筑波大学 情報学群 情報メディア創成学類

卒業研究論文

値依存時相仕様検証のための型システム

南條 陽史

指導教員　久野 誉人

2018年 1月

概要

本研究は高階関数型言語に対して線形時相的な性質を検証する型ベースの手法を提案する. 本研究の貢献は大きく分けて二つある. 一つは型が付いたプログラムが与えられた時相仕様を満たすことを保証する dependent-refinement 型システムの提案である. この型システムの特筆すべき点は値依存エフェクトを扱えることである. これは近年提案された時相的な性質を検査する型システムで使われている非値依存エフェクトの拡張である. 二つ目の貢献として本研究はその型システムの上での型検査と型付け可能性問題が一階の不動点論理制約を解くことに帰着されることを示し, さらにその制約を解くための推論システムを提案する. 推論システムは不変条件と整礎関係によって最小不動点と最大不動点を含むような制約をそれらを含まないような論理式を解く問題へと帰着させることができる.

目 次

図 目 次

第1章　序論

プログラム形式検証はソフトウェア開発において重要な役割を担っている．コンピュータは現代の生活の基盤であり特に医療や金融分野のプログラムに問題があると人々の生活に大きな影響を与える．しかし現在動いているプログラムの多くはバグを抱えておりバグ修正のみの更新が後を絶たない．プログラムのバグを検出する手法としてテストが広く知られているが, テストでは用意したテストケースの範囲でしか安全性を保証できず, また実行にコストのかかるプログラムは安易にテストできないといった欠点がある．これらの欠点を持たない問題の検出手法に形式検証がある．形式検証とはプログラムが仕様を満たすか否かを判定することを指す．特に仕様にプログラム状態の時間変化に関する制限を記述できる形式検証は時相仕様検証と呼ばれる．本論文は時相仕様の記述に実行時の値を使えるような値依存時相仕様検証のための型システムを提案し, 同時に提案する型システムで扱う論理式制約の解消手法も提案する．

本研究で提案する型システムが対象とする言語は高階関数や整数を扱うことができる．整数はいわずもがな高階関数も近年多くの有名な言語がサポートしているため本研究の対象言語は十分一般的な機能をもっているといえる．逆に本研究の提案する型システムが対象とする言語の特徴にイベントがある．プログラム中での注目したい操作にイベントと呼ばれる印をつけることで, 実行時にそのような操作がどのような順番で何回起こったかをイベントの列として扱うことができる．プログラムが停止する場合はこのイベントの列は有限の長さを持ち, 逆に停止しない場合はイベントの列は無限の長さを持つ. 以下に例を用意した.

1 つ目の Messenger は値依存時相仕様の例である． 関数 `messenger` は準備ができた状態 (**`Ready`**) になるまで待機 (**`Wait`**) して受け取った引数 `n` 回だけメッセージを送信 (**`Send`**) する．`until_ready` は状態 **`Ready`** になるまで **`Wait`** し続ける関数, `send_msgs` は引数に受け取った数 n だけメッセージを **`Send`** して停止する関数である．この例の示すように提案する型システムではプログラムが停止しない場合についてもプログラム状態の遷移についての仕様を書くことができる．さらにこの仕様に n が使われているように提案する型システムでは時相仕様を実行時の値に依存させることができる．これは既存の時相仕様検証システムではできなかったことである．

2 つ目の Amortized Complexity は高階関数を使った複雑な liveness の例である．このプログラム上で整数リストの 2 つ組ははじめのリストの末尾に後ろのリストを反転させたものを連結して得られる一つのリストを表している．一般にリストの末尾に要素を追加するときはそのリストの長さに比例した時間がかかるがこのようにリストを表現することで先頭にも末尾にも定数時間で要素を追加することができる．また先頭要素の削除は多くの場合通常のリストと同様

Messenger	Amortized Complexity
`let until_ready () =` `  if * then (event[Ready]; ())` `  else (event[Wait]; until_ready ())` `let rec send_msgs n =` `  if n = 0 then ()` `  else (event[Send]; send_msgs (n-1))` `let rec messenger n =` `  until_ready ();` `  send_msgs n;` `  messenger n`	`let rev l =` `  let rec aux l acc = match l with` `	[] -> acc` `	h::t -> event[Tick]; aux t (h::acc)` ` in` ` aux l []`  `let is_empty (f,r) = f = [] && r = []` `let enqueue e (f,r) = event[Enq]; (f,e::r)` `let rec dequeue (f,r) = match f with` `	[] -> dequeue (rev r, [])` `	e::f -> event[Deq]; (e, (f, r))`  `let rec main (f,r) =` ` if * then main (enqueue 42 (f,r))` ` else if is_empty (f,r) then ()` ` else main (snd (dequeue (f,r)))`
`messenger` : $(n : \{n \mid n \geq 0\}) \to \Phi$ $\Phi^{\mu} = \lambda x.\ \bot$ $\Phi^{\nu} = \lambda x.\ x = ((\underline{\textbf{Ready}} \cdot \underline{\textbf{Send}}^{n}) \mid \underline{\textbf{Wait}})^{\omega}$	`main` : $(q : \texttt{int list} \times \texttt{int list}) \to (\texttt{unit} \,\&\, \Phi)$ $\Phi^{\mu} = \lambda x.\ \#_{\underline{\texttt{Enq}}} + \lvert r \rvert = \#_{\underline{\texttt{Tick}}} = \#_{\underline{\texttt{Deq}}} - \lvert f \rvert$ $\Phi^{\nu} = \lambda x.\ \top$

図 1.1: Running Examples

に定数時間しかかからないがリストの 1 つ目が空である場合には 2 つ目のリストを 1 つ目のリストに反転させてコピーする必要がある. 本研究で提案する型システムではこのコピーがどのぐらいの頻度で発生するのかを型で表現することができる. 関数 `main` は任意の上記のリストを受け取り非決定的に末尾への要素の追加と先頭要素の削除を繰り返しリストが空になったら停止するというものである. 直観的には停止するまでにコピーが発生する回数は後ろのリストに含まれたセルの数に等しいから $\#_{\underline{\texttt{Tick}}} = |r| + \#_{\underline{\texttt{Enq}}}$ である. また, 停止するまでに先頭要素が削除された回数はリストに含まれたセルに数に等しいから $\#_{\underline{\texttt{Deq}}} = |f| + |r| + \#_{\underline{\texttt{Enq}}} = |f| + \#_{\underline{\texttt{Tick}}}$. 以上から $\#_{\underline{\texttt{Enq}}} + |r| = \#_{\underline{\texttt{Tick}}} = \#_{\underline{\texttt{Deq}}} - |f|$

第2章　対象の言語

2.1　対象言語の構文

この章では検証の対象となる call by value で ML-like な高階の関数型言語 $\mathcal{L}$ を定義する．$\mathcal{L}$ の文法は以下で与えられる．

$$
\begin{aligned}
&\text{(events)}\ \underline{\mathtt{a}} ::\in \Sigma \\
&\text{(expressions)}\ e ::= x \mid n \mid \mathtt{rec}(f, \widetilde{x}, e) \mid v_1\ v_2 \mid \mathtt{ifz}\ v\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \\
&\qquad\qquad \mid v_1\ op\ v_2 \mid \mathtt{let}\ x\ =\ e_1\ \mathtt{in}\ e_2 \mid \mathtt{ev[}\underline{\mathtt{a}}\mathtt{]} \\
&\text{(values)}\ v ::= x \mid n \mid \mathtt{rec}(f, \widetilde{x}, e)\ \widetilde{v} \qquad (\text{ where } |\widetilde{x}| > |\widetilde{v}|) \\
&\text{(simple types)}\ T ::= \mathtt{int} \mid T_1 \to T_2
\end{aligned}
$$

図 2.1: Syntax of $\mathcal{L}$

ただしここでは単純型付けが可能な式のみを扱い, n と x はそれぞれ整数と変数上のメタ変数である．

簡単のために $\mathtt{rec}(f, \widetilde{x}, e)$ の e と $\mathtt{let}\ x\ =\ e_1\ \mathtt{in}\ e_2$ の e_2 は整数型を持つ．また, 式 $\mathtt{ev[}\underline{\mathtt{a}}\mathtt{]}$ が評価されたときイベント $\underline{\mathtt{a}}$ と呼ばれる目印が発行される．式の評価に伴って発行されたイベントの列によってプログラム状態の遷移を表すことができる．イベントの有限列と無限列をまとめてイベント列と呼び, イベントの有限列を表すメタ変数に ϖ を, イベントの無限列を表すメタ変数に π を使う．$\mathtt{rec}(f, \widetilde{x}, e)$ の e の中では再帰が起こる前に少なくとも一つはイベントが発行されるものとする．これは停止しない関数呼び出しの起こすイベント列が有限列にならないようにするためであり, この制限は e の一番外側を $\mathtt{let}\ \_\ =\ \mathtt{ev[}\underline{\mathtt{a}}\mathtt{]}\ \mathtt{in}\ e$ などとすることで簡単に達成できる．

ここで派生形式として $\mathtt{let}\ \_\ =\ e_1\ \mathtt{in}\ e_2$ を $e_1\,;\,e_2$ と書くことにする．

式や値の列を $\widetilde{x}$ のように書き, その長さを $|\widetilde{x}|$ と書く．長さが 0 の列を ϵ と書く．

演算子 op は $+$, $-$, $\times$, $=$, $<$ のような整数上の二項演算を表す．ここで $=$ や $<$ は真偽値を整数にエンコード ($\mathtt{true}$ であれば 0, $\mathtt{false}$ であれば 1) したものを返すとする．また $() \triangleq 0$, $\mathtt{unit} \triangleq \{u \mid u = 0\}$ と定義する．

簡単のために対象言語のベースデータを整数に限定しているがこれは検証可能な範囲を狭めるものではなく, 標準的なリスト, タプル, 代数的データ型などは拡張によって扱うことが

できる. [3]

2.2 対象言語の操作的意味論

言語 $\mathcal{L}$ の操作的意味論は以下のように定義される.

Terminating Run

$$v \Downarrow v \,\&\, \epsilon \qquad \text{(RT-Val)}$$

$$\frac{|\widetilde{x}| = |\widetilde{v}| \qquad [\mathtt{rec}(f, \widetilde{x}, e)/f, \widetilde{v}/\widetilde{x}]e \Downarrow v \,\&\, \varpi}{\mathtt{rec}(f, \widetilde{x}, e)\ \widetilde{v} \Downarrow v \,\&\, \varpi} \qquad \text{(RT-App)}$$

$$\frac{e_1 \Downarrow v \,\&\, \varpi}{\mathtt{ifz}\ 0\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \Downarrow v \,\&\, \varpi} \qquad \text{(RT-IfTrue)}$$

$$\frac{n \neq 0 \qquad e_2 \Downarrow v \,\&\, \varpi}{\mathtt{ifz}\ n\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \Downarrow v \,\&\, \varpi} \qquad \text{(RT-IfFalse)}$$

$$\frac{[\![op]\!](v_1, v_2) = v}{v_1\ op\ v_2 \Downarrow v \,\&\, \epsilon} \qquad \text{(RT-Op)}$$

$$\frac{e_1 \Downarrow v \,\&\, \varpi_1 \qquad [v/x]e_2 \Downarrow v' \,\&\, \varpi_2}{\mathtt{let}\ x\ =\ e_1\ \mathtt{in}\ e_2 \Downarrow v' \,\&\, \varpi_1 \cdot \varpi_2} \qquad \text{(RT-Let)}$$

$$\mathtt{ev[\underline{a}]} \Downarrow 0 \,\&\, \underline{\mathtt{a}} \qquad \text{(RT-Event)}$$

NonTerminating Run

$$\frac{|\widetilde{x}| = |\widetilde{v}| \qquad [\mathtt{rec}(f, \widetilde{x}, e)/f, \widetilde{v}/\widetilde{x}]e \Uparrow \bot \,\&\, \pi}{\mathtt{rec}(f, \widetilde{x}, e)\ \widetilde{v} \Uparrow \bot \,\&\, \pi} \qquad \text{(RN-App)}$$

$$\frac{e_1 \Uparrow \bot \,\&\, \pi}{\mathtt{ifz}\ 0\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \Uparrow \bot \,\&\, \pi} \qquad \text{(RN-IfTrue)}$$

$$\frac{n \neq 0 \qquad e_2 \Uparrow \bot \,\&\, \pi}{\mathtt{ifz}\ n\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 \Uparrow \bot \,\&\, \pi} \qquad \text{(RN-IfFalse)}$$

$$\frac{e_1 \Uparrow \bot \,\&\, \pi}{\mathtt{let}\ x\ =\ e_1\ \mathtt{in}\ e_2 \Uparrow \bot \,\&\, \pi} \text{(RN-Let1)}$$

$$\frac{e_1 \Downarrow v \,\&\, \varpi \qquad [v/x]e_2 \Uparrow \bot \,\&\, \pi}{\mathtt{let}\ x\ =\ e_1\ \mathtt{in}\ e_2 \Uparrow \bot \,\&\, \varpi \cdot \pi} \qquad \text{(RN-Let2)}$$

図 2.2: Operation Semantics of $\mathcal{L}$

ここで $[\![op]\!]$ は op の意味をあらわす. 例えば任意の整数 n, m について $[\![+]\!](n, m) = n + m$ である.

$e \Downarrow v \,\&\, \varpi$ は式 e の計算が停止し, 計算によって得られた値が v であり計算に伴って発行されたイベントの有限列が ϖ であることを表す. 一方 $e \Uparrow \bot \,\&\, \pi$ は式 e の計算が停止せずに計算に伴って発行されたイベントの無限列が π であることを表す.

Terminating Run の規則は帰納的に定義されているのに対し NonTerminating Run の規則は余帰納的に定義されている.

第3章　型システム

3.1　一階の不動点論理式

型を定義するにあたって先に型システムが扱う一階の不動点論理式 ϕ を図 3.1 のように定義する.

$$
\begin{aligned}
\text{(formulas) } \phi ::= {} & \top \mid \bot \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \forall x : s.\ \phi \mid \exists x : s.\ \phi \\
\mid {} & A(\widetilde{t}) \mid X(\widetilde{t}) \mid (\mu X(\widetilde{x}).\ \phi)(\widetilde{t}) \mid (\nu X(\widetilde{x}).\ \phi)(\widetilde{t}) \qquad (\text{ where } |\widetilde{x}| = |\widetilde{t}|) \\
\text{(terms) } t ::= {} & x \mid f(\widetilde{t}) \\
\text{(predicates) } p ::= {} & \lambda\widetilde{x}.\ \phi \\
\text{(sorts) } s ::= {} & \texttt{int} \mid \texttt{finstr} \mid \texttt{infstr}
\end{aligned}
$$

図 3.1: Syntax of Fixpoint logic formula

ここで, メタ変数 X, t, p はそれぞれ述語変数, 項, 述語を表す. $A(\widetilde{t})$ は整数やイベント列上の等値性などの原始命題を表す. f は列の連結や四則演算のような関数を表し, リテラル整数 n や空列 ϵ や要素が 1 つだけのイベント列 $\underline{\texttt{a}}$ は定数関数とみなす.

また述語 $\mu X(\widetilde{x}).\ \phi$, $\nu X(\widetilde{x}).\ \phi$ はそれぞれ関数 $\lambda X.\ \lambda\widetilde{x}.\ \phi$ の最小不動点と最大不動点を表す. $\mu X(\widetilde{x}).\ \phi$ の X と $\nu X(\widetilde{x}).\ \phi$ の X はそれぞれ ϕ の positive な位置にだけ出現するとする. つまり ϕ 中に自由な X は偶数回の否定のもとで出現する. メタ変数 q は不動点述語 $\mu X(\widetilde{x}).\ \phi$, $\nu X(\widetilde{x}).\ \phi$ を表すものとする.

また $p_1 \sqsubseteq p_2 \triangleq \forall\widetilde{x}.\ p_1(\widetilde{x}) \Rightarrow p_2(\widetilde{x})$, $(\lambda\widetilde{x}.\ \phi)(\widetilde{t}) \triangleq [\widetilde{t}/\widetilde{x}]\phi$ と定義する.

メタ変数 ψ は不動点論理式のうち不動点述語 $\mu X(\widetilde{x}).\ \phi$, $\nu X(\widetilde{x}).\ \phi$ を含まない式を表すとする.

