逐次一貫性下の知識伝達を表す直観主義様相論理

平井 洋一 [1]

[1] 東京大学大学院 情報理工学系研究科コンピュータ科学専攻
yh@is.s.u-tokyo.ac.jp

概 要 Herlihy と Shavit は，wait-free 計算を単体的複体で幾何的に特徴づけた．この論文では，wait-free 計算を論理的に特徴づける．まず，非同期通信のための直観主義知識論理を与える．この論理の意味論は，Herlihy と Shavit が用いた単体的複体の分割の一般化である．次に，この直観主義知識論理の上に，Lamport が定義した共有メモリの逐次一貫性を特徴づける公理型を与える．最後に，逐次一貫性のもとで，wait-free 仕様と呼ぶある種の論理式と wait-free 計算のスケジュールが成すモデルとの間での健全性と完全性とを示す．おもしろいことに，逐次一貫性を特徴づける公理型は，Kripke フレームの擬線形性を特徴づける公理型 $(\varphi \supset \psi) \vee (\psi \supset \varphi)$ と類似している．この類似は，共有メモリの逐次一貫性も Kripke フレームの擬線形性も，スケジュールやモデルに，ある種の全順序性を求めることが似ていることによる．(LPAR-16 に類似の論文を投稿した．)

1 導入

Wait-free 計算を，できる限り単純な論理で特徴付けたい．Herlihy と Shavit による wait-free 計算の特徴づけは，共有メモリの逐次一貫性を暗黙のうちに前提にしているので，まずは逐次一貫性を特徴づける知識論理をつくりたい．なるべく単純な枠組みで特徴づけできるとよいので，既存研究をみてみる．

知識伝達を扱うための論理で，知識様相をもつものは，多数ある．[3–6, 10, 13, 17, 20, 21, 27]．直観主義様相論理も多数ある [1, 7, 19, 20, 22]．どちらの場合も，Kripke 意味論で考えると，論理が多数あるのは，状態間の二項関係二種類について，相互の制限を多種類考えられるからである．直観主義様相論理で二種類の二項関係とは，(a) 直観主義の意味論をつけるための順序と (b) どの状態で様相がどの状態を指すのかを表す二項関係のことである．知識伝達のための論理たちでは，二種類の二項関係とは，(a') どの状態がどの状態より時間的に先行するかを表す順序と (b') どの状態からどの状態に (どんな種類の) 知識伝達が起きたのかを表す二項関係のことである．

この状況を単純にするために，この論文では，状態空間上の二項関係に加えて，もうひとつの二項関係の代わりに状態空間上の関数を用いて意味論を記述できるような論理を考える．こうすることによって，論理を設計するさいの選択の余地が少なくなるために，状況が単純になる．選択の余地が少なくなるといえるのは，状態集合上のほとんどの二項関係は状態集合上の関数としては書き表せないけれども，逆に状態集合上の関数を二項関係とみなすことは，いつでもできるからである．さらに，順序 (a) と (a') を同一視し，二項関係 (b) と (b') とを同一視する．

逐次一貫性がスケジュールに対する制限であるのに対して，wait-free という概念は並列プログラムに対する制限である．並列プログラムの振舞いは，スケジュールによって左右される[1]．並列プログラムの正しさは，任意のスケジュールについて，正しい振舞いをするという形で定義できる．この定義の形は，論理式の恒真性の，任意のモデルによって充足されるという定義の形に類似しているので，スケジュールと並列プログラムとの対決は，論理式とモデルの対決に類似していると考える．第 3 節では，スケジュールの制限である逐次一貫性をモデルのクラスとして表現し，そのうえで第 3.5 小節で並列プログラムの制限である wait-free 性を，論理式のクラスとして表現する．

[1] このことにより並列プログラムのテストが極めて難しいことが，本研究のような形式的手法を導入する動機である．

$$\text{(axiom)}\ \frac{}{\varphi \vdash \varphi} \qquad \text{(weakening)}\ \frac{\Gamma \vdash \varphi}{\psi,\, \Gamma \vdash \varphi} \qquad \text{(contraction)}\ \frac{\varphi,\, \varphi,\, \Gamma \vdash \varphi'}{\varphi,\, \Gamma \vdash \varphi'}$$

$$\text{(exchange)}\ \frac{\Gamma, \varphi, \psi,\, \Gamma' \vdash \varphi'}{\Gamma,\, \psi, \varphi,\, \Gamma' \vdash \varphi'} \qquad (\wedge\text{-I})\ \frac{\Gamma \vdash \varphi \qquad \Gamma' \vdash \psi}{\Gamma, \Gamma' \vdash \varphi \wedge \psi} \qquad (\vee\text{-I}_0)\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}$$

$$(\vee\text{-I}_1)\ \frac{\Gamma \vdash \varphi}{\Gamma \vdash \psi \vee \varphi} \qquad (\wedge\text{-E}_0)\ \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi} \qquad (\wedge\text{-E}_1)\ \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}$$

$$(\vee\text{-E})\ \frac{\Gamma \vdash \psi_0 \vee \psi_1 \qquad \Gamma,\, \psi_0 \vdash \varphi \qquad \Gamma,\, \psi_1 \vdash \varphi}{\Gamma \vdash \varphi}$$

$$(\supset\text{-I})\ \frac{\varphi,\, \Gamma \vdash \psi}{\Gamma \vdash \varphi \supset \psi} \qquad (\supset\text{-E})\ \frac{\Gamma \vdash \psi_0 \supset \psi_1 \qquad \Gamma \vdash \psi_0}{\Gamma \vdash \psi_1} \qquad (\bot\text{-E})\ \frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}$$

$$\text{(T)}\ \frac{}{K_a\varphi \vdash \varphi}$$

$$\text{(introspection)}\ \frac{}{K_a\varphi \vdash K_aK_a\varphi} \qquad \text{(nec)}\ \frac{\Gamma \vdash \varphi}{K_a\Gamma \vdash K_a\varphi} \qquad (\vee K)\ \frac{}{K_a(\varphi \vee \psi) \vdash K_a\varphi \vee K_a\psi}$$

