一階不動点論理の循環証明体系とプログラム検証への応用

南條 陽史　海野 広志

本論文で我々は最小・最大不動点で一階述語論理を拡張した一階不動点論理の証明体系を提案する．本体系は証明木を正則木で表現する循環証明の考えに基づいており，既存の証明体系 [2] と比べて帰納法・余帰納法を柔軟に適用できる．既存体系には論理式中の不動点を過小・過大近似する規則があり，それらは帰納法・余帰納法に対応するが，適用可能な判断の形や仮定の適用条件が制限されていた．本論文では既存体系の証明が提案体系の証明に変換可能であることを示す．さらに提案体系が様々なプログラム検証問題に応用できることを明らかにする．具体的には制約付きホーン節制約解消問題や状態遷移系の安全性・停止性の証明・反証問題，トレース等価性といった関係的仕様検証問題が一階不動点論理式の妥当性判定問題に帰着できることを示す．特に関係的仕様は, 既存証明体系では十分に扱えない仕様であった．

1　はじめに

プログラム検証とは与えられたプログラムが仕様を満たすか否かを判定する技術であり, 高信頼ソフトウェアを開発するうえで重要である．本論文では状態遷移系の安全性・停止性・非安全性・非停止性検証問題, ラベル付き状態遷移系のトレース等価性検証問題, 制約付きホーン節制約解消問題といったプログラム検証問題が一階述語論理を不動点で拡張した一階不動点論理の妥当性判定問題に帰着されることを示し, 妥当性判定のための新しい証明体系を提案する．

一階不動点論理の妥当性判定には大きく分けて以下の 2 つのアプローチがあった．一つは最小・最大不動点の過小・過大近似に基づいたアプローチである．これは不動点を含む論理式を不動点を含まない背景理論 (例えば線形算術) の論理式で健全に近似した上で背景理論のソルバを用いて妥当性判定するものである．[2] はこのアプローチを採用した証明体系を提案している．このアプローチの利点として, 背景理論のソルバによる各種データ型の値に関する強力な推論の恩恵を受けられる点や近似の際に不変条件やランキング関数の合成といったプログラム検証の技術を応用することができるという点が挙げられるが, 一階不動点論理式中の個々の最小・最大不動点を別々に背景理論の論理式によって近似しなければならないため, 仕様の検証に必要な近似が背景理論で表現できなかったり, 表現できたとしても複雑 (例えば非線形算術を用いたもの) になって発見するのが難しくなったりすることがあるという欠点も存在する．例えば 3 節の制約付きホーン節制約解消およびトレース等価性検証の例や 4 節の図 2 中の, 自然数ならば偶数もしくは奇数であることの証明のように, 複数の不動点が出現するような論理式の妥当性判定が必要になる関係的仕様検証では必要な不動点近似の発見が困難になる傾向がある．別の言い方をすると, [2] の不動点近似の規則は帰納法・余帰納法に対応するが, それらが適用可能な判断の形や仮定の適用条件には制限がある．

一階不動点論理の妥当性判定の二つ目のアプローチは帰納的・余帰納的定理証明に基づいたものである．特に [3] は, 証明木を健全性のために必要なある条件を満たす ω-正則木として表すという循環証明の

A Cyclic Proof System for First-Order Fixpoint Logic and Applications to Program Verification

南條 陽史, 筑波大学, University of Tsukuba.
海野 広志, 筑波大学, University of Tsukuba.

アイデアによって証明体系 LK を拡張したものを提案している．循環証明体系は帰納法をどのように使うかの決定を遅延させることができるため証明探索が非循環証明体系に比べて自動化しやすいといわれている．こちらのアプローチの利点として，一つ目のアプローチとは異なり帰納法・余帰納法の適用に制限がないため，証明できる論理式の範囲が広い点があげられる．これによって一つ目のアプローチで解くのが困難であった関係的仕様検証問題をこちらのアプローチでは解くことができる場合がある．一方欠点として証明探索に背景理論のソルバやプログラム検証の技術を応用する方法が自明でないという点が挙げられる．

本論文ではこれら二つの体系の利点を併せ持ち欠点を補った体系を提案することを目指した．提案する体系では [3] の循環証明体系をもとに背景理論のソルバを使えるように規則を追加した．しかし，背景理論のソルバは背景理論のデータ型に対する帰納法を扱えないため，前述の規則を追加しただけでは証明能力が不十分である．例えば，4 節の図 2 中の 0 以上の整数は自然数であることの証明ができない．この問題を解決するため，我々は証明木を表す ω-正則木が満たすべき条件 [3] を緩和することによって背景理論のデータ型に対する整礎帰納法を可能とした．その条件の検査で必要な整礎関係の発見にはプログラムの停止性検証で研究されてきたランキング関数の合成法を利用することができる．

本論文ではさらに提案体系が既存体系 [2,3] のどちらと比べても同等以上の証明能力を持つことを示す．提案体系は [3] を拡張したものであるから [3] で証明可能な論理式は提案体系で証明可能である．それに加えて [2] の体系の証明から提案体系の証明への変換法を与えることで，[2] によって証明可能な論理式は提案体系でも証明可能であることを示す．

以下に本論文の構成を示す．2 節では本論文が扱う一階不動点論理の構文と意味を与える．3 節では検証分野で重要な制約付きホーン節制約解消問題，プログラムの安全性・停止性・非安全性・非停止性問題，ラベル付き状態遷移系のトレース等価性の検証問題がどのように一階不動点論理式の妥当性判定問題に帰着されるかを説明し具体例を与える．4 節では 2 節で導入した一階不動点論理のための循環証明体系を提案する．5 節では [2] で提案された証明体系の証明から本論文で提案する証明体系の証明への変換を与えることで提案体系の証明能力は既存の証明体系のそれと比べて同等以上であることを示す．最後に 6 節で本論文のまとめと今後の課題について議論する．

2 一階不動点論理

本論文で対象とする一階不動点論理を導入する．

一階不動点論理式の構文

シグネチャ Σ 上の論理式の構文を以下で定義する．

(論理式) $\phi ::= \bot \mid \top \mid A(\widetilde{t}) \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2$
$\mid \kappa_1 < \kappa_2 \mid \forall x.\phi \mid \exists x.\phi \mid \forall\kappa.\phi \mid \exists\kappa.\phi \mid \Phi(\widetilde{t})$

(項) $t ::= x \mid f(\widetilde{t})$

(述語) $\Phi ::= X \mid \mu X(\widetilde{x}).\ \phi \mid \mu^{\kappa} X(\widetilde{x}).\ \phi$

ここで X, x, κ, α はそれぞれ述語変数，項変数，順序数変数，順序数を表すメタ変数である．A, f はそれぞれ Σ の述語シンボルと関数シンボルである．項の列を $\widetilde{t}$ のように書き，その長さを $|\widetilde{t}|$ と書く．長さが 0 の列を ϵ と書く．最小不動点 $\mu X(\widetilde{x}).\ \phi$ とその近似 $\mu^{\kappa} X(\widetilde{x}).\ \phi$ において ϕ 中の X は常に正の位置に出現するものとする．$\phi_1 \Rightarrow \phi_2$ を $\neg\phi_1 \vee \phi_2$ の略記，最大不動点 $\nu X(\widetilde{x}).\ \phi$ を $\neg\mu X(\widetilde{x}).\ \neg[\neg X/X]\phi$ の略記とする．ψ を不動点を含まない論理式を表すメタ変数として用いる．ϕ 中の自由項変数の集合を $\mathit{fv}(\phi)$，自由述語変数の集合を $\mathit{fpv}(\phi)$ と書く．

一階不動点論理式の意味論

$\mathrm{Pred}(S) = S \to \{\bot, \top\}$ を S 上の述語が点ごとの順序でなす束とする．単調関数 $f\colon \mathrm{Pred}(S) \to \mathrm{Pred}(S)$ について不動点 μf とその近似 $\mu^{\alpha} f$ を以下で定義する．

$$\mu^0 f = \lambda x.\ \bot \qquad \mu^{\gamma} f = \bigvee_{\alpha<\gamma} \mu^{\alpha} f \ (\gamma \text{ は極限順序数})$$

$$\mu^{\alpha+1} f = f(\mu^{\alpha} f) \qquad \mu f = \bigvee_{\alpha} \mu^{\alpha} f$$

