一階様相 μ 計算

First-order Modal Mu-Calculus

岡本 圭史 †
Keishi OKAMOTO

†(独) 産業技術総合研究所 システム検証研究センター
Research Center for Verification and Semantics, AIST
keishi-okamoto@aist.go.jp

本論文では，モデル検査の検査式としても利用されている命題様相 μ 計算を拡張した，一階様相 μ 計算を定義し，不完全性などの性質を示す．また応用例として，相互排除を一階様相 μ 計算の論理式で記述する．

1 はじめに

命題様相 μ 計算 (Propositional Modal μ-calculus) [3] は命題様相論理に不動点演算子を加えて得られる論理であり，モデル検査の検査式など，様々な場面で利用されている．例えば，ふたつのプロセス間の相互排除などは，命題様相 μ 計算の式として記述可能である．しかし，同じ相互排除でも，プロセスが動的に生成・消滅する場合のプロセス間の相互排除などは，命題様相 μ 計算の式では記述できない．(詳細は 3 章参照)

本論文では，これらの性質を記述するために，命題様相 μ 計算の一階への拡張である**一階様相 μ 計算** (First-order Modal μ-calculus) を構成し、不完全性を含むいくつかの性質示す．また応用例として，プロセスが動的に生成・消滅する場合のプロセス間の相互排除を一階様相 μ 計算の論理式で記述し，その有用性を示す．

2 文法

命題様相 μ 計算の一階への拡張は，同時に一階様相論理 (First-order Modal Logic) [2] の拡張でもあるので，一般的には一階様相 μ 計算の言語は定数記号を含むべきである．しかし，定数記号や関数記号を含む一階様相論理は完全でないことが多いので，今回は述語記号のみを含むよう定義する．

また一階様相 μ 計算は，命題に関する変数を持つ命題様相 μ 計算と対象に関する変数を持つ一階様相論理の両方の性質を持つので，それら二種類の変数記号を同時に持つよう定義する．

定義 2.1 (記号) 一階様相 μ 計算は定数記号として，述語記号 $P, Q, \cdots$ を持つ．さらに変数記号として，可算無限個の**対象変数記号** $(x, y, \cdots)$ と，可算無限個の**命題変数記号** $(X, Y, \cdots)$ を持つ。

対象変数記号全体の集合を $\mathcal{V}_o$，命題変数記号全体の集合を $\mathcal{V}_p$ と書くことにする．また，$\mathcal{V}_o \cap \mathcal{V}_p = \emptyset$ であると仮定し，$\mathcal{V}_o \cup \mathcal{V}_p$ を $\mathcal{V}$ と単に書く．

命題様相 μ 計算は束縛記号 μ, ν を持ち，一階様相論理は束縛記号 $\forall, \exists$ を持つ．したがって一階様相 μ 計算では，これらの束縛記号が同時に現れることを許すよう，以下のように論理式を定義する．

定義 2.2 (論理式) 一階様相 μ 計算の論理式を以下のように定義する．

1. P が n 変数述語記号かつ $x_1, , \cdots, x_n \in \mathcal{V}_o$ ならば，$P(x_1, \cdots, x_n)$ は論理式
2. X が命題変数ならば， X は論理式
3. φ, ψ が論理式ならば、$\neg\varphi, \varphi \vee \psi, \Box\varphi$ は論理式
4. $x \in \mathcal{V}_o$ かつ φ が論理式ならば、$\forall x.\varphi$ は論理式
5. $X \in \mathcal{V}_p$, φ は論理式かつ X の φ での全ての出現が肯定的 (*positive*) ならば，$\mu X.\varphi$ は論理式

$\wedge, \supset, \exists, \Diamond, \nu$ は上の定義を使って通常通り定義される．

3 相互排除

前章で定義した論理式を用いると、いくつかの重要な性質を記述できる．ここでは，動的に生成・消滅するプロセス間の相互排除を記述する．この問題を一階様相 μ 計算で定式化するために，対象変数 $x, y, \cdots$ はプロセスを，フレーム (S, R) は状態遷移を，領域 D は将来に渡って生成されるプロセス全体を表すとする．