割り当て θ のもとで不動点論理式 ϕ が妥当であることを示す関係 $\theta \models_{\mu,\nu} \phi$ を図 3.2 に定義する. ここで $\mathcal{D} \triangleq \Sigma^* \cup \Sigma^\omega \cup \mathbb{Z}$ と定義する.

$$
D_{\cdot} \triangleq \{\texttt{true} \mid \texttt{false}\} \qquad D_{\texttt{int}} \triangleq \mathbb{Z} \qquad D_{\texttt{finstr}} \triangleq \Sigma^* \qquad D_{\texttt{infstr}} \triangleq \Sigma^\omega
$$

$$
\begin{aligned}
\theta &\models_{\mu,\nu} \top \\
\theta &\not\models_{\mu,\nu} \bot \\
\theta &\models_{\mu,\nu} \neg\phi \text{ iff } \theta \not\models_{\mu,\nu} \phi \\
\theta &\models_{\mu,\nu} \phi_1 \wedge \phi_2 \text{ iff } \theta \models_{\mu,\nu} \phi_1 \text{かつ} \theta \models_{\mu,\nu} \phi_2 \\
\theta &\models_{\mu,\nu} \phi_1 \vee \phi_2 \text{ iff } \theta \models_{\mu,\nu} \phi_1 \text{または} \theta \models_{\mu,\nu} \phi_2 \\
\theta &\models_{\mu,\nu} \forall x : s.\ \phi \text{ iff すべての } t \in \mathcal{D}_s \text{ について } [x \mapsto t]\theta \models_{\mu,\nu} \phi \\
\theta &\models_{\mu,\nu} \exists x : s.\ \phi \text{ iff } [x \mapsto t]\theta \models_{\mu,\nu} \phi \text{ なる } t \in \mathcal{D}_s \text{ が存在する} \\
\theta &\models_{\mu,\nu} A(\widetilde{t}) \text{ iff } [\![A]\!](\theta(\widetilde{t})) \\
\theta &\models_{\mu,\nu} X(\widetilde{x}) \text{ iff} \\
\theta &\models_{\mu,\nu} (\mu X(\widetilde{x}).\ \phi)(\widetilde{t}) \text{ iff } \theta \models_{\mu,\nu} \mathit{lfp}(\lambda\widetilde{x}.\ \phi)(\widetilde{t}) \\
\theta &\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \phi)(\widetilde{t}) \text{ iff } \theta \models_{\mu,\nu} \mathit{gfp}(\lambda\widetilde{x}.\ \phi)(\widetilde{t}) \\
\mathit{lfp}(F) &\triangleq \bigsqcap\{X \mid\ F(X) \sqsubseteq X\} \\
\mathit{gfp}(F) &\triangleq \bigsqcup\{X \mid\ X \sqsubseteq F(X)\}
\end{aligned}
$$

図 3.2: Semantics of Fixpoint logic formula

3.2 型の構文

次に, 型の構文は図 3.3 のように定義される. Φ について $\Phi^{\mu} \triangleq \lambda x \in \Sigma^*.\ \phi_{\mu}$, $\Phi^{\nu} \triangleq \lambda x \in \Sigma^{\omega}.\ \phi_{\nu}$ と定義する. 特に $\Phi_{val} \triangleq (\lambda x \in \Sigma^*.\ x = \epsilon,\ \lambda x.\ \Sigma^{\omega}\bot)$ と定義する.

Φ^{μ} は式の評価が停止する時に生じる有限のイベント列に対しての仕様であり, Φ^{ν} は式の評価が停止しない時に生じる無限のイベント列に対しての仕様である. qualified types $(\tau\ \&\ \Phi)$ は Φ に沿ったイベント列を生じて τ を満たす値に評価される式の型である. dependent refinement types $\{u \mid \phi\}$ は ϕ を満たす整数値 u の型であり $(x : \tau) \to \sigma$ は τ を満たす引数 x を受け取って σ を満たす値を返す関数値の型である. ここで $(x : \tau) \to (\tau\ \&\ \Phi)$ の Φ は引数 x に依存しうることに注意すること. $\{u \mid \top\}$ を単に `int` と略記し, 曖昧でなければ $(\tau\ \&\ \Phi_{val})$ を単に τ と略記する.

例えば $((x : \texttt{int}) \to (\texttt{int}\ \&\ \Phi_1)\ \&\ \Phi_2)$ という型は, その型がつく式を評価するときに Φ_2 に沿ったイベント列が生成され, 評価した結果得られた関数を値に適用すると Φ_1 に沿ったイベント列が生成されるという意味である.

$\mathit{sty}(\sigma)$, $\mathit{sty}(\tau)$ はそれぞれ σ, τ の型が付く式や値に対して simple typing によって得られる型である. $\mathit{sty}(\Gamma)$ は Γ 内の型 τ を全て $\mathit{sty}(\tau)$ に置き換えたものである. また, $\mathit{fv}(\sigma)$, $\mathit{fv}(\tau)$, $\mathit{fv}(\Phi)$ はそれぞれ σ, τ, Φ に出現する自由変数の集合を表し $\mathit{fpv}(\sigma)$, $\mathit{fpv}(\tau)$, $\mathit{fpv}(\Phi)$ はそれぞれ σ, τ, Φ に出現する自由述語変数の集合を表す. それぞれ以下のように定義される.

$$
\begin{aligned}
\text{(qualifiers)}\ \Phi &::= (\lambda x \in \Sigma^*.\ \phi_\mu,\ \lambda x \in \Sigma^\omega.\ \phi_\nu) \\
\text{(qualified types)}\ \sigma &::= (\tau\ \&\ \Phi) \\
\text{(dependent refinement types)}\ \tau &::= \{u \mid \phi\} \mid (x:\tau) \to \sigma \\
\text{(type environments)}\ \Gamma &::= \emptyset \mid \Gamma, x:\tau
\end{aligned}
$$

図 3.3: Syntax of Types and Effects

$$
\begin{aligned}
sty((\tau\ \&\ \Phi)) &\triangleq sty(\tau) \\
sty(\{u \mid \phi\}) &\triangleq \mathtt{int} \\
sty((x:\tau) \to \sigma) &\triangleq sty(\tau) \to sty(\sigma) \\
sty(\emptyset) &\triangleq \emptyset \\
sty(\Gamma, x:\tau) &\triangleq sty(\Gamma), x : sty(\tau)
\end{aligned}
$$

$$
\begin{aligned}
fv((\tau\ \&\ \Phi)) &\triangleq fv(\tau) \cup fv(\Phi) \\
fv(\{u \mid \phi\}) &\triangleq fv(\phi) \backslash u \\
fv((x:\tau) \to \sigma) &\triangleq fv(\tau) \cup (fv(\sigma) \backslash \{x\}) \\
fpv((\tau\ \&\ \Phi)) &\triangleq fpv(\tau) \cup fpv(\Phi) \\
fpv(\{x \mid \phi\}) &\triangleq fpv(\phi) \\
fpv((x:\tau) \to \sigma) &\triangleq fpv(\tau) \cup fpv(\sigma)
\end{aligned}
$$

w は自由変数をふくまない値に対して使うメタ変数である.
型環境 Γ は変数束縛 $x:\tau$ の列である. 型環境を変数から型への関数とみなすこともある.
ν を fresh な変数名として $\Gamma, \nu : \{\nu \mid \phi\}$ を Γ, ϕ と略記する.
$\lfloor\Gamma\rfloor$, $\lfloor\Gamma \vdash \phi\rfloor$ を以下のように定義する

$$
\begin{aligned}
\lfloor\emptyset\rfloor &\triangleq \top \\
\lfloor\Gamma, x:\{u \mid \phi\}\rfloor &\triangleq \lfloor\Gamma\rfloor \wedge [x/u]\phi \\
\lfloor\Gamma, x:(y:\tau) \to \sigma\rfloor &\triangleq \lfloor\Gamma\rfloor \\
\lfloor\Gamma \vdash \phi\rfloor &\triangleq \lfloor\Gamma\rfloor \Rightarrow \phi
\end{aligned}
$$

$(\widetilde{x}\colon \widetilde{\tau}) \to \sigma$ を $(x_1:\tau_1) \to ((x_2:\tau_2) \to (\cdots (x_{n-1}:\tau_{n-1}) \to ((x_n:\tau_n) \to \sigma\ \&\ \Phi_{val}) \cdots\ \&\ \Phi_{val})\ \&\ \Phi_{val})$ の略記とする.

ここで型環境中の型や関数の略記の引数の型を τ としてよいのは, 対象の言語は正格評価であるため束縛される式や関数の引数は常に値だからである.

T を単純型を表すメタ変数とし, $\widetilde{T} \to \mathtt{int}$ を単純型 $T_1 \to T_2 \to \ldots \to T_n \to \mathtt{int}$ の略とする.

Φ の連結を

$$
\begin{aligned}
\Phi_1 \cdot \Phi_2 \quad \triangleq \quad & (\lambda x \in \Sigma^*.\ \exists x_1, x_2 \in \Sigma^*.\ x = x_1 \cdot x_2 \wedge \Phi_1^\mu(x_1) \wedge \Phi_2^\mu(x_2), \\
& \lambda x \in \Sigma^\omega.\ \Phi_1^\nu(x) \vee (\exists y \in \Sigma^*, z \in \Sigma^\omega.\ x = y \cdot z \wedge \Phi_1^\mu(y) \wedge \Phi_2^\nu(z)))
\end{aligned}
$$

と定義する. ここで任意の Φ について $\Phi_{val} \cdot \Phi = \Phi \cdot \Phi_{val} = \Phi$ である.

3.3 型付け規則

型判断式 $\Gamma \vdash e : \sigma$ は型環境 Γ の下で式 e に型 σ が付くことを表しておりその導出規則は図 3.4 の通りである.

T-Const, T-VInt, T-VFun はそれぞれ整数リテラル, 整数の変数, 関数の変数に対する型付け規則である. これらの規則は既存の refinement type system とほとんど同様である. 本論文で提案する型システムでは base type が整数のみであるから変数の simple type が `int` か否かによって変数は整数に束縛されているか関数に束縛されているかが判別できることを利用している.

T-Op は定数演算子の適用に対する型付けである. この演算子はイベントを起こさないので値と同じ副作用を持つ. T-If は条件分岐に対する型付けである. ifz 式の then 節が評価されるときは $v = 0$ であり else 節が評価されるときは $v \neq 0$ である. T-Let は変数束縛に対する型付け規則である. 評価の順序と同じように e_1 の副作用の後に e_2 の副作用を連結する. T-App は関数適用に対する型付け規則である. 特に特別なところはなく x を v_2 に置換する. T-Event はイベント発行に対する型付け規則である. 指定された有限イベントのみを持つ副作用を生じて 0 を返す.

T-Fun は関数に対する型付け規則である. まず関数の本体 e が起こす副作用のうち有限部分を述語変数 X_μ, 無限部分を述語変数 X_ν でおき, そのもとで本体 e の副作用 Φ を得る. 実際の関数の本体の副作用の有限部分は Φ^μ の最小不動点をとった述語 q_μ であり, 無限部分は Φ^ν の最大不動点をとった述語 q_ν である. ここで q_ν を求める際に X_μ に q_μ を代入するのは副作用の連結の定義から Φ^μ には X_ν が出現し得ないが Φ^ν には X_μ が出現しうるからである.

T-Sub は部分型関係に関する型付け規則である. 式 e が仕様 σ_2 を満たすことをいうためには e がより強い仕様 σ_1 を満たせばよい.

$$\Gamma \vdash n : (\{x \mid x = n\} \,\&\, \Phi_{val}) \qquad \text{(T-Const)}$$

$$\frac{\begin{array}{c}\tau'_f = (\widetilde{x}\colon \widetilde{\tau}) \to (\tau \,\&\, (\lambda x \in \Sigma^*.\ X_\mu(\widetilde{x}, x),\ \lambda x \in \Sigma^\omega.\ X_\nu(\widetilde{x}, x))) \\ \Gamma, f : \tau'_f, \widetilde{x} : \widetilde{\tau} \vdash e : (\tau \,\&\, \Phi) \\ q_\mu = \mu X_\mu(\widetilde{x}, x).\ \Phi^\mu(x) \qquad q_\nu = \nu X_\nu(\widetilde{x}, x).\ [q_\mu / X_\mu]\Phi^\nu(x) \\ \tau_f = (\widetilde{x}\colon \widetilde{\tau}) \to (\tau \,\&\, (\lambda x \in \Sigma^*.\ q_\mu(\widetilde{x}, x),\ \lambda x \in \Sigma^\omega.\ q_\nu(\widetilde{x}, x)))\end{array}}{\Gamma \vdash \mathtt{rec}(f, \widetilde{x}, e) : (\tau_f \,\&\, \Phi_{val})} \qquad \text{(T-Fun)}$$

$$\frac{sty(\Gamma(x)) = \mathtt{int}}{\Gamma \vdash x : (\{u \mid u = x\} \,\&\, \Phi_{val})} \qquad \text{(T-VInt)}$$

$$\frac{sty(\Gamma(x)) \neq \mathtt{int}}{\Gamma \vdash x : (\Gamma(x) \,\&\, \Phi_{val})} \qquad \text{(T-VFun)}$$

$$\frac{\Gamma \vdash e_1 : (\tau_1 \,\&\, \Phi_1) \qquad \Gamma, x : \tau_1 \vdash e_2 : (\tau_2 \,\&\, \Phi_2) \qquad x \notin fv(\tau_2) \cup fv(\Phi_2)}{\Gamma \vdash \mathtt{let}\ x\ =\ e_1\ \mathtt{in}\ e_2 : (\tau_2 \,\&\, \Phi_1 \cdot \Phi_2)} \qquad \text{(T-Let)}$$

$$\frac{\Gamma \vdash v_1 : ((x : \tau) \to (\tau' \,\&\, \Phi) \,\&\, \Phi_{val}) \qquad \Gamma \vdash v_2 : (\tau \,\&\, \Phi_{val})}{\Gamma \vdash v_1\ v_2 : [v_2/x](\tau' \,\&\, \Phi)} \qquad \text{(T-App)}$$

$$\frac{\Gamma \vdash v_1 : (\mathtt{int} \,\&\, \Phi_{val}) \qquad \Gamma \vdash v_2 : (\mathtt{int} \,\&\, \Phi_{val})}{\Gamma \vdash v_1\ op\ v_2 : (\{x \mid x = v_1\ op\ v_2\} \,\&\, \Phi_{val})} \qquad \text{(T-Op)}$$

$$\frac{\Gamma, v = 0 \vdash e_1 : \sigma \qquad \Gamma, v \neq 0 \vdash e_2 : \sigma}{\Gamma \vdash \mathtt{ifz}\ v\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2 : \sigma} \qquad \text{(T-If)}$$

$$\Gamma \vdash \mathtt{ev[\underline{a}]} : (\{x \mid x = 0\} \,\&\, (\lambda x \in \Sigma^*.\ x = \underline{\mathtt{a}},\ \lambda x \in \Sigma^\omega.\ \bot)) \qquad \text{(T-Event)}$$

$$\frac{\Gamma \vdash e : \sigma_1 \qquad \Gamma \vdash \sigma_1 <: \sigma_2}{\Gamma \vdash e : \sigma_2} \qquad \text{(T-Sub)}$$

図 3.4: Typing Rules

部分型判断式 $\Gamma \vdash \sigma_1 <: \sigma_2$, $\Gamma \vdash \tau_1 <: \tau_2$ はそれぞれ型環境 Γ の下で σ_1 は σ_2 の部分型, τ_1 は τ_2 の部分型であることを表す. この導出規則は以下の通りである.

ここに出てくる式 $\Vdash \phi$ は不動点論理式 ϕ が妥当であることを示す式である. 4 章でこの式について詳しく述べる.

S-QFun は関数の式に付く型の部分型関係を表している. $(\tau_1 \,\&\, \Phi_1)$ が $(\tau_2 \,\&\, \Phi_2)$ の部分型であるということは評価して得られた値の型に部分型関係がなりたちかつ評価の途中に生じ

る副作用の列の集合にも包含関係が成り立つということである.

S-QInt は整数の式に付く型の部分型関係を表している. $(\{u \mid \phi\}\ \&\ \Phi)$ の ϕ とは評価が停止した時に得られた値が満たすべき条件であるから停止した時に成り立つ制約を Φ^μ から $\phi \wedge \Phi^\mu$ に強めることができる.