構造 $\mathcal{A}$ の領域を $|\mathcal{A}|$ と書き，a を $|\mathcal{A}|$ の要素を表すメタ変数とする．$\mathcal{A}(A)\colon |A|^{\mathrm{arity}(A)} \to \{\bot, \top\}$, $\mathcal{A}(f)\colon |A|^{\mathrm{arity}(f)} \to |A|$ はそれぞれ A, f の意味である．ただし $\mathrm{arity}(A)$, $\mathrm{arity}(f)$ はそれぞれ A と f の

アリティを表す. 構造 $\mathcal{A}$ および述語・順序数・項変数の値割り当て ρ からなる Σ-モデル $\mathcal{M} = (\mathcal{A}, \rho)$ が与えられたとき, 一階不動点論理式の意味は以下で定義される.

$$\begin{aligned}
\mathcal{M} &\models \top \\
\mathcal{M} &\models A(\widetilde{t}) \textit{ iff } \mathcal{A}(A)([\![\widetilde{t}]\!]_{\mathcal{M}}) \\
\mathcal{M} &\models \neg\phi \textit{ iff } \mathcal{M} \not\models \phi \\
\mathcal{M} &\models \phi_1 \wedge \phi_2 \textit{ iff } \mathcal{M} \models \phi_1 \text{ かつ } \mathcal{M} \models \phi_2 \\
\mathcal{M} &\models \phi_1 \vee \phi_2 \textit{ iff } \mathcal{M} \models \phi_1 \text{ または } \mathcal{M} \models \phi_2 \\
\mathcal{M} &\models \kappa_1 < \kappa_2 \textit{ iff } \rho(\kappa_1) < \rho(\kappa_2) \\
\mathcal{M} &\models \forall x.\phi \textit{ iff 任意の } a \text{ で } \mathcal{M}[x \mapsto a] \models \phi \\
\mathcal{M} &\models \exists x.\phi \textit{ iff ある } a \text{ で } \mathcal{M}[x \mapsto a] \models \phi \\
\mathcal{M} &\models \forall \kappa.\phi \textit{ iff 任意の順序数 } \alpha \text{ で } \mathcal{M}[\kappa \mapsto \alpha] \models \phi \\
\mathcal{M} &\models \exists \kappa.\phi \textit{ iff ある順序数 } \alpha \text{ で } \mathcal{M}[\kappa \mapsto \alpha] \models \phi \\
\mathcal{M} &\models \Phi(\widetilde{t}) \textit{ iff } [\![\Phi]\!]_{\mathcal{M}}([\![\widetilde{t}]\!]_{\mathcal{M}}) \\
[\![X]\!]_{\mathcal{M}} &\triangleq \rho(X) \\
[\![\mu X(\widetilde{x}).\ \phi]\!]_{\mathcal{M}} &\triangleq \mu\Psi \\
[\![\mu^{\kappa} X(\widetilde{x}).\ \phi]\!]_{\mathcal{M}} &\triangleq \mu^{\rho(\kappa)}\Psi \\
[\![x]\!]_{\mathcal{M}} &\triangleq \rho(x) \\
[\![f(\widetilde{t})]\!]_{\mathcal{M}} &\triangleq \mathcal{A}(f)([\![\widetilde{t}]\!]_{\mathcal{M}})
\end{aligned}$$

ここで $\Psi(P)(\widetilde{a}) = [\![\phi]\!]_{\mathcal{M}[X \mapsto P, \widetilde{x} \mapsto \widetilde{a}]}$ であるとし, $\mathcal{M}[x \mapsto a]$ は $\mathcal{M}$ の値割り当て ρ を $\rho(x) = a$ となるように拡張したものを表すとする. $\mathcal{M} \models \phi$ のときモデル $\mathcal{M}$ は論理式 ϕ を充足させるといい, $\mathcal{M} \models \phi$ と書く. 任意のモデル $\mathcal{M}$ について $\mathcal{M} \models \phi$ のとき論理式 ϕ は妥当であるという. $\mathcal{A}$ が文脈から明らかな場合は $\mathcal{M} \models \phi$ を $\rho \models \phi$ と書く.

3 プログラム検証への応用

様々なプログラム検証問題が一階不動点論理式の妥当性判定問題に帰着できる. ここでは制約付きホーン節制約解消問題, プログラムの安全性・停止性・非安全性・非停止性検証問題, ラベル付き状態遷移系のトレース等価性検証問題がそれぞれどのように一階不動点論理式で表現されるかを説明し，具体例を与える.

制約付きホーン節とは以下の形をした論理式である.

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n \Rightarrow B$$

ここで A_i, B は述語変数適用 $X(\widetilde{t})$ か述語変数を含まない論理式である. 特に B が $\bot$ であるホーン節をゴール節, そうでないホーン節を確定節という.

制約付きホーン節制約解消問題とは与えられたすべての節を妥当にするような述語変数代入の存在の判定問題である [1, 4]. 例として [4] で扱われている, 異なる定義をされた 2 つの掛け算の等価性検証問題から得られた以下の制約付きホーン節制約解消問題を考える.

$$\top \Rightarrow P(x, 0, 0) \quad \top \Rightarrow Q(x, 0, a, a)$$
$$P(x, y-1, r) \wedge (y \neq 0) \Rightarrow P(x, y, x+r)$$
$$Q(x, y-1, a+x, r) \wedge (y \neq 0) \Rightarrow Q(x, y, a, r)$$
$$P(x, y, r_1) \wedge Q(x, y, a, r_2) \wedge r_1 + a \neq r_2 \Rightarrow \bot$$

ここで述語 P, Q は異なる 2 つの掛け算に対応する. この制約解消問題は以下の一階不動点論理式の妥当性判定問題に帰着される.

$$P(x, y, r_1) \wedge Q(x, y, a, r_2) \wedge r_1 + a \neq r_2 \Rightarrow \bot$$

ただし

$$\begin{aligned}
P &= \mu X(x, y, r). \\
&\quad (y = 0 \wedge r = 0) \vee X(x, y-1, x+r) \wedge y \neq 0 \\
Q &= \mu X(x, y, a, r). \\
&\quad (y = 0 \wedge a = r) \vee X(x, y-1, a+x, r) \wedge y \neq 0
\end{aligned}$$

である.

次に値の組 $\langle\widetilde{a}\rangle$ として表される状態が遷移関係 $\rightarrow$ によって次のステップの状態 $\langle\widetilde{b}\rangle$ に移されるような状態遷移系の安全性, 停止性, 非安全性, 非停止性がどのように一階不動点論理で表現されるかを説明する. この状態遷移系の初期状態を表す述語を *Init*, エラー状態を表す述語を *Error* と書く.

まず到達可能な状態を表す述語 Reachable と計算が発散しうる状態を表す述語 MayDiverge を定義する. ある状態が到達可能であるとは初期状態であるかそこに遷移可能な到達可能状態が存在することである. 一方で, ある状態が発散しうるとは, 発散しうる状態に遷移可能であることである. よってそれぞれ最小・最大不動点を使って以下のように書ける.

$$\text{Reachable} \triangleq \mu X(\widetilde{x}).\ \mathit{Init}(\widetilde{x}) \vee \exists\widetilde{y}.(X(\widetilde{y}) \wedge (\langle\widetilde{y}\rangle \rightarrow \langle\widetilde{x}\rangle))$$
$$\text{MayDiverge} \triangleq \nu X(\widetilde{x}).\ \exists\widetilde{y}.((\langle\widetilde{x}\rangle \rightarrow \langle\widetilde{y}\rangle) \wedge X(\widetilde{y}))$$

安全性. 遷移システムが安全であるとは到達可能なすべての状態がエラー状態ではないということであるから以下のように書ける.

$$\forall\widetilde{x}.(\text{Reachable}(\widetilde{x}) \Rightarrow \neg \mathit{Error}(\widetilde{x}))$$

停止性. 遷移システムが停止するとは初期状態は発

散しないということであるから以下のように書ける.

$$\forall \widetilde{x}.(\mathrm{MayDiverge}(\widetilde{x}) \Rightarrow \neg \mathit{Init}(\widetilde{x}))$$

非安全性. 遷移システムが安全でないとは到達可能なエラー状態が存在するということであるから以下のように書ける.

$$\exists \widetilde{x}.(\mathit{Error}(\widetilde{x}) \wedge \mathrm{Reachable}(\widetilde{x}))$$

非停止性. 遷移システムが停止しないとは発散しうる初期状態が存在するということであるから以下のように書ける.

$$\exists \widetilde{x}.(\mathit{Init}(\widetilde{x}) \wedge \mathrm{MayDiverge}(\widetilde{x}))$$

上述の安全性, 停止性の検証の例としてプログラム 1, 非安全性, 非停止性の例としてプログラム 2 を示す.