図 1. $\mathbf{K}\vee$ の推論規則たち

2　非同期通信のための直観主義知識論理

2.1　統語論

命題変項の集合 $PVar$ と，主体の集合 A とを固定する．メタ変項 $P, Q, \ldots$ は，命題変項を走ることとする．

定義 1 論理式 φ を *BNF* で定義する*:*

$$\varphi ::= \bot \mid P \mid (K_a\varphi) \mid (\varphi \vee \varphi) \mid (\varphi \wedge \varphi) \mid (\varphi \supset \varphi)$$

*(*ここで $a \in A$ とする*)*．論理式の集合を Fml と書く．

単項演算子は二項演算子よりも強く結び付く．曖昧にならないときには，括弧を省略することがある．論理式同士を $=$ で結んだら，統語論的な等しさを表すこととする．記法 $(\neg\varphi)$ は $(\varphi \supset \bot)$ の略記とする．論理式の列 $\Gamma = (\varphi_i)$ について，記法 $K_a\Gamma$ は列 $(K_a\varphi_i)$ の略記とする．命題変項と $\bot$ とをあわせて，原子論理式と呼ぶ．

定義 2 論理 $\mathbf{K}\vee$ の演繹体系を図 *1* により定義する．

論理式の集合 Γ と論理式 φ について，関係 $\Gamma \vdash \varphi$ が成り立つのは，Γ の元の有限列 Γ_0 があって，$\Gamma_0 \vdash \varphi$ が導出可能であるときである．

モデルと，モデルの中の状態を決めると，論理式が充足されるか否かが定まる．モデルとは，Kripke フレームに写像 f_a たちが，それぞれの主体 $a \in A$ について，追加されたものである．

写像が f_a 状態 w を状態 v に写すのはどういうときかというと，気分として[2]，実際の状態が w であるときに，主体 a は状態が v に達したことにしか気付いていないようなときである．

定義 3 モデル $\langle W, \preceq, (f_a)_{a\in A}, \rho\rangle$ とは，こういうものの組である*:*

[2] この説明が気分に過ぎないと述べるのは，我々は「実際の状態」を定義しようとしないからである．

1. $\langle W, \preceq \rangle$ は順序である．
2. 各 $f_a \colon W \to W$ は，任意の $w \in W$ について，
   (a) (減少性) $f_a(w) \preceq w$,
   (b) (巾等性) $f_a(f_a(w)) = f_a(w)$,
   (c) (単調性) $w \preceq v$ ならば $f_a(w) \preceq f_a(v)$
   を満たす関数である．
3. $\rho \colon PVar \to \mathcal{P}(W)$ は関数で，各 $\rho(P)$ が $\preceq$ に関して上のほうに閉じている, つまり， $w' \succeq w \in \rho(P)$ ならば $w' \in \rho(P)$ である．

先の気分の説明をふまえると，f_a たちに課された条件の気分を，このように説明できる:

- 減少性は，主体 a は真実しか認識しないことを表している．
- 巾等性は，主体 a がなにかを認識するならば，a はまた，a 自身がそのことを認識していることを認識するはずであるというとを表している．
- 単調性は，a はいちど認識したことを忘れないということを表している．

定義 4 充足関係 $\models$ を定義する．充足関係は，モデル $\langle W, \preceq, (f_a)_{a \in A}, \rho \rangle$ と，状態 $w \in W$ と，論理式 φ との関係である．モデルを固定しよう: $M = \langle W, \preceq, (f_a)_{a \in A}, \rho \rangle$． 関係 $\models$ の定義は，φ の構造に関して帰納的になされる:

($\varphi = \bot$ の場合) $M, w \models \bot$ はどうあれ成立しない．

($\varphi = P$ の場合) $M, w \models P$ が成立するのは，ただ $w \in \rho(P)$ なときである．

($\varphi = K_a\psi$ の場合) $M, w \models K_a\psi$ が成立するのは，ただ $M, f_a(w) \models \psi$ なときである．

($\varphi = \psi_0 \wedge \psi_1$ の場合) $M, w \models \psi_0 \wedge \psi_1$ が成立するのは，ただ $M, w \models \psi_0$ と $M, w \models \psi_1$ とが両方成立するときである．

($\varphi = \psi_0 \vee \psi_1$ の場合) $M, w \models \psi_0 \vee \psi_1$ が成立するのは, $M, w \models \psi_0$ か $M, w \models \psi_1$ の少なくとも片方が成立するときに限る．

($\varphi = \psi_0 \supset \psi_1$ の場合) $M, w \models \psi_0 \supset \psi_1$ が成立するのは，いかなる $w' \in W$ についても，$w' \succeq w$ と $M, w' \models \psi_0$ が $M, w' \models \psi_1$ を含意するときに限る．

定理 5 (Kripke 単調性) $M, w \models \varphi$ かつ $w \preceq v$ とすると，$M, v \models \varphi$ が成立する．

証明 主張に現れる φ の構成に関する帰納法で示せる．f_a の単調性を用いる． ∎

2.2 判断の意味論

定義 6 モデル M とそのモデルの状態 w と論理式の集合 Γ とについて，$M, w \models \Gamma$ と書くのは，Γ に属する任意の論理式 φ について $M, w \models \varphi$ が成立するときである．

定義 7 記法 $\Gamma \models \varphi$ は，論理式の列 Γ と論理式 φ の右の関係を表す: 任意のモデル M と任意の状態 $w \in M$ について，$M, w \models \Gamma$ ならば $M, w \models \varphi$ である．

2.3 健全性

定理 8 (健全性) $\Gamma \vdash \varphi$ は $\Gamma \models \varphi$ を含意する．

証明 健全性を，$\vdash$ の定義に関する帰納法で示す．

(introspection) f_a が巾等であることを用いる．

(nec) $\models$ の定義が，あらゆるモデルのあらゆる状態についての言明であることから，導ける．

($\vee K_a$) $\Gamma \models K_a(\varphi \vee \psi)$ を仮定する．任意のモデル M の 任意の状態 w について，$M, w \models \Gamma$ を仮定すると $M, w \models K_a(\varphi \vee \psi)$ である．$\models$ の定義から，$M, f_a(w) \models \varphi \vee \psi$ である．$\models$ の定義をもう一度使うと，$M, f_a(w) \models \varphi$ か $M, f_a(w) \models \psi$ の少くとも片方が成り立つ．つまり，$M, w \models K_a\varphi$ か $M, w \models K_a\psi$ の少なくとも片方が成り立つ．$\models$ の定義より，$M, w \models K_a\varphi \vee K_a\psi$ を示せた．