S-Int は整数の値に付く型の部分関係を表している. つまり左辺の条件を満たす整数すべてが右辺の条件を満たせばよい. S-Fun は関数の値の付く型の部分関係を表している. つまり関数の本体の式に付く型の間に関数の型と同じ向きの部分関係が成り立ち関数の引数の値に付く型の間に関数の型と逆向きの部分関係が成り立てばよい.

$$\frac{sty(\tau_1) \neq \mathtt{int} \qquad \Gamma \vdash \tau_1 <: \tau_2 \qquad \Vdash \lfloor \Gamma \vdash \forall x \in \Sigma^*.\ \Phi_1^\mu(x) \Rightarrow \Phi_2^\mu(x) \rfloor \qquad \Vdash \lfloor \Gamma \vdash \forall x \in \Sigma^\omega.\ \Phi_1^\nu(x) \Rightarrow \Phi_2^\nu(x) \rfloor}{\Gamma \vdash (\tau_1\ \&\ \Phi_1) <: (\tau_2\ \&\ \Phi_2)} \text{(S-QFun)}$$

$$\frac{\Vdash \lfloor \Gamma \vdash \forall x \in \Sigma^*.\ (\phi_1 \wedge \Phi_1^\mu(x)) \Rightarrow (\phi_2 \wedge \Phi_2^\mu(x)) \rfloor \qquad \Vdash \lfloor \Gamma \vdash \forall x \in \Sigma^\omega.\ \Phi_1^\nu(x) \Rightarrow \Phi_2^\nu(x) \rfloor}{\Gamma \vdash (\{u \mid \phi_1\}\ \&\ \Phi_1) <: (\{u \mid \phi_2\}\ \&\ \Phi_2)} \text{(S-QInt)}$$

$$\frac{\Vdash \lfloor \Gamma \vdash \phi_1 \Rightarrow \phi_2 \rfloor}{\Gamma \vdash \{u \mid \phi_1\} <: \{u \mid \phi_2\}} \text{(S-Int)}$$

$$\frac{\Gamma \vdash \tau_2 <: \tau_1 \qquad \Gamma, x : \tau_2 \vdash \sigma_1 <: \sigma_2}{\Gamma \vdash (x : \tau_1) \to \sigma_1 <: (x : \tau_2) \to \sigma_2} \text{(S-Fun)}$$

図 3.5: Subtyping Rules

3.4 型の表示的意味論

型の意味は次のように表示的に定義される.

$$\begin{aligned}
[\![(\tau\ \&\ \Phi)]\!] &\triangleq \left\{ e \in sty(\tau) \;\middle|\; \begin{array}{l} (\forall \varpi, w.\ (e \Downarrow w\ \&\ \varpi) \Rightarrow (w \in [\![\tau]\!]) \wedge (\models_{\mu,\nu} \Phi^\mu(\varpi))) \wedge \\ (\forall \pi.\ (e \Uparrow \bot\ \&\ \pi) \Rightarrow (\models_{\mu,\nu} \Phi^\nu(\pi))) \end{array} \right\} \\
[\![\Gamma \vdash \sigma]\!] &\triangleq \{e \mid \forall \theta \in sty(\Gamma).\ (\theta \models_{\mu,\nu} \Gamma) \Rightarrow \theta(e) \in [\![\theta(\sigma)]\!]\} \\
[\![\{x \mid \phi\}]\!] &\triangleq \{n \mid \models_{\mu,\nu} [n/x]\phi\} \\
[\![(x : \tau) \to \sigma]\!] &= \{w \in sty((x : \tau) \to \sigma) \mid \forall w' \in [\![\tau]\!].\ w\ w' \in [\![[w'/x]\sigma]\!]\}
\end{aligned}$$

図 3.6: Semantics of Types

式 e が単純型 T を持つとき $e \in T$ と書く. 閉じた値割り当て θ と単純型環境 E について

$\mathrm{dom}(\theta) = \mathrm{dom}(E)$ かつ任意の $x \in \mathrm{dom}(\theta)$ で $\theta(x) \in E(x)$ であるとき $\theta \in E$ と書く．さらに $\mathrm{dom}(\theta) = \mathrm{dom}(\Gamma)$ かつ $\forall (x:\tau) \in \Gamma.\ \theta(x) \in [\![\theta(\tau)]\!]$ のとき $\theta \models_{\mu,\nu} \Gamma$ と書く．

$[\![\Gamma \vdash \sigma]\!]$ は型環境 Γ の下で σ に沿うように評価される式の集合である．$[\![\sigma]\!]$ と $[\![\tau]\!]$ はそれぞれ σ, τ に沿うように評価される閉じた式と値の集合である．

部分型判断の意味は次のように定義される．

$$[\![\Gamma \ \vdash\ \sigma_1 \texttt{<:}\ \sigma_2]\!] \triangleq \forall \theta \in sty(\Gamma).\ \theta \models_{\mu,\nu} \Gamma \Rightarrow [\![\theta(\sigma_1)]\!] \subseteq [\![\theta(\sigma_2)]\!]$$
$$[\![\Gamma \ \vdash\ \tau_1 \texttt{<:}\ \tau_2]\!] \triangleq \forall \theta \in sty(\Gamma).\ \theta \models_{\mu,\nu} \Gamma \Rightarrow [\![\theta(\tau_1)]\!] \subseteq [\![\theta(\tau_2)]\!]$$

図 3.7: Semantics of Subtyping

$[\![\Gamma \ \vdash\ \sigma_1 \texttt{<:}\ \sigma_2]\!]$ は型環境 Γ のもとで σ_1 に沿って評価される式の集合が σ_2 に沿って評価される式の集合に含まれることを表している．$[\![\Gamma \ \vdash\ \tau_1 \texttt{<:}\ \tau_2]\!]$ についても同様．

以上のように定義された型システムと型の意味について次の健全性が成り立つ．証明は付録にゆずる．

定理 1 (Soundness)**.** ρ を $\mathrm{dom}(\rho) = fpv(\Gamma) \cup fpv(\sigma)$ なる任意の述語割り当てとすると
$\Gamma \ \vdash\ e :\ \sigma$ ならば $e \in [\![\rho(\Gamma) \vdash \rho(\sigma)]\!]$

3.5 型付け導出の例

ここで $\texttt{rec}(f, n, \texttt{ifz}\ n\ \texttt{then}\ 1\ \texttt{else}\ (\texttt{ev[}\underline{\texttt{a}}\texttt{]}\ ;\ \texttt{let}\ n' = n-1\ \texttt{in}\ f\ n'))$ を例にどのように型付け規則が使われるか見てみる．これは引数に非負整数が与えられたら $\underline{\texttt{a}}$ を引数の数だけ連ねたイベント列を生じて停止し，引数に負数が与えられたら $\underline{\texttt{a}}$ の無限列を生じて停止しないプログラムである．

紙面の都合で $\texttt{int}$ を $\mathbb{N}$ と表記し $\{u \mid u = t\}$ where $u \notin fv(t)$ を $\texttt{int}(t)$ と略し T-Const は自明なので省略する．

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dots}{\Gamma_= \ \vdash\ 1 :\ (\texttt{int}(1)\ \&\ \Phi)}\quad \dfrac{\dots}{\Gamma_{\neq} \ \vdash\ n-1 :\ \sigma_{\mathbb{N}}}\quad \dfrac{\dots}{\Gamma_{\neq}, n' : \mathbb{N} \ \vdash\ f\ n' :\ (\texttt{int}(1)\ \&\ \Phi')}\ \text{(T-App)}}{\Gamma_{\neq} \ \vdash\ \texttt{ev[}\underline{\texttt{a}}\texttt{]} :\ (\texttt{int}(0)\ \&\ \Phi_a)\quad \Gamma_{\neq} \ \vdash\ \texttt{let}\ n' = n-1\ \texttt{in}\ f\ n' :\ (\texttt{int}(1)\ \&\ [n-1/n']\Phi')}\ \text{(T-Let)}}{\Gamma_{\neq} \ \vdash\ \texttt{ev[}\underline{\texttt{a}}\texttt{]}\ ;\ \texttt{let}\ n' = n-1\ \texttt{in}\ f\ n' :\ (\texttt{int}(1)\ \&\ \Phi_a \cdot [n-1/n']\Phi')}\ \text{(T-Let)}}{\Gamma_{\neq} \ \vdash\ \texttt{ev[}\underline{\texttt{a}}\texttt{]}\ ;\ \texttt{let}\ n' = n-1\ \texttt{in}\ f\ n' :\ (\texttt{int}(1)\ \&\ \Phi)}\ \text{(T-Sub)}}{f : \tau'_f, n : \mathbb{N} \ \vdash\ \texttt{ifz}\ n\ \texttt{then}\ 1\ \texttt{else}\ (\texttt{ev[}\underline{\texttt{a}}\texttt{]}\ ;\ \texttt{let}\ n' = n-1\ \texttt{in}\ f\ n') :\ (\texttt{int}(1)\ \&\ \Phi)}\ \text{(T-If)}}{\vdash\ \texttt{rec}(f, n, \texttt{ifz}\ n\ \texttt{then}\ 1\ \texttt{else}\ (\texttt{ev[}\underline{\texttt{a}}\texttt{]}\ ;\ \texttt{let}\ n' = n-1\ \texttt{in}\ f\ n')) :\ (\tau_f\ \&\ \Phi_{val})}\ \text{(T-Fun)}$$

図 3.8: Derivation Example of Typing

ここで

$$\Gamma_{=} = f : \tau'_f, n : \mathbb{N}, n = 0 \qquad \Phi_a = (\lambda x.\ x = \underline{\mathbf{a}},\ \lambda x.\ \bot)$$
$$\Gamma_{\neq} = f : \tau'_f, n : \mathbb{N}, n \neq 0 \qquad \sigma_{\mathbb{N}} = (\mathbb{N}\ \&\ \Phi_{val})$$
$$\tau'_f = (n : \mathtt{int}) \to (\mathtt{int}(1)\ \&\ (\lambda x.\ X_\mu(n,x),\ \lambda x.\ X_\nu(n,x)))$$
$$\Phi' = (\lambda x.\ X_\mu(n',x),\ \lambda x.\ X_\nu(n',x))$$
$$\Phi = \begin{pmatrix} \lambda x.\ n = 0 \wedge x = \epsilon \vee n \neq 0 \wedge \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\mu(n-1,y) \\ \lambda x.\ n \neq 0 \wedge \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\nu(n-1,y) \end{pmatrix}$$
$$q_\mu = \mu X_\mu(n,x).\ \Phi^\mu(x) \qquad q_\mu = \nu X_\nu(n,x).\ [q_\mu/X_\mu]\Phi^\nu(x)$$
$$\tau_f = (n : \mathtt{int}) \to (\mathtt{int}(1)\ \&\ (\lambda x.\ q_\mu(n,x),\ \lambda x.\ q_\nu(n,x)))$$

副作用のみ注目してそれ以外をすべて省略した場合は以下のようになる.
ただし根は関数の内部の副作用を見せるために値の型全体を書いている.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dots}{\left(\begin{array}{l} \lambda x.\ n = 0 \wedge x = \epsilon \vee \\ \quad n \neq 0 \wedge \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\mu(n-1,y) \\ \lambda x.\ n \neq 0 \wedge \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\nu(n-1,y) \end{array}\right)}\ (\text{T-Sub}) \qquad \dfrac{\dfrac{(\lambda x.\ x = \underline{\mathbf{a}},\ \lambda x.\ \bot) \quad \dfrac{\Phi_{val} \quad \dfrac{\dots}{(\lambda x.\ X_\mu(n',x),\ \lambda x.\ X_\nu(n',x))}\ (\text{T-App})}{(\lambda x.\ X_\mu(n-1,x),\ \lambda x.\ X_\nu(n-1,x))}\ (\text{T-Let})}{\left(\begin{array}{l} \lambda x.\ \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\mu(n-1,y) \\ \lambda x.\ \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\nu(n-1,y) \end{array}\right)}\ (\text{T-Let})}{\left(\begin{array}{l} \lambda x.\ n = 0 \wedge x = \epsilon \vee \\ \quad n \neq 0 \wedge \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\mu(n-1,y) \\ \lambda x.\ n \neq 0 \wedge \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\nu(n-1,y) \end{array}\right)}\ (\text{T-If})}{((n : \mathbb{N}) \to (\mathtt{int}(1)\ \&\ \left(\begin{array}{l} \lambda x.\ (\mu X_\mu(n,x).\ n = 0 \wedge x = \epsilon \vee n \neq 0 \wedge \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\mu(n-1,y))(n,x) \\ \lambda x.\ (\nu X_\nu(n,x).\ n \neq 0 \wedge \exists y.\ x = \underline{\mathbf{a}} \cdot y \wedge X_\nu(n-1,y))(n,x) \end{array}\right)\ \&\ \Phi_{val})}\ (\text{T-Fun})$$

図 3.9: Derivation Example of Effects

これは確かに節のはじめに述べた通り引数に非負整数が与えられたら $\underline{\mathbf{a}}$ を引数の数だけ連ねたイベント列を生じて停止し, 引数に負数が与えられたら $\underline{\mathbf{a}}$ の無限列を生じて停止しないプログラムであるが, 不動点演算子が含まれた論理式の妥当性を判定する必要があり検証が困難である. 4 章の不動点論理の妥当性判定の例で型システムにより得られたこの式が確かに健全に所要の制約に近似されることを示す.

第4章　不動点論理の妥当性判定

本章では3.1で導入した一階不動点論理式の推論システムを提案する．ここで提案する推論システムは3の型システムで得られた制約を解消するためのものであるが, 扱う一階不動点論理式は一般的なものであり置かれている前提も特別なものではないのでより広い範囲の問題を解くのに有用である．

この推論システムは不変条件と整礎関係によって最小不動点と最大不動点を含む論理式を不動点を含まない論理式に健全に近似することができる．そして近似して得られる論理式は整数と有限アルファベット上の有限/無限の文字列を扱える既存のSMTソルバによって判定可能である．

推論システムの判断式 $\Vdash \phi$ は ϕ が妥当であることを意味する．この導出規則は図4.1の通りである．

$$\frac{\models \psi}{\Vdash \psi} \quad (\textsc{Fp-Valid})$$

$$\frac{X(\widetilde{x}); p_1; p_2; \top \downarrow nnf(\psi) \qquad \Vdash C^+[p_1(\widetilde{t})] \qquad \models WF(p_2)}{\Vdash C^+[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]} \quad (\textsc{Fp-Lfp}^+)$$

$$\frac{\Vdash [(\lambda \widetilde{x}.\ \psi')/X]\psi \Rightarrow \psi' \qquad \Vdash C^-[[\widetilde{t}/\widetilde{x}]\psi']}{\Vdash C^-[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]} \quad (\textsc{Fp-Lfp}^-)$$

$$\frac{\Vdash \psi' \Rightarrow [(\lambda \widetilde{x}.\ \psi')/X]\psi \qquad \Vdash C^+[[\widetilde{t}/\widetilde{x}]\psi']}{\Vdash C^+[(\nu X(\widetilde{x}).\ \psi)(\widetilde{t})]} \quad (\textsc{Fp-Gfp}^+)$$

$$\frac{X(\widetilde{x}); p_1; p_2; \top \overline{\uparrow} nnf(\psi) \qquad \Vdash C^-[\neg p_1(\widetilde{t})] \qquad \models WF(p_2)}{\Vdash C^-[(\nu X(\widetilde{x}).\ \psi)(\widetilde{t})]} \quad (\textsc{Fp-Gfp}^-)$$

図 4.1: Fixpoint rule

ここで $nnf(\psi)$ は ψ をnnf変換してえられた論理式. $X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi$ は $p_1(\widetilde{x})$ が $\mu X(\widetilde{x}).\ \neg\psi' \vee \psi$ の過少近似になっていることを表す関係であり，一方 $X(\widetilde{x}); p_1; p_2; \psi' \ \overline{\uparrow}\ \psi$ は $\neg p_1(\widetilde{x})$ が $\nu X(\widetilde{x}).\ \psi' \wedge \psi$ の過大近似になっていることを表す関係である．

NOTE: C^+ は偶数個の否定を通った文脈でありこの場合健全性の為には過小近似しなければならない．一方 C^- は奇数個の否定を通った文脈でありこの場合は健全性の為には過大近似しなければならない．

Fp-Valid は不動点述語を持たない妥当な論理式は不動点述語を許された式としても妥当であることを表す．Fp-Lfp$^+$ は全体の positive な位置に出現する最小不動点述語は過小近似をとって置換したものが妥当であればよいことを表す．Fp-Lfp$^-$ は全体の negative な位置に出現する最小不動点述語は過大近似をとって置換したものが妥当であればよいことを表す．Fp-Gfp$^+$ は全体の positive な位置に出現する最大不動点述語は過少近似をとって置換したものが妥当であればよいことを表す．Fp-Gfp$^-$ は全体の negative な位置に出現する最大不動点述語は過大近似をとって置換したものが妥当であればよいことを表す．

$X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi$ と $X(\widetilde{x}); p_1; p_2; \psi' \uparrow \psi$ の導出は図 4.2 のように定義される．これらの ψ は $\mu X(\widetilde{x}).\ \phi$ や $\nu X(\widetilde{x}).\ \phi$ や $\neg\phi$ を含まないことと $X \notin fv(\psi')$ に注意する．

このように定義された $X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi$, $X(\widetilde{x}); p_1; p_2; \psi' \uparrow \psi$ について以下の健全性が成り立つ．証明は付録にゆずる．

定理 2 (Soundness of Fixpoint Approximation)**.**

$$X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi \text{ならば } \models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee \psi)(\widetilde{x})$$
$$X(\widetilde{x}); p_1; p_2; \psi' \uparrow \psi \text{ならば } \models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$$

ここで ψ は nnf であり $X \notin fpv(\psi')$ であり $\models WF(p_2)$ とする．

例えば $\mu X(n).\ (n = 0) \vee (n \neq 0 \wedge X(n-1))$ を考える．

$$\dfrac{\dfrac{\models (p_1(n) \wedge n = 0) \Rightarrow n = 0}{X(n); p_1; p_2; n = 0 \downarrow n = 0} \quad \dfrac{\dfrac{\models (p_1(n) \wedge n \neq 0) \Rightarrow n \neq 0}{X(n); p_1; p_2; n \neq 0 \downarrow n \neq 0} \quad \dfrac{\models (p_1(n) \wedge n \neq 0) \Rightarrow (p_1(n-1) \wedge p_2(n, n-1))}{X(n); p_1; p_2; n \neq 0 \downarrow X(n-1)}}{X(n); p_1; p_2; n \neq 0 \downarrow n \neq 0 \wedge X(n-1)}}{X(n); p_1; p_2; \top \downarrow (n = 0) \vee (n \neq 0) \wedge X(n-1)}$$