プログラム 1

```
main(x, y, z) {
  assume(y >= z);
  while (x < y) {
    x++;
  }
  assert(x >= z);
}
```

プログラム 2

```
main(x, y, z) {
  assume(y >= z);
  while x < y {
    x = x + 1 + z;
  }
  assert(x+z >= y);
}
```

以下の関係 R_1 はプログラム 1 をモデル化した状態遷移関係であり, 関係 R_2 はプログラム 2 をモデル化した状態遷移関係である.

$$\begin{aligned} R_1 =& \{\, (\langle x,y,z,0\rangle, \langle x,y,z,1\rangle) \mid y \geq z \,\} \cup \\ & \{\, (\langle x,y,z,1\rangle, \langle x+1,y,z,1\rangle) \mid x < y \,\} \cup \\ & \{\, (\langle x,y,z,1\rangle, \langle x,y,z,2\rangle) \mid x \geq y \,\} \\ R_2 =& \{\, (\langle x,y,z,0\rangle, \langle x,y,z,1\rangle) \mid y \geq z \,\} \cup \\ & \{\, (\langle x,y,z,1\rangle, \langle x+1+z,y,z,1\rangle) \mid x < y \,\} \cup \\ & \{\, (\langle x,y,z,1\rangle, \langle x,y,z,2\rangle) \mid x+z \geq y \,\} \end{aligned}$$

$R_i(\langle x,y,z,p\rangle, \langle x',y',z',p'\rangle)$ はプログラム i において状態 $\langle x,y,z,p\rangle$ が $\langle x',y',z',p'\rangle$ に遷移することを意味する. R_1, R_2 ぞれぞれについて 1 行目は `assume` を満たして次の行へ遷移, 2 行目は `while` ループの条件を満たしてループ内を評価してループ先頭に遷移, 3 行目は `while` ループから脱出して次の行に遷移することを表している.

前述の安全性・停止性. 非安全性・非停止性をプログラム 1 とプログラム 2 について関係 R_1 と R_2 を使って具体化して得られる一階不動点論理式は以下の通りである.

安全性
$(\mu X(\widetilde{x}).\ p = 0 \vee \exists \widetilde{x'}.R_1(\widetilde{x'}, \widetilde{x}) \wedge X(\widetilde{x'}))(\widetilde{x}) \Rightarrow (p = 2 \Rightarrow x \geq z)$

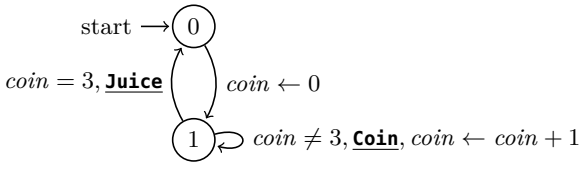
停止性
$(\nu X(\widetilde{x}).\ \exists \widetilde{x'}.R_1(\widetilde{x}, \widetilde{x'}) \wedge X(\widetilde{x'}))(\widetilde{x}) \Rightarrow \neg(p = 0)$

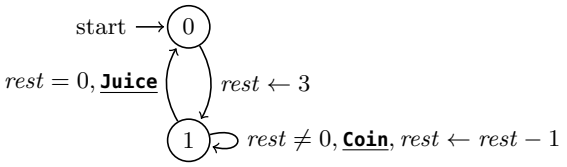
非安全性
$\exists \widetilde{x}.\left(\begin{array}{l}(p = 2 \wedge \neg(x + z \geq y)) \wedge \\ (\mu X(\widetilde{x}).\ p = 0 \vee \exists \widetilde{x'}.R_2(\widetilde{x'}, \widetilde{x}) \wedge X(\widetilde{x'}))(\widetilde{x})\end{array}\right)$

非停止性
$\exists \widetilde{x}.\left(\begin{array}{l}p = 0 \wedge \\ (\nu X(\widetilde{x}).\ \exists \widetilde{x'}.R_2(\widetilde{x}, \widetilde{x'}) \wedge X(\widetilde{x'}))(\widetilde{x})\end{array}\right)$

ここで $\widetilde{x}$ は x, y, z, p, $\widetilde{x'}$ は x', y', z', p' を表している.

最後に以下の 2 つの停止しないラベル付き状態遷移系を例に関係的仕様の一つであるトレース等価性問題がどのように一階不動点論理の妥当性判定問題に帰着されるのかを説明する.





ここで $\underline{\mathbf{e}}$ は状態が遷移するときにイベント $\underline{\mathbf{e}}$ が起こることを意味する. 二つの状態遷移系はジュース

販売機をモデル化している．一つ目の遷移系ではまずコイン投入枚数 $coin$ を 0 で初期化し，コイン投入枚数 $coin$ が 3 になるまで購入者がコインを投入する (**Coin**) のを待つ．コイン投入枚数 $coin$ が 3 になるとジュースを購入者に渡し (**Juice**) 初期状態に戻る．二つ目の遷移系ではまず，あと残り何枚のコインが必要かを表す $rest$ を 3 で初期化し，必要コイン枚数 $rest$ が 0 になるまで購入者がコインを投入する (**Coin**) のを待つ．必要コイン枚数 $rest$ が 0 になるとジュースを購入者に渡し (**Juice**) 初期状態に戻る．二つのジュース販売機はどちらも同じイベント列を生成する．

遷移系から生じるイベントの列 x が満たす一階不動点論理述語はそれぞれ以下のように書ける．

$$
\begin{aligned}
&P_1 \triangleq \nu X(c,s,x).\\
&\quad s=0 \wedge X(0,1,x) \vee\\
&\quad s=1 \wedge c \neq 3 \wedge \exists x'.x = \underline{\textbf{Coin}} \cdot x' \wedge X(c+1,1,x') \vee\\
&\quad s=1 \wedge c = 3 \wedge \exists x'.x = \underline{\textbf{Juice}} \cdot x' \wedge X(c,0,x')\\
&P_2 \triangleq \nu X(r,s,x).\\
&\quad s=0 \wedge X(3,1,x) \vee\\
&\quad s=1 \wedge r \neq 0 \wedge \exists x'.x = \underline{\textbf{Coin}} \cdot x' \wedge X(r-1,1,x') \vee\\
&\quad s=1 \wedge r = 0 \wedge \exists x'.x = \underline{\textbf{Juice}} \cdot x' \wedge X(r,0,x')
\end{aligned}
$$

$P_1(c,s,x)$ は一つ目の遷移系についてコイン投入枚数 c, 状態 s から遷移して得られるイベントの無限列が x であること，$P_1(r,s,x)$ は二つ目の遷移系について必要コイン枚数 r, 状態 s から遷移して得られるイベントの無限列が x であることを表している．よって二つの遷移系から生じるトレースが等しいことは次の一階不動点論理式の妥当性判定問題に帰着できる．

$$\forall c,r,x,y.(P_1(c,0,x) \wedge P_2(r,0,y) \Rightarrow x = y)$$

4 循環証明体系

$\Gamma \vdash_{\mathcal{O}} \Delta$ をシーケントとよぶ．ここで Γ と Δ は論理式の列であり，$\mathcal{O}$ は順序数変数の集合である．シーケント $\Gamma \vdash_{\mathcal{O}} \Delta$ は直感的には Γ のすべての要素を"$\wedge$"で結んだものを前提としたときに Δ のすべての要素を "$\vee$" で結んだものが含意されることを証明できることを表している．シーケント全体の集合を Seq と書く．