(他) 標準的な証明 [26, Th. 5.10] を使える． ∎

2.4 強い完全性

定義 9 論理式の集合 Γ が**飽和**しているのは，下記のすべてを満たすときである*:*

1. Γ が演繹について閉じている．つまり，$\Gamma \vdash \varphi \Rightarrow \varphi \in \Gamma$ である．
2. $\varphi \vee \psi \in \Gamma$ とすると，$\varphi \in \Gamma$ または $\psi \in \Gamma$ が成立する．
3. $\Gamma \nvdash \bot$ である．

補題 10 (飽和補題) 論理式の集合 Γ で $\Gamma \nvdash \varphi$ を満たすものに対して，論理式の飽和集合 Γ^ω で，$\Gamma^\omega \nvdash \varphi$ と $\Gamma \subseteq \Gamma^\omega$ を満たすものがある[3]．

証明 標準的な証明 [26, Lem. 6.3] をそのまま使える． ∎

定義 11 (正準モデルの候補) 組 $M^c = \langle W^c, \preceq^c, (f_a^c)_{a \in A}, \rho^c \rangle$ を定義する．

- W^c を，論理式の飽和集合たちの集合とする．
- $\Gamma \preceq^c \Delta$ を $\Gamma \subseteq \Delta$ で定義する．
- $f_a^c(\Gamma) = \{\varphi \in \mathrm{Fml} \mid K_a\varphi \in \Gamma\}$ と定義する．
- $\rho^c(P) = \{\Gamma \in W^c \mid P \in \Gamma\}$ とする．

補題 12 (正準モデル) 組 $M^c = \langle W^c, \preceq^c, (f_a^c)_{a \in A}, \rho^c \rangle$ はモデルである．

証明 まず，f_a^{c} が実際に関数 $W^{\mathrm{c}} \to W^{\mathrm{c}}$ であることを確かめよう．仮定: $\Gamma \in W^{\mathrm{c}}$．主張: $f_a^{\mathrm{c}}(\Gamma)$ は論理式の飽和集合である．主張を示すために，飽和集合の定義の条件をいちいち確かめる．

1. $f_a^{\mathrm{c}}(\Gamma) \vdash \varphi$ を仮定する．規則 (introspection) があるので， $K_a(f_a^{\mathrm{c}}(\Gamma)) \vdash K_a\varphi$ である．このことに加えて，$K_a(f_a^{\mathrm{c}}(\Gamma)) \subseteq \Gamma$ であるから，関係 $\Gamma \vdash K_a\varphi$ が成立する．Γ は演繹に関して閉じているので，$K_a\varphi \in \Gamma$ である．f_a^{c} の定義から，$\varphi \in f_a^{\mathrm{c}}(\Gamma)$ である．
2. $\varphi \vee \psi \in f_a^{\mathrm{c}}(\Gamma)$ を仮定する．f_a^{c} の定義から，$K_a(\varphi \vee \psi) \in \Gamma$ である．規則 ($\vee K_a$) により，$K_a(\varphi \vee \psi) \vdash K_a\varphi \vee K_a\psi$ が成立する．Γ は演繹に関して閉じているから，$K_a\varphi \vee K_a\psi \in \Gamma$ である．Γ は飽和しているので，$K_a\varphi \in \Gamma$ または $K_a\psi \in \Gamma$ の少なくとも片方は成立する．f_a^{c} の定義から，$\varphi \in f_a^{\mathrm{c}}(\Gamma)$ か $\psi \in f_a^{\mathrm{c}}(\Gamma)$ の少なくとも片方は成立する．

[3] Saturation Lemma.

3. 矛盾を求めて，$f_a^{\mathrm{c}}(\Gamma) \vdash \bot$ を仮定する．$f_a^{\mathrm{c}}(\Gamma)$ は演繹に関して閉じているので，$\bot \in f_a^{\mathrm{c}}(\Gamma)$ である．f_a^{c} の定義から， $K_a\bot \in \Gamma$ である．規則 (T) によって，$\Gamma \vdash \bot$ である．Γ が飽和集合という仮定に反する．

次に，定義 3 の条件をいちいち確かめよう．

1. $\preceq^{\mathrm{c}}$ は順序である．なぜならば集合の包含関係 $\subseteq$ が順序だからである．
2. (a) 規則 (T) によって $f_a^{\mathrm{c}}(\Gamma) \preceq \Gamma$ である．
   (b) $f_a^{\mathrm{c}}(f_a^{\mathrm{c}}(\Gamma)) \subseteq f_a^{\mathrm{c}}(\Gamma)$ は，前項から明らかである．逆を示そう．$\varphi \in f_a^{\mathrm{c}}(\Gamma)$ を仮定する．f_a^{c} の定義から， $K_a\varphi \in \Gamma$ である．規則 (introspection) から，$\Gamma \vdash K_aK_a\varphi$ である．Γ は演繹に関して閉じているから，$K_aK_a\varphi \in \Gamma$ である．従って $\varphi \in f_a^{\mathrm{c}}(f_a^{\mathrm{c}}(\Gamma))$ である．
   (c) $\Gamma \preceq \Delta$ を仮定する．どの $K_a\varphi \in \Delta$ も，Γ にも入っている．従って， $f_a^{\mathrm{c}}(\Gamma) \preceq f_a^{\mathrm{c}}(\Delta)$ である．
3. $\Gamma' \succeq \Gamma \in \rho^{\mathrm{c}}(P)$ を仮定する．$P \in \Gamma$ である．よって $P \in \Gamma'$ である．従って $\Gamma' \in \rho^{\mathrm{c}}(P)$ である． ∎