以上から p_1, p_2 の満たすべき条件は

- $\models (p_1(n) \wedge n = 0) \Rightarrow n = 0$
- $\models (p_1(n) \wedge n \neq 0) \Rightarrow n \neq 0$
- $\models (p_1(n) \wedge n \neq 0) \Rightarrow (p_1(n-1) \wedge p_2(n, n-1))$

これを満たす p_1, p_2 として例えば $p_1 = \lambda n.\ n \geq 0$, $p_2 = \lambda n_1, n_2.\ n_1 > n_2 \geq 0$ がある．

よって結果的にこの場合は $n \geq 0$ に過小近似される．

一方 $X(\widetilde{x}); p_1; p_2; \psi' \uparrow \psi$ の例に $\nu X(n).\ n \neq 0 \wedge X(n-1)$ を考える．

$$\dfrac{\dfrac{\models (p_1(n) \wedge n = 0) \Rightarrow \neg(n \neq 0)}{X(n); p_1; p_2; n = 0 \uparrow n \neq 0} \quad \dfrac{\models (p_1(n) \wedge n = 0) \Rightarrow p_1(n) \wedge p_2(n, n-1)}{X(n); p_1; p_2; n = 0 \uparrow X(n-1)}}{X(n); p_1; p_2; \top \uparrow n \neq 0 \wedge X(n-1)}$$

以上から p_1, p_2 が満たすべき条件は

- $\models (p_1(n) \wedge n = 0) \Rightarrow \neg(n \neq 0)$
- $\models (p_1(n) \wedge n \neq 0) \Rightarrow p_1(n-1) \wedge p_2(n, n-1)$

これを満たす p_1, p_2 として例えば $p_1 = \lambda n.\ n \geq 0$, $p_2 = \lambda n_1, n_2.\ n_1 > n_2 \geq 0$ がある.
よって結果的にはこの場合は $\neg(n \geq 0) = n < 0$ に過大近似される.

$$\frac{\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \psi}{X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi}\ (\text{Apx}^{\mu}\text{-Base})$$

$$\frac{\models p_1(\widetilde{x}) \wedge \psi \Rightarrow p_1(\widetilde{t}) \wedge p_2(\widetilde{x}, \widetilde{t})}{X(\widetilde{x}); p_1; p_2; \psi \downarrow X(\widetilde{t})}\ (\text{Apx}^{\mu}\text{-Rec})$$

$$\frac{X(\widetilde{x}); p_1; p_2; \psi \downarrow \psi_1 \qquad X(\widetilde{x}); p_1; p_2; \psi \downarrow \psi_2}{X(\widetilde{x}); p_1; p_2; \psi \downarrow \psi_1 \wedge \psi_2}\ (\text{Apx}^{\mu}\text{-}\wedge)$$

$$\frac{\begin{array}{c}\models (p_1(\widetilde{x}) \wedge \psi) \Rightarrow (\psi'_1 \vee \psi'_2) \\ fv(\psi'_i) \subseteq \{\widetilde{x}\} \qquad X \notin fpv(\psi'_i) \\ X(\widetilde{x}); p_1; p_2; \psi \wedge \psi'_i \downarrow \psi_i \qquad (i = 1, 2)\end{array}}{X(\widetilde{x}); p_1; p_2; \psi \downarrow \psi_1 \vee \psi_2}\ (\text{Apx}^{\mu}\text{-}\vee)$$

$$\frac{\begin{array}{c}X(\widetilde{x}); p_1; p_2; \psi' \downarrow [x'/x]\psi \\ x' \notin fv(\psi') \cup fv(\psi) \cup \{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)\end{array}}{X(\widetilde{x}); p_1; p_2; \psi' \downarrow \forall x.\ \psi}\ (\text{Apx}^{\mu}\text{-}\forall)$$

$$\frac{\begin{array}{c}\models (p_1(\widetilde{x}) \wedge \psi') \Rightarrow \exists x'.\ \psi'' \\ fv(\psi'') \subseteq \{\widetilde{x}\} \cup \{x'\} \qquad X \notin fpv(\psi'') \\ X(\widetilde{x}); p_1; p_2; \psi' \wedge \psi'' \downarrow [x'/x]\psi \\ x' \notin fv(\psi') \cup fv(\psi) \cup \{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)\end{array}}{X(\widetilde{x}); p_1; p_2; \psi' \downarrow \exists x.\ \psi}\ (\text{Apx}^{\mu}\text{-}\exists)$$

$$\frac{\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \neg\psi}{X(\widetilde{x}); p_1; p_2; \psi' \uparrow \psi}\ (\text{Apx}^{\nu}\text{-Base})$$

$$\frac{\models p_1(\widetilde{x}) \wedge \psi \Rightarrow p_1(\widetilde{t}) \wedge p_2(\widetilde{x}, \widetilde{t})}{X(\widetilde{x}); p_1; p_2; \psi \uparrow X(\widetilde{t})}\ (\text{Apx}^{\nu}\text{-Rec})$$

$$\frac{\begin{array}{c}\models (p_1(\widetilde{x}) \wedge \psi) \Rightarrow (\psi'_1 \vee \psi'_2) \\ fv(\psi'_i) \subseteq \{\widetilde{x}\} \qquad X \notin fpv(\psi'_i) \\ X(\widetilde{x}); p_1; p_2; \psi \wedge \psi'_i \uparrow \psi_i \qquad (i = 1, 2)\end{array}}{X(\widetilde{x}); p_1; p_2; \psi \uparrow \psi_1 \wedge \psi_2}\ (\text{Apx}^{\nu}\text{-}\wedge)$$

$$\frac{X(\widetilde{x}); p_1; p_2; \psi \uparrow \psi_1 \qquad X(\widetilde{x}); p_1; p_2; \psi \uparrow \psi_2}{X(\widetilde{x}); p_1; p_2; \psi \uparrow \psi_1 \vee \psi_2}\ (\text{Apx}^{\nu}\text{-}\vee)$$

$$\frac{\begin{array}{c}\models (p_1(\widetilde{x}) \wedge \psi') \Rightarrow \exists x'.\ \psi'' \\ fv(\psi'') \subseteq \{\widetilde{x}\} \cup \{x'\} \qquad X \notin fpv(\psi'') \\ X(\widetilde{x}); p_1; p_2; \psi' \wedge \psi'' \uparrow [x'/x]\psi \\ x' \notin fv(\psi') \cup fv(\psi) \cup \{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)\end{array}}{X(\widetilde{x}); p_1; p_2; \psi' \uparrow \forall x.\ \psi}\ (\text{Apx}^{\nu}\text{-}\forall)$$

$$\frac{\begin{array}{c}X(\widetilde{x}); p_1; p_2; \psi' \uparrow [x'/x]\psi \\ x' \notin fv(\psi') \cup fv(\psi) \cup \{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)\end{array}}{X(\widetilde{x}); p_1; p_2; \psi' \uparrow \exists x.\ \psi}\ (\text{Apx}^{\nu}\text{-}\exists)$$

図 4.2: Fixpoint Approximation

第5章　関連研究

本研究と同様に無限ドメインのデータと高階関数を扱える言語に対する時相仕様を記述できる既存の型システムに [1] がある．しかし [1] では仕様の記述に実行時の値を使えないため図 1.1 に例を出したような値依存時相エフェクトを扱うことができない．よって本研究で提案する型システムは [1] より真に強いものとなっている．また既存の高階関数を持つプログラムに対する時相仕様検証が可能な型システムとして [2] がある．この研究で提案されている型システムでは本研究で提案している型システムでは検証できない分岐時間仕様を検証できるが，整数のような無限の定義域を持つデータを扱うことができないのでこの点で本研究に優位性がある．また本研究で提案した論理式の妥当性判定手法は本研究の型システムの制約を解消するだけではなくもっと広い範囲で有用なものである．

第6章　結論

本研究では高階関数と整数を扱えるプログラムに対して実行時の値に依存した時相仕様を記述できる型システムを提案した. また不変条件と整礎関係を基にした導出ゲームを考えることでその型システムによって得られる不動点論理式の妥当性を判定する手法も提案した. ここで提案した不動点述語を含む論理式の妥当性判定手法は十分一般的な論理式に使えるので, この型システムを離れても有用なものである.

今後の課題としてあるプログラム状態遷移の経路だけでなくプログラムの状態に対する仕様も記述できるように拡張する, 相対完全性を持つ型システムとなるように改良する, 型検査器や型推論器を実装する, などが挙げられる.

謝辞

本研究を進めるにあたって手厚い指導, 助言および配慮を下さった亀山幸義教授および海野広志准教授に深く感謝申し上げます. 研究に協力していただいた寺内多智弘氏並びに Eric Koskinen 氏に感謝いたします. また, 多大なご厚意を頂いたシステム数理研究室久野誉人教授に多謝いたします. さらに様々なご協力をしてくださったプログラム論理研究室の皆様にお礼を申し上げます.

参考文献

[1] Eric Koskinen and Tachio Terauchi, Local Temporal Reasoning, *CSL-LICS 2014*

[2] N. Kobayashi and C.-H.L. Ong, A Type System Equivalent to the Modal Mu-Calculus Model Checking of Higher-Order Recursion Schemes *LICS 2009*

[3] Hiroshi Unno and Naoki Kobayashi, Dependent Type Inference with Interpolants, *PPDP 2009*

付 録A　型システムの健全性の証明

補題 1 (Soundness of Subtyping)**.**

- $\Gamma \vdash \sigma_1 <: \sigma_2$ ならば $\mathrm{dom}(\rho) = fpv(\Gamma) \cup fpv(\sigma_1) \cup fpv(\sigma_2)$ なる述語割り当て ρ について $[\![\rho(\Gamma) \vdash \rho(\sigma_1) <: \rho(\sigma_2)]\!]$
- $\Gamma \vdash \tau_1 <: \tau_2$ ならば $\mathrm{dom}(\rho) = fpv(\Gamma) \cup fpv(\tau_1) \cup fpv(\tau_2)$ なる述語割り当て ρ について $[\![\rho(\Gamma) \vdash \rho(\tau_1) <: \rho(\tau_2)]\!]$

証明. $\Gamma \vdash \tau_1 <: \tau_2$ と $\Gamma \vdash \sigma_1 <: \sigma_2$ の導出に関する相互帰納法により証明する.
θ を $\theta \models_{\mu,\nu} \rho(\Gamma)$ を満たす値割り当てであるとする. 最後に用いた規則が

- S-Int 規則の場合,
  - $\tau_1 = \{u \mid \phi_1\}$, $\tau_2 = \{u \mid \phi_2\}$
  - $\Vdash \lfloor \Gamma \vdash \phi_1 \Rightarrow \phi_2 \rfloor$

  を得る.

  ここで補題 4, 5 から $\models_{\mu,\nu} \theta(\rho(\phi_1 \Rightarrow \phi_2))$ である.

  よって $\{n \mid \models_{\mu,\nu} [n/u]\theta(\rho(\phi_1))\} \subseteq \{n \mid \models_{\mu,\nu} [n/u]\theta(\rho(\phi_2))\}$ である.

  $[\![\{u \mid \phi\}]\!]$ の定義より $[\![\{u \mid \theta(\rho(\phi_1))\}]\!] \subseteq [\![\{u \mid \theta(\rho(\phi_2))\}]\!]$

  したがってこの場合は $[\![\rho(\Gamma) \vdash \rho(\{u \mid \phi_1\}) <: \rho(\{u \mid \phi_2\})]\!]$ が成り立つ.

- S-Fun 規則の場合,
  - $\tau_1 = (x : \tau_1') \to \sigma_1'$, $\tau_2 = (x : \tau_2') \to \sigma_2'$
  - $\Gamma \vdash \tau_2' <: \tau_1'$
  - $\Gamma, x : \tau_2' \vdash \sigma_1' <: \sigma_2'$

  を得る.

  さらに帰納法の仮定と組み合わせて

  - $[\![\rho(\Gamma) \vdash \rho(\tau_2') <: \rho(\tau_1')]\!]$
  - $[\![\rho(\Gamma, x : \tau_2') \vdash \rho(\sigma_1') <: \rho(\sigma_2')]\!]$

を得る. よって

$$[\![\theta(\rho(\tau_2'))]\!] \subseteq [\![\theta(\rho(\tau_1'))]\!] \tag{A.1}$$
$$\forall \theta' \in sty(\Gamma, x:\tau_2').\ (\theta' \models_{\mu,\nu} \rho(\Gamma, x:\tau_2')) \Rightarrow [\![\theta'(\rho(\sigma_1'))]\!] \subseteq [\![\theta'(\rho(\sigma_2'))]\!]$$
$$\text{よって } \forall w' \in [\![\theta(\rho(\tau_2'))]\!].\ [\![\theta(\rho([w'/x]\sigma_1'))]\!] \subseteq [\![\theta(\rho([w'/x]\sigma_2'))]\!] \tag{A.2}$$

$w \in sty((x:\tau_1') \to \sigma_1')$ について $\forall w' \in [\![\theta(\rho(\tau_1'))]\!].\ w\ w' \in [\![\theta(\rho([w'/x]\sigma_1'))]\!]$ と仮定すると A.1 と A.2 より $\forall w' \in [\![\theta(\rho(\tau_2'))]\!].\ w\ w' \in [\![\theta(\rho([w'/x]\sigma_2'))]\!]$

したがって

$$\{w \mid \forall w' \in [\![\theta(\rho(\tau_1'))]\!].\ w\ w' \in [\![\theta(\rho([w'/x]\sigma_1'))]\!]\}$$
$$\subseteq \{w \mid \forall w' \in [\![\theta(\rho(\tau_2'))]\!].\ w\ w' \in [\![\theta(\rho([w'/x]\sigma_2'))]\!]\}$$

$[\![\tau]\!]$ の定義より, $[\![(x:\theta(\rho(\tau_1'))) \to \theta(\rho(\sigma_1'))]\!] \subseteq [\![(x:\theta(\rho(\tau_2'))) \to \theta(\rho(\sigma_2'))]\!]$

以上から $[\![\theta(\rho((x:\tau_1') \to \sigma_1'))]\!] \subseteq [\![\theta(\rho((x:\tau_2') \to \sigma_2'))]\!]$

よってこの場合も $[\![\rho(\Gamma) \vdash \rho((x:\tau_1') \to \sigma_1') <: \rho((x:\tau_2') \to \sigma_2')]\!]$ である.

- S-QInt 規則の場合,
  - $\sigma_1 = (\{u \mid \phi_1\}\ \&\ \Phi_1)$
  - $\sigma_2 = (\{u \mid \phi_2\}\ \&\ \Phi_2)$
  - $\Vdash \lfloor \Gamma \vdash \forall x \in \Sigma^*.\ \phi_1 \wedge \Phi_1^\mu(x) \Rightarrow \phi_2 \wedge \Phi_2^\mu(x) \rfloor$
  - $\Vdash \lfloor \Gamma \vdash \forall x \in \Sigma^\omega.\ \Phi_1^\nu(x) \Rightarrow \Phi_2^\nu(x) \rfloor$

  を得る.

  ここで補題 4, 5 から

$$\models_{\mu,\nu} \forall \varpi.\ \theta(\rho(\phi_1 \wedge \Phi_1^\mu(\varpi))) \Rightarrow \theta(\rho(\phi_2 \wedge \Phi_2^\mu(\varpi))) \tag{A.3}$$
$$\models_{\mu,\nu} \forall \pi.\ \theta(\rho(\Phi_1^\nu(\pi))) \Rightarrow \theta(\rho(\Phi_2^\nu(\pi))) \tag{A.4}$$

  $(\forall \varpi, w.\ (e\ \Downarrow\ w\ \&\ \varpi) \Rightarrow \models_{\mu,\nu} \theta(\rho([w/u]\phi_1 \wedge \Phi_1^\mu(\varpi)))) \wedge (\forall \pi.\ (e\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi_1^\nu(\pi))))$ と仮定すると補題 4, 5 より

  $(\forall \varpi, w.\ (e\ \Downarrow\ w\ \&\ \varpi) \Rightarrow \models_{\mu,\nu} \theta(\rho([w/u]\phi_2 \wedge \Phi_2^\mu(\varpi)))) \wedge (\forall \pi.\ (e\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi_2^\nu(\pi))))$

  よって

$$\{e \mid (\forall \varpi, w.\ (e \Downarrow w\ \&\ \varpi) \Rightarrow \models_{\mu,\nu} \theta(\rho([w/u]\phi_1 \wedge \Phi_1^\mu(\varpi)))) \wedge (\forall \pi.\ (e \Uparrow \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi_1^\nu(\pi))))\}$$
$$\subseteq \{e \mid (\forall \varpi, w.\ (e \Downarrow w\ \&\ \varpi) \Rightarrow \models_{\mu,\nu} \theta(\rho([w/u]\phi_2 \wedge \Phi_2^\mu(\varpi)))) \wedge (\forall \pi.\ (e \Uparrow \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi_2^\nu(\pi))))\}$$

  $[\![\sigma]\!]$ の定義より $[\![\theta(\rho((\{u \mid \phi_1\}\ \&\ \Phi_1)))]\!] \subseteq [\![\theta(\rho((\{u \mid \phi_2\}\ \&\ \Phi_2)))]\!]$

  よってこの場合も $[\![\rho(\Gamma) \vdash \rho((\{u \mid \phi_1\}\ \&\ \Phi_1)) <: \rho((u\ \&\ \Phi_2))]\!]$ がなりたつ.