与えられた Σ-model $\mathcal{M} = (\mathcal{A}, \rho)$ について，すべての $\phi \in \Gamma$ で $\mathcal{M} \models \phi$ となることが，ある $\phi' \in \Delta$ について $\mathcal{M} \models \phi'$ となることを含意するとき，$\mathcal{M}$ は $\Gamma \vdash_{\mathcal{O}} \Delta$ を充足させるという．任意のモデルが $\Gamma \vdash_{\mathcal{O}} \Delta$ を充足させるとき，$\Gamma \vdash_{\mathcal{O}} \Delta$ は妥当であるという．

提案する証明体系の規則を図 4 に示す．提案体系は実質的に [3] を Valid 規則で拡張したものである．Valid 規則以外の Structural Rules と Logical Rules はどれもシーケント計算と同様である．$\models_{th} \phi$ とは ϕ に出現する不動点述語を未解釈としたときに背景理論のソルバで妥当であると判定されることを意味しており，Valid 規則によって [3] と比べて証明探索に背景理論のソルバを使うことができるという利点がある．μ_1-L 規則はシーケントの左辺に現れた不動点述語適用を順序数変数で注釈された不動点述語適用に置き換える規則である．μ_0-R 規則はシーケントの右辺に現れた不動点述語適用を展開する規則である．μ_1-L 規則，μ_0-R 規則との対称性を考えると自然に得られる μ_1-R, μ_0-L は提案する証明体系で導出可能である．μ^κ-L 規則と μ^κ-R 規則はそれぞれシーケントの左辺と右辺に現れた近似された不動点を展開する規則である．$\exists\kappa$-L 規則は負の位置で存在量化された順序数変数をシーケント全体では全称量化されているとみて $\mathcal{O}$ に追加する規則，$\exists\kappa$-R 規則は右辺で存在量化されている順序数変数にすでに出現している自由変数を代入する規則である．$\forall\kappa$-L と $\forall\kappa$-R はそれぞれ $\exists\kappa$-R と $\exists\kappa$-L に対応した規則である．$<$-L は前提部に恒偽式 $\kappa < \kappa$ が現れたとき，爆発律によってシーケント全体は妥当であるという規則，$<$-R 規則は順序数の公理から得られる規則である．Subst 規則において θ は述語・順序数・項変数への代入を表す．規則すべての集合を $Rules$ と書く．

定義 1 (導出木)**.** 導出木 $\mathcal{D} = (\mathcal{V}, \mathcal{E}, s)$ とは以下を満たす木 $(\mathcal{V}, \mathcal{E})$ である．

- $\mathcal{V}$ はノード集合，$\mathcal{E}\colon \mathcal{V} \times \mathcal{V}$ は辺集合，$s\colon \mathcal{V} \to Seq$ は頂点から対応するシーケントへの写像である．
- $v \in \mathcal{V}$ とその子ノード $v_1, \cdots, v_n \in \mathcal{V}$ について

$$\frac{s(v_1) \ \cdots \ s(v_n)}{s(v)}$$

がある規則 $r \in Rules$ のインスタンスである．

このような規則 r を $Rule(v)$ と書くことにする．

Structural Rules

$$\frac{\models_{th} \bigwedge \Gamma \Rightarrow \bigvee \Delta}{\Gamma \vdash_{\mathcal{O}} \Delta}\ \textsc{Valid} \qquad \frac{\Gamma' \vdash_{\mathcal{O}'} \Delta' \quad \mathcal{O}' \subseteq \mathcal{O} \quad \Gamma' \subseteq \Gamma \quad \Delta' \subseteq \Delta}{\Gamma \vdash_{\mathcal{O}} \Delta}\ \textsc{Weak} \qquad \frac{\Gamma, \phi \vdash_{\mathcal{O}} \Delta \quad \Gamma \vdash_{\mathcal{O}} \phi, \Delta}{\Gamma \vdash_{\mathcal{O}} \Delta}\ \textsc{Cut} \qquad \frac{\Gamma \vdash_{\mathcal{O}} \Delta}{\theta(\Gamma) \vdash_{\theta(\mathcal{O})} \theta(\Delta)}\ \textsc{Subst}$$

Logical Rules

$$\frac{\Gamma \vdash_{\mathcal{O}} \phi, \Delta}{\Gamma, \neg\phi \vdash_{\mathcal{O}} \Delta}\ \neg\text{-L} \qquad \frac{\Gamma, \phi \vdash_{\mathcal{O}} \Delta}{\Gamma \vdash_{\mathcal{O}} \neg\phi, \Delta}\ \neg\text{-R}$$

$$\frac{\Gamma, \phi_1, \phi_2 \vdash_{\mathcal{O}} \Delta}{\Gamma, \phi_1 \wedge \phi_2 \vdash_{\mathcal{O}} \Delta}\ \wedge\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O}} \phi_1, \Delta \quad \Gamma \vdash_{\mathcal{O}} \phi_2, \Delta}{\Gamma \vdash_{\mathcal{O}} \phi_1 \wedge \phi_2, \Delta}\ \wedge\text{-R} \qquad \frac{\Gamma, \phi_1 \vdash_{\mathcal{O}} \Delta \quad \Gamma, \phi_2 \vdash_{\mathcal{O}} \Delta}{\Gamma, \phi_1 \vee \phi_2 \vdash_{\mathcal{O}} \Delta}\ \vee\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O}} \phi_1, \phi_2, \Delta}{\Gamma \vdash_{\mathcal{O}} \phi_1 \vee \phi_2, \Delta}\ \vee\text{-R}$$

$$\frac{\Gamma, [t/x]\phi \vdash_{\mathcal{O}} \Delta}{\Gamma, \forall x.\phi \vdash_{\mathcal{O}} \Delta}\ \forall\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O}} [x'/x]\phi, \Delta \quad x' \text{ is fresh}}{\Gamma \vdash_{\mathcal{O}} \forall x.\phi, \Delta}\ \forall\text{-R} \qquad \frac{\Gamma, [x'/x]\phi \vdash_{\mathcal{O}} \Delta \quad x' \text{ is fresh}}{\Gamma, \exists x.\phi \vdash_{\mathcal{O}} \Delta}\ \exists\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O}} [t/x]\phi, \Delta}{\Gamma \vdash_{\mathcal{O}} \exists x.\phi, \Delta}\ \exists\text{-R}$$

Fixpoint Rules

$$\frac{\Gamma, \exists\kappa.(\mu^{\kappa} X(\widetilde{x}).\ \phi)(\widetilde{t}) \vdash_{\mathcal{O}} \Delta}{\Gamma, (\mu X(\widetilde{x}).\ \phi)(\widetilde{t}) \vdash_{\mathcal{O}} \Delta}\ \mu_1\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O}} [\mu X(\widetilde{x}).\ \phi/X, \widetilde{t}/\widetilde{x}]\phi, \Delta}{\Gamma \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \phi)(\widetilde{t}), \Delta}\ \mu_0\text{-R}$$

$$\frac{\Gamma, \exists\kappa'.\kappa' < \kappa \wedge [\mu^{\kappa'} X(\widetilde{x}).\ \phi/X, \widetilde{t}/\widetilde{x}]\phi \vdash_{\mathcal{O}} \Delta}{\Gamma, (\mu^{\kappa} X(\widetilde{x}).\ \phi)(\widetilde{t}) \vdash_{\mathcal{O}} \Delta}\ \mu^{\kappa}\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O}} \exists\kappa'.\kappa' < \kappa \wedge [\mu^{\kappa'} X(\widetilde{x}).\ \phi/X, \widetilde{t}/\widetilde{x}]\phi, \Delta}{\Gamma \vdash_{\mathcal{O}} (\mu^{\kappa} X(\widetilde{x}).\ \phi)(\widetilde{t}), \Delta}\ \mu^{\kappa}\text{-R}$$