補題 13 論理式の飽和集合 Γ と正準モデル M^c について，$\varphi \in \Gamma \Leftrightarrow M^c, \Gamma \vdash \varphi$ が成り立つ．

証明 φ の構成に関する帰納法で示す．

($\varphi = \bot$ の場合) 左右どちらも，決して成立しない．

($\varphi = P$ の場合) ρ^{c} の定義より，$\varphi \in \Gamma \Leftrightarrow \Gamma \in \rho(P) \Leftrightarrow M^{\mathrm{c}}, \Gamma \models P$ である．

($\varphi = \psi_0 \wedge \psi_1, \psi_0 \vee \psi_1$ の場合) 帰納法の仮定から直接示せる．

($\varphi = K_a\psi$ の場合) ($\Rightarrow$) $M^{\mathrm{c}}, \Gamma \models K_a\psi$ を仮定する．$\models$ の定義から，$M^{\mathrm{c}}, f_a^{\mathrm{c}}(\Gamma) \models \psi$ である．帰納法の仮定から，$\psi \in f_a^{\mathrm{c}}(\Gamma)$ である．f_a^{c} の定義から， $K_a\psi \in \Gamma$ である．
($\Leftarrow$) $K_a\psi \in \Gamma$ を仮定する．f_a^{c} の定義から，$\psi \in f_a^{\mathrm{c}}(\Gamma)$ である．帰納法の仮定から，$f_a^{\mathrm{c}}(\Gamma) \models \psi$ である．$\models$ の定義より，$\Gamma \models K_a\psi$ である．

($\varphi = \psi_0 \supset \psi_1$ の場合) ($\Rightarrow$) $M^{\mathrm{c}}, \Gamma \models \psi_0 \supset \psi_1$ を仮定する．矛盾を求めて，$\psi_0 \supset \psi_1 \notin \Gamma$ と仮定する．Γ は演繹に関して閉じているので，$\Gamma, \psi_0 \nvdash \psi_1$ である．補題 10 より，飽和集合 Γ' が存在して，$\Gamma' \supseteq \Gamma \cup \{\psi_0\}$ かつ $\Gamma' \nvdash \psi_1$ を満たす．帰納法の仮定から，$M^{\mathrm{c}}, \Gamma' \models \psi_0$ であるが，$M^{\mathrm{c}}, \Gamma' \models \psi_1$ ではない．$\Gamma' \succeq \Gamma$ であるから，これは $M^{\mathrm{c}}, \Gamma \models \psi_0 \supset \psi_1$ に矛盾する．
($\Leftarrow$) $\psi_0 \supset \psi_1 \in \Delta$ を仮定する．$\Delta' \succeq \Delta$ かつ $M^{\mathrm{c}}, \Delta' \models \psi_0$ である．$M^{\mathrm{c}}, \Delta' \models \psi_1$ を示せばよい．帰納法の仮定から，$\psi_0 \in \Delta'$ である．Δ' は演繹に関して閉じていて，かつ $\psi_0 \supset \psi_1 \in \Delta'$ なので，$\psi_1 \in \Delta'$ である．帰納法の仮定より， $M^{\mathrm{c}}, \Delta' \models \psi_1$ である．

これで補題を示せた． ∎

定理 14 (強い完全性) $\Gamma \models \varphi$ は $\Gamma \vdash \varphi$ を含意する．

証明 対偶を示す: $\Gamma \nvdash \varphi$ を仮定して，$\Gamma \not\models \varphi$ を示す．補題 10 より，論理式の飽和集合 Γ' が存在して $\Gamma' \nvdash \varphi$ と $\Gamma' \supseteq \Gamma$ を満たす．補題 13 より，$M^{\mathrm{c}}, \Gamma' \models \Gamma$ だが，$M^{\mathrm{c}}, \Gamma' \not\models \varphi$ である．これは $\Gamma \models \varphi$ に反する． ∎

3 逐次一貫性のための公理型

この節では，ある公理型で，逐次一貫性を特徴づける．逐次一貫性 [16] は，メモリの状態が時間的に全順序に並ぶことを要求する条件である．我々は $\mathbf{K}\vee$ に推論規則を追加することによって演繹体系 $\vdash_{SC}$ を定義して，逐次一貫性を表す．

3.1 逐次一貫モデル

逐次一貫性は，メモリの状態が時間的に全順序に並ぶことを要求する．直観主義知識論理のモデルでメモリの状態を特徴づけるには，状態 $w \in W$ のうち $f_{\mathsf{m}}(w) = w$ を満たすものを，w から見たメモリの状態が w 自身であることを根拠にして，メモリの状態とみなせばよい．このように定義したメモリの状態たちに制限した $\preceq$ が全順序であることを，逐次一貫モデルと呼ぶ．

定義 15 逐次一貫モデルとは，任意の状態 v と w とについて，$f_{\mathsf{m}}(v) = v$ と $f_{\mathsf{m}}(w) = w$ とが成り立つならば，$v \preceq w$ または $w \preceq v$ が成立するモデルである．

加えて技術的な理由から，擬逐次一貫モデルを定義する．擬逐次一貫モデルは，大雑把には，逐次一貫モデルをいくつか互いに無関係に並べて得られるようなモデルのことである．

定義 16 擬逐次一貫モデルとは，任意の状態 v と w と x とについて，$f_{\mathsf{m}}(v) = v$ と $f_{\mathsf{m}}(w) = w$ とが成り立ちかつ x が $x \preceq v$ と $x \preceq w$ とを満たすならば，$v \preceq w$ または $w \preceq v$ が成立するモデルである．

3.2 公理型の定義

SC を，右のような形をした論理式の集合とする: $(K_{\mathsf{m}}\varphi \supset K_{\mathsf{m}}\psi) \vee (K_{\mathsf{m}}\psi \supset K_{\mathsf{m}}\varphi)$.
$\mathbf{K}\vee$ の演繹体系に規則 (SC) を追加して，$\Gamma \vdash_{SC} \varphi$ を定義する． $\dfrac{}{\vdash \varphi}\ (\varphi \in SC)$ (SC)
集合 SC に属する任意の論理式は古典論理のトートロジーであるために，これらの論理式を古典論理に追加しても無意味であることに注意されたい．このことが，古典論理でなく直観主義論理を用いた利点である．

