数理解析研究所講究録
927 巻 1995 年 56-65

命題様相論理の充足可能性問題の計算量について

名古屋工業大学大学院工学研究科　松岡 聡　(Matsuoka, Satoshi)

1 序

様相論理の充足可能性問題の計算量の研究は R.E. Ladner [6] により始められた。 [6] では **S4** の充足可能性問題の計算量 (以下では論理と計算量のクラスが結びつけられる場合は "充足可能性問題の計算量" という言葉は省略される) が **PSPACE**-complete, **S5** が **NP**-complete であることが証明されている。
本稿では、Ladner の手法を改良した Halpern と Moses の手法 [3] を用いて **S4.2** が **PSPACE**-complete であることを証明する。また、 様相論理が **NP**-complete であるための十分条件を提示する。
本稿は次のように構成される。2 節では計算量のクラスの定義を行う。3 節では様相論理が **NP**-complete であるための十分条件を提示する。4 節では **S4.2** が **PSPACE**-complete であることを示す。

2 計算量のクラス

チューリングマシンの定義や計算量のクラスの定義は基本的には [8] にしたがう。

Definition 1 (決定性) チューリングマシンは 4 つ組 $M = (K, \Sigma, \delta, s)$ である。ここで K は状態の有限集合であり, s は $s \in K$ であり、初期状態と呼ばれる。Σ は記号の有限集合である。そして $K \cap \Sigma = \emptyset$ を満たしている。また、Σ はそれぞれブランク、初期記号とよばれる記号 $\sqcup$, $\triangleright$ をふくんでいる。さらにδ は $K \times \Sigma$ から $(K \cup \{\text{"yes"}, \text{"no"}\}) \times \Sigma \times \{\rightarrow, \leftarrow, -\}$ への関数となっていなければならない。そして、δ は$\delta(q, \triangleright) = (p, q, D)$ ならば $\rho = \triangleright$ かつ $D = \rightarrow$ をみたしていなければならない。

"yes" と "no" は informal には、それぞれ受理状態、拒否状態を表す。同じように $\rightarrow$, $\leftarrow$ それに $-$ はそれぞれチューリングマシンのヘッドの左方向、右方向それに一時停止の動作を表している。
δ に対して$\delta(q, \triangleright) = (p, q, D)$ ならば $\rho = \triangleright$ かつ $D = \rightarrow$ であることを、満たすという条件はチューリングマシンの動作は、入力はかならず $\triangleright$ で始まる Σ^* の要素とし、チューリングマシンのヘッドは最初に $\triangleright$ をみていて、状態は初期状態 s で始められると定義されるためで、δ をこのように定義する目的は $\triangleright$ の左側へはチューリングマシンのヘッドがいかないような定義したいということである。

また、δ の出力の 3 番目が $\rightarrow$ で、ヘッドが移動した場所に記号が存在していない場合は次の δ によるチューリングマシンの状態の遷移ではヘッドは $\sqcup$ をみているという状態で遷移がおこる。テープの記号の並びの右端に $\sqcup$ が継ぎ足されるということになる。チューリングマシンの動作の定義は次のように時点表示 (configuration) という概念を用いて定義される。

Definition 2 configuration は 3 つ組 (q, w, u) である。ここで $q \in (K \cup \{\text{“yes''}, \text{“no''}\})$ かつ $w, u \in \Sigma^*$ である。

Definition 3 configuration (q, w, u) が (q', w', u') へ one-step 遷移 ($(q, w, u) \xrightarrow{M} (q', w', u')$ であらわされる) されるとは次の条件を満すことをいう:
σ を w の最後の記号とし、$\delta(q, \sigma) = (p, \rho, D)$ であると仮定する。このとき $q' = p$ でなければならない。D は $\rightarrow, \leftarrow, -$ のいずれかであるが、$D = \rightarrow$ ならば、w' は、w に一番最後記号の σ を ρ で置き換えをほどこした $\in \Sigma^*$ で、u' は u に最初の記号の削除をほどこした $\in \Sigma^*$ である。$D = \leftarrow$ ならば、w' は w から最後の記号 σ を取り去った $\in \Sigma^*$ で、u' は u の最初に ρ を付け加えた $\in \Sigma^*$ である。$D = -$ ならば w' は w の最後の記号のσ を ρ で置き換えた $\in \Sigma^*$ で、$u' = u$ である。