注意 3.1 このような相互排除を命題様相 μ 計算の論理式で記述する場合は，将来に渡って生成されるプロセス全体が予め分かっている必要がある．しかし，一階様相 μ 計算の場合は，D がどのような集合であるかは予め分からなくてもよい．

この問題に関する様々な性質を一階様相 μ 計算の論理式として記述するために，以下の定数記号を導入する．

- 一変数述語記号 E ($E(x)$ はプロセス x がその状態で存在することを表す)
- 一変数述語記号 CS ($CS(x)$ はプロセス x が危険領域 (critical section) を実行中であることを表す),
- 一変数述語記号 Ent ($Ent(x)$ は x が危険領域の実行を要求していることを表す),
- 一変数述語記号 Run ($Run(x)$ は x が次に実行されることを表す).

これらの定数記号を用いると，プロセスが動的に生成・消滅する場合のプロセス間の相互排除は，次の論理式で表される．

$$\nu X.\neg(\exists y.\exists z.(y \neq z \wedge CS(y) \wedge CS(z))) \wedge \Box X$$

論理式の意味は次章で定義するが，命題様相 μ 計算や一階様相論理の意味論から，この論理式の意味が目的としている性質:

「異なるふたつのプロセス y と z で，同時に危険領域を実行中であるような y と z が存在する」ということは決して起こらない

を表していることが類推される．(実際に一階様相 μ 計算の意味の定義でもそのような意味を持つ)

例題 3.2 相互排除以外の性質の記述例を以下に示す．

1. $\forall x.E(x) \supset (\nu Y.(\mu Z.Run(x) \vee \Diamond Z) \wedge \Box Y)$ (*fairness*)
2. $\forall x.E(x) \supset \nu Y.(Ent(x) \supset (\mu Z.CS(x) \vee \Diamond Z)) \wedge \Box Y$ (*non blocking*)

4 意味論

この章では意味論，すなわち一階様相 μ 計算のモデルとモデルにおける論理式の真偽を定義する．一階様相 μ 計算のモデルは，命題様相 μ 計算のモデルである遷移系 (S, R) と，一階様相論理の対象領域 D のふたつのデータを含む必要があるので，以下のように定義する．

定義 4.1 (フレーム) S を空でない集合，R を S 上の二項関係とするとき，(S, R) を一階様相 μ 計算の**フレーム** (*frame*) と呼ぶ．また D を空でない集合とするとき，(S, R, D) を**拡張フレーム** (*augmented frame*) と呼び，D を (S, R, D) の**領域** (*domain*) と呼ぶ．

拡張フレームとその上の解釈が決まれば，一階様相論理のときと同様に，モデルが定義できる．

定義 4.2 (解釈) (S, R, D) を拡張フレーム，$\mathcal{C}$ を定数記号全体の集合とする．$\mathcal{C} \times S$ から D 上の述語への写像 I で，P が n 変数述語記号かつ $s \in S$ のとき，$I(P, s)$ が D 上の n 変数述語であるようなものを (S, R, D) 上の**解釈** (*interpretation*) と呼ぶ．

定義 4.3 (モデル) (S, R, D) を拡張フレーム，I をその上の解釈とするとき，四つ組み (S, R, D, I) を一階様相 μ 計算の**モデル** (*model*) と呼ぶ．このとき，(S, R, D, I) は**拡張フレーム** (S, R, D) **に基づく**という．

モデルにおける論理式の真偽を定義するには，論理式に意味を与えればよいので，命題様相 μ 計算の論理式に意味を与える関数を拡張したものを考える．そのために，自由変数の意味を決める付値を定義する．

定義 4.4 (付値) $M = (S, R, D, I)$ はモデルとする．変数全体の集合 $\mathcal{V}$ から集合 $D \cup \mathcal{P}(S)$ への写像 v で

$$v(x) = \begin{cases} D \text{ のある要素 } d, & (x \in \mathcal{V}_o \text{のとき}) \\ S \text{ のある部分集合 } T, & (x \in \mathcal{V}_p \text{のとき}) \end{cases}$$