3.3 健全性

補題 17 $\vdash_{SC} \varphi \Rightarrow M \models \varphi$ が任意の逐次一貫モデル M について成り立つ．

証明 補題 8 を示すときに使った数学的帰納法に，規則 (SC) に関する条を追加すれば，証明できる．

(SC) 矛盾を求めて，$M, w \not\models (K_{\mathsf{m}}\varphi \supset K_{\mathsf{m}}\psi) \vee (K_{\mathsf{m}}\psi \supset K_{\mathsf{m}}\varphi)$ と仮定する．関係 $\models$ の定義によると，状態 $w_0, w_1 \succeq w$ があって，$M, w_0 \models K_{\mathsf{m}}\varphi$ と $M, w_1 \models K_{\mathsf{m}}\psi$ とを満たし，さらに $M, w_1 \not\models K_{\mathsf{m}}\psi$ と $M, w_0 \not\models K_{\mathsf{m}}\varphi$ とを満たす．これらと Kripke 単調性 (補題 5) は，M が逐次一貫モデルという仮定に矛盾する． ∎

3.4 強い完全性

まず，擬逐次一貫モデルに対する強い完全性を言ってから，逐次一貫モデルに対する強い完全性を言う．

定義 18 論理式の集合 Γ が SC-**飽和**であるとは，これらの条件をみたすことである*:*

1. Γ は演繹に関して閉じている，すなわち，$\Gamma \vdash_{\mathrm{SC}} \varphi \Rightarrow \varphi \in \Gamma$ を満たす．
2. $\varphi \vee \psi \in \Gamma$ ならば $\varphi \in \Gamma$ または $\psi \in \Gamma$ である．
3. $\Gamma \nvdash_{\mathrm{SC}} \bot$ である．

補題 19 (飽和補題) 論理式の集合 Γ で $\Gamma \nvdash_{\mathrm{SC}} \varphi$ を満たすものについて，論理式の SC-飽和な集合 Γ^ω で， $\Gamma^\omega \nvdash_{\mathrm{SC}} \varphi$ と $\Gamma \subset \Gamma^\omega$ とを満たすものがある．

証明 補題 10 の証明と同じで，ただ，$\vdash$ を $\vdash_{\mathrm{SC}}$ で置き換えればよい． ∎

定義 20 (擬逐次一貫な正準モデルの候補) 組 $M^{sc} = \langle W^{\mathrm{SC}}, \preceq^{\mathrm{SC}}, (f_a^{\mathrm{SC}})_{a\in A}, \rho^{\mathrm{SC}} \rangle$ を定義する．

- W^{sc} は論理式の SC-飽和集合たちの集合とする．
- $\Gamma \preceq^{sc} \Delta$ を $\Gamma \subset \Delta$ で定義する．
- $f_a^{sc}(\Gamma) = \{\varphi \mid K_a\varphi \in \Gamma\}$ とする．
- $\rho^{sc}(P) = \{\Gamma \mid P \in \Gamma\}$ とする．

補題 21 (擬逐次一貫な正準モデル) 組 $M^{sc} = \langle W^{\mathrm{SC}}, \preceq^{\mathrm{SC}}, (f_a^{\mathrm{SC}})_{a\in A}, \rho^{\mathrm{SC}}\rangle$ は擬逐次一貫モデルである．

証明 最初に，前と同じようにして，f_a^{SC} が実際に関数 $W^{\mathrm{SC}} \to W^{\mathrm{SC}}$ であることを確かめることができる．さらに，定義 3 のいちいちの条件を確かめるのも，前と同様にできて，M^{SC} がモデルであることがわかる．最後に，モデル M^{SC} が擬逐次一貫モデルであることを示す．Γ, Δ, Θ をモデル M^{SC} の状態とし，仮定 $\Theta \preceq^{\mathrm{SC}} \Delta$ と仮定 $\Theta \preceq^{\mathrm{SC}} \Delta$ と仮定 $f_{\mathsf{m}}^{\mathrm{SC}}(\Gamma) = \Gamma$ と仮定 $f_{\mathsf{m}}^{\mathrm{SC}}(\Delta) = \Delta$ をおく．$\Delta \preceq^{\mathrm{SC}} \Gamma$ か $\Gamma \preceq^{\mathrm{SC}} \Delta$ の少なくとも片方が成立すると主張する．矛盾を求めて，主張の否定を仮定する．関係 $\preceq^{\mathrm{SC}}$ が実際には集合の包含関係なので，論理式 φ と ψ が存在して，$\varphi \in \Gamma$ と $\varphi \notin \Delta$ と $\psi \in \Delta$ と $\psi \notin \Gamma$ とを満たす．$f_{\mathsf{m}}^{\mathrm{SC}}(\Gamma) = \Gamma$ であるので，$K_a\psi \notin \Gamma$ と $K_a\varphi \in \Gamma$ が成立する．同様に，$K_a\varphi \notin \Delta$ と $K_a\psi \in \Delta$ が成立する．集合 Θ は SC 飽和なので，$(K_a\varphi \supset K_a\psi) \vee (K_a\varphi \supset K_a\psi)$ は Θ の元である．飽和の定義によると，$K_a\varphi \supset K_a\psi \in \Theta$ か $K_a\psi \supset K_a\varphi \in \Theta$ の少なくとも片方が成立する．結果として，$K_a\varphi \supset K_a\psi \in \Gamma$ か $K_a\psi \supset K_a\varphi \in \Delta$ の少なくとも片方が成立する．それぞれの場合が，Γ も Δ も演繹に関して閉じていることから，矛盾に至る． ∎

補題 22 論理式の飽和集合 Γ と擬逐次一貫正準モデル M^{sc} について，$\varphi \in \Gamma \iff M^{sc}, \Gamma \vdash_{\mathrm{SC}} \varphi$ が成立する．