決定性チューリングマシンでは、 configuration (q, w, u) からの one-step の遷移は存在しないか必ず 1 つだけ存在するかである。
configuration の k-step の遷移$\xrightarrow{M^k}$ や、reflexive transitive closure $\xrightarrow{M^*}$ も通常のように定義される。

Definition 4 (非決定性) チューリングマシンは 4 つ組 $N = (K, \Sigma, \delta, s)$ である。$N = (K, \Sigma, \delta, s)$ についての条件はδ が関数ではなく$\delta \subseteq (K \times \Sigma) \times (K \cup \{\text{“yes''}, \text{“no''}\}) \times \Sigma \times \{\rightarrow, \leftarrow, -\}$ という関係であることを除き、あとは決定性チューリングマシンと同様である。

非決定性チューリングマシンの場合にも configuration が決定性の場合と同様に定義される。違いは configuration (q, w, u) からの one-step 遷移は存在するか複数個存在するということである。しかし無限個存在するわけではなくある定数 $k \geq 0$ が存在し、任意の configuration (q, w, u) からの one-step 遷移の個数は k で押えられることに注意。

k-tape 決定性チューリングマシンは決定性チューリングマシンの δ を$\delta \colon K \times \Sigma^k \rightarrow (K \cup \{\text{“yes''}, \text{“no''}\}) \times (\Sigma \times \{\rightarrow, \leftarrow, -\})^k$ に変更することで定義される。k-tape 非決定性チューリングマシンも同様に定義される。この場合の configuration は $(q, w_1, u_1, \ldots, w_k, u_k)$ (ここで $q \in K \cup \{\text{“yes''}, \text{“no''}\}$ かつ $w_1, u_1, \ldots, w_k, u_k \in \Sigma^*$) と変更される。

Definition 5 f を $\mathbf{N}$ から $\mathbf{N}$ への関数とする。チューリングマシン M が operating within time $f(n)$ であるとは、任意の input x に対して M が $f(|x|)$ 以内に停止すること、すなわち、configuration (s, x, ε) から $f(n)$ ステップ以内に $(\text{“yes''}, w, u)$ か $(\text{“no''}, w, u)$ かの configuration への遷移が存澆垢襪海箸鬚い A

$L \in \mathbf{TIME}(f(n))$ であることは、ある $k > 1$ があり operating within time $f(n)$ である k-tape 決定性チューリングマシン M が存在し M が $L \subseteq \Sigma^*$ を受理することと定義する。
$L \in \mathbf{NTIME}(f(n))$ も非決定性チューリングマシンに変更して同じように定義される。

Definition 6 チューリングマシン M とこれに対する入力 x に対して
$(s, \triangleright, x, \triangleright, \varepsilon, \ldots, \triangleright, \varepsilon) \stackrel{M^*}{\to} (H, w_1, u_1, w_2, u_2, \ldots, w_k, u_k)$ (ただし $H \ni \{$"yes", "no"$\}$) であるとする。このとき space required by M on input x は$\sum_{i=1}^{k} |w_i u_i|$ であると定義される。f を $\mathbf{N}$ から $\mathbf{N}$ への関数とすると、チューリングマシン M が operating withing space bound $f(n)$ であるとは任意の入力 x に対し、 space required by M on input x が $f(|x|)$ で押えられることをいう。
$L \in \mathbf{SPACE}(f(n))$ であることは、ある $k > 1$ があり operating within space bound $f(n)$ である k-tape 決定性チューリングマシン M が存在し M が $L \subseteq \Sigma^*$ を受理することと定義する。
$L \in \mathbf{NSPACE}(f(n))$ も非決定性チューリングマシンに変更して同じように定義される。