上の条件をみたすものを M における**付値** (*valuation*) と呼ぶ．

モデル M が明らかか，あるいは重要でないときは，M の付値と呼ばず，単に付値と呼ぶことにする．また理解を助けるために，次のような表記を用いる．

v を付値，x を対象変数記号，d を D の要素とするとき，付値 $v[d/x]$ を次のように決める．

$$v[d/x](y) = \begin{cases} d, & y = x \text{ のとき} \\ v(y), & y \neq x \text{ のとき} \end{cases}$$

また X を命題変数記号，T を S の部分集合とするとき，付値 $v[T/X]$ を次のように決める．

$$v[T/X](Y) = \begin{cases} T, & Y = X \text{ のとき} \\ v(Y), & Y \neq X \text{ のとき} \end{cases}$$

命題様相 μ 計算同様，論理式 φ の意味は φ が成り立つ S の要素 (状態) s 全体の集合とする．さらに，一階様相 μ 計算のモデルは S の要素に依存せず領域 D の定まっている固定領域モデルなので，対象変数の動く範囲が常に D であることに注意して，束縛記号を含む論理式の意味を以下のように定義する．

定義 4.5 (意味関数) $M = (S, R, D, I)$ をモデル，v を M 上の付値とする．このとき，論理式全体の集合から $\mathcal{P}(S)$ への写像 $[\![-]\!]_v^M$ を次のように定義する．

1. $[\![P(x_1, \cdots, x_n)]\!]_v^M = \{s \mid (v(x_1), \cdots, x(x_n)) \in I(P, s)\}$ ただし P は n 変数述語記号かつ $x_1, \cdots, x_n \in \mathcal{V}_o$ とする，
2. $[\![X]\!]_v^M = v(X)$ ただし $X \in \mathcal{V}_p$ とする，
3. $[\![\neg\varphi]\!]_v^M = S \setminus [\![\varphi]\!]_v^M$，
4. $[\![\varphi \wedge \psi]\!]_v^M = [\![\varphi]\!]_v^M \cap [\![\psi]\!]_v^M$，
5. $[\![\forall x.\varphi]\!]_v^M = \bigcap_{d \in D} [\![\varphi]\!]_{v[d/x]}^M$，
6. $[\![\Box\varphi]\!]_v^M = \{s \mid$ 任意の t に対し，$R(s,t)$ が成り立つならば $t \in [\![\varphi]\!]_v^M\}$，
7. $[\![\mu X.\varphi]\!]_v^M = \bigcap\{T \subseteq S | [\![\varphi]\!]_{v[T/X]}^M \subseteq T\}$.

$[\![\varphi]\!]_v^M$ のことを論理式 φ の (M, v における) **意味**と呼ぶ．なお，文脈から M が明らかな場合は，単に $[\![\varphi]\!]_v$ と書く．

定義 4.6 (真偽と恒真) φ は論理式とする．$M = (S, R, D, I)$ をモデル，v を付値，$s \in S$ とする．$s \in [\![\varphi]\!]_v^M$ のとき，$M, s \models_v \varphi$ と書き，φ は s で v について**真** (*true*) であるという．また M における任意の付値 v と S 任意の要素 s に対し $M, s \models_v \varphi$ となるとき，φ は**モデル** M **で恒真**であるという．さらに，任意のモデル M に対し φ が M で恒真となるとき，φ は**恒真** (*valid*) であるという．

5 形式的体系

一階様相 μ 計算の形式的体系は，以下に示す，ふたつの公理と 12 の推論規則から構成される．

5.1 公理

- $\forall x.\Box\varphi \supset \Box\forall x.\varphi$ (φ は論理式)
- $\Diamond\exists x.\varphi \supset \exists x.\Diamond\varphi \supset$ (φ は論理式)