証明 補題 13 と同じである． ∎

補題 23 (擬逐次一貫モデルへの強い完全性) 任意の擬逐次一貫モデル M について $M \models \Gamma$ ならば $M \models \varphi$ とすると，$\Gamma \vdash_{\mathrm{SC}} \varphi$ である．

証明 対偶を示す．$\Gamma \nvdash_{\mathrm{SC}} \varphi$ を仮定して，擬逐次一貫モデル M が存在して $M \models \Gamma$ を満たすが $M \models \varphi$ は満たさないということを示す．補題 19 によって，SC 飽和な論理式の集合 Γ' で $\Gamma' \nvdash \varphi$ と $\Gamma' \supset \Gamma$ とを満たすものがある．補題 22 によって，$M^{\mathrm{SC}}, \Gamma' \models \Gamma$ であるけれども $M^{\mathrm{SC}}, \Gamma' \models \varphi$ ではない． ∎

定理 24 (逐次一貫モデルへの強い完全性) 任意の逐次一貫モデル M について $M \models \Gamma$ ならば $M \models \varphi$ とすると，$\Gamma \vdash_{\mathrm{SC}} \varphi$ である．

証明 対偶を示す．$\Gamma \nvdash_{\mathrm{SC}} \varphi$ を仮定すると，補題 23 によって擬逐次一貫モデル M と M の状態 w が存在して，$M, w \models \Gamma$ を満たすが $M, w \models \varphi$ を満たさない．ここで M の状態のうち，$\preceq$ に関して w 以下のある状態 v について，$\preceq$ に関して v 以上である状態だけを集めて制限すると，逐次一貫モデル $\bar{M}$ が得られ，$\bar{M}, w \models \Gamma$ は成立するが，$\bar{M}, w \models \varphi$ は成立しない． ∎

3.5 Wait-free 計算

スケジュールは，ステップをプロセスに割りふる．Wait-free な並列プログラムとは，ある定数 k が存在して，どのようなスケジュールのもとでも，参加するすべてのプロセスが k ステップ与えられる前に終了するような並列プログラムのことである．この条件の狙いは，プロセスが他のプロセスを待つことを禁止することである．仮にプロセス p がプロセス q が何かをするのを待つとすると，いじわるなスケジュールのもとで，wait-free の条件は破れてしまう．実際，最初からプロセス p に

連続して k ステップ与えてしまうようなスケジュールのもとで，最初の k ステップの間，プロセス q は何もできない一方で，プロセス p は k ステップの間プロセス q が何かをするのを polling して待ちつづけ，wait-free の条件に反してしまう．

並列プログラムは，完了するとどのプロセスからどのプロセスに信号が伝達されるか，保証する．プロセスからプロセスへの信号伝達を，論理式で表現することを考える．プロセスを主体とみなす．プロセス p が起動したことを表す命題記号を I_p と書く．論理式 $K_qK_pI_p$ を，「プロセス p が起動したことをプロセス p が知って，それをプロセス q に伝えた」と読める．同様に，論理式 $K_pK_qK_pI_p$ を「プロセス p が起動したことをプロセス p が知って，それをプロセス q に伝達したら，プロセス q がプロセス p に返事して伝達を受理したことを伝えた」と読める．このような信号伝達を実現する並列プログラムを，いろいろなプログラミング言語で，下のように記述することができる[4]．

1. プロセス p は，起動したらプロセス q に信号を送り，q からの返事を待って終了する．
2. プロセス q は，起動したらプロセス p の信号を待ち，p あてに返事を送って終了する．

残念ながら，このような並列プログラムは wait-free ではないので，論理式 $K_pK_qK_pI_p$ を wait-free 性を表す論理式のクラスに含めることはできない．このような気分で定まる論理式のクラスを，wait-free 動作と名付けて，下のほうで定義したい．

ところで，wait-free 計算といえども，プロセスは共有メモリを待つことだけは許されている[5]．共有メモリに値の読み込みを求めてから読み込めた値を待ったり，共有メモリに値の書き込みを求めてから書き込み完了の信号を待ったりすることはできる．この節では，メモリを表す特殊な主体 m があって，メモリ以外の主体はプロセスの集合 P の元であるとする．要するに，$A = \{\mathsf{m}\} \cup P \quad (\mathsf{m} \notin P)$ とおく．

固定した wait-free な分散プログラムについて興味があるとき，ある定数があってその定数回しかメモリにアクセスできないはずである．しかも，プロセスとメモリ間の通信はあってもプロセス間の通信はないので，プロトコルが保証できる知識伝達は，$K_pK_{\mathsf{m}}K_p \cdots K_{\mathsf{m}}K_pI_p$ とメモリとプロセスの二種類の様相が交互に現れる形の論理式だけである．

スケジュールと分散プログラム以外に，実行が完了した状況が満たすべき性質も，論理式で記述したい．なにか知識が無いことを保証させたい場面は無いと勝手に決めて，プロトコル実行後に欲しい性質として positive な論理式 (wait-free 性質) だけ考えることにする．

定義 25 各プロセスに相異なる原子論理式が割り当てられていることにする $(I_p)_{p\in P}$.

Wait-free 動作 φ とは，下の形をした論理式である*:*

$$\varphi = \bigwedge_{p\in P} K_pK_{\mathsf{m}}K_p \cdots K_pI_p$$

ただし K_p と K_{m} は，$\cdots$ の中で交互に現れることとする．

Wait-free 性質 ψ とは，下の *BNF* で定義される形をした論理式である*:*

$$\psi ::= K_p\psi \mid (\psi \wedge \psi) \mid (\psi \vee \psi) \mid I_p.$$

Wait-free 仕様 とは 論理式 $\varphi \supset \psi$ で，φ は *wait-free* 動作であり ψ は *wait-free* 性質であるもののことである．

Wait-free 仕様は，特殊な有限モデル性を持っている．Wait-free 仕様が体系 $\vdash_{\mathrm{SC}}$ の定理でないならば，特殊な形をした有限モデルが存在して，そのモデルには，定理でない wait-free 仕様が充足されない状態がある．特殊な形をした有限モデルというのは，Saks と Zaharoglou [23] によって定義された共有メモリのスケジューリングを真似したものである．