よく知られている計算量のクラスは次のように定義される。
Definition 7

$$\mathbf{P} \stackrel{\mathrm{def}}{\equiv} \bigcup_{j>0} \mathbf{TIME}(n^j)$$

$$\mathbf{NP} \stackrel{\mathrm{def}}{\equiv} \bigcup_{j>0} \mathbf{NTIME}(n^j)$$

$$\mathbf{PSPACE} \stackrel{\mathrm{def}}{\equiv} \bigcup_{j>0} \mathbf{SPACE}(n^j)$$

$$\mathbf{NPSPACE} \stackrel{\mathrm{def}}{\equiv} \bigcup_{j>0} \mathbf{NSPACE}(n^j)$$

$$\mathbf{EXP} \stackrel{\mathrm{def}}{\equiv} \bigcup_{j>0} \mathbf{TIME}(2^{n^j})$$

また **NP**-complete や **PSPACE**-complete などの計算量のクラスは次のように定義される。

Definition 8 言語 L_1 が L_2 へ (p-time) reducible であるとは、ある Σ^* から Σ^* への関数 R で決定性チューリングマシンで $\mathbf{TIME}(n^i)$ for some i で computable なものが存在し、すべての入力 x に対して

$$x \in L_1 \text{ iff } R(x) \in L_2.$$

が成立することをいう。
$\mathcal{C}$ を計算量のクラス, $L \in \mathcal{C}$ としたとき L が $\mathcal{C}$-complete であるとは、任意の $L' \in \mathcal{C}$ が L へ (p-time) reducible であることである。

3 NP-completeness であるための十分条件

様相論理の基本的な用語は [2] にしたがう。
Φ を可算個の命題変数集まり、$Fma(\Phi)$ を$\perp, \to, \Box$ を用いて通常のように Φ から生成される論理式とする。$Sf(A)$ を論理式 A の部分論理式の集まりとする。$|A|$ で A を構成する際に使用された記号の数 (記号は $\Phi \cup \{\perp, \to, (,), \Box\}$ の要素) をあらわす。

Proposition 1 論理式 A の部分論理式の個数を $\|Sf(A)\|$ であらわすと $\|Sf(A)\| \leq |A|$

証明 A の構成に関する帰納法による。□

クリプキフレームは通常のように空でない集合 M と M 上の 2 項関係 R の対 (M, R) である。**S4** や **S5** などのよく知られている命題様相論理は R に関してある性質 (R が transitive であるとか reflexive であるとか) が成り立つクリプキフレームのクラスに関して健全かつ完全になることはよく知られている。さらに、 filtration method を用いて、M を有限集合に制限したクリプキフレームのクラスに関して健全かつ完全になることを示すことができることもよく知られている。filtration method を用いれば、よく知られた様相論理 (**S4** や **S5** など) では、与えられた論理式 A が充足可能かどうか調べるのに $2^{|A|}$ 個以下の可能世界の個数をもつクリプキフレームについてのみの充足可能性を調べればよいことがわかる。
ここで示すことは、与えられた論理式 A の充足可能性を R がある first order formula で記述され、M が $p(|A|)$ 個以下 (p はある多項式) であるようなクリプキフレームのクラスに関する充足可能性に還元できるような論理は **NP** に属すことである。(normal な) 様相論理が古典論理の保守的拡大になっていることと古典論理の充足可能性問題が **NP** $-$ *complete* であることから **NP** に属する (normal な) 様相論理が **NP**-complete に属すことがわかる。
M の可能世界の個数を $\|M\|$ であらわすことにする。

Proposition 2 任意の c に対してある c' が存在し、任意の論理式 A に対して、
$\|M\| \leq |A|^c$ である (M, R) が述語として 2 項述語 $R, =$ のみをもつ first order ϕ で特徴づけられる性質 P_ϕ をもつかどうかという問題は $\mathbf{TIME}(|A|^{c'})$ に属す。

証明 ϕ の構成に関する帰納法による。
原子論理式の場合は xRy か $x = y$ の形であるが、すべての $x, y \in M$ について xRy や $x = y$ が成り立つかどうか調べるためにはせいぜい $|A|^{2c}$ 回 xRy や $x = y$ が成り立つかどうかの判定をすればよいので $c' := 2c$ として問題が $\mathbf{TIME}(|A|^{c'})$ に属すことがわかる。
ϕ が $\neg\psi, \psi_1 \wedge \psi_2, \psi_1 \vee \psi_2, \psi_1 \to \psi_2$ などの場合は帰納法の仮定を用いれば明らか。
ϕ が $\forall x.\psi$ の場合は ψ が成り立つかどうかの判定がそのまま $\forall x.\psi$ が成り立つかどうかの判定となる。
ϕ が $\exists x.\psi$ の場合は $\exists x.$ ということは $\exists x \in M.$ ということで、$\|M\| \leq |A|^c$ が成り立っているので $\exists x.\psi$ が成り立つかどうかという問題はψ が成り立つかどうかという問題と同じクラスに属すことがわかる。□