- S-QFun 規則の場合,
  - $\sigma_1 = ((x : \tau_1') \to \sigma_1' \ \& \ \Phi_1), \sigma_2 = ((x : \tau_2') \to \sigma_2' \ \& \ \Phi_2)$
  - $\Gamma \vdash (x : \tau_1') \to \sigma_1' <: (x : \tau_2') \to \sigma_2'$
  - $\Vdash \lfloor \Gamma \vdash \forall \varpi.\ \Phi_1^{\mu}(\varpi) \Rightarrow \Phi_2^{\mu}(\varpi) \rfloor$
  - $\Vdash \lfloor \Gamma \vdash \forall \pi.\ \Phi_1^{\nu}(\pi) \Rightarrow \Phi_2^{\nu}(\pi) \rfloor$

  を得る.

  ここで帰納法の仮定と補題 4, 5 から

  $$[\![\theta(\rho((x : \tau_1') \to \sigma_1'))]\!] \subseteq [\![\theta(\rho((x : \tau_2') \to \sigma_2'))]\!] \tag{A.5}$$
  $$\models_{\mu,\nu} \forall \varpi.\ \theta(\rho(\Phi_1^{\mu}(\varpi) \Rightarrow \Phi_2^{\mu}(\varpi))) \tag{A.6}$$
  $$\models_{\mu,\nu} \forall \pi.\ \theta(\rho(\Phi_1^{\nu}(\pi) \Rightarrow \Phi_2^{\nu}(\pi))) \tag{A.7}$$

  ここで $e \in [\![\theta(\rho(((x : \tau_1') \to \sigma_1' \ \& \ \Phi_1)))]\!]$ とすると $[\![\sigma]\!]$ の定義より

  $$(\forall \varpi, w \in sty((x : \tau_1') \to \sigma_1').\ (e \Downarrow w \ \& \ \varpi) \Rightarrow (w \in [\![\theta(\rho((x : \tau_1') \to \sigma_1'))]\!]) \wedge (\theta \models_{\mu,\nu} \rho(\Phi_1^{\mu}(\varpi)))) \wedge$$
  $$(\forall \pi.\ e \Uparrow \bot \ \& \ \pi \Rightarrow (\theta \models_{\mu,\nu} \rho(\Phi_1^{\nu}(\pi))))$$

  が成り立つ

  したがって A.5, A.6, A.7 より

  $$(\forall \varpi, w \in sty((x : \tau_2') \to \sigma_2').\ (e \Downarrow w \ \& \ \varpi) \Rightarrow (w \in [\![\theta(\rho((x : \tau_2') \to \sigma_2'))]\!]) \wedge (\theta \models_{\mu,\nu} \rho(\Phi_2^{\mu}(\varpi)))) \wedge$$
  $$(\forall \pi.\ e \Uparrow \bot \ \& \ \pi \Rightarrow (\theta \models_{\mu,\nu} \rho(\Phi_2^{\nu}(\pi))))$$

  したがって $e \in [\![\theta(\rho(((x : \tau_2') \to \sigma_2' \ \& \ \Phi_2)))]\!]$

  よって $[\![\theta(\rho(((x : \tau_1') \to \sigma_1' \ \& \ \Phi_1)))]\!] \subseteq [\![\theta(\rho(((x : \tau_2') \to \sigma_2' \ \& \ \Phi_2)))]\!]$

  以上より, この場合も $[\![\rho(\Gamma) \vdash \rho(((x : \tau_1') \to \sigma_1' \ \& \ \Phi_1)) <: \rho(((x : \tau_2') \to \sigma_2' \ \& \ \Phi_1))]\!]$

以上よりすべての場合において $\Gamma \vdash \sigma_1 <: \sigma_2$ ならば $[\![\rho(\Gamma) \vdash \rho(\sigma_1) <: \rho(\sigma_2)]\!]$ であり,
$\Gamma \vdash \tau_1 <: \tau_2$ ならば $[\![\rho(\Gamma) \vdash \rho(\tau_1) <: \rho(\tau_2)]\!]$ である. □

補題 2 (Effect Composition)**.** 任意の Φ_1, Φ_2 について以下が成り立つ.

- 任意の ϖ_1, ϖ_2 について, $\models_{\mu,\nu} \Phi_1^{\mu}(\varpi_1)$ かつ $\models_{\mu,\nu} \Phi_2^{\mu}(\varpi_2)$ であれば $\models_{\mu,\nu} (\Phi_1 \cdot \Phi_2)^{\mu}(\varpi_1 \cdot \varpi_2)$
- 任意の ϖ_1, π_2 について, $\models_{\mu,\nu} \Phi_1^{\mu}(\varpi_1)$ かつ $\models_{\mu,\nu} \Phi_2^{\nu}(\pi_2)$ であれば $\models_{\mu,\nu} (\Phi_1 \cdot \Phi_2)^{\nu}(\varpi_1 \cdot \pi_2)$
- 任意の π_1 について, $\models_{\mu,\nu} \Phi_1^{\nu}(\pi_1)$ であれば $\models_{\mu,\nu} (\Phi_1 \cdot \Phi_2)^{\nu}(\pi_1)$

補題 3 (Soundness of Fun)**.**

ρ は $\mathrm{dom}(\rho) = fpv(\tau_f)$ を満たす任意の述語割り当てとする.

$\forall \rho'$ s.t. $\mathrm{dom}(\rho') = \{X_\mu, X_\nu\}$. $e \in [\![\rho(f : \rho'(\tau'_f), \widetilde{x} : \widetilde{\tau}) \vdash \rho(\tau \,\&\, \rho'(\Phi))]\!]$ ならば $\mathsf{rec}(f, \widetilde{x}, e) \in [\![(\rho(\tau_f) \,\&\, \Phi_{val})]\!]$ である. ただし

- $\tau'_f = (\widetilde{x}\colon \widetilde{\tau}) \to (\tau \,\&\, (\lambda x \in \Sigma^*.\ X_\mu(\widetilde{x}, x),\ \lambda x \in \Sigma^\omega.\ X_\nu(\widetilde{x}, x)))$
- $q_\mu = \mu X_\mu(\widetilde{x}, x).\ \Phi^\mu(x)$
- $q_\nu = \nu X_\nu(\widetilde{x}, x).\ [q_\mu / X_\mu]\Phi^\nu(x)$
- $\tau_f = (\widetilde{x}\colon \widetilde{\tau}) \to (\tau \,\&\, (\lambda x \in \Sigma^*.\ q_\mu(\widetilde{x}, x),\ \lambda x \in \Sigma^\omega.\ q_\nu(\widetilde{x}, x)))$

証明. 補題 4, 5 より $\mathrm{dom}(\rho') = \{X_\mu, X_\nu\}$ を満たす任意の述語割り当て ρ' と $\theta \models_{\mu,\nu} \rho(f : \rho'(\tau'_f), \widetilde{x} : \widetilde{\tau})$ を満たす任意の値割り当て θ に対して次の A.8, A.9 が成り立つ.

$$\forall w, \varpi.\ (\theta(e) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]^\wedge \models_{\mu,\nu} \theta(\rho(\rho'(\Phi^\mu)))(\varpi) \tag{A.8}$$

$$\forall \pi.\ (\theta(e) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\rho'(\Phi^\nu)))(\pi) \tag{A.9}$$

まず $\forall w, \varpi.\ (\mathsf{rec}(f, \widetilde{x}, e)\ \theta(\widetilde{x}) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]^\wedge \models_{\mu,\nu} \theta(\rho(q_\mu(\widetilde{x}, \varpi)))$ を示す.

v_i^μ, p_i^μ を以下のように定義する. ただし e^μ は $e^\mu \Downarrow w \,\&\, \varpi$ なる w, ϖ が存在しない閉じた式である.

$$\begin{aligned}
v_0^\mu &= \mathsf{rec}(f, \widetilde{x}, e^\mu) & p_0^\mu &= \lambda(\widetilde{x}, x).\ \bot \\
v_1^\mu &= \mathsf{rec}(f, \widetilde{x}, [v_0^\mu / f]e') & p_1^\mu &= \lambda(\widetilde{x}, x).\ [p_0^\mu / X_\mu]\Phi^\mu(x) \\
&\vdots & &\vdots \\
v_{i+1}^\mu &= \mathsf{rec}(f, \widetilde{x}, [v_i^\mu / f]e) & p_{i+i}^\mu &= \lambda(\widetilde{x}, x).\ [p_i^\mu / X_\mu]\Phi^\mu(x)
\end{aligned}$$

ここで

$$\forall i, w, \varpi.\ (v_{i+1}^\mu\ \theta(\widetilde{x}) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]^\wedge \models_{\mu,\nu} \theta(\rho([p_i^\mu / X_\mu]\Phi^\mu(\varpi))) \tag{A.10}$$

を数学的帰納法によって示す.

- $i = 0$ の場合

  e^μ は閉じていることより $\theta(e^\mu) = e^\mu = [v_0^\mu / f, \theta(\widetilde{x})/\widetilde{x}]e^\mu$

  よって A.8 より

  $\forall w, \varpi.\ ([v^m u_0 / f, \theta(\widetilde{x})/\widetilde{x}]e^\mu \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]^\wedge \models_{\mu,\nu} \theta(\rho(\rho'(\Phi^\mu)))(\varpi)$

  ここで $\rho' = \{X_\mu \mapsto p_0^\mu, X_\nu \mapsto \lambda(\widetilde{x}, x).\ \top\}$ とすると RT-App より

  $\forall w, \varpi.\ (v_1^\mu\ \theta(\widetilde{x}) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]^\wedge \models_{\mu,\nu} \theta(\rho([p_0^\mu / X_\mu]\Phi^\mu))(\varpi)$

  より A.10 を満たす.

- $i = k$ のとき A.10 が成り立つと仮定すると

  $\forall w, \varpi.\ (v^{\mu}_{k+1}\ \theta(\widetilde{x})\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \theta(\rho([p^{\mu}_{k}/X_{\mu}]\Phi^{\mu}(\varpi)))$

  また自明に $\forall \pi.\ (v^{\mu}_{k+1}\ \theta(\widetilde{x})\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow\models_{\mu,\nu} \theta(\rho(\lambda x.\ \top)(\pi))$ であるから

  $v^{\mu}_{k+1}\ \theta(\widetilde{x}) \in [\![\theta(\rho(\tau\ \&\ (\lambda x \in \Sigma^{*}.\ [p^{\mu}_{k}/X_{\mu}]\Phi^{\mu}(x),\ \lambda x \in \Sigma^{\omega}.\ \top)))]\!]$

  つまり $v^{\mu}_{k+1} \in [\![\theta(\rho([p^{\mu}_{k+1}/X_{\mu}, \lambda(\widetilde{x}, x).\ \top/X_{\nu}]\tau'_{f}))]\!]$

  ここで A.8 の $\rho' = \{X_{\mu} \mapsto p^{\mu}_{k+1}, X_{\nu} \mapsto \lambda(\widetilde{x}, x).\ \top\}$ である場合を考えると

  $\forall w, \varpi.\ (\theta(e)\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \rho([p^{\mu}_{k+1}/X_{\mu}]\Phi^{\mu})(\varpi)$

  $v^{\mu}_{k+1} \in [\![\theta(\rho([p^{\mu}_{k+1}/X_{\mu}, \lambda(\widetilde{x}, x).\ \top/X_{\nu}]\tau'_{f}))]\!]$ であることから

  $\forall w, \varpi.\ (\theta([v^{\mu}_{k+1}/f]e)\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \rho([p^{\mu}_{k+1}/X_{\mu}]\Phi^{\mu})(\varpi)$

  よって $\forall w, \varpi.\ (v^{\mu}_{k+2}\ \theta(\widetilde{x})\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \rho([p^{\mu}_{k+1}/X_{\mu}]\Phi^{\mu})(\varpi)$

  以上から $i = k + 1$ のときも A.10 を満たす.

ここで $\mathsf{rec}(f, \widetilde{x}, e)\ \theta(\widetilde{x})\ \Downarrow\ w\ \&\ \varpi$ であるとすると仮定する.
v^{μ}_{i} の構成から帰納法によって $\exists i.\ v^{\mu}_{i}\ \theta(\widetilde{x})\ \Downarrow\ w\ \&\ \varpi$ が得られる.
これと A.10 から $\exists i.\ w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \theta(\rho(p^{\mu}_{i}(\widetilde{x}, \varpi)))$ であり, 無限和をとって
$w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \bigvee_{i=0}^{\omega} \theta(\rho(p^{\mu}_{i}(\widetilde{x}, \varpi)))$ iff $w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \theta(\rho(\mu X(\widetilde{x}, x).\ \Phi^{\mu}(x))(\widetilde{x}, \varpi))$
よって $\forall w, \varpi.\ (\mathsf{rec}(f, \widetilde{x}, e)\ \theta(\widetilde{x})\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \theta(\rho(\mu X(\widetilde{x}, x).\ \Phi^{\mu}(x))(\widetilde{x}, \varpi))$

次に $\forall \pi.\ (\mathsf{rec}(f, \widetilde{x}, e)\ \theta(\widetilde{x})\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow\models_{\mu,\nu} \theta(\rho(q_{\nu}(\widetilde{x}, \pi))$ を示す.
v^{π}_{i}, p^{ν}_{i} を以下のように定義する. ただし e^{π} は $e^{\pi}\ \Uparrow\ \bot\ \&\ \pi$ を満たす閉じた式である.

$$
\begin{array}{ll}
v^{\pi}_{0} = \mathsf{rec}(f, \widetilde{x}, e^{\pi}) & p^{\nu}_{0} = \lambda(\widetilde{x}, x).\ \top \\
v^{\pi}_{1} = \mathsf{rec}(f, \widetilde{x}, [v^{\pi}_{0}/f]e) & p^{\nu}_{1} = \lambda(\widetilde{x}, x).\ [p^{\nu}_{0}/X_{\nu}]\Phi^{\nu}(x) \\
\quad\vdots & \quad\vdots \\
v^{\pi}_{i+1} = \mathsf{rec}(f, \widetilde{x}, [v^{\pi}_{i}/f]e) & p^{\nu}_{i+1} = \lambda(\widetilde{x}, x).\ [p^{\nu}_{i}/X_{\nu}]\Phi^{\nu}(x)
\end{array}
$$

ここで

$$
\forall i, \pi, \pi', w, \varpi.\ \left(\begin{array}{l}((v^{\pi}_{i+1}\ \theta(\widetilde{x})\ \Uparrow\ \bot\ \&\ \pi') \Rightarrow\models_{\mu,\nu} \theta(\rho([q_{\mu}/X_{\mu}, p^{\nu}_{i}/X_{\nu}]\Phi^{\nu}(\pi'))))\wedge \\ ((v^{\pi}_{i+1}\ \theta(\widetilde{x})\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \rho(q_{\mu})(\theta(\widetilde{x}), \varpi))\end{array}\right) \tag{A.11}
$$

を数学的帰納法によって示す.

- $i = 0$ の場合

  e^{π} は閉じていることより $\theta(e^{\pi}) = e^{\pi} = [v^{\pi}_{0}/f, \theta(\widetilde{x})/\widetilde{x}]e^{\pi}$

よって A.9, A.8 より

$\forall \pi'.\ ([v_0^\pi/f, \theta(\widetilde{x})/\widetilde{x}]e^\pi \Uparrow \bot \,\&\, \pi') \Rightarrow \models_{\mu,\nu} \theta(\rho(\rho'(\Phi^\nu)))(\pi')$

$\forall w, \varpi.\ ([v_0^\pi/f, \theta(\widetilde{x})/\widetilde{x}]e \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \theta(\rho(\rho'(\Phi^\mu)))(\varpi)$

ここで $\rho' = \{X_\mu \mapsto q_\mu, X_\nu \mapsto p_0^\nu\}$ とすると. RN-App, RT-App より

$\forall \pi'.\ (v_1^\pi\ \theta(\widetilde{x}) \Uparrow \bot \,\&\, \pi') \Rightarrow \models_{\mu,\nu} \theta(\rho([q_\mu/X_\mu, p_0^\nu/X_\nu]\Phi^\nu(\pi)))$ かつ

$\forall w, \varpi.\ (v_1^\pi\ \theta(\widetilde{x}) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \rho(q_\mu)(\theta(\widetilde{x}), \varpi)$

よって A.11 は成り立つ.