5.2 推論規則

$$\frac{\varphi}{\varphi \vee \psi}\ \vee I1 \qquad \frac{\psi}{\varphi \vee \psi}\ \vee I2$$

$$\frac{\varphi \vee \psi \quad \begin{array}{c}[\varphi] \\ \vdots \\ \theta\end{array} \quad \begin{array}{c}[\psi] \\ \vdots \\ \theta\end{array}}{\theta}\ \vee E$$

$$\frac{\begin{array}{c}[\varphi] \\ \vdots \\ \bot\end{array}}{\neg\varphi}\ \neg I \qquad \frac{\varphi \quad \neg\varphi}{\bot}\ \neg E$$

$$\frac{\varphi[a/x]}{\forall x.\varphi}\ \forall I \qquad \frac{\forall x.\varphi}{\varphi[a/x]}\ \forall E$$

推論規則 $\forall I$ の中で，対象変数記号 a は $\varphi[a/x]$ の証明のいかなる仮定にも自由に現れないとする．

$$\frac{\begin{array}{c}[\neg\varphi] \\ \vdots \\ \bot\end{array}}{\varphi}\ \text{RAA}$$

$$\frac{\varphi}{\Box\varphi}\ \Box I \qquad \frac{\Box(\varphi \supset \psi) \quad \Box\varphi}{\Box\psi}\ \supset \Box E$$

推論規則 $\Box I$ の中で，φ はいかなる仮定も持たないとする．

$$\frac{\varphi[(\mu X.\varphi)/X]}{\mu X.\varphi}\ \mu I \qquad \frac{\mu X.\varphi \qquad \begin{array}{c}[\varphi[\psi/X]] \\ \vdots \\ \psi\end{array}}{\psi}\ \mu E$$

推論規則 μE の中で，ψ は $\varphi[\psi/X]$ 以外の仮定を持たないとする．

以上が一階様相μ計算の公理と推論規則である．これらの公理と推論規則と，4 章で与えた意味論の間には次の関係が成り立つ．

定理 5.1 一階様相μ計算は健全 (*sound*)．すなわち，証明可能な論理式は恒真である．

6 不完全性

この章では，一階様相μ計算が完全でないこと，すなわち証明可能でない恒真式が存在することを示す．論理が完全でないことを示す方法はいくつかあるが，ここでは，[4] と同様に，恒真な論理式の全体が帰納的枚挙可能 (recursively enumerable) でないことを示す方法を用いる．まずは，次の注意を行なう．

注意 6.1 一階様相μ計算で証明可能な論理式の全体は帰納的枚挙可能 .

次に一階様相μ計算の充足問題が Σ^1_1-完全であること，したがって帰納的枚挙可能でないことを，Σ^1_1-完全であることが知られている $\omega\times\omega$ 循環タイル貼り問題 (recurrent tiling problem) を用いて示す．タイル貼り問題に関しては [1] などに詳しく解説されているので，ここでは簡単な説明にとどめる．

四辺に色が付いた，上下左右が決められている 1×1 の正方形のことを**タイル**と呼び，上下左右の色が同じタイルたち全体を**タイル型**と呼ぶ．上下左右が決められているので，タイルとタイル型に対し，それぞれ上下左右の辺の色を返す関数 up, down, left, right が用意されているとする．この定義の基で，次の問題を $\omega\times\omega$ 循環タイル貼り問題と呼ぶことにする．

定義 6.2 ($\omega\times\omega$ 循環タイル貼り問題) $\mathcal{T}$ はタイル型の有限集合で，特別なタイル型 t_0 を含むとする．$\mathcal{T}$ を使った $\omega\times\omega$ の正方形に対するタイルの貼り方で，隣り合うタイルが共有する辺は同じ色を持ち，かつ t_0 が第一列に無限回現れるようなタイルの貼り方は存在するか？

$\omega\times\omega$ の正方形に対するタイルの貼り方は，各格子点にタイルを貼ると考えれば，格子点 (x,y) からタイル型 t_i への関数と考えることができる．すると上の問題は,「関数 $f\colon \omega\times\omega\to\mathcal{T}$ で，$\{n\in\omega\colon f(0,n)=t_0\}$ が無限集合になるものが存在するか？」と言い換えることができる．