(M,R) が与えられたとき (M,R) 上の付値 V は Φ から 2^M への関数である。V が与えられたとき M の要素と論理式の間の 2 項関係 $\models$ は通常のように定義される。$(M,R,\models)$ のことをクリプキモデルという。

Proposition 3 ある論理式 A と $(M,R,\models)$ が与えられたとき $(M,R,V)\models_a A$ が成り立つような $a\in M$ があるかどうかという問題は $\mathbf{TIME}(\|M\|^3\cdot|A|)$ に属する。

証明 (M,R,V) から論理式 A の部分論理式と任意の M の可能世界との 2 項関係 $\models$ を $\mathbf{TIME}(\|M\|^2\cdot|A|)$ で判定できれば命題が証明できることは明らか。
$B\in Sf(A)$ と $s\in M$ があたえられたとき $\models_s B$ であるかどうかを $\mathbf{TIME}(\|M\|^2\cdot|B|)$ で判定できることを論理式の複雑さに関する帰納法で証明する。$B:=\Box C$ の場合のみが問題となる。sRt が成り立つ t について $\models_t C$ を調べればよいわけだが、これは $\mathcal{O}((\|M\|^2\cdot|C|)\times\|M\|^2)$ かかるわけでなく、$\mathcal{O}((\|M\|^2\cdot|C|)+\|M\|^2)$ で判定できることに注意。$|C|+1=|B|$ なので $\models_s B$ が成り立つかどうかという問題は $\mathbf{TIME}(\|M\|^2\cdot|B|)$ に属す。□

Theorem 1 normal modal logic L が次の条件をみたすならば、L の充足可能性問題は **NP**-complete である：ある $c>0$ が存在して、

$$
\begin{array}{lll}
\nvdash_L \neg A & \Leftrightarrow & \text{ある first-order formula で特徴づけられる} \\
 & & \text{クリプキモデルのクラス } \mathcal{F} \text{ に属する} \\
 & & \|M\|\le|A|^c \text{ である structure } (M,R,V) \text{ があり} \\
 & & \text{ある } a\in M \text{ で } (M,R,V)\models_a A \text{ が成り立つ。}
\end{array}
$$

証明 実際に $\Leftrightarrow$ の右の条件が成り立つかどうかを判定するための非決定性多項式時間限定チューリングマシンを構成してみればよい。
まず $|A|^c$ 個以下の可能世界をもつクリプキフレームを非決定的に列挙する。$|A|^c$ 個以下の可能世界をもつクリプキフレームの個数はせいぜい $|A|^c\cdot 2^{|A|^c\cdot|A|^c}$ 個以下でこれは $2^{|A|^{3\cdot c}}$ で押さえられるので、多項式時間で非決定的に列挙することは可能である。
列挙されたクリプキフレームの一つを (M,R) とする。論理式 A の (M,R) におけるとりうる可能な付値の個数はせいぜい $2^{\|M\|\cdot|Sf(A)|}$ 個であるが、$\|M\|\le|A|^c$ かつ $|Sf(A)|\le|A|$ よりこれは $2^{|A|^{c+1}}$ で押さえられるので、A と (M,R) についての可能な付値を列挙することは多項式時間で非決定的に可能である。
A と (M,R) についての列挙された付値を V とする。(M,R,V) は A に出現しない命題変数に関する付値を適当に決めておくことでクリプキモデルとみなせる。R が与えられた $\mathcal{F}$ を特徴づける first order formula の性質を満たすかどうかの判定は $\|M\|\le|A|^c$ より命題 2 より多項式時間で判定できる。そして同じように A が (M,R,V) で充足可能かどうか判定することも命題 3 より多項式時間で判定できる。
したがって以上のことから $\Leftrightarrow$ の右の条件が成り立つかどうかを判定するための非決定性多項式時間限定チューリングマシンが構成できることが示された。□

