\,[x : = t]$ is defined similarly. We will write $M\tau\sigma\rho$ to denote $((M\tau)\,\sigma)\,\rho$. We will also use $t\tau\sigma\rho$, $A\tau\sigma\rho$, and $T\tau\sigma\rho$ in a similar way. Note that $t\sigma\rho$ is always t, $A\rho$ is always A, and $T\rho$ is always T.

Note that $(u^A)\,[X : = T] \equiv u^{A\,[\,X\,:\,=\,T\,]}$.

Theorem 4.14 *For any set valuation σ, any valuation ρ, and any first order valuation τ, if $M : A$ is provable and $\rho\,(u^{B\tau\sigma})$ is in $sv^{\sigma}_{B\tau}$ for every free term variable u^B of M, then we have $M\tau\sigma\rho \in sv^{\sigma}_{A\tau}$.*

Proof. We will use induction on the proof of $M : A$. We will consider cases according to the last rule used in the proof.

Case (Assumption). The proof is $u^A : A$. By the assumption, we have $u^A\tau\sigma\rho = \rho\,(u^{A\tau\sigma}) \in sv^{\sigma}_{A\tau}$.

Case ($\to I$). The proof is

$$\dfrac{\begin{array}{c}[u^A : A]\\ \vdots\\ M : B\end{array}}{\lambda u^A.\, M : A \to B}$$

Assume $N \in sv^{\sigma}_{A\tau}$. Let ρ' be $\rho[u^{A\tau\sigma} : = N]$. By IH, we have $M\tau\sigma\rho' \in sv^{\sigma}_{B\tau}$, that is, $(M\tau\sigma\rho)\,[u^{A\tau\sigma} : = N]$. Then $N \in sv^{\sigma}_{A\tau}$ implies $(M\tau\sigma\rho)\,[u^{A\tau\sigma} : = N] \in sv^{\sigma}_{B\tau}$. Hence we have $\lambda u^{A\tau\sigma}.\, M\tau\sigma\rho \in sv^{\sigma}_{A\tau \to B\tau}$, that is, $(\lambda u^A.\, M)\;\tau\sigma\rho \in sv^{\sigma}_{(A \to B)\,\tau}$.

Case ($\to E$). The proof is

$$\dfrac{M : A \to B \quad N : A}{MN : B}$$

By IH, we have $M\tau\sigma\rho \in sv^{\sigma}_{(A \to B)\tau}$ and $N\tau\sigma\rho \in sv^{\sigma}_{A\tau}$. By Lemma 4.12 (1), we have $(M\tau\sigma\rho)\,(N\tau\sigma\rho) \in sv^{\sigma}_{B\tau}$, that is, $(MN)\;\tau\sigma\rho \in sv^{\sigma}_{B\tau}$.

Case ($\&I$). The proof is

$$\dfrac{M : A \qquad N : B}{\langle M, N\rangle : A \;\&\; B}$$

By IH, we have $M\tau\sigma\rho \in sv^{\sigma}_{A\tau}$ and $N\tau\sigma\rho \in sv^{\sigma}_{B\tau}$. By the definition of sv, we have $\langle M\tau\sigma\rho, N\tau\sigma\rho\rangle \in sv^{\sigma}_{A\tau\,\&\,B\tau}$, that is, $\langle M, N\rangle\tau\sigma\rho \in sv^{\sigma}_{(A\&B)\tau}$.

Case ($\&E1$). The proof is

$$\dfrac{M : A \;\&\; B}{Mp_0 : A}$$

By IH, $M\tau\sigma\rho$ is in $sv^{\sigma}_{(A\&B)\tau}$. By Lemma 4.12 (2), we have $(M\tau\sigma\rho)\;p_0 \in sv^{\sigma}_{A\tau}$, that is, $(Mp_0)\;\tau\sigma\rho \in sv^{\sigma}_{A\tau}$.

Case ($\&E2$). This case is similar to the previous case.