Ordinal Rules

$$\frac{\Gamma, \phi \vdash_{\mathcal{O},\kappa} \Delta \quad \kappa \notin \mathcal{O}}{\Gamma, \exists\kappa.\phi \vdash_{\mathcal{O}} \Delta}\ \exists\kappa\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O}} [\kappa'/\kappa]\phi, \Delta \quad \kappa' \in \mathcal{O}}{\Gamma \vdash_{\mathcal{O}} \exists\kappa.\phi, \Delta}\ \exists\kappa\text{-R}$$

$$\frac{\Gamma, [\kappa'/\kappa]\phi \vdash_{\mathcal{O}} \Delta \quad \kappa' \in \mathcal{O}}{\Gamma, \forall\kappa.\phi \vdash_{\mathcal{O}} \Delta}\ \forall\kappa\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O},\kappa} \phi, \Delta \quad \kappa \notin \mathcal{O}}{\Gamma \vdash_{\mathcal{O}} \forall\kappa.\phi, \Delta}\ \forall\kappa\text{-R}$$

$$\frac{}{\Gamma, \kappa < \kappa \vdash_{\mathcal{O}} \Delta}\ <\text{-L} \qquad \frac{\Gamma \vdash_{\mathcal{O}} \kappa' < \kappa'', \Delta \quad \Gamma \vdash_{\mathcal{O}} \kappa'' < \kappa, \Delta}{\Gamma \vdash_{\mathcal{O}} \kappa' < \kappa, \Delta}\ <\text{-R}$$

図 1　証明体系の規則

定義 2 (Repeat)**.** 導出木 $\mathcal{D}$ 中の Repeat $R = (v, v')$ とは以下を満たす $\mathcal{D}$ 中のノードのペアである.

- v は葉ノードである
- v' は $\mathcal{D}$ の root ノードから v へのパス上に存在する
- $s(v) = s(v')$

v を bud ノード, v' を v に対する companion ノードと呼ぶ. $\mathcal{D}$ 上のパス $v' \cdots v$ を $\pi(R)$ と書く.

定義 3 (前証明)**.** 導出木 $\mathcal{D} = (\mathcal{V}, \mathcal{E}, s)$ と Repeat の集合 $\mathcal{R}$ について $Rule(v)$ が公理でないようなす

べての葉ノード v に対してちょうど一つの repeat $(v, v') \in \mathcal{R}$ が存在するとき $\mathcal{P} = (\mathcal{D}, \mathcal{R})$ を前証明という.
グラフ $\mathcal{G}_{\mathcal{P}} = (\mathcal{V}, \mathcal{E} \cup \mathcal{R}, s)$ を $\mathcal{P}$ の前証明グラフという.

導出木 $\mathcal{D}$ について, 関係 $\to \subseteq \mathcal{R} \times \mathcal{R}$ を 2 つの repeat $R_1 = (v_1, v_1')$, $R_2 = (v_2, v_2')$ について $\mathcal{D}$ 中にパス $v_1' \cdots v_2$ が存在するときまたそのときに限り $R_1 \to R_2$ となる関係として定義する.

定義 4 (保存)**.** $\pi(R) = v_0 \cdots v_m$, $s(v_i) = \Gamma_i \vdash_{\mathcal{O}_i} \Delta_i$ なる repeat R について

- R が順序数変数 κ を保存するとは以下を満たすことである
  - すべての i で $\kappa \in \mathcal{O}_i$
  - $\mathit{Rule}(v_j) = \textsc{Subst}$ かつ $\theta(s(v_j)) = s(v_{j+1})$ となるすべての j, θ について, $\Gamma_j \vdash_{\mathcal{O}_j} \theta(\kappa) < \kappa, \Delta_j$ の前証明 $(\mathcal{D}, \emptyset)$ が存在するか, もしくは $\theta(\kappa) = \kappa$
- R が変数列と順序関係の組 $(\widetilde{x}, \prec)$ を保存するとは以下を満たすことである
  - すべての $y \in \{\widetilde{x}\}, i$ について y は $\Gamma_i \vdash_{\mathcal{O}_i} \Delta_i$ の自由項変数である
  - $\mathit{Rule}(v_j) = \textsc{Subst}$ かつ $\theta(s(v_j)) = s(v_{j+1})$ となるすべての j, θ について, $\Gamma_j \vdash_{\mathcal{O}_j} \theta(\widetilde{x}) \prec \widetilde{x}, \Delta_j$ の前証明 $(\mathcal{D}, \emptyset)$ が存在するか, もしくは $\theta(\widetilde{x}) = \widetilde{x}$

定義 5 (進行)**.** $\pi(R) = v_0 \cdots v_m$, $s(v_i) = \Gamma_i \vdash_{\mathcal{O}_i} \Delta_i$ なる repeat R について

- R が順序数変数 κ で進行するとは以下を満たすことである.
  - R が κ を保存する
  - $\mathit{Rule}(v_j) = \textsc{Subst}$ かつ $\theta(s(v_j)) = s(v_{j+1})$ となるある j, θ について, $\Gamma_j \vdash_{\mathcal{O}_j} \theta(\kappa) < \kappa, \Delta_j$ の前証明 $(\mathcal{D}, \emptyset)$ が存在する
- R が変数列と順序関係の組 $(\widetilde{x}, \prec)$ で進行するとは以下を満たすことである
  - R が $(\widetilde{x}, \prec)$ を保存する
  - $\mathit{Rule}(v_j) = \textsc{Subst}$ かつ $\theta(s(v_j)) = s(v_{j+1})$ となるある j, θ について, $\Gamma_j \vdash_{\mathcal{O}_j} \theta(\widetilde{x}) \prec \widetilde{x}, \Delta_j$ の前証明 $(\mathcal{D}, \emptyset)$ が存在する

定義 6 (証明)**.** 前証明 $\mathcal{P} = (\mathcal{D}, \mathcal{R})$ についてグラフ $(\mathcal{R}, \to)$ の各強連結部分グラフ $S \subseteq \mathcal{R}$ が以下のいずれかを満たすとき, $\mathcal{P}$ は証明という.

- 以下を満たす順序数変数 κ が存在する
  - すべての repeat $R \in S$ が κ を保存する
  - ある repeat $R \in S$ が κ で進行する
- 以下を満たす自由項変数列 $\widetilde{x}$, 値の列上の整礎関係 $\prec$ が存在する
  - すべての repeat $R \in S$ が $(\widetilde{x}, \prec)$ を保存する
  - ある repeat $R \in S$ が $(\widetilde{x}, \prec)$ で進行する

図 2, 3 に提案体系の証明の例を示す.

次に提案体系の健全性を示す. 健全性証明は, もとにした循環証明体系 [3] と同様にできる.

補題 1 (局所健全性)**.** *Rules* に含まれる規則はいずれも局所的に健全である. つまり前提がすべて妥当であれば帰結も妥当である.

補題 2. ある規則の結論を満たさない Σ-model $\mathcal{M} = (A, \rho)$ があるとき, (A, ρ') がその規則のある前提を満たさないような ρ' が存在する. つまり, $\Gamma \vdash_{\mathcal{O}} \Delta$ の証明 $((\mathcal{V}, \mathcal{E}, s), \mathcal{R})$ が与えられてかつ $\Gamma \vdash_{\mathcal{O}} \Delta$ を充足しない $\mathcal{M} = (A, \rho_0)$ があるとき, ρ_i に対してある ρ_{i+1} を次々に決めることにより, (A, ρ_i) が $\Gamma \vdash_{\mathcal{O}} \Delta$ の証明のパスに沿った i 番目のシーケント $s(v_i) = \Gamma_i \vdash_{\mathcal{O}_i} \Delta_i$ を妥当でなくするような無限列 (v_i, ρ_i) を作ることができる.