- $i = k$ で A.11 が成り立つと仮定すると

  $\forall \pi, \pi'.\ (v_{k+1}^\pi\ \theta(\widetilde{x}) \Uparrow \bot \,\&\, \pi') \Rightarrow \models_{\mu,\nu} \theta(\rho([q_\mu/X_\mu, p_k^\nu/X_\nu]\Phi^\nu(\pi')))$ かつ

  $\forall \pi, w, \varpi.\ (v_{k+1}^\pi\ \theta(\widetilde{x}) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \rho(q_\mu)(\theta(\widetilde{x}), \varpi)$

  よって $v_{k+1}^\pi \in [\![\theta(\rho(\tau \,\&\, (\lambda x \in \Sigma^*.\ q_\mu(\widetilde{x}, x),\ \lambda x \in \Sigma^\omega.\ [q_\mu/X_\mu]p_{k+1}^\nu(x))))]\!]$

  つまり $v_{k+1}^\pi \in [\![\theta(\rho([q_\mu/X_\mu, p_{k+1}^\nu/X_\nu]\tau_f'))]\!]$

  ここで A.8, A.9 の $\rho' = \{X_\mu \mapsto q_\mu, X_\nu \mapsto p_{k+1}^\nu\}$ である場合を考えると

  $\forall w, \varpi.\ (\theta(e) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \rho([q_\mu/X_\mu, p_{k+1}^\nu/X_\nu]\Phi^\mu)(\varpi)$ かつ

  $\forall \pi.\ (\theta(e) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \rho([q_\mu/X_\mu, p_{k+1}^\nu/X_\nu]\Phi^\nu)$

  $v_{k+1}^\pi \in [\![\theta(\rho([q_\mu/X_\mu, p_{k+1}^\nu/X_\nu]\tau_f'))]\!]$ であるから

  $\forall w, \varpi.\ (\theta([v_{k+1}^\pi/f]e) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \theta(\rho(q_\mu(\widetilde{x}, x)))$ かつ

  $\forall \pi.\ (\theta([v_{k+1}^\pi/f]e) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \rho([q_\mu/X_\mu, p_{k+1}^\nu/X_\nu]\Phi^\nu)$

  よって RT-App, RN-App より

  $\forall w, \varpi.\ (\mathtt{rec}(f, \widetilde{x}, [v_{k+1}^\pi/f]e)\ \theta(\widetilde{x}) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \theta(\rho(q_\mu(\widetilde{x}, x)))$

  $\forall \pi.\ (\mathtt{rec}(f, \widetilde{x}, [v_{k+1}^\pi/f]e)\ \theta(\widetilde{x}) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \rho([q_\mu/X_\mu, p_{k+1}^\nu/X_\nu]\Phi^\nu)$

  以上から

  $\forall w, \varpi.\ (v_{k+2}^\pi\ \theta(\widetilde{x}) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!]\wedge \models_{\mu,\nu} \theta(\rho(q_\mu(\widetilde{x}, x)))$

  $\forall \pi.\ (v_{k+2}^\pi\ \theta(\widetilde{x}) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \rho([q_\mu/X_\mu, p_{k+1}^\nu/X_\nu]\Phi^\nu)$

  より $i = k+1$ の時も A.11 が成り立つ.

A.11 が成り立つことより $\forall i, \pi, \pi'.\ (v_{i+1}^\pi\ \theta(\widetilde{x}) \Uparrow \bot \,\&\, \pi') \Rightarrow \models_{\mu,\nu} \theta(\rho([q_\mu/X_\mu, p_i^\nu/X_\nu]\Phi^\nu(\pi')))$
よって $\forall i, \pi, \pi'.\ (v_{i+1}^\pi\ \theta(\widetilde{x}) \Uparrow \bot \,\&\, \pi') \Rightarrow \models_{\mu,\nu} \theta(\rho([q_\mu/X_\mu]p_{i+1}^\nu(\widetilde{x}, \pi')))$
ここで $\mathtt{rec}(f, \widetilde{x}, e)\ \theta(\widetilde{x}) \Uparrow \bot \,\&\, \pi$ であると仮定する.
v_i^π の構成から帰納法によって $\forall i.\ \exists \pi'.\ v_{i+1}^{\pi'}\ \theta(\widetilde{x}) \Uparrow \bot \,\&\, \pi$ が得られる.
これと上から $\forall i.\ \models_{\mu,\nu} \theta(\rho([q_\nu/X_\nu]p_{i+1}^\nu(\widetilde{x}, \pi)))$ であり, 無限積をとって
$\models_{\mu,\nu} \bigwedge_{i=1}^{\omega} \theta(\rho([q_\nu/X_\nu]p_i^\nu(\widetilde{x}, \pi)))$ iff $\models_{\mu,\nu} \theta(\rho((\nu X(\widetilde{x}, x).\ [q_\mu/X_\mu]\Phi^\nu(x))(\widetilde{x}, x)))$

よって $\forall\pi.\ (\mathsf{rec}(f,\widetilde{x},e)\ \theta(\widetilde{x})\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow\models_{\mu,\nu} \theta(\rho(q_\nu(\widetilde{x},\pi)))$

以上から $\mathsf{rec}(f,\widetilde{x},e)\ \theta(\widetilde{x}) \in [\![\rho(\tau\ \&\ (\lambda x\in\Sigma^*.\ q_\mu(\widetilde{x},x),\ \lambda x\in\Sigma^\omega.\ q_\nu(\widetilde{x},x)))]\!]$
ここで $[\![(\widetilde{x}:\widetilde{\tau})\to\sigma]\!]$ の定義を $|\widetilde{x}|$ 回だけ繰り返し使うことで
$\mathsf{rec}(f,\widetilde{x},e) \in [\![(\rho(\tau_f)\ \&\ \Phi_{val})]\!]$ を得る. □

定理 3 (Soundness)**.** ρ を $\mathrm{dom}(\rho) = \mathit{fpv}(\Gamma)\cup\mathit{fpv}(\sigma)$ なる任意の述語割り当てとすると
$\Gamma\ \vdash\ e:\ \sigma$ ならば $e \in [\![\rho(\Gamma)\vdash\rho(\sigma)]\!]$

証明. θ を $\theta\models_{\mu,\nu}\rho(\Gamma)$ を満たす任意の値割り当てとする.
型付け関係 $\Gamma\ \vdash\ e:\ \sigma$ の導出についての帰納法で示す.

- T-Const の場合,
  - $e = n$
  - $\sigma = (\{x\mid x=n\}\ \&\ \Phi_{val})$

  を得る.

  ここで n に使える Non Terminating Run の規則は存在しないので $n\ \Uparrow\ \bot\ \&\ \pi$ なる π は存在しない. よって $\forall\pi.\ (n\ \Uparrow\ \bot\ \&\ \pi)\Rightarrow\models_{\mu,\nu}\Phi^\nu_{val}(\pi)$

  また n に使える Terminating Run の規則は RT-Val だけであるから $n\ \Downarrow\ w\ \&\ \varpi$ なる w,ϖ が存在すれば $w=n,\varpi=\epsilon$. よって $\forall\varpi,w.\ n\ \Downarrow\ w\ \&\ \varpi\Rightarrow(\models_{\mu,\nu} w=n\wedge\Phi^\mu_{val}(\varpi))$

  よって $n\in[\![(\{x\mid x=n\}\ \&\ \Phi_{val})]\!]$

  ここで $\theta(n)=n$, $\theta(\rho(\{x\mid x=n\}\ \&\ \Phi_{val}))=(\{x\mid x=n\}\ \&\ \Phi_{val})$ であるから

  $\theta(n)\in[\![\theta(\rho(\{x\mid x=n\}\ \&\ \Phi_{val}))]\!]$ したがって $n\in[\![\rho(\Gamma)\vdash\rho(\{x\mid x=n\}\ \&\ \Phi_{val})]\!]$

- T-Fun の場合
  - $e=\mathsf{rec}(f,\widetilde{x},e')$, $\sigma=(\tau_f\ \&\ \Phi_{val})$
  - $\tau'_f=(\widetilde{x}\colon\widetilde{\tau})\to(\tau\ \&\ (\lambda x\in\Sigma^*.\ X_\mu(\widetilde{x},x),\ \lambda x\in\Sigma^\omega.\ X_\nu(\widetilde{x},x)))$
  - $\Gamma, f:\tau'_f, \widetilde{x}:\widetilde{\tau}\ \vdash\ e':\ (\tau\ \&\ \Phi)$
  - $p_\mu=\mu X_\mu(\widetilde{x},x).\ \Phi^\mu(x)$, $p_\nu=\nu X_\nu(\widetilde{x},x).\ \Phi^\nu(x)$
  - $\tau_f=(\widetilde{x}\colon\widetilde{\tau})\to(\tau\ \&\ (\lambda x\in\Sigma^*.\ q_\mu(\widetilde{x},x),\ \lambda x\in\Sigma^\omega.\ q_\nu(\widetilde{x},x)))$

  を得る.

  帰納法の仮定より $\theta(e')\in[\![\theta(\rho(f:\tau'_f,\widetilde{x}:\widetilde{\tau}))\vdash\theta(\rho(\tau\ \&\ \Phi))]\!]$

  ここで τ'_f と Φ 中の X_μ, X_ν は自由に出現するので任意の述語に置換してもよい.

  よって $\mathrm{dom}(\rho')=\{X_\mu,X_\nu\}$ を満たす任意の述語割り当て ρ' について

$\theta(e') \in [\![\theta(\rho(f : \rho'(\tau'_f), \widetilde{x} : \widetilde{\tau})) \vdash \theta(\rho(\tau \,\&\, \rho'(\Phi)))]\!]$

よって補題 3 より, $\theta(\mathtt{rec}(f, \widetilde{x}, e')) \in [\![\theta(\rho(\tau_f) \,\&\, \Phi_{val})]\!]$

したがって $\mathtt{rec}(f, \widetilde{x}, e') \in [\![\rho(\Gamma) \vdash \rho(\tau_f \,\&\, \Phi_{val})]\!]$

- T-VInt の場合
  - $e = x$
  - $\sigma = (\{u \mid u = x\} \,\&\, \Phi_{val})$
  - $sty(\Gamma(x)) = \mathtt{int}$

  を得る.

  ここで $\theta(x)$ は整数の値であることより $\theta(x) \in [\![\rho(\{u \mid u = \theta(x)\} \,\&\, \Phi_{val})]\!]$

  よって $\theta(x) \in [\![\theta(\rho(\{u \mid u = x\} \,\&\, \Phi_{val}))]\!]$ であるから $x \in [\![\rho(\Gamma) \vdash \rho(\{u \mid u = x\} \,\&\, \Phi_{val})]\!]$
- T-VFun の場合
  - $e = x$
  - $\sigma = (\Gamma(x) \,\&\, \Phi_{val})$
  - $sty(\Gamma(x)) \neq \mathtt{int}$

  を得る.

  ここで $\theta \models_{\mu,\nu} \rho(\Gamma)$ の定義から $\theta(x) \in [\![\theta(\rho(\Gamma(x)))]\!]$

  また $\theta(x)$ は値であるから $\theta(x) \in [\![\theta(\rho(\Gamma(x) \,\&\, \Phi_{val}))]\!]$

  以上より $x \in [\![\rho(\Gamma) \vdash \rho(\Gamma(x) \,\&\, \Phi_{val})]\!]$
- T-Let の場合
  - $e = \mathtt{let}\ x\ =\ e_1\ \mathtt{in}\ e_2$
  - $\sigma = (\tau_2 \,\&\, \Phi_1 \cdot \Phi_2)$
  - $\Gamma\ \vdash\ e_1 :\ (\tau_1 \,\&\, \Phi_1)$
  - $\Gamma, x : \tau_1\ \vdash\ e_2 :\ (\tau_2 \,\&\, \Phi_2)$
  - $x \notin fv(\tau_2) \cup fv(\Phi_2)$

  を得る.

  帰納法の仮定と補題 4, 5 より
  - $\forall w, \varpi.\ (\theta(e_1)\ \Downarrow\ w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau_1))]\!] \wedge \models_{\mu,\nu} \theta(\rho(\Phi_1^{\mu}))(\varpi)$
  - $\forall \pi.\ (\theta(e_1)\ \Uparrow\ \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi_1^{\nu}))(\pi)$

- $\forall w, \varpi, w_1 \in [\![\theta(\rho(\tau_1))]\!]$. $([w_1/x]\theta(e_2) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![[w_1/x]\theta(\rho(\tau_2))]\!]\wedge \models_{\mu,\nu} [w_1/x]\theta(\rho(\Phi_2^{\mu}))(\varpi)$
- $\forall \pi, w_1 \in [\![\theta(\rho(\tau_1))]\!]$. $([w_1/x]\theta(e_2) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} [w_1/x]\theta(\rho(\Phi_2^{\nu}))(\pi)$

ここで, $\texttt{let}\ x\ =\ \theta(e_1)\ \texttt{in}\ \theta(e_2)$ に使える Terminating Run の規則は RT-Let のみであるから補題 2 より

$\forall w, \varpi$. $(\texttt{let}\ x\ =\ \theta(e_1)\ \texttt{in}\ \theta(e_2) \Downarrow w \,\&\, \varpi) \Rightarrow w \in [\![\theta(\rho(\tau_2))]\!]\wedge \models_{\mu,\nu} \theta((\rho(\Phi_1 \cdot \Phi_2))^{\mu})(\varpi)$

また $\texttt{let}\ x\ =\ \theta(e_1)\ \texttt{in}\ \theta(e_2)$ に使える NonTerminating Run の規則は RT-Let1 と RT-Let2 のみである.

- RN-Let1 の場合, $\forall \pi$. $(\texttt{let}\ x\ =\ \theta(e_1)\ \texttt{in}\ \theta(e_2) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi_1^{\nu}))(\pi)$
  補題 2 より $\forall \pi$. $(\texttt{let}\ x\ =\ \theta(e_1)\ \texttt{in}\ \theta(e_2) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho((\Phi_1 \cdot \Phi_2)^{\nu}))(\pi)$
- RN-Let2 の場合, 補題 2 より $\forall \pi$. $(\texttt{let}\ x\ =\ \theta(e_1)\ \texttt{in}\ \theta(e_2) \Uparrow \bot \,\&\, \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho((\Phi_1 \cdot \Phi_2)^{\nu}))(\pi)$

以上より $\forall \pi$. $(\texttt{let}\ x\ =\ \theta(e_1)\ \texttt{in}\ \theta(e_2) \Uparrow \bot \,\&\, \pi) \Rightarrow \theta(\rho((\Phi_1 \cdot \Phi_2)^{\nu}))(\pi)$

よって $\theta(\texttt{let}\ x\ =\ e_1\ \texttt{in}\ e_2) \in [\![\theta(\rho(\tau_2 \,\&\, \Phi_1 \cdot \Phi_2))]\!]$ である.

したがって $\texttt{let}\ x\ =\ e_1\ \texttt{in}\ e_2 \in [\![\rho(\Gamma) \vdash \rho(\tau_2 \,\&\, \Phi_1 \cdot \Phi_2)]\!]$.

- T-App の場合
  - $e = v_1\ v_2$
  - $\sigma = [v_2/x](\tau' \,\&\, \Phi)$
  - $\Gamma \vdash v_1 : ((x : \tau) \to (\tau' \,\&\, \Phi) \,\&\, \Phi_{val})$
  - $\Gamma \vdash v_2 : (\tau \,\&\, \Phi_{val})$

  を得る.

  ここで帰納法の仮定と補題 4, 5 より

  $$\theta(v_1) \in [\![\theta(\rho((x : \tau) \to (\tau' \,\&\, \Phi)) \,\&\, \Phi_{val})]\!] \subseteq [\![\theta(\rho((x : \tau) \to (\tau' \,\&\, \Phi)))]\!]$$
  したがって $\forall w' \in [\![\theta(\rho(\tau))]\!]$. $\theta(v_1)\ w' \in [\![[w'/x]\theta(\rho(\tau' \,\&\, \Phi))]\!]$
  $$\theta(v_2) \in [\![\theta(\rho(\tau \,\&\, \Phi_{val}))]\!] \subseteq [\![\theta(\rho(\tau))]\!]$$

  以上から $\theta(v_1)\ \theta(v_2) \in [\![[\theta(v_2)/x]\theta(\rho(\tau' \,\&\, \Phi))]\!]$, つまり $\theta(v_1\ v_2) \in [\![\theta(\rho([v_2/x](\tau' \,\&\, \Phi)))]\!]$

  よって $v_1\ v_2 \in [\![\rho(\Gamma) \vdash \rho([v_2/x](\tau' \,\&\, \Phi))]\!]$ である.

- T-Op の場合

- $e = v_1\ op\ v_2$
- $\sigma = (\{x \mid x = v_1\ op\ v_2\}\ \&\ \Phi_{val})$
- $\Gamma\ \vdash\ v_1\ :\ (\mathtt{int}\ \&\ \Phi_{val})$
- $\Gamma\ \vdash\ v_2\ :\ (\mathtt{int}\ \&\ \Phi_{val})$

を得る.