Case ($\forall I$). The proof is

$$\dfrac{M : A}{\lambda x.\, M : \forall xA}$$

Assume that t is a first order term. We can suppose that x is fresh by replacing every free occurrence of x in the proof by a fresh variable and renaming bound variables. Let τ' be $\tau[x : = t]$. By IH, we have $M\tau'\sigma\rho \in sv^{\sigma}_{A(\tau')}$, that is, $(M\tau\sigma\rho)\;[x : = t] \in sv^{\sigma}_{(A\tau)[x\,:\,=\,t]}$ by the variable condition. Hence $(M\tau\sigma\rho)[x : =t] \in sv^{\sigma}_{(A\tau)\,[x\,:\,=\,t]}$ holds for any first order term t. Then by definition we have $\lambda x.\, M\tau\sigma\rho \in sv^{\sigma}_{\forall x\,(A\tau)}$, that is, $(\lambda x.\, M)\tau\sigma\rho \in sv^{\sigma}_{(\forall xA)\tau}$.

Case ($\forall E$). The proof is

$$\dfrac{M : \forall xA}{Mt : A[x : = t]}$$

We can suppose that x is fresh by renaming bound variables. By IH, $M\tau\sigma\rho$ is in $sv^{\sigma}_{(\forall xA)\tau}$. By letting t be $t\tau$ in Lemma 4.12 (3), we have $(M\tau\sigma\rho)\;(t\tau) \in sv^{\sigma}_{(A\tau)\,[x\,:\,=\,t\tau]}$, that is, $(Mt)\tau\sigma\rho \in sv^{\sigma}_{A[x\,:\,=\,t]\tau}$.

Case ($\bigvee I$). This case is similar to the case ($\&I$).

Case ($\bigvee E$). The proof is

$$\dfrac{M : A \bigvee B \qquad \begin{matrix} [u^A : A] \\ \vdots \\ N : C \end{matrix} \qquad \begin{matrix} [v^B : B] \\ \vdots \\ L : C \end{matrix}}{(M, N, L)_{u^A, v^B} : C}$$

We will show each clause in the definition of $(M\tau\sigma\rho, N\tau\sigma\rho, L\tau\sigma\rho)_{u^{A\tau\sigma}, v^{B\tau\sigma}} \in sv^{\sigma}_{C\tau}$.

By IH, $M\tau\sigma\rho$ is in $sv^{\sigma}_{(A\bigvee B)\tau}$. By Proposition 4.7, $M\tau\sigma\rho$ is in SN.

By IH, $N\tau\sigma\rho$ and $L\tau\sigma\rho$ are in $sv^{\sigma}_{C\tau}$.

Assume $M\tau\sigma\rho \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$. By Proposition 4.8, $\mathcal{C}\,[\langle 0, P\rangle]$ is in $sv^{\sigma}_{(A\bigvee B)\tau}$. By the definition of sv, $\langle 0, P\rangle$ is in $sv^{\sigma}_{(A\bigvee B)\tau}$, so P is in $sv^{\sigma}_{A\tau}$ by definition. Let ρ' be $\rho[u^{A\tau\sigma} := P]$. Then, by IH, we have $N\tau\sigma\rho' \in sv^{\sigma}_{C\tau}$, that is, $(N\tau\sigma\rho)\,[u^{A\tau\sigma} := P] \in sv^{\sigma}_{C\tau}$. Hence we can conclude that $M\tau\sigma\rho \to^{*} \mathcal{C}\,[\langle 0, P\rangle]$ implies $(N\tau\sigma\rho)\,[u^{A\tau\sigma} := P] \in sv^{\sigma}_{C\tau}$.

Similarly we can prove that $M\tau\sigma\rho \to^{*} \mathcal{C}\,[\langle 1, P\rangle]$ implies $(L\tau\sigma\rho)\,[v^{B\tau\sigma} := P] \in sv^{\sigma}_{C\tau}$.

Since we have shown each condition in the definition, we have $(M\tau\sigma\rho, N\tau\sigma\rho, L\tau\sigma\rho)_{u^{A\tau\sigma}, v^{B\tau\sigma}} \in sv^{\sigma}_{C\tau}$, that is, $(M, N, L)_{u^A, v^B}\tau\sigma\rho \in sv^{\sigma}_{C\tau}$.

Case ($\exists I$). The proof is

$$\dfrac{M : A\,[x := t]}{\langle t, M\rangle : \exists x A}$$

We can suppose that x is fresh by renaming bound variables. By IH, we have $M\tau\sigma\rho \in sv^{\sigma}_{A[x := t]\tau}$, that is, $M\tau\sigma\rho \in sv^{\sigma}_{(A\tau)[x := t\tau]}$. Hence we have $\langle t\tau, M\tau\sigma\rho\rangle \in sv^{\sigma}_{\exists x(A\tau)}$, that is, $\langle t, M\rangle\tau\sigma\rho \in sv^{\sigma}_{(\exists x A)\tau}$.