実際にこの条件を満たしている様相論理としては **S5** [6], **S4.3** [7], **K45, KD45** [3] などが知られている。これらのどれも与えられた論理式 A のこの論理での充足可能性問題を A の中の $\Box B$ という形の部分論理式の個数 $\leq Sub(A) \leq |A|$ の可能世界のクリプキモデルについての充足可能性に還元できる。また $|A|^k$ (k は任意の定数) 個以下の可能世界のクリプキモデルについての充足可能性問題に還元できる論理も知られている [1]。

4 S4.2 が PSPACE-complete であること

4.1 S4.2 が PSPACE-hard であること

S4.2 は **S4** に公理スキーマ $\Diamond\Box A \supset \Box\Diamond A$ を加えた体系である。canonical model の手法により

reflexive:	$\forall x.xRx.$
transitive:	$\forall x, y, z.(xRy \wedge yRz \rightarrow xRz).$
weakly directed:	$\forall x, y, z.(xRy \wedge xRz \rightarrow \exists w.(yRw \wedge zRw).$

で特徴づけられるクリプキフレームに関し健全かつ完全になっていることが示される。さらに generated frame の概念と filtration method を用いることにより reflexive, transitive かつ

directed: $\forall x, y.\exists z.(xRz \wedge yRz).$

で特徴づけられる有限クリプキフレームに関し **S4.2** が健全かつ完全になっていることが示される [5]。

ここでは [3] で **S4** に対して適用された手法を **S4.2** について適用することにより、**PSPACE**-hardness を示す。その方法は、**PSPACE**-complete であることが知られている2階の古典命題論理 **QBF** [4, 8] の論理式 A から様相論理式 $(A)^\circ$ への多項式時間変換 $()^\circ$ を定義し、

QBF $\models A \;\Leftrightarrow\;$ reflexive, transitive, directed で特徴づけられる有限クリプキフレームのクラス $\mathcal{F}$ の中のクリプキフレーム (M, R) が存在して $(M, R) \models (A)^\circ$.

を示すという方法である。

最初に、**QBF** formula $A = \mathcal{Q}_1 p_1 \ldots \mathcal{Q}_m p_m A'$ から $(A)^\circ$ を作る。$(A)^\circ$ に出現する命題変

数は $p_1,\ldots,p_m,d_0,\ldots,d_{m+1}$ に限られる。$(A)^\circ$ の部分論理式を定義する。

$$
\begin{aligned}
depth &\stackrel{\text{def}}{\equiv} \bigwedge_{i=1}^{m+1} (d_i \supset d_{i-1}).\\
determined &\stackrel{\text{def}}{\equiv} \bigwedge_{i=1}^{m} \quad (d_i \supset ((p_i \supset \Box(d_i \land \neg d_{m+1} \supset p_i))\\
&\qquad\qquad \land(\neg p_i \supset \Box(d_i \land \neg d_{m+1} \supset \neg p_i))).\\
branch_A &\stackrel{\text{def}}{\equiv} \bigwedge_{\{i|\mathcal{Q}_{i+1}=\forall\}} ((d_i \land \neg d_{i+1}) \supset \quad (\Diamond(d_{i+1} \land \neg d_{i+2} \land p_{i+1})\\
&\qquad\qquad \land\Diamond(d_{i+1} \land \neg d_{i+2} \land \neg p_{i+1})))\\
&\qquad \bigwedge_{\{i|\mathcal{Q}_{i+1}=\exists\}} ((d_i \land \neg d_{i+1}) \supset \quad (\Diamond(d_{i+1} \land \neg d_{i+2} \land p_{i+1})\\
&\qquad\qquad \lor\Diamond(d_{i+1} \land \neg d_{i+2} \land \neg p_{i+1}))).
\end{aligned}
$$

これらの部分論理式を用いて $(A)^\circ$ を次の論理式と定義する：

$$
d_0 \land \neg d_1 \land \Box(depth \land determined \land branching_A \land (d_m \land \neg d_{m+1} \supset A')).
$$

Theorem 2 任意の 2 階古典命題閉論理式 A に対し

$\mathbf{QBF} \models A \quad \Leftrightarrow \quad$ reflexive, transitive, directed で特徴づけられる
有限クリプキフレームのクラス $\mathcal{F}$
の中のクリプキフレーム (M,R) と
valuation V と $s \in M$ が存在して
$(M,R,V) \models_s (A)^\circ$.