また, 帰納法の仮定より $v_1 \in [\![\Gamma \vdash (\mathtt{int}\ \&\ \Phi_{val})]\!]$, $v_2 \in [\![\Gamma \vdash (\mathtt{int}\ \&\ \Phi_{val})]\!]$

ここで$\theta(v_1\ op\ v_2)$に使える Non Terminating Run の規則は存在しないので$\theta(v_1\ op\ v_2)\ \Uparrow \bot\ \&\ \pi$ なる π は存在しない. よって $\forall\pi.\ (\theta(v_1\ op\ v_2)\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi^{\nu}_{val}))(\pi)$.

さらに $\theta(v_1\ \ op\ \ v_2)$ に使える Terminating Run の規則は Rt-Op だけであるから $\theta(v_1\ op\ v_2)\ \Downarrow\ w\ \&\ \varpi$ なる w, ϖ が存在すれば $w = [\![op]\!](\theta(v_1), \theta(v_2))$, $\varpi = \epsilon$.

よって $\forall\varpi, w.\ \theta(v_1\ op\ v_2)\ \Downarrow\ w\ \&\ \varpi \Rightarrow \models_{\mu,\nu} w = \rho([\![op]\!](\theta(v_1), \theta(v_2))) \wedge \theta(\rho(\Phi^{\mu}_{val}))(\varpi)$

以上より $\theta(v_1\ op\ v_2) \in [\![\theta(\rho(\{x \mid x = v_1\ op\ v_2\}\ \&\ \Phi_{val}))]\!]$

よって $v_1\ op\ v_2 \in [\![\rho(\Gamma) \vdash \rho(\{x \mid x = v_1\ op\ v_2\}\ \&\ \Phi_{val})]\!]$

- T-If の場合
  - $e = \mathtt{ifz}\ v\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2$
  - $\sigma = (\tau\ \&\ \Phi)$
  - $\Gamma, v = 0\ \vdash\ e_1\ :\ (\tau\ \&\ \Phi)$
  - $\Gamma, v \neq 0\ \vdash\ e_2\ :\ (\tau\ \&\ \Phi)$

  を得る.

  帰納法の仮定と補題 4, 5 より
  - $\models \theta(v) = 0 \wedge \forall w, \varpi.\ (\theta(e_1)\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!] \wedge \models_{\mu,\nu} \theta(\rho(\Phi^{\mu}))(\varpi)$
  - $\models \theta(v) = 0 \wedge \forall\pi.\ (\theta(e_1)\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi^{\nu}))(\pi)$
  - $\models \theta(v) \neq 0 \wedge \forall w, \varpi.\ (\theta(e_2)\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!] \wedge \models_{\mu,\nu} \theta(\rho(\Phi^{\mu}))(\varpi)$
  - $\models \theta(v) \neq 0 \wedge \forall\pi.\ (\theta(e_2)\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi^{\nu}))(\pi)$

  ここで$\theta(\mathtt{ifz}\ v\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2) = \mathtt{ifz}\ \theta(v)\ \mathtt{then}\ \theta(e_1)\ \mathtt{else}\ \theta(e_2)$に使える Terminating Run の規則は RT-IfTrue と RT-IfFalse だけである.
  - RT-IfTrue の時,

    $\models\ \theta(v) = 0$ より $\forall w, \varpi.\ (\mathtt{ifz}\ \theta(v)\ \mathtt{then}\ \theta(e_1)\ \mathtt{else}\ \theta(e_2)\ \ \Downarrow\ \ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!] \wedge \models_{\mu,\nu} \theta(\rho(\Phi^{\mu})(\varpi))$

– RT-IfFalse の時,

$\models \theta(v) \neq 0$ より $\forall w, \varpi.\ (\texttt{ifz}\ \theta(v)\ \texttt{then}\ \theta(e_1)\ \texttt{else}\ \theta(e_2)\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!] \wedge \models_{\mu,\nu} \theta(\rho(\Phi^{\mu})(\varpi))$

以上から

$\forall w, \varpi.\ (\theta(\texttt{ifz}\ v\ \texttt{then}\ e_1\ \texttt{else}\ e_2)\ \Downarrow\ w\ \&\ \varpi) \Rightarrow w \in [\![\theta(\rho(\tau))]\!] \wedge \models_{\mu,\nu} \theta(\rho(\Phi^{\mu})(\varpi))$

また, $\texttt{ifz}\ \theta(v)\ \texttt{then}\ \theta(e_1)\ \texttt{else}\ \theta(e_2)$ に使える NonTerminating Run の規則は RN-IfTrue と RN-IfFalse だけである.

– RN-IfTrue の時,

$\models \theta(v) = 0$ より $\forall \pi.\ (\texttt{ifz}\ \theta(v)\ \texttt{then}\ \theta(e_1)\ \texttt{else}\ \theta(e_2)\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi^{\nu}))(\pi)$

– RN-IfFalse の時,

$\models \theta(v) \neq 0$ より $\forall \pi.\ (\texttt{ifz}\ \theta(v)\ \texttt{then}\ \theta(e_1)\ \texttt{else}\ \theta(e_2)\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi^{\nu}))(\pi)$

よって

$\forall \pi.\ (\texttt{ifz}\ \theta(v)\ \texttt{then}\ \theta(e_1)\ \texttt{else}\ \theta(e_2)\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi^{\nu}))(\pi)$

以上から $\theta(\texttt{ifz}\ v\ \texttt{then}\ e_1\ \texttt{else}\ e_2) \in [\![\theta(\rho(\tau\ \&\ \Phi))]\!]$, よって $\texttt{ifz}\ v\ \texttt{then}\ e_1\ \texttt{else}\ e_2 \in [\![\rho(\Gamma) \vdash \rho(\tau\ \&\ \Phi)]\!]$.

- T-Event の場合

– $e = \texttt{ev[}\underline{\mathbf{a}}\texttt{]}$

– $\sigma = (\{x \mid x = 0\}\ \&\ (\lambda x \in \Sigma^*.\ x = \underline{\mathbf{a}},\ \lambda x \in \Sigma^{\omega}.\ \bot))$

を得る.

ここで $\theta(\texttt{ev[}\underline{\mathbf{a}}\texttt{]})$ に使える Non Terminating Run の規則は存在しないので $\texttt{ev[}\underline{\mathbf{a}}\texttt{]}\ \Uparrow \bot\ \&\ \pi$ なる π は存在しない. よって $\forall \pi.\ (\theta(\texttt{ev[}\underline{\mathbf{a}}\texttt{]})\ \Uparrow\ \bot\ \&\ \pi) \Rightarrow \models_{\mu,\nu} \theta(\rho(\Phi^{\nu}_{val}(\pi)))$

また $\theta(\texttt{ev[}\underline{\mathbf{a}}\texttt{]})$ に使える Terminating Run の規則は RT-Event だけであるから

$\theta(\texttt{ev[}\underline{\mathbf{a}}\texttt{]})\ \Downarrow\ w\ \&\ \varpi$ なる w, ϖ が存在すれば $w = 0,\ \varpi = \underline{\mathbf{a}}$

よって $\forall w, \varpi.\ (\theta(\texttt{ev[}\underline{\mathbf{a}}\texttt{]})\ \Downarrow\ w\ \&\ \varpi) \Rightarrow \models_{\mu,\nu} \theta(\rho(w = 0 \wedge (\lambda x \in \Sigma^*.\ x = \underline{\mathbf{a}})(\varpi)))$

よって $\theta(\texttt{ev[}\underline{\mathbf{a}}\texttt{]}) \in [\![\theta(\rho(\{x \mid x = 0\}\ \&\ (\lambda x \in \Sigma^*.\ x = \underline{\mathbf{a}},\ \lambda x \in \Sigma^{\omega}.\ \bot)))]\!]$

したがって $\texttt{ev[}\underline{\mathbf{a}}\texttt{]} \in [\![\rho(\Gamma) \vdash \rho((\{x \mid x = 0\}\ \&\ (\lambda x \in \Sigma^*.\ x = \underline{\mathbf{a}}\ \&\ \lambda x \in \Sigma^{\omega}.\ \bot)))]\!]$

- T-Sub の場合

– $\sigma = \sigma_2$

- $\Gamma \vdash e : \sigma_1$
- $\Gamma \vdash \sigma_1 <: \sigma_2$

を得る.

帰納法の仮定より $e \in [\![\rho(\Gamma) \vdash \rho(\sigma_1)]\!]$ である.

よって定義より $\forall\theta \in sty(\Gamma).\ (\theta \models_{\mu,\nu} \rho(\Gamma)) \Rightarrow \theta(e) \in [\![\theta(\rho(\sigma_1))]\!]$

ここで補題 1 より $\forall\theta \in sty(\Gamma).\ (\theta \models_{\mu,\nu} \rho(\Gamma)) \Rightarrow [\![\theta(\rho(\sigma_1))]\!] \subseteq [\![\theta(\rho(\sigma_2))]\!]$ であるからこれを使うと $\forall\theta \in sty(\Gamma).\ (\theta \models_{\mu,\nu} \rho(\Gamma)) \Rightarrow \theta(e) \in [\![\theta(\rho(\sigma_2))]\!]$

よって $e \in [\![\rho(\Gamma) \vdash \rho(\sigma_2)]\!]$

□

付 録B　不動点論理式妥当性判定の健全性の証明

補題 4.

$\Vdash \phi$ならば $\models_{\mu,\nu} \phi$

証明. $\Vdash \phi$ の導出に関する帰納法により示す.
最後に使った規則が

- Fp-Valid の場合

  $\models \psi$ を得るので即座に成り立つ.

- Fp-Lfp$^+$ の場合

  - $\phi = C^+[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]$
  - $X(\widetilde{x}); p_1; p_2; \top \downarrow nnf(\psi)$
  - $\Vdash C^+[p_1(\widetilde{t})]$
  - $\models WF(p_2)$

  を得る.

  帰納法の仮定より $\models_{\mu,\nu} C^+[p_1(\widetilde{t})]$

  定理 B.1 より $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \psi)(\widetilde{x})$

  よって $\models_{\mu,\nu} C^+[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]$ が成り立つ.

- Fp-Lfp$^-$ の場合

  - $\phi = C^-[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]$
  - $\Vdash [\lambda\widetilde{x}.\ \psi'/X]\psi \Rightarrow \psi'$
  - $\Vdash C^-[[\widetilde{t}/\widetilde{x}]\psi']$

  を得る.

  帰納法の仮定より $\models_{\mu,\nu} [\lambda\widetilde{x}.\ \psi'/X]\psi \Rightarrow \psi'$, $\models_{\mu,\nu} C^-[[\widetilde{t}/\widetilde{x}]\psi']$

  よって $\models_{\mu,\nu} (\mu X(\widetilde{x}).\ \psi)(\widetilde{x}) \Rightarrow \psi'$

  以上から $\models_{\mu,\nu} C^-[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]$

- Fp-Gfp$^+$ の場合
  - $\phi = C^+[(\nu X(\widetilde{x}).\ \psi)(\widetilde{t})]$
  - $\Vdash \psi' \Rightarrow [\lambda\widetilde{x}.\ \psi'/X]\psi$
  - $\Vdash C^+[[\widetilde{t}/\widetilde{x}]\psi']$

  を得る.

  帰納法の仮定より $\models_{\mu,\nu} \psi \Rightarrow [\lambda\widetilde{x}.\ \psi'/X]\psi$, $\models_{\mu,\nu} C^+[[\widetilde{t}/\widetilde{x}]\psi']$

  よって $\models_{\mu,\nu} \psi' \Rightarrow (\nu X(\widetilde{x}).\ \psi)(\widetilde{x})$

  以上から $\models_{\mu,\nu} C^+[(\nu X(\widetilde{x}).\ \psi)(\widetilde{t})]$

- Fp-Gfp$^-$ の場合
  - $X(\widetilde{x}); p_1; p_2; \top \overline{\uparrow}\ nnf(\psi)$
  - $\Vdash C^-[\neg p_1(\widetilde{t})]$
  - $\models WF(p_2)$

  を得る.

  帰納法の仮定より $\models_{\mu,\nu} C^-[\neg p_1(\widetilde{t})]$

  また定理 B.2 より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$

  以上から $\models_{\mu,\nu} C^-[(\nu X(\widetilde{x}).\ \psi)(\widetilde{t})]$

□

補題 5.
$\mathrm{dom}(\rho) \supseteq fpv(\Gamma) \cup fpv(\phi)$ を満たす任意の述語割り当て ρ について $\models_{\mu,\nu} \rho(\lfloor \Gamma \vdash \phi \rfloor)$ ならば $\theta \models_{\mu,\nu} \rho(\Gamma)$ をを満たす任意の値割り当て θ について $\models_{\mu,\nu} \theta(\rho(\phi))$

補題 6.
$\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi_1)(\widetilde{x})$ かつ $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi_2)(\widetilde{x})$ ならば $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi_1 \wedge \psi_2)(\widetilde{x})$.

証明. ψ_i^j を以下のように定義する. ただし $i = 1, 2$

$$\begin{aligned} \psi_i^0 &= \bot \\ \psi_i^{j+1} &= [\lambda\widetilde{x}.\ \psi_i^j/X]\psi_i \end{aligned}$$

$\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi_i)(\widetilde{x})$ より $\models_{\mu,\nu} \phi \Rightarrow \exists j.\ \psi_i^j$. よってある j_i について $\models_{\mu,\nu} \phi \Rightarrow [j_i/j]\psi_i^j$. $j' = max(j_1, j_2)$ なる j' をとると, $\models_{\mu,\nu} \phi \Rightarrow [j'/j](\psi_1^j \wedge \psi_2^j)$. よって $\models_{\mu,\nu} \phi \Rightarrow \exists j.\ \psi_1^j \wedge \psi_2^j$. 以上から $\models_{\mu,\nu} \phi \Rightarrow \mu X(\widetilde{x}).\ \psi_1 \wedge \psi_2$ □

補題 7.
$\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi)(\widetilde{x})$ かつ $\models_{\mu,\nu} \phi \Rightarrow (\psi \Rightarrow \psi')$ ならば $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi')(\widetilde{x})$

証明. ψ_i, ψ'_i を以下によって定義する.

$$\begin{aligned} \psi_0 &= \bot & \psi'_0 &= \bot \\ \psi_{i+1} &= [\lambda\widetilde{x}.\ \psi_i/X]\psi & \psi'_{i+1} &= [\lambda\widetilde{x}.\ \psi'_i/X]\psi' \end{aligned}$$

$\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi)(\widetilde{x})$ より $\models_{\mu,\nu} \phi \Rightarrow \exists i.\ \psi_i$. ここで $\models_{\mu,\nu} \phi \Rightarrow (\psi \Rightarrow \psi')$ より $\models_{\mu,\nu} \phi \Rightarrow (\psi_i \Rightarrow \psi'_i)$ であるから $\models_{\mu,\nu} \phi \Rightarrow \exists i.\ \psi'_i$. よって $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi')(\widetilde{x})$ □

補題 8.
$\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ [x'/x]\psi)(\widetilde{x})$ かつ $x' \notin fv(\psi) \cup \{\widetilde{x}\}$ ならば $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \forall x.\ \psi)(\widetilde{x})$

証明. ψ_i を以下によって定義する.

$$\begin{aligned} \psi_0 &= \bot \\ \psi_{i+1} &= [\lambda\widetilde{x}.\ \psi_i/X]\psi \end{aligned}$$

$\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ [x'/x]\psi)(\widetilde{x})$ より $\models_{\mu,\nu} \phi \Rightarrow \exists i.\ [x'/x]\psi_i$ である. $x' \notin fv(\psi) \cup \{\widetilde{x}\}$ より $\models_{\mu,\nu} \phi \Rightarrow \exists i.\ \forall x.\ \psi_i$. よって $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \forall x.\ \psi)(\widetilde{x})$ □

補題 9.
$\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ (\psi' \wedge \psi'') \Rightarrow [x'/x]\psi)(\widetilde{x})$ かつ $\models_{\mu,\nu} (\phi \wedge \psi') \Rightarrow \exists x'.\ \psi''$ ならば $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi' \Rightarrow \exists x.\ \psi)(\widetilde{x})$

証明. 題意より $\phi \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee \neg(\exists x'.\ \psi'') \vee [x'/x]\psi)(\widetilde{x})$ $\models_{\mu,\nu}$ と $\models_{\mu,\nu} \phi \Rightarrow (\neg\psi' \vee \exists x'.\ \psi'')$ を得る. ここで $\models_{\mu,\nu} \phi \Rightarrow (\neg\psi' \vee \exists x'.\ \psi'')$ から $\models_{\mu,\nu} \phi \Rightarrow ((\neg\psi' \vee \neg\exists x'.\ \psi'' \vee [x'/x]\psi) \Rightarrow (\neg\psi' \vee [x'/x]\psi))$ と補題 7 より $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee [x'/x]\psi)(\widetilde{x})$ である. よって $\models_{\mu,\nu} \phi \Rightarrow (\mu X(\widetilde{x}).\ \psi' \Rightarrow \exists x.\ \psi)(\widetilde{x})$. □