Case ($\exists E$). The proof is

$$\dfrac{M : \exists x A \qquad \begin{matrix} [u^A : A] \\ \vdots \\ N : C \end{matrix}}{(M, N)_{x, u^A} : C}$$

We can suppose that x and u^B are fresh for any type B by replacing every occurrence of x and u^B in the proof by fresh variables and renaming bound variables. By IH, $M\tau\sigma\rho$ is in $sv^{\sigma}_{(\exists x A)\tau}$. By Proposition 4.7, $M\tau\sigma\rho$ is in SN. By IH, $N\tau\sigma\rho$ is in $sv^{\sigma}_{C\tau}$.

Assume $M\tau\sigma\rho \to^{*} \mathcal{C}\,[\langle t, P\rangle]$. By Proposition 4.8, $\mathcal{C}\,[\langle t, P\rangle]$ is in $sv^{\sigma}_{(\exists x A)\tau}$. By the definition of sv, we have $\langle t, P\rangle \in sv^{\sigma}_{(\exists x A)\tau}$. Therefore P is in $sv^{\sigma}_{(A\tau)[x := t]}$ by the definition of sv. Let τ' be $\tau[x := t]$ and ρ' be $\rho[u^{(A\tau)\,[x := t]\sigma} := P]$. By IH, we have $N\tau'\sigma\rho' \in sv^{\sigma}_{C\tau'}$. From the variable condition, $N\tau'\sigma\rho' = N\tau\sigma\rho\,[x := t, u^{A\tau\sigma} := P]$ and $C\tau' = C\tau$ hold. Then we have $(N\tau\sigma\rho)\,[x := t, u^{A\tau\sigma} := P] \in sv^{\sigma}_{C\tau}$. Hence $M\tau\sigma\rho \to^{*} \mathcal{C}\,[\langle t, P\rangle]$ implies $(N\tau\sigma\rho)\,[x := t, u^{A\tau\sigma} := P] \in sv^{\sigma}_{C\tau}$.

Since we have shown each condition in the definition, we have $(M\tau\sigma\rho, N\tau\sigma\rho)_{x, u^{A\tau\sigma}} \in sv^{\sigma}_{C\tau}$, that is, $(M, N)_{x, u^A}\tau\sigma\rho \in sv^{\sigma}_{C\tau}$.

Case ($\forall^2 I$). The proof is

$$\dfrac{M : A}{\lambda X^n.\, M : \forall X^n A}$$

Assume that T is an abstraction term of arity n and F is a regular$_T$ set function. We can suppose that X is fresh by replacing every occurrence of X in the proof by a fresh variable and renaming bound variables. Let σ' be $\sigma\,[X := (T, F)]$. By IH, we have $M\tau\sigma'\rho \in sv^{\sigma'}{}_{\mathrm{A}\tau}$. By the variable condition, we have $(M\tau\sigma\rho)\,[X := T] \in sv^{\sigma'}{}_{\mathrm{A}\tau}$. Hence $(M\tau\sigma\rho)\,[X := T] \in sv^{\sigma[X := (T, F)]}_{A\tau}$ holds for any T and any F. Then by definition we have $\lambda X.\, M\tau\sigma\rho \in sv^{\sigma}_{\forall X\,(A\tau)}$, that is, $(\lambda X.\, M)\,\tau\sigma\rho \in sv^{\sigma}_{(\forall X A)\tau}$.

Case ($\forall^2 E$). The proof is

$$\dfrac{M : \forall X A}{MT : A\,[X := T]}$$

By IH, $M\tau\sigma\rho$ is in $sv^{\sigma}_{(\forall X A)\tau}$. By letting T be $T\tau$, M be $M\tau\sigma\rho$, and A be $A\tau$ in Lemma 4.12 (4), we have $(M\tau\sigma\rho)\,(T\tau\sigma) \in sv^{\sigma}_{(A\tau)\,[X := T\tau]}$, that is, $(MT)\tau\sigma\rho \in sv^{\sigma}_{A\,[X := T]\,\tau}$.