定理 7 (健全性)**.** $\Gamma \vdash_{\mathcal{O}} \Delta$ の証明 $\mathcal{P}$ が存在するならば $\Gamma \vdash_{\mathcal{O}} \Delta$ は妥当である

証明. 背理法による. $\Gamma \vdash_{\mathcal{O}} \Delta$ が妥当でないとすると補題 2 から $\Gamma \vdash_{\mathcal{O}} \Delta$ の証明グラフのパスに沿った無限列 (v_i, ρ_i) を作ることができる. しかし, これは証明の定義から順序数の無限降下列が存在するか, もしくは整礎関係にある項の列の無限降下列が存在することになるので矛盾. よって前提は誤りで $\Gamma \vdash_{\mathcal{O}} \Delta$ は妥当である. □

5 既存の証明体系との証明能力の比較

本節では提案体系の証明能力が, 既存の体系 [2, 3] の証明能力以上であることを示す. 提案体系は [3] で

シーケントに注釈されている † は対応するシーケント間に repeat があることを意味する.

n が 0 以上ならば n は自然数であることの証明

$$\dfrac{\dfrac{}{n \geq 0 \vdash n = 0, n \neq 0}\ \textsc{Valid} \quad \dfrac{\dfrac{\dfrac{}{n \geq 0 \vdash n - 1 \geq 0, n = 0}\ \textsc{Valid}}{n \geq 0 \vdash n - 1 \geq 0, n = 0, N(n-1)}\ \textsc{Weak} \quad \dfrac{\dfrac{n \geq 0 \vdash N(n)^{\dagger}}{n - 1 \geq 0 \vdash N(n-1)}\ \textsc{Subst}}{n \geq 0, n - 1 \geq 0 \vdash n = 0, N(n-1)}\ \textsc{Weak}}{n \geq 0 \vdash n = 0, N(n-1)}\ \textsc{Cut}}{\dfrac{n \geq 0 \vdash n = 0, (n \neq 0 \wedge N(n-1))}{n \geq 0 \vdash n = 0 \vee (n \neq 0 \wedge N(n-1))}\ \vee\text{-R}}{n \geq 0 \vdash N(n)^{\dagger}}\ \wedge\text{-R}\ \ \mu\text{-R}$$

$N \triangleq \mu X(n).\ n = 0 \vee (n \neq 0 \wedge X(n-1))$

Subst with $\{\, n \to n - 1 \,\}$

進行のため, ある整礎関係 $\prec$ について $n - 1 \geq 0 \vdash_{\mathcal{O}} n - 1 \prec n, N(n-1)$ の repeat を用いない証明が必要.

$\prec \triangleq \lambda(x, y).\ y > x \geq 0$ とすれば Weak 規則と Valid 規則でそのような証明を得られる.

n が自然数であれば n は 0 以上であることの証明

$$\dfrac{\dfrac{}{\kappa' < \kappa, n = 0 \vdash_{\kappa,\kappa'} n \geq 0}\ \textsc{Valid} \quad \dfrac{\dfrac{\dfrac{}{n - 1 \geq 0 \vdash_{\kappa,\kappa'} n \geq 0}\ \textsc{Valid} \quad \dfrac{\dfrac{N^{\kappa}(n) \vdash_{\kappa} n \geq 0^{\dagger}}{\kappa < \kappa'', N^{\kappa}(n) \vdash_{\kappa'',\kappa} n \geq 0}\ \textsc{Weak}}{\kappa' < \kappa, N^{\kappa'}(n-1) \vdash_{\kappa,\kappa'} n - 1 \geq 0}\ \textsc{Subst}}{\kappa' < \kappa, n \neq 0, N^{\kappa'}(n-1) \vdash_{\kappa,\kappa'} n \geq 0}\ \textsc{Cut, Weak}}{\kappa' < \kappa, n = 0 \vee n \neq 0 \wedge N^{\kappa'}(n-1) \vdash_{\kappa,\kappa'} n \geq 0}\ \vee\text{-L}, \wedge\text{-L}}{\dfrac{N^{\kappa}(n) \vdash_{\kappa} n \geq 0^{\dagger}}{N(n) \vdash n \geq 0}\ \mu_1\text{-L}, \exists\kappa\text{-L}}\ \mu^{\kappa}\text{-L}, \exists\kappa\text{-L}, \wedge\text{-L}$$

$N \triangleq \mu X(n).\ n = 0 \vee n \neq 0 \wedge X(n-1) \quad N^{\kappa} \triangleq \mu^{\kappa} X(n).\ n = 0 \vee n \neq 0 \wedge X(n-1)$

Subst with $\{\, \kappa'' \to \kappa, \kappa \to \kappa', n \to n - 1 \,\}$

進行のため, $\kappa' < \kappa, N^{\kappa'}(n-1) \vdash_{\kappa,\kappa'} \kappa' < \kappa, n - 1 \geq 0$ の repeat を用いない証明が必要.

そのような証明は Valid によって得られる.

図 2　提案体系における循環証明の例

提案された循環証明体系を拡張したものである. よって [3] の証明体系の証明は提案体系の証明でもあるため, 提案体系の証明能力は明らかに [3] の循環証明体系の証明能力以上である. 一方で提案体系と [2] との比較は自明ではない. ここでは [2] の証明体系の証明から提案体系の証明への変換を与えることで提案体系が [2] の証明体系以上の証明能力を持つことを示す. [2] の証明体系が対象とする論理式は提案体系が対象とする論理式のサブセットであり, 具体的には提案体系の対象とする論理式の構文から $\kappa_1 < \kappa_2$, $\forall\kappa.\phi$, $\exists\kappa.\phi$, $\mu^{\kappa} X(\widetilde{x}).\ \phi$ を抜いた構文である. [2] の証明体系の規則を図 4 に示す. ここで C^{+}, C^{-} はそれぞれ hole が正, 負の位置に出現する文脈を表し, p は $\lambda\widetilde{x}.\ \psi$ の形の述語を表すメタ変数である. $WF(p)$ は p が整礎関係を表す述語であることを意味する.

補題 3. $X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \psi_2$ かつ p_2 が値の列上の整礎関係であるとき, $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee \psi_2)(\widetilde{x})$ の循環証明が存在する.

証明. $X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \psi_2$ の導出についての帰納法による.

- Fp-ApxBase の場合,
  - $\models_{th} p_1(\widetilde{x}) \wedge \psi_1 \Rightarrow \psi_2$

  Valid より $p_1(\widetilde{x}), \psi_1 \vdash_{\mathcal{O}} \psi_2$ の循環証明図が存

n が自然数ならば n は偶数もしくは奇数であることの証明

$$\dfrac{\dfrac{}{\kappa' < \kappa, x = 0 \vdash_{\kappa,\kappa'} x = 0, \cdots}\ \textsc{Valid} \quad \dfrac{\dfrac{N^{\kappa}(x) \vdash_{\kappa} EO(x,\mathrm{true}), EO(x,\mathrm{false})^{\dagger}}{\kappa < \kappa'', N^{\kappa}(x) \vdash_{\kappa'',\kappa} x+1 = 0, EO(x,\mathrm{false}), EO(x,\mathrm{true})}\ \textsc{Weak}}{\kappa' < \kappa, N^{\kappa'}(x-1) \vdash_{\kappa,\kappa'} x = 0, EO(x-1,\mathrm{false}), EO(x-1,\mathrm{true})}\ \textsc{Subst}}{\kappa' < \kappa, x = 0 \vee N^{\kappa'}(x-1) \vdash_{\kappa,\kappa'} x = 0, EO(x-1,\mathrm{false}), EO(x-1,\mathrm{true})}\ \vee\text{-L}$$

$$\dfrac{\dfrac{\dfrac{\vdots \quad \text{(右辺の展開と分解, 弱化)}}{\kappa' < \kappa, x = 0 \vee N^{\kappa'}(x-1) \vdash_{\kappa,\kappa'} EO(x,\mathrm{true}), EO(x,\mathrm{false})}\ \mu^{\kappa}\text{-L}, \exists\kappa\text{-L}}{N^{\kappa}(x) \vdash_{\kappa} EO(x,\mathrm{true}), EO(x,\mathrm{false})}\ \mu_1\text{-L}, \exists\kappa\text{-L}}{N(x) \vdash EO(x,\mathrm{true}), EO(x,\mathrm{false})^{\dagger}}\ \vee\text{-R}$$

$$N \triangleq \mu X(x).\ x = 0 \vee X(x-1) \quad EO \triangleq \mu X(x,y).\ \left(\begin{array}{l} y \wedge (x = 0 \vee X(x-1,\mathrm{false})) \vee \\ \neg y \wedge X(x-1,\mathrm{true}) \end{array}\right)$$

$$N^{\kappa} \triangleq \mu^{\kappa} X(x).\ x = 0 \vee X(x-1) \quad EO^{\kappa} \triangleq \mu^{\kappa} X(x,y).\ \left(\begin{array}{l} y \wedge (x = 0 \vee X(x-1,\mathrm{false})) \vee \\ \neg y \wedge X(x-1,\mathrm{true}) \end{array}\right)$$

$EO(n,\mathrm{true})$ は n が偶数であること, $EO(n,\mathrm{false})$ は n が奇数であることを表す

Subst with $\{\ \kappa \to \kappa'', \kappa' \to \kappa, x \to x-1\ \}$

進行のため, $\kappa' < \kappa, N^{\kappa'}(x-1) \vdash_{\kappa,\kappa'} \kappa' < \kappa, x = 0, EO(x-1,\mathrm{false}), EO(x-1,\mathrm{true})$ の repeat を用いない証明が必要

そのような証明は Valid 規則によって得られる.