[4] 互いのプロセス ID を知ったりする手順は，省く．このことは，主体の集合が固定されている直観主義知識論理の制限による．

[5] さもなくば，いかなる通信も不可能になってしまっただろう．

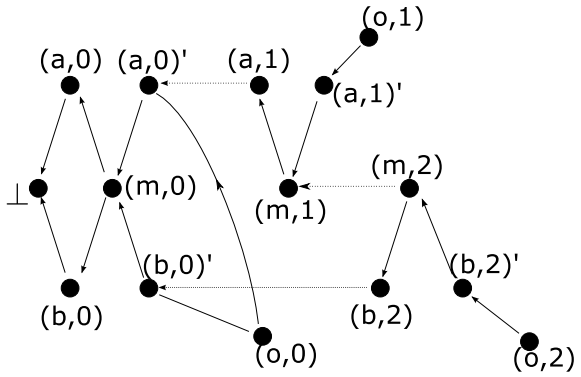

図 2. スケジュール $\sigma = (\{a,b\},\{a\},\{b\})$ が定めるモデル $R(\text{-},\sigma)$ の形．実線の矢印の先が $(x,\cdot)$ を指すときは，その矢印の元の状態を f_x によって写すとその矢印の先へ写ることを表す．点線の矢印は，それ以外の，$\preceq$ を表す．推論できる矢印を省いた．

定義 26 スケジュール[6] $(\sigma_i)_{i\in I}$ とは， P の部分集合の有限列のことである．

定義 27 プロセス $p \in P$ とスケジュール $(\sigma_i)_{i\in I}$ について，$count_p(\sigma)$ を集合の濃度 $|\{i \in I \mid p \in \sigma_i\}|$ と定義する．

Wait-free 動作 $\varphi = \bigwedge_{p\in P} K_p K_{\mathsf{m}} \cdots K_p I_p$ について，$count_p(\varphi)$ を $K_p K_{\mathsf{m}} \cdots K_p I_p$ における K_{m} の出現の個数と定義する．

スケジュール σ が *wait-free* 動作 φ と**整合的**であるとは， 任意のプロセス p について $count_p(\varphi) = count_p(\sigma)$ であることである．

定義 28 *Wait-free* 動作 φ と整合的なスケジュール $(\sigma_i)_{i\in I}$ について，スケジュールに従って定まるモデル $R(\varphi,\sigma) = \langle W, \preceq, (f_x)_{x\in P\cup\{\mathsf{m}\}}\rangle$ を下のように定義する*:*

- $W = \{(p,i) \in P\times\mathbb{N} \mid a \in \sigma_i\} \cup \{(p,i)' \in P\times\mathbb{N} \mid a \in \sigma_i\} \cup \{(\mathsf{m},i) \mid i \in I\} \cup \{(o,i) \mid i \in I\} \cup \{\bot\}$. ただし $o \notin P \cup \{\mathsf{m}\}$ とする．
- $\bot \preceq w$ は任意の $w \in W$ について成り立つ．
- $(p,i) \preceq (\mathsf{m},i) \preceq (p,i)'$ である *$(p \in P, \quad i \in I)$*.
- $(p,i)' \leq (p,j)$ であるのは，ちょうど $i < j$ なときである *$(p \in P, \quad i,j \in I)$*.
- $(x,j) \preceq (o,i)$ であるのは $j \leq i$ なときである *$(x \in P \cup \{\mathsf{m},o\})$*.
- $(p,j)' \preceq (o,i)$ であるのは $j \leq i$ のときである *$(p \in P, \quad i,j \in I)$*.
- $x \in P \cup \{\mathsf{m}\}$ について，

$$f_x(w) = \begin{cases} (x,j) \text{ か } (x,j)' \text{ の形をした状態 } v \text{ が存在して } v \preceq w \text{ を満たすとき，その最大のもの} \\ \qquad\qquad\qquad\qquad (\preceq \text{ の定義により，最大のものは存在する}). \\ \text{そのような } (x,j) \text{ が存在しないとき，} \bot. \end{cases}$$

さらに付値 ρ を定義する*:* $\rho(I_p) = \{w \in W \mid (p,0) \preceq w\}$ *$(p \in P)$*.

スケジュールに従って定まるモデルの例を図 2 に示す．

定理 29 (Wait-free 計算への wait-free 仕様の完全性) $\varphi \supset \psi$ が *wait-free* 仕様であると仮定する．任意の整合的なスケジュール σ について関係 $R(\varphi,\sigma),(o,n) \models \psi$ が成りたつならば関係 $\vdash_{SC} (\varphi \supset \psi)$ が成立する．ただし状態 (o,n) はモデル $R(\varphi,\sigma)$ の最後の状態であるとする．

[6]Saks と Zaharoglou [23] は，無限列を schedule とし有限列を partial schedule としているが，本稿では有限列しか用いないので，有限列をスケジュールと呼んでしまう．

完全性を示すために，順列スケジュールモデルという特殊なモデルだけを用いる．プロセスの集合上の順列が定める特殊な形のスケジュールを定義 34 で定めた上で，その特殊なスケジュールの定めるモデルを順列スケジュールモデルと名付ける．この完全性の証明は，逐次一貫性をメタに利用しているともいえる．

定義 30 有限集合 P について， $\mathsf{S}(P)$ は，P 上の順列の集合を表すものとする．

定義 31 順列 $\pi \in \mathsf{S}(P)$ について，$SC(\pi)$ をこの集合だと定義する*:* $\{K_{\mathsf{m}}K_aI_a \supset K_{\mathsf{m}}K_bI_b \mid \pi$に b が a 以前に登場する $\}$.