証明 ($\Rightarrow$ の証明)
$A = \mathcal{Q}_1 p_1 \ldots \mathcal{Q}_m p_m A'$ とし、$\mathbf{QBF} \models A$ を仮定する。
枝分かれが 1 か 2 かである有限木の reflexive transitive closure (M,R) を考える。すなわち:
M は有限集合であり、R は

$$
\begin{aligned}
&\forall x \in M.xRx.\\
&\forall x,y,z \in M.(xRy \land yRz \to xRz).\\
&\forall x,y \in M.(xRy \land yRx \to x = y).\\
&\forall u,v \in \{y|yR^{-1}x\} \subseteq M.(uRv \lor vRu).
\end{aligned}
$$

さらに

$$
x\ succ\ y \stackrel{\text{def}}{\equiv} xRy \land \forall z \in M.((xRz \land y \neq z \land x \neq z) \to \not(zRy)) \land \not(yRx).
$$

と定義して

$$
x\ succ\ x1 \land x\ succ\ x2 \land x\ succ\ x3 \to (x1 = x2 \lor x2 = x3 \lor x3 = x2).
$$

を満たしているものとする。
さらに (M,R) から $a \notin M$ である a をとり、
$\forall x, y \in M \cup \{a\}.(xR'y \leftrightarrow xRy \vee y = a)$, $M' = M \cup \{a\}$ で定義される (M', R') は reflexive, transitive, directed で特徴づけられる有限クリプキフレームのクラス $\mathcal{F}$ に属している。このような (M', R') の中で (M,R) の高さが m であるものを考えるとこの中に M の root $r_0 \in M$ で "$i \leq j$ ならば高さ j の可能世界で d_i を true に、$i \leq j$ で p_i が高さ i の可能世界で true ならば高さ j でも p_i が true, $i \leq j$ で p_i が高さ i の可能世界で false ならば高さ j でも p_i が false" を満たすような valuation V が存在して

$$(M', R', V) \models_{r_0} (A)^\circ$$

となるような (M', R') が存在する。
なぜなら $\mathbf{QBF} \models \mathcal{Q}_1 p1 \ldots \mathcal{Q}_m p_m A'$ なので $\mathcal{Q}_1 p_1 \ldots \mathcal{Q}_m p_m . A'$ を

- $\forall p_i . B(p_i)$ ならば $B[p_i/\text{true}]/\ B[p_i/\text{false}]$.
- $\exists p_i . B(p_i)$ ならば
  $\mathbf{QBF} \models B[p_i/\text{true}]$ ならば $B[p_i/\text{true}]$,
  $\mathbf{QBF} \models B[p_i/\text{false}]$ ならば $B[p_i/\text{false}]$.

と展開する。
$p_i, \ldots, p_m$ の (古典論理の) valuation の集まりを
$Val = \{\rho_i | i \leq 2^m, \rho_i \colon \{p_1, \ldots, p_m\} \to \{\text{true}, \text{false}\}\}$ と書くと、ある $Val_0 \subseteq Val$ が存在して展開された論理式は$\bigwedge_{\rho \in Val_0} A'\rho$ と書ける。そしてそれぞれの $A'\rho$ は正しいブール式になっている。p_i が $\forall$ ならば高さ $i-1$ の可能世界から高さ i の可能世界への枝分かれは 2 つ、p_i が $\exists$ ならば高さ $i-1$ の可能世界から高さ i の可能世界への枝分かれは 1 つというような (M,R) を選び、高さ m の可能世界での $p_1, \ldots, p_m$ の valuation が $\rho \in Val_0$ を満たすような valuation V を選んでやれば (M', R', V') が root r_0 で