補題 10.
$\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi_1)(\widetilde{x}) \Rightarrow \phi$ かつ $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi_2)(\widetilde{x}) \Rightarrow \phi$ ならば $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi_1 \vee \psi_2)(\widetilde{x}) \Rightarrow \phi$

証明. ψ_i^j を以下によって定義する. ただし $i = 1, 2$

$$\begin{aligned} \psi_i^0 &= \top \\ \psi_i^{j+1} &= [\lambda\widetilde{x}.\ \psi_i^j/X]\psi_i \end{aligned}$$

$\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi_i)(\widetilde{x}) \Rightarrow \phi$ より $\models_{\mu,\nu} \forall j.\ \psi_i^j \Rightarrow \phi$. よって $\models_{\mu,\nu} \forall j.\ \psi_1^j \vee \psi_2^j \Rightarrow \phi$ であるから $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi_1 \vee \psi_2)(\widetilde{x}) \Rightarrow \phi$ を得る. □

補題 11.
$\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi)(\widetilde{x}) \Rightarrow \phi$ かつ $\models_{\mu,\nu} \neg\phi \Rightarrow (\psi' \Rightarrow \psi)$ ならば $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi')(\widetilde{x}) \Rightarrow \phi$

証明. ψ_i, ψ'_i を以下によって定義する.

$$\psi_0 = \top \qquad \psi'_0 = \top$$
$$\psi_{i+1} = [\lambda\widetilde{x}.\ \psi_i/X]\psi \qquad \psi'_{i+1} = [\lambda\widetilde{x}.\ \psi'_i/X]\psi'$$

$\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi)(\widetilde{x}) \Rightarrow \phi$ より $\models_{\mu,\nu} \neg\phi \Rightarrow \neg\forall i.\ \psi_i$. ここで $\models_{\mu,\nu} \neg\phi \Rightarrow (\psi' \Rightarrow \psi)$ より $\models_{\mu,\nu} \neg\phi \Rightarrow (\neg\psi \Rightarrow \neg\psi')$ であるから $\models_{\mu,\nu} \neg\phi \Rightarrow \neg\forall i.\ \psi'_i$ である. よって $\models_{\mu,\nu} \neg\phi \Rightarrow \neg(\nu X(\widetilde{x}).\ \psi')(\widetilde{x})$ を得て, これの対偶をとって $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi')(\widetilde{x}) \Rightarrow \phi$ である. □

補題 12.
$\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi'' \wedge [x'/x]\psi)(\widetilde{x}) \Rightarrow \phi$ かつ $\models_{\mu,\nu} (\neg\phi \wedge \psi') \Rightarrow \exists x'.\ \psi''$ ならば $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \forall x.\ \psi)(\widetilde{x}) \Rightarrow \phi$

証明. 題意より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \exists x'.\ \psi'' \wedge [x'/x]\psi)(\widetilde{x}) \Rightarrow \phi$ かつ $\models_{\mu,\nu} \neg\phi \Rightarrow (\neg\psi' \vee \exists x'.\ \psi'')$ を得る. これより $\models_{\mu,\nu} \neg\phi \Rightarrow (\psi' \wedge \forall x.\ \psi \Rightarrow \psi' \wedge \exists x'.\ \psi'' \wedge [x'/x]\psi)$ であるからこれと補題 11 より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \forall x.\ \psi)(\widetilde{x}) \Rightarrow \phi$ である. □

補題 13.
$\models_{\mu,\nu} (\nu X(\widetilde{x}).\ [x'/x]\psi)(\widetilde{x}) \Rightarrow \phi$ かつ $x' \notin fv(\psi) \cup \{\widetilde{x}\}$ ならば $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \exists x.\ \psi)(\widetilde{x}) \Rightarrow \phi$

証明. ψ_i を以下によって定義する.

$$\psi_0 = \top$$
$$\psi_{i+1} = [\lambda\widetilde{x}.\ \psi_i/X]\psi$$

$\models_{\mu,\nu} (\nu X(\widetilde{x}).\ [x'/x]\psi)(\widetilde{x}) \Rightarrow \phi$ より $\models_{\mu,\nu} (\forall i.\ [x'/x]\psi_i) \Rightarrow \phi$ である. $x' \notin fv(\psi) \cup \{\widetilde{x}\}$ より $\models_{\mu,\nu} (\forall i.\ \exists x.\ \psi_i) \Rightarrow \phi$ よって $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \exists x.\ \psi)(\widetilde{x}) \Rightarrow \phi$ □

定理 4 (Soundness of Fixpoint Approximation)**.**

$$X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi \text{ならば } \models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee \psi)(\widetilde{x}) \tag{B.1}$$
$$X(\widetilde{x}); p_1; p_2; \psi' \uparrow \psi \text{ならば } \models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x}) \tag{B.2}$$

ここで ψ は nnf であり $X \notin fpv(\psi')$ であり $\models WF(p_2)$ とする.

証明. B.1 を $X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi$ の導出に関する帰納法により証明する.
最後に用いた規則が

- Apx$^{\mu}$-Base の場合,

  $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \psi$ を得る. よって $\models p_1(\widetilde{x}) \Rightarrow \neg\psi' \vee \psi$.

  $\neg\psi' \vee \psi$ 中に出現する X は自由述語変数なので X に $\mu X(\widetilde{x}).\ \neg\psi' \vee \psi$ を代入して,
  $\models p_1(\widetilde{x}) \Rightarrow [\mu X(\widetilde{x}).\ \neg\psi' \vee \psi/X](\neg\psi' \vee \psi)$. $[\mu X(\widetilde{x}).\ \neg\psi' \vee \psi]$ は $(\mu X(\widetilde{x}).\ \neg\psi' \vee \psi)(\widetilde{x})$ と同値であるから, $\models p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee \psi)(\widetilde{x})$ を得る. よって B.1 を満たす.

- Apx$^{\mu}$-Rec の場合

  - $\psi = X(\widetilde{t})$
  - $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow p_1(\widetilde{t}) \wedge p_2(\widetilde{x}, \widetilde{t})$

  を得る. 以下のように ψ_i を定義する

  $$\psi_0 = \bot$$
  $$\psi_{i+1} = \neg\psi' \vee [\widetilde{t}/\widetilde{x}]\psi_i$$

  ここで $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow p_1(\widetilde{t})$ かつ $\models p_1(\widetilde{x}) \Rightarrow \neg\psi' \vee p_1(\widetilde{t})$ であるから $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \neg\psi' \vee [\widetilde{t}/\widetilde{x}]p_1(\widetilde{t})$. これを繰り返して. $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \neg\psi' \vee [\widetilde{t}/\widetilde{x}](\neg\psi' \vee \cdots [\widetilde{t}/\widetilde{x}]p_1(\widetilde{t}) \cdots)$ を得る. ここで, $p_1(\widetilde{x}) \wedge \psi' \Rightarrow p_2(\widetilde{x}, \widetilde{t})$ かつ $\models WF(p_2)$ であるから $\models \neg[\widetilde{t}/\widetilde{x}]^i p_1(\widetilde{t})$ なる自然数 i が存在する. よって $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \exists i.\ \psi_i$ が成り立つ. より $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \bigvee_{i=0}^{\omega} \psi_i$ である. ここで補題**??**より, $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee X(\widetilde{t}))(\widetilde{x})$ を得る. よって $\models p_1(\widetilde{x}) \Rightarrow \neg\psi' \vee (\mu X(\widetilde{x}).\ \neg\psi' \vee X(\widetilde{t}))(\widetilde{x})$ であるから $\models p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee X(\widetilde{t}))(\widetilde{x})$ であり補題 B.1 を満たす.

- Apx$^{\mu}$-$\wedge$ の場合

  - $\psi = \psi_1 \wedge \psi_2$
  - $X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi_1$
  - $X(\widetilde{x}); p_1; p_2; \psi' \downarrow \psi_2$

  を得る.

  帰納法の仮定より

  - $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee \psi_1)(\widetilde{x})$
  - $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee \psi_2)(\widetilde{x})$

  よって補題 6 より $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee \psi_1 \wedge \psi_2)(\widetilde{x})$

- Apx$^{\mu}$-$\vee$ の場合, $i = 1, 2$ について

  - $\psi = \psi_1 \vee \psi_2$

- $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow (\psi'_1 \vee \psi'_2)$
- $fv(\psi'_i) \subseteq \{\widetilde{x}\}$
- $X \notin fpv(\psi'_i)$
- $X(\widetilde{x}); p_1; p_2; \psi' \wedge \psi'_i \downarrow \psi_i$

を得る.

帰納法の仮定より

- $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg(\psi' \wedge \psi'_1) \vee \psi_1)(\widetilde{x})$
- $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg(\psi' \wedge \psi'_2) \vee \psi_2)(\widetilde{x})$

よって 6 より $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee ((\neg\psi'_1 \vee \psi_1) \wedge (\neg\psi'_2 \vee \psi_2)))(\widetilde{x})$ ここで $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow (\psi'_1 \vee \psi'_2)$, つまり $\models p_1(\widetilde{x}) \Rightarrow (\neg\psi' \vee \psi'_1 \vee \psi'_2)$ であるから $\models p_1(\widetilde{x}) \Rightarrow ((\neg\psi' \vee (\neg\psi'_1 \vee \psi_1) \wedge (\neg\psi'_2 \vee \psi_2)) \Rightarrow (\neg\psi' \vee \psi_1 \vee \psi_2))$ より, 7 から $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi \vee \psi_1 \vee \psi_2)(\widetilde{x})$.

- Apx$^{\mu}$-$\forall$ の場合
  - $\psi = \forall x.\ \psi_1$
  - $X(\widetilde{x}); p_1; p_2; \psi' \downarrow [x'/x]\psi_1$
  - $x' \notin fv(\psi') \cup fv(\psi_1) \cup fv(p_1) \cup fv(p_2)$

  を得る.

  帰納法の仮定より $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee [x'/x]\psi_1)(\widetilde{x})$

  x' は完全に自由な変数であるから $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ \neg\psi' \vee \forall x.\ \psi_1)(\widetilde{x})$

- Apx$^{\mu}$-$\exists$ の場合
  - $\psi = \exists x.\ \psi_1$
  - $\models_{\mu,\nu} p_1(\widetilde{x}) \wedge \psi' \Rightarrow \exists x'.\ \psi''$
  - $fv(\psi'') \subseteq \{\widetilde{x}\} \cup \{x'\}$
  - $X \notin fpv(\psi'')$
  - $X(\widetilde{x}); p_1; p_2; \psi' \wedge \psi'' \downarrow [x'/x]\psi_1$

  を得る.

  帰納法の仮定より $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ (\psi' \wedge \psi'') \Rightarrow [x'/x]\psi_1)(\widetilde{x})$ を得る. これと $\models_{\mu,\nu} p_1(\widetilde{x}) \wedge \psi' \Rightarrow \exists x'.\ \psi'' \Rightarrow$ より補題 9 から $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\mu X(\widetilde{x}).\ (\psi' \wedge \psi'') \Rightarrow \exists x.\ \psi_1)(\widetilde{x})$ が成り立つ.

B.2 を $X(\widetilde{x}); p_1; p_2; \psi' \uparrow \psi$ の導出に関する帰納法により証明する.
最後に用いた規則が

- Apx$^\nu$-Base の場合

  $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \neg\psi$ を得る. よって $\models p_1(\widetilde{x}) \Rightarrow \neg(\psi' \wedge \psi)$ である.

  $\psi' \wedge \psi$ 中に出現する X は自由述語変数なので X に $\nu X(\widetilde{x}).\ \psi' \wedge \psi$ を代入して,
  $\models p_1(\widetilde{x}) \Rightarrow \neg[\nu X(\widetilde{x}).\ \psi' \wedge \psi / X](\psi' \wedge \psi)$ を得る. $[\nu X(\widetilde{x}).\ \psi' \wedge \psi](\psi' \wedge \psi)$ と $(\nu X(\widetilde{x}).\ \psi' \wedge \psi)(\widetilde{x})$ は同値であるから. $\models p_1(\widetilde{x}) \Rightarrow \neg(\nu X(\widetilde{x}).\ \psi' \wedge \psi)(\widetilde{x})$ が成り立つ.

  よって $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$ であり B.2 を満たす.

- Apx$^\nu$-Rec の場合

  - $\psi = X(\widetilde{t})$
  - $p_1(\widetilde{x}) \wedge \psi' \Rightarrow p_1(\widetilde{t}) \wedge p_2(\widetilde{x}, \widetilde{t})$

  を得る. ψ'_i を以下のように定義する.

  $$\begin{aligned} \psi'_0 &= \top \\ \psi'_{i+1} &= \psi' \wedge [\widetilde{t}/\widetilde{x}]\psi'_i \end{aligned}$$

  ここで Apx$^\mu$-Rec の ψ_i について $\psi'_i = \neg\psi_i$ であるから, $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \exists i.\ \neg\psi_i$ を得る. これより $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \neg\forall i.\ \psi'_i$ よって $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \neg \bigwedge_{i=0}^{\omega} \psi'_i$ を得, 補題**??**から $\models p_1(\widetilde{x}) \wedge \psi' \Rightarrow \neg(\nu X(\widetilde{x}).\ \psi' \wedge X(\widetilde{t}))(\widetilde{x})$. が成り立つ. よって $\models \psi' \wedge (\nu X(\widetilde{x}).\ \psi' \wedge X(\widetilde{t}))(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$ であり. $\psi' \wedge \nu X(\widetilde{x}).\ \psi' \wedge X(\widetilde{t})$ は $\nu X(\widetilde{x}).\ \psi' \wedge X(\widetilde{t})$ と同値であるから $\models (\nu X(\widetilde{x}).\ \psi' \wedge X(\widetilde{t})) \Rightarrow \neg p_1(\widetilde{x})$ を得る. よって B.2 を満たす.

- Apx$^\nu$-$\wedge$ の場合, $i = 1, 2$ について

  - $\psi = \psi_1 \wedge \psi_2$
  - $\models_{\mu,\nu} p_1(\widetilde{x}) \wedge \psi \Rightarrow (\psi'_1 \vee \psi'_2)$
  - $fv(\psi'_i) \subseteq \{\widetilde{x}\}$
  - $X \notin fpv(\psi'_i)$
  - $X(\widetilde{x}); p_1; p_2; \psi \wedge \psi'_i \downarrow \psi_i$

  を得る.

  帰納法の仮定より

  - $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi'_1 \wedge \psi_1)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$
  - $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi'_2 \wedge \psi_2)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$

よって補題 10 より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge (\psi'_1 \wedge \psi_1 \vee \psi'_2 \wedge \psi_2))(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$. また, $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow (\psi \Rightarrow (\psi'_1 \vee \psi'_2))$ より $\models_{\mu,\nu} p_1(\widetilde{x}) \Rightarrow ((\psi' \wedge (\psi_1 \vee \psi_2)) \Rightarrow (\psi' \wedge (\psi'_1 \wedge \psi_1 \vee \psi'_2 \wedge \psi_2)))$ であるから補題 11 より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge (\psi_1 \vee \psi_2))(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$ が成り立つ.

- Apx$^{\nu}$-$\vee$ の場合
  - $\psi = \psi_1 \vee \psi_1$
  - $X(\widetilde{x}); p_1; p_2; \psi' \overline{\uparrow} \psi_1$
  - $X(\widetilde{x}); p_1; p_2; \psi' \overline{\uparrow} \psi_2$

  を得る.

  帰納法の仮定より
  - $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi_1)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$
  - $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi_2)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$

  よって補題 10 より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi_1 \wedge \psi_2)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$.

- Apx$^{\nu}$-$\forall$ の場合
  - $\psi = \forall x.\ \psi_1$
  - $\models_{\mu,\nu} (p_1(\widetilde{x}) \wedge \psi') \Rightarrow \exists x'.\ \psi''$
  - $fv(\psi'') \subseteq \{\widetilde{x}\} \cup \{x'\}$
  - $X \notin fpv(\psi'')$
  - $X(\widetilde{x}); p_1; p_2; \psi' \wedge \psi'' \overline{\uparrow} [x'/x]\psi$
  - $x' \notin fv(\psi') \cup fv(\psi) \cup \{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)$

  を得る.

  帰納法の仮定より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \psi'' \wedge [x'/x]\psi)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$. さらに $\models_{\mu,\nu} (p_1(\widetilde{x}) \wedge \psi') \Rightarrow \exists x'.\ \psi''$ であるから補題 12 より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \forall x.\ \psi_1)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$ が成り立つ.

- Apx$^{\nu}$-$\exists$ の場合
  - $\psi = \exists x.\ \psi_1$
  - $X(\widetilde{x}); p_1; p_2; \psi' \overline{\uparrow} [x'/x]\psi_1$
  - $x' \notin fv(\psi') \cup fv(\psi_1) \cup \{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)$

  を得る.

  帰納法の仮定より $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge [x'/x]\psi_1)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$

  x' は完全に自由な変数であるから $\models_{\mu,\nu} (\nu X(\widetilde{x}).\ \psi' \wedge \exists x.\ \psi_1)(\widetilde{x}) \Rightarrow \neg p_1(\widetilde{x})$

□