図 3　関係的仕様検証のための提案体系における循環証明の例

在する. よって以下の $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee \psi_2)(\widetilde{x})$ の循環証明が得られる.

$$\dfrac{\dfrac{\dfrac{p_1(\widetilde{x}), \psi_1 \vdash_{\mathcal{O}} \psi_2}{p_1(\widetilde{x}) \vdash_{\mathcal{O}} \neg\psi_1 \vee \psi_2}\ \vee\text{-R}, \neg\text{-R}}{p_1(\widetilde{x}) \vdash_{\mathcal{O}} [\mu X(\widetilde{x}).\ \neg\psi_1 \vee \psi_2 / X](\neg\psi_1 \vee \psi_2)}\ \textsc{Subst}}{p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee \psi_2)(\widetilde{x})}\ \mu_0\text{-R}$$

Subst with $\theta = \{X \to \mu X(\widetilde{x}).\ \neg\psi_1 \vee \psi_2\}$

- Fp-ApxRec の場合,
  - $\psi_2 = X(\widetilde{t})$
  - $\models_{th} p_1(\widetilde{x}) \wedge \psi_1 \Rightarrow p_1(\widetilde{t}) \wedge p_2(\widetilde{t}, \widetilde{x})$

  $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee X(\widetilde{t}))(\widetilde{x})$ の不動点を展開して整理すると $p_1(\widetilde{x}), \psi_1 \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee X(\widetilde{t}))(\widetilde{t})$ を得る. ここで Subst 規則と Weak を使って $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee X(\widetilde{t}))(\widetilde{x})$ を得る. よってここに repeat を結ぶことができる. この repeat が進行するための条件は $p_1(\widetilde{x}) \vdash_{\mathcal{O}} p_2(\widetilde{t}, \widetilde{x}), (\mu X(\widetilde{x}).\ \neg\psi_1 \vee X(\widetilde{t}))(\widetilde{t})$ の repeat のない証明が存在することであり, これは $\models_{th} p_1(\widetilde{x}) \wedge \psi_1 \Rightarrow p_1(\widetilde{t}) \wedge p_2(\widetilde{t}, \widetilde{x})$ から得られる.

- Fp-Apx∧ の場合

  証明は容易.

- Fp-Apx∨ の場合, $i = 1, 2$ について
  - $\psi_2 = \psi_1' \vee \psi_2'$
  - $\models_{th} (p_1(\widetilde{x}) \wedge \psi_1) \Rightarrow (\psi_1'' \vee \psi_2'')$
  - $fv(\psi_i'') \subseteq \{\widetilde{x}\}$
  - $X \notin fpv(\psi_i'')$
  - $X(\widetilde{x}); p_1; p_2; \psi_1 \wedge \psi_i'' \downarrow \psi_i'$

  帰納法の仮定より $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg(\psi_1 \wedge \psi_i'') \vee \psi_i')(\widetilde{x})$ の循環証明が存在する. ここから $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee \neg\psi_i'' \vee \psi_i')(\widetilde{x})$ の循環証明を得られる. これらと $\models_{th} (p_1(\widetilde{x}) \wedge \psi_1) \Rightarrow (\psi_1'' \vee \psi_2'')$ から Cut 規則を使って $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee (\psi_1' \vee \psi_2'))(\widetilde{x})$ の証明が得られる.

- Fp-Apx∀ の場合,

  証明は容易.

- Fp-Apx∃ の場合,
  - $\psi_2 = \exists x.\psi$
  - $\models_{th} (p_1(\widetilde{x}) \wedge \psi_1) \Rightarrow \exists x'.\psi'$

$$\frac{\models_{th} \psi}{\vdash_{fp} \psi}\ \textsc{Fp-Valid}$$

$$\frac{\models_{th} [(\lambda\widetilde{x}.\ \psi')/X]\psi \Rightarrow \psi' \quad \vdash_{fp} C^-[[\widetilde{t}/\widetilde{x}]\psi']}{\vdash_{fp} C^-[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]}\ \textsc{Fp-ApxOver} \qquad \frac{X(\widetilde{x}); p_1; p_2; \top \downarrow nnf(\psi) \quad \vdash_{fp} C^+[p_1(\widetilde{t})] \quad \models WF(p_2)}{\vdash_{fp} C^+[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]}\ \textsc{Fp-ApxUnder}$$

$$\frac{\models_{th} p_1(\widetilde{x}) \wedge \psi_1 \Rightarrow \psi_2}{X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \psi_2}\ \textsc{Fp-ApxBase} \qquad \frac{\models_{th} p_1(\widetilde{x}) \wedge \psi_1 \Rightarrow p_1(\widetilde{t}) \wedge p_2(\widetilde{t}, \widetilde{x})}{X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow X(\widetilde{t})}\ \textsc{Fp-ApxRec}$$

$$\frac{X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \psi_1' \quad X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \psi_2'}{X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \psi_1' \wedge \psi_2'}\ \textsc{Fp-Apx}\wedge \qquad \frac{\models_{th} (p_1(\widetilde{x}) \wedge \psi_1) \Rightarrow (\psi_1'' \vee \psi_2'') \quad fv(\psi_i'') \subseteq \{\widetilde{x}\} \quad X \notin fpv(\psi_i'') \quad X(\widetilde{x}); p_1; p_2; \psi_1 \wedge \psi_i'' \downarrow \psi_i' \quad (i = 1, 2)}{X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \psi_1' \vee \psi_2'}\ \textsc{Fp-Apx}\vee$$

$$\frac{X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow [x'/x]\psi \quad x' \notin fv(\psi_1) \cup fv(\psi) \cup \{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)}{X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \forall x.\psi}\ \textsc{Fp-Apx}\forall \qquad \frac{\models_{th} (p_1(\widetilde{x}) \wedge \psi_1) \Rightarrow \exists x'.\psi' \quad fv(\psi') \subseteq \{\widetilde{x}, x'\} \quad X \notin fpv(\psi') \quad X(\widetilde{x}); p_1; p_2; \psi_1 \wedge \psi' \downarrow [x'/x]\psi \quad x' \notin fv(\psi_1) \cup fv(\psi) \cup \{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)}{X(\widetilde{x}); p_1; p_2; \psi_1 \downarrow \exists x.\psi}\ \textsc{Fp-Apx}\exists$$

図 4　既存の証明体系 [2] の規則

- $fv(\psi') \subseteq \{\widetilde{x}, x'\}$
- $X \notin fpv(\psi')$
- $X(\widetilde{x}); p_1; p_2; \psi_1 \wedge \psi' \downarrow [x'/x]\psi$
- $x' \notin fv(\psi_1) \cup fv(\psi)\{\widetilde{x}\} \cup fv(p_1) \cup fv(p_2)$

帰納法の仮定より $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg(\psi_1 \wedge \psi') \vee [x'/x]\psi)(\widetilde{x})$ の循環証明が存在する．ここから $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee \neg\psi' \vee [x'/x]\psi)(\widetilde{x})$ の循環証明を得る．これらと $fv(\psi') \subseteq \{\widetilde{x}, x'\}$, $\models_{th} (p_1(\widetilde{x}) \wedge \psi_1) \Rightarrow \exists x'.\psi'$ から Cut 規則によって $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee (\psi_1' \vee \psi_2'))(\widetilde{x})$ の証明が得られる．$p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \neg\psi_1 \vee \exists x.\psi)(\widetilde{x})$ の循環証明を得る．