このような関数の存在と充足可能性が同値になる一階様相μ計算の論理式 φ を構成できれば，一階様相μ計算の充足問題が Σ^1_1-完全であることが示される．ここでは $\omega\times\omega$ 循環タイル貼りそのものを一階様相μ計算の論理式で記述することを目指し，それを φ とする．

6.1 $\omega\times\omega$ 循環タイル貼りの記述

M を自然数，$\mathcal{T}$ を有限個のタイル型 $t_0,t_1,\ldots,t_M$ からなる集合とする．このとき φ は，以下の論理式たちの論理積として表される．

- $\omega\times\omega$ の格子点を表す論理式 φ_{grid}
- $\mathcal{T}$ を使った $\omega\times\omega$ の格子点へのタイル貼りを表す論理式 $\varphi_{\mathcal{T}}$,
- タイル型 t_0 が第一列に無限回現れることを表す論理式 φ_{rec}

このような論理式たちを構成するために，(隣り合う要素であることを表す) 二変数述語記号 N と，タイル型 t_i 毎に一変数述語記号 $T_i(0\le i\le M)$ を用意する．

φ_{grid} は以下の論理式を論理積で結んだものとする．ただし論理式 $\mathrm{fst}(x)$ は，$\neg\exists y.N(y,x)$ の略記.

1. $\nu X.\Diamond(x=x)\wedge\Box X$,
2. $(\exists!x.\mathrm{fst}(x))\wedge(\forall x.\exists!y.N(x,y))\wedge(\forall y.\neg\mathrm{fst}(y)\supset\exists!x.N(x,y))$
3. $\forall x,y((N(x,y)\supset\nu Y.N(x,y)\wedge\Box Y)\wedge(\neg N(x,y)\supset\nu Z.\neg N(x,y)\wedge\Box Z))$

あるモデル $M=(S,R,D,I),M$ 上の付値 v と $s\in S$ で，$M,s\models_v\varphi_{grid}$ が成り立っているとする．このとき 1. により，(S,R) において，s から到達可能な状態 s' に対し，$R(s',s'')$ となる s'' が常に存在する．また 2. により，D は N に関して離散的に並んでいて，かつ左隣を持たない唯一の要素，すなわち最初の要素を持つ．さらに 3. により，s から到達可能な状態において，N による関係は保存される．したがって $M,s\models_v\varphi_{grid}$ が成り立つならば，(S,R) の中の s から始まる状態遷移のすべて無限列の中に，D の中の N により隣り合う要素達の無限列が存在して，下図のような格子点を構成する．

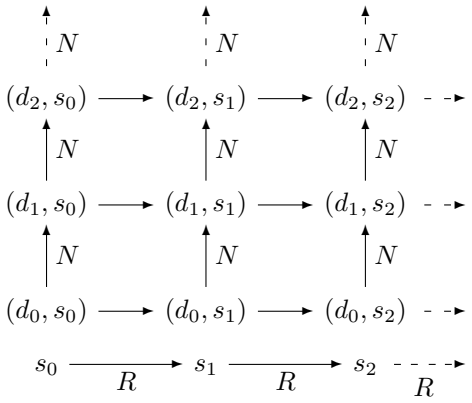

図 1: R と N による格子

$\varphi_{\mathcal{T}}$ は以下の論理式を論理積で結んだものとする．

1. $\nu X.(\forall x. \bigvee\{T_i(x) \mid 0 \le i \le M\}) \wedge \Box X$,
2. $\nu X.(\forall x. \bigwedge\{T_i(x) \supset \neg T_j(x) \mid 0 \le i, j \le M \text{ and } j \ne i\}) \wedge \Box X$,
3. $\nu X.(\forall x. \forall y. N(x,y) \wedge T_i(x) \supset \bigvee\{T_j(y) \mid \mathrm{up}(t_i) = \mathrm{down}(t_j)\}) \wedge \Box X \ (0 \le i \le M)$,
4. $\nu X.(\forall x. T_i(x) \supset \Box \bigvee\{T_j(x) \mid \mathrm{right}(t_i) = \mathrm{left}(t_j)\}) \wedge \Box X \ (0 \le i \le M)$,