Case ($\exists^2 I$). The proof is

$$\frac{M : A[X := T]}{\langle T, M\rangle : \exists XA}$$

We can suppose that X is fresh by renaming bound variables. By IH, we have $M\tau\sigma\rho \in sv^{\sigma}_{A[X := T]\tau}$, that is, $M\tau\sigma\rho \in sv^{\sigma}_{(A\tau)[X := T\tau]}$. By Lemma 4.11 (3), we have $M\tau\sigma\rho \in sv^{\sigma[X := (T\tau\sigma,\, sv^{\sigma}{}_{T\tau})]}_{A\tau}$. Hence we have $\langle T\tau\sigma, M\tau\sigma\rho\rangle \in sv^{\sigma}_{\exists X(A\tau)}$, that is, $\langle T, M\rangle\tau\sigma\rho \in sv^{\sigma}_{(\exists XA)\tau}$.

Case ($\exists^2 E$). The proof is

$$\frac{M : \exists XA \qquad \begin{matrix}[u^A : A] \\ \vdots \\ N : C\end{matrix}}{(M, N)_{X,\, u^A} : C}$$

We can suppose that X and u^B are fresh for any type B by replacing every occurrence of x and u^B in the proof by fresh variables and renaming bound variables. We will show each condition in the definition $(M\tau\sigma\rho, N\tau\sigma\rho)_{X,\, u^{A\tau\sigma}} \in sv^{\sigma}_{C\tau}$. By IH, $M\tau\sigma\rho$ is in $sv^{\sigma}_{(\exists XA)\tau}$. By Proposition 4.7, $M\tau\sigma\rho$ is in SN. By IH, $N\tau\sigma\rho$ is in $sv^{\sigma}_{C\tau}$.

Assume $M\tau\sigma\rho \to^{*} \mathcal{C}[\,\langle T, P\rangle\,]$. By Proposition 4.8, $\mathcal{C}[\,\langle T, P\rangle\,]$ is in $sv^{\sigma}_{(\exists XA)\tau}$. By the definition of sv, we have $\langle T, P\rangle \in sv^{\sigma}_{(\exists XA)\tau}$. Therefore by the definition of sv we have $P \in sv^{\sigma[X := (T, F)]}_{A\tau}$ for some regular$_T$ set function F. Let σ' be $\sigma[X := (T, F)]$ and ρ' be $\rho[u^{A\tau\sigma[X := T]} := P]$. By IH, we have $N\tau\sigma'\rho' \in sv^{\sigma'}{}_{C\tau}$. From the variable condition, $N\tau\sigma'\rho' = N\tau\sigma\rho\,[X := T, u^{A\tau\sigma} := P]$ holds and X does not occur in $C\tau$. Then we have $sv^{\sigma'}{}_{C\tau} = sv^{\sigma}_{C\tau}$ by Lemma 4.11 (3). By combining them, we have $(N\tau\sigma\rho)\,[X := T, u^{A\tau\sigma} := P] \in sv^{\sigma}_{C\tau}$. Hence $M\tau\sigma\rho \to^{*} \mathcal{C}[\langle T, P\rangle]$ implies $(N\tau\sigma\rho)\,[X := T, u^{A\tau\sigma} := P] \in sv^{\sigma}_{C\tau}$ for every T and every P.

Since we have shown each condition in the definition, we have $(M\tau\sigma\rho, N\tau\sigma\rho)_{X,\, u^{A\tau\sigma}} \in sv^{\sigma}_{C\tau}$, that is, $(M, N)_{X,\, u^A}\tau\sigma\rho \in sv^{\sigma}_{C\tau}$. □

Theorem 4.15 (Strong normalization) *If M is a term of NJ^2, then M is strongly normalizable.*

Proof. Suppose $M : A$. Let the first order valuation τ and the valuation ρ be the identity function. Define the set valuation σ by $\sigma(X) = (X, SN_X)$. Then, by Theorem 4.14, we have $M\tau\sigma\rho \in sv^{\sigma}_{A\tau}$, that is, $M \in sv^{\sigma}_{A}$. By Proposition 4.7, M is in SN. □

Acknowledgments

We would like to thank Prof. Grigori Mints to give me a chance to think of the problem. We would like to thank Prof. Anne Troelstra and Dr. Kazushige Terui for information on related work.