□

補題 4. $\vdash_{\mathcal{O}} nnf(\phi)$ の循環証明が存在するなら $\vdash_{\mathcal{O}} \phi$ の循環証明が存在する．ただし $nnf(\phi)$ は ϕ の否定標準形である．

定理 8. $\vdash_{fp} \phi$ ならば $\vdash_{\mathcal{O}} \phi$ の循環証明が存在する．

証明. $\vdash_{fp} \phi$ の導出についての帰納法による．

- Fp-Valid の場合,
  - ϕ は不動点を含まない
  - $\models_{th} \phi$

  $\models_{th} \top \Rightarrow \phi$ であるから Valid 規則より $\top \vdash_{\mathcal{O}} \phi$ の循環証明が存在する．よって $\vdash_{\mathcal{O}} \phi$ の循環証明が存在する．
- Fp-ApxOver の場合,
  - $\phi = C^-[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]$
  - $\models_{th} [\lambda\widetilde{x}.\ \psi'/X]\psi \Rightarrow \psi'$
  - $\vdash_{fp} C^-[[\widetilde{t}/\widetilde{x}]\psi']$

  帰納法の仮定より, $\vdash_{\mathcal{O}} C^-[[\widetilde{t}/\widetilde{x}]\psi']$ の循環証明が存在する．また, $\models [\lambda\widetilde{x}.\ \psi'/X]\psi \Rightarrow \psi'$ は不動点を含んでいないので Fp-Valid 規則の場合と同様に $[\lambda\widetilde{x}.\ \psi'/X]\psi \vdash_{\mathcal{O}} \psi'$ の循環証明が存在する．$\vdash_{\mathcal{O}} C^-[[\widetilde{t}/\widetilde{x}]\psi']$ の証明で前提部に出現する $[\widetilde{t}/\widetilde{x}]\psi'$ が存在しない場合，証明の $[\widetilde{t}/\widetilde{x}]\psi'$ を $(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})$ に置き換えるだけで求める証明が得られる．そうではない場合, $\Gamma, [\widetilde{t}/\widetilde{x}]\psi' \vdash_{\mathcal{O}} \Delta$ の証明が与えられたもとで $\Gamma, (\mu X(\widetilde{x}).\ \psi)(\widetilde{t}) \vdash_{\mathcal{O}} \Delta$ の証明を作ることができればそれによって求める証明を得られる．

  $\models_{th} [\lambda\widetilde{x}.\ \psi'/X]\psi \Rightarrow \psi'$ から $[\lambda\widetilde{x}.\ \psi'/X, \widetilde{t}/\widetilde{x}]\psi \vdash_{\mathcal{O}} [\widetilde{t}/\widetilde{x}]\psi'$ の循環証明が得られる．これと Cut 規

則を使って欲しい証明 $\Gamma, (\mu X(\widetilde{x}).\ \psi)(\widetilde{t}) \vdash_{\mathcal{O}} \Delta$ は $\Gamma, (\mu X(\widetilde{x}).\ \psi)(\widetilde{t}) \vdash_{\mathcal{O}} [\lambda\widetilde{x}.\ \psi'/X, \widetilde{t}/\widetilde{x}]\psi, \Delta$ と $\Gamma \vdash_{\mathcal{O}} [\lambda\widetilde{x}.\ \psi'/X, \widetilde{t}/\widetilde{x}]\psi', \Delta$ に分けられる．後者はすでに得られた証明であり，前者は $(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})$ に対して μ_1-L を使ったときに得られる順序数変数について進行する repeat によって証明を作ることができる．よって求める証明は得られた．

- Fp-ApxUnder の場合，
  - $\phi = C^+[(\mu X(\widetilde{x}).\ \psi)(\widetilde{t})]$
  - $X(\widetilde{x}); p_1; p_2; \top \downarrow nnf(\psi)$
  - $\vdash_{fp} C^+[p_1(\widetilde{t})]$
  - $\models WF(p_2)$

  帰納法の仮定より $\vdash_{\mathcal{O}} C^+[p_1(\widetilde{t})]$ の循環証明が存在する．Fp-ApxOver の場合と同様の議論により $\Gamma \vdash_{\mathcal{O}} p_1(\widetilde{t}), \Delta$ の証明が与えられたうえで $\Gamma \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \psi)(\widetilde{t}), \Delta$ の循環証明が存在すればよい．Cut 規則を使うことで $\Gamma \vdash_{\mathcal{O}} p_1(\widetilde{t})$ と $\Gamma, p_1(\widetilde{t}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \psi)(\widetilde{t}), \Delta$ の循環証明が存在すればよい．前者は $\vdash_{\mathcal{O}} p_1(\widetilde{t})$ の証明から作ることができ，後者は補題 3 と補題 4 により得られる $p_1(\widetilde{x}) \vdash_{\mathcal{O}} (\mu X(\widetilde{x}).\ \psi)(\widetilde{x})$ の循環証明から作ることができる．よって求める証明は得られた．

□

6 おわりに

6.1 まとめ

本論文では状態遷移系の安全性・停止性・非安全性・非停止性検証問題，ラベル付き状態遷移系のトレース等価性検証問題，制約付きホーン節制約解消問題といったプログラム検証問題が一階不動点論理の妥当性判定問題に帰着されることを示した．さらに妥当性判定のための新しい証明体系を提案した．提案体系は最小・最大不動点の過小・過大近似に基づいたアプローチ [2] と帰納的・余帰納的定理証明に基づいたアプローチ [3] の利点を組み合わせたものであり，背景理論のソルバの恩恵を最大限得られるように，[3] で提案された体系を整礎帰納法で拡張している．また，証明探索の自動化のため，整礎帰納法で用いる整礎関係の発見にプログラム検証分野で提案されているランキング関数合成法を応用可能なように体系が設計されている．本論文ではさらに，提案体系の健全性を示し，既存の証明体系 [3] の証明から提案体系の証明への変換手法を与えることで提案体系が既存の証明体系以上の証明能力を持っていることを示した．さらに提案体系の有用性を示すため，重要なプログラム検証問題から帰着された，既存体系では解くのが困難な一階不動点論理の妥当性判定問題が提案体系で解ける場合があることを例を用いて示した．

6.2 今後の課題

本論文では既存体系の証明から提案体系の証明への変換を示したが，逆に提案体系の証明から既存体系の証明木の変換がどのような背景理論のもとで存在するのかまたは存在しないのかは分かっていない．これは両証明体系の証明能力の違いを論じる上で重要だが自明な問題ではない．

本論文では整礎帰納法に基づいた推論の自動化に背景理論のソルバやランキング関数合成法が応用可能であることを指摘したが，プログラム検証の技術は他にも，Cut 規則，∀-R 規則，∃-L 規則で前提部に新たに生じる論理式や項の探索，Subst 規則の代入の発見，スコーレム化による量化子の除去にも有用であると考えられる．このような循環証明とプログラム検証技術のより深い融合による高度な証明探索の自動化は興味深い研究課題である．

参 考 文 献

[1] Grebenshchikov, S., Lopes, N. P., Popeea, C., and Rybalchenko, A.: Synthesizing Software Verifiers from Proof Rules, *PLDI '12*, ACM, 2012, pp. 405–416.

[2] Nanjo, Y., Unno, H., Koskinen, E., and Terauchi, T.: A Fixpoint Logic and Dependent Effects for Temporal Property Verification, *LICS '18*, ACM, 2018, pp. 759–768.

[3] Sprenger, C. and Dam, M.: On the Structure of Inductive Reasoning: Circular and Tree-Shaped Proofs in the μCalculus, *FoSSaCS '03*, Springer, 2003, pp. 425–440.

[4] Unno, H., Torii, S., and Sakamoto, H.: Automating Induction for Solving Horn Clauses, *CAV '17*, Springer, 2017, pp. 571–591.