$$(M', R', V) \models_{r_0} (A)^\circ$$

となることは簡単に確かめられる。
($\Leftarrow$ の証明)
reflexive, transitive, directed で特徴づけられる有限クリプキフレームのクラス $\mathcal{F}$ の中のクリプキフレーム (M,R) と valuation V と $r_0 \in M$ が存在して $(M,R,V) \models_{r_0} (A)^\circ$ となっていると仮定する。t を任意の $t \in M$ とする。A^t_j を $\mathcal{Q}_{j+1} p_{j+1} \ldots \mathcal{Q}_m p_m . A'$ から $i < j$ であるすべての p_i に対して $p_i \in V(t)$ ならば $p_i = \text{true}$ と $p_i \notin V(t)$ ならば $p_i = \text{false}$ と置き換えてできる QBF の論理式とする。$A^t_0 = A$ であり、 A^t_m は A' に可能世界 t での valuation にしたがい $p_1, \ldots, p_m$ に関するある (古典論理の) valuation ρ をほどこした $A'\rho$ であることに注意。$(M,R,V) \models_{r_0} \Box(d_m \supset A')$ が成立っているので、 $r_0 Rt$ かつ $(M,R,V) \models_t d_m$ ならば A^t_m は true である。
j についての簡単な帰納法により、 $r_0 Rt$ かつ $(M,R,V) \models_t d_{m-j} \wedge \neg d_{m-j+1}$ ならば $\mathbf{QBF}$ A^t_{m-j} が true であることを示すことができる。$(M,R,V) \models_{r_0} d_0 \wedge \neg d_1$ なので $A^s_0 = A$ は true であることがいえたことになる。□

Theorem 3 **S4.2** の充足可能性問題は **PSPACE**-hard である。

4.2 S4.2 が PSPACE に入ること

Theorem 4 **S4.2** の充足可能性問題は **PSPACE** に属す。

証明 [10] の Theorem 4.4. の一部である、
任意の論理式 A に対して

$$\mathbf{S4.2} \vdash A \Leftrightarrow \mathbf{S4} \vdash \bigwedge_{\Box B \in Sf(A)} (\Diamond\Box B \supset \Box\Diamond\Box B) \supset A.$$

を用いる。$\|Sf(A)\| \leq |A|$ なので A から$\bigwedge_{\Box B \in Sf(A)}(\Diamond\Box B \supset \Box\Diamond\Box B) \supset A$ への変換は線形時間で可能である。そして **S4** が **PSPACE**-complete であることから **S4.2** が bf PSPACE に属すことがわかる。□

定理 3 と定理 4 より

Theorem 5 **S4.2** の充足可能性問題は **PSPACE**-complete である。

5 謝辞

本研究に際し、さまざまな助言をしていただいた日本大学の志村立矢さんに感謝します。

参考文献

[1] A.V. Chagrov and M. V. Zakharyashchev. An essay in complexity aspects of intermediate calculi. Proceedings of the Fourth Asian Logic Conferences, 1990.

[2] R. Goldblatt. Logic for Time and Computation. Second edition. Center for the Study of Languages and Information, 1992

[3] J.Y. Halpern and Y.Moses. A guide to completeness and complexity for modal logics of knowledge and belief. *Artificial Intelligence*, 54:319–379, 1992.

[4] J.E. Hopcroft and J.D. Ullman. Introduction to Automata Theory, Languages and Computation. Addison-Wesley, 1979.

[5] G.E. Hughes and M.J. Cresswell. A Companion to Modal Logic. Methuen, 1984.

[6] R.E. Ladner. The computational complexity of provability in systems of modal propositional logic. *Siam. J. Comput.*, 6:467–480, 1977.

[7] H. Ono and A. Nakamura. On the size of refutation Kripke models for some linear modal and tense logics. *Studia Logica*, 39:325-333.

[8] C.H. Papadimitriou. Computational Complexity. Addison-Wesley, 1994.

[9] T. Shimura. Cut-free systems for the modal logic S4.3 and S4.3Grz. *Reports on Mathematical Logic*, 25:57–73, 1991.

[10] T. Shimura. Cut-free systems for some modal logics containing S4. *Reports on Mathematical Logic*, 26:39–65, 1992.

[11] R. Statman. Intuitionistic Propositional Logic is Polynomial-Space Complete. *Theoretical Computer Science*, 9:67-72, 1979.