References

[1] H. P. Barendregt, "Lambda calculi with types," In *Hand book of Logic in Computer Science*, vol. 2, S. Abramsky et al., Eds., Oxford University Press, pp.118–309, 1992.

[2] R. David and K. Nour, "A short proof of the strong normalization of classical natural deduction with disjunction," *Journal of Symbolic Logic*, vol. 68, no. 4, pp.1277–1288, 2003.

[3] P. de Groote, "On the Strong Normalisation of Intuitionistic Natural Deduction with Permutative-Conversions," *Inf. Comput.* vol. 178, pp.441–464, 2002.

[4] J. H. Gallier, On Girard's "Candidats de reducibilite", In *Logic and Computer Science*, P. Odifreddi, Ed., Academic Press, pp.123–203, 1990.

[5] J. Y. Girard, "Une extension de l'interprétation de Gödel à l'analyse, et son application à l'élimination des coupures dans l'analyse et la théorie des types," In *Proc. of the Second Scandinavian Logic Symposium*, J. E. Fenstad, Ed., North-Holland, pp.63–92, 1971.

[6] J. Y. Girard, "Interprétation fonctionelle et élimination des coupures de l'arithmétique d´ordre supérieur," *Thèse de Doctorat d'Etat*, Université de Paris VII, 1972.

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

[8] W. A. Howard, "The formulae-as-types notion of construction," In *To H. B. Curry : essays on combinatory logic, lambda calculus and formalism*, J. P. Seldin and J. R. Hindley, Eds., Academic Press, pp.480–490, 1980.

[9] F. Joachimski and R. Matthes, "Short proofs of normalization for the simply-typed lambda-calculus, permutative conversions and Gödel's T," *Archive for Mathematical Logic*, vol. 42, pp.59–87, 2003.

[10] D. Leivant, "Strong normalization for arithmetic," *Lecture Notes in Mathematics*, vol, 500, pp.182–197, 1975.

[11] P. Martin-Löf, "Hauptsatz for the theory of species," In *Proc. of the Second Scandinavian Logic Symposium*, J. E. Fenstad, Ed., North-Holland, pp.217–233, 1971.

[12] R. Matthes, “Non-Strictly Positive Fixed-Points for Classical Natural Deduction,” *Annals of Pure and Applied Logic*, vol. 133, pp.205–230, 2005.

[13] J. C. Mitchell and G. Plotkin, “Abstract types have existential type,” *ACM Transactions on Programming Languages and Systems*, vol. 10, no. 3, pp.470–502, 1988.

[14] D. Prawitz, *Natural Deduction*, Almquist and Wiksell, 1965.

[15] D. Prawitz, “Ideas and results of proof theory,” In *Proc. Second Scandinavian Logic Symposium*, J. E. Fenstad, Ed. North-Holland, pp.235–307, 1971.

[16] J. C. Reynolds, “Towards a Theory of Type Structure,” *Lecture Notes in Computer Science*, vol. 19, pp.408–425, 1974.

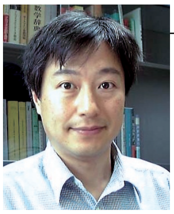
[17] W. W. Tait, “A realizability interpretation of the theory of species,” *Lecture Notes in Mathematics*, vol. 453, pp.240–251, 1975.

[18] W. W. Tait, “The completeness of Heyting first-order logic,” *Journal of Symbolic Logic*, vol. 68, no. 3, 751–763, 2003.

[19] M. Tatsuta and G. Mints, “A Simple Proof of Second Order Strong Normalization with Permutative Conversions,” *Annals of Pure and Applied Logic*, 136(1–2) (2005)134–155.

[20] A. S. Troelstra, “Metamathematical Investigation of Intuitionistic Arithmetic and Analysis,” *Lecture Notes in Mathematics*, vol. 344, 1973.

[21] A. S. Troelstra and H. Schwichtenberg, *Basic Proof Theory*, Cambridge University Press, 2nd. ed., 2000.



Makoto TATSUTA

Makoto TATSUTA is a Professor at National Institute of Informatics in Japan. He graduated with a Bachelor’s in Law, and another BSc in Information Science from the University of Tokyo. His MSc and PhD degrees are also from the University of Tokyo. He is also an adjunct professor at the Graduate University for Advanced Studies. His research interests are theoretical computer science and mathematical logic. He is a member of ASL, MSJ, JSSST, and IPSJ.