あるモデル $M = (S, R, D, I), M$ 上の付値 v と $s \in S$ で，$M, s \models_v \varphi_{\mathcal{T}}$ が成り立っているとする．このとき 1. により，すべての D の要素は，いずれかのタイル型 t_i $(0 \le i \le M)$ であり，2. により同時にふたつ以上のタイル型であることはない．また 3. により，上下に隣り合うタイルが共有する辺は同じ色である．さらに 4. により，左右に隣り合うタイルが共有する辺も同じ色である．

φ_{rec} は $\forall x[\mathrm{fst}(x) \supset \nu X.(\mu Y.T_0(x) \vee \Diamond Y) \wedge \Box X]$ とする．

あるモデル $M = (S, R, D, I), M$ 上の付値 v と $s \in S$ で，$M, s \models_v \varphi_{grid} \wedge \varphi_{rec}$ が成り立っているとする．φ_{rec} の定義から，D の中の N による最初の要素は，タイル型 t_0 を無限回持つ．さらに φ_{grid} の 2. より，D の中の N による最初の要素は必ず存在する．

以上の議論から，あるモデル $M = (S, R, D, I), M$ 上の付値 v と $s_0 \in S$ で $M, s_0 \models_v \varphi$ が成り立つとき，格子を構成するような S の中の s_0 から始まる列 $S' = \{s_i \mid R(s_i, s_{i+1}), i \in \omega\}$ と D の中の列 $D' = \{d_j \mid N(d_j, d_{j+1}), j \in \omega\}$ で，S' の無限個の要素に対し $T_0(d_0)$ が成り立つ，すなわち d_0 がタイル型 t_0 を持つようなものが存在する．このとき，$\mathcal{T}$ を使った $\omega \times \omega$ 循環タイルの貼り方 $f\colon D' \times S' \to \mathcal{T}$ は次のように定義される．

$$f(d', s') = t_i \iff d' \in I(T_i, s')$$

以上の準備から，次の補題と定理が導かれる．

補題 6.3 次の二つは同値

1. φ は充足可能
2. $\mathcal{T}$ を使った $\omega \times \omega$ 循環タイルの貼り方が存在する

証明. $(2 \Rightarrow 1)$ $\{n \in \omega\colon f(0,n) = t_0\}$ が無限集合となるようなタイルの貼り方 $f\colon \omega \times \omega \to \mathcal{T}$ が存在すると仮定する．このとき，一階様相 μ 計算のモデル (ω, R, ω, I) で，明らかに φ が成立する．ただし

- $R = \{(s, s+1) \mid s \in \omega\}$,
- 各 $0 \le i \le M$ と $s \in \omega$ に対し $I(T_i, s) = \{d \in \omega \mid f(s,d) = t_i\}$,
- 各 $s \in \omega$ に対し $I(N, s) = \{(d, d+1) \mid d \in \omega\}$

$(1 \Rightarrow 2)$ φ の定義の解説より明らか． □

定理 6.4 一階様相 μ 計算で恒真な論理式全体は帰納的枚挙可能ではない．したがって，一階様相 μ 計算は完全ではない．

証明. 補題 6.3 から，恒真な論理式全体が帰納的枚挙可能でないことが導かれる．したがって，注意 6.1 から，一階様相 μ 計算は完全ではない． □

参考文献

[1] P.Blackburn, M.de Rijke and Y.Venema, *Modal Logic*, Cambridge Tracts in Theoretical Computer Science 53

[2] G.E.Hughes and M.J.Cresswell, *A new introduction to Modal Logic*, Routledge 1996

[3] D.Kozen, *Results on the Propositional μ-calculus*, Theoretical Computer Science 27 (1983) 333-354

[4] Frank Wolter, *First order common knowledge logics*, Studia Logica 65, 2000, 249-271