ただし Index が小さいほうが前である．

定義 32 順列 $\pi \in \mathsf{S}(P)$ と $0 \leq k \leq |P|$ について，論理式の集合 $SC(\pi, k)$ を，$\{K_{\mathsf{m}}K_aI_a \supset K_{\mathsf{m}}K_bI_b \mid (\pi_0 \cdots \pi_k)$ に b が a 以前に登場する $\}$ と定義する．

補題 33 $\vdash_{\mathrm{sc}} \bigvee_{\pi \in \mathsf{S}(A)} SC(\pi)$ が成り立つ．

証明 規則 (SC) を多用すればよい． ∎

定義 34 P の順列 π と，*wait-free* 動作 φ について，スケジュール $\sigma(\varphi, \pi)$ を

$$\sigma(\varphi, p) = \overbrace{\pi_0, \cdots, \pi_0}^{count_{\pi_0}(\varphi)}, \overbrace{\pi_1, \cdots, \pi_1}^{count_{\pi_1}(\varphi)}, \cdots\cdots\cdots, \overbrace{\pi_n, \cdots, \pi_n}^{count_{\pi_n}(\varphi)}$$

と定義する．

下の定義で，$f_x(w) = w$ なる状態 w のことを x 状態と呼ぶことにする．それとは別に，外部観察者状態とは，(o, i) という形の状態のことである．

定義 35 順列スケジュールモデルとは， $R(\varphi, \sigma(\varphi, \pi))$ と作れるモデルのことである．このモデルのことを $R(\varphi, \pi)$ とも書く．順列スケジュールモデルと，インデックス $k \in I$ について，w_k は，任意の $j < k$ について，$\preceq$ に関して任意の π_j 状態以上であるような状態 (o, l) のうち，l が最小のものを指す．

完全性の証明のために，順列スケジュールモデル上の各状態が充足する論理式を，証明可能性で特徴づけていきたい．順列スケジュールの途中の状態で成立する論理式を，証明可能性で特徴づけるために，Wait-free プログラムを途中まで実行したことにより保証される性質を，wait-free 動作の制限と名付けて定義する．

定義 36 *Wait-free* 動作 $\varphi = \bigwedge_{p \in P} \overbrace{K_pK_{\mathsf{m}}K_p \cdots K_p}^{n_p} I_p$ について，**制限**を定義する*:*

$$\varphi \restriction_{\pi,k} = \bigwedge_{p \in P \restriction_{\pi,k}} \overbrace{K_pK_{\mathsf{m}}K_p \cdots K_p}^{n_p} I_p.$$

ただし $P \restriction_{\pi,k} = \{p \in P \mid \pi_j = p$ がある $j < k$ について成り立つ $\}$ とする．

補題 37 *Wait-free* 性質 ψ について，$R(\varphi, \pi), w_k \models \psi \Longrightarrow SC(\pi, k) \vdash \varphi \restriction_{\pi,k} \supset \psi$.

一般化されたこの補題を示したのちに，定理 29 を証明するのは簡単である．

定理 29 の証明 $R(\varphi, \pi), w_n \models \psi$ より $SC(\pi, n) \vdash \varphi \supset \psi$(補題 37)．補題 33 より $\vdash \varphi \supset \psi$. ∎

残りは補題 37 の証明だけである．Wait-free 性質には含意の結合子 $\supset$ が現れないので，モデルのどの状態でどの wait-free 性質が充足されるかは，$\preceq$ に関して下のほうから決めていくことができる．充足される wait-free 性質を，スケジュールに関する情報 $SC(\pi, k)$ とプログラムに関する情報 $\varphi \restriction_{\pi,k}$ から，形式的に証明可能であるということを示していく．

補題 37 の証明 k に関する帰納法で示す．この証明の中では，$R(\varphi, \pi), w \models \varphi$ を $w \models \varphi$ と略して書く．

($k = 0$ の場合) より強い命題

$$w_0 \models \psi \quad \Longrightarrow \quad f_{\pi_0}(w_0) \models \psi\text{かつ } SC(\pi, 0) \vdash \varphi \restriction_{\pi,0} \supset \psi\text{かつ } SC(\pi, 0) \vdash \varphi \restriction_{\pi,0} \supset K_{\pi_0}\psi.$$

を，ψ の構成に関する内側の帰納法で示す．

(ψ が原子論理式であるとき) $R(\varphi, \pi)$ の付値の定義より $\psi = I_{p_0}$ のはずである．$\varphi \restriction_{\pi,0} = K_{p_0}K_{\mathsf{m}}K_{p_0} \cdots K_{\mathsf{m}}K_{p_0}I_{p_0}$ であるから，$\vdash \varphi \restriction_{\pi,0} \supset K_{\pi_0}P$ が成り立つ．よって，$SC(\pi, 0) \vdash \varphi \restriction_{\pi,0} \supset K_{\pi_0}P$ が成り立つ．結果として，$SC(\pi, 0) \vdash \varphi \restriction_{\pi,0} \supset P$ も成り立つ．

(ψ の最上位の論理結合子が $\vee$ か $\wedge$ であるとき) 帰納法の仮定を素直に使える．

($\psi = K_p\psi'$ であるとき) $w_0 \models K_p\psi'$ を仮定する．主張: $p = \pi_0$ である．矛盾を求めて，$p \neq \pi_0$ と仮定する．すると $f_p(w_0) = \bot$ となる．しかし，どの wait-free 性質も状態 $\bot$ では成立しないので，矛盾である．$p = \pi_0$ を示せた．これを使って，$f_p(w_0) \models \psi'$ であることをしめせる．f_p が巾等なので，$f_p(f_p(w_0)) \models \psi'$ も成り立つ．つまり $f_p(w_0) \models K_p\psi'$ である．$w_0 \models \psi'$ より，内側の帰納法の仮定より，$\vdash \varphi \restriction_{\pi,0} \supset K_p\psi'_p$ である．推論規則 (introspection) より，$\vdash \varphi \restriction_{\pi,0} \supset K_pK_p\psi'$ も成り立つ．$\vdash$ の左に $SC(\pi, 0)$ を追加できる．

($k = k' + 1$ の場合) $k = 0$ の場合とおなじように，強めの命題

$$w_k \models \psi \Leftrightarrow f_{\pi_k}(w_k)) \models \psi \Rightarrow SC(\pi, k) \vdash \varphi \restriction_{\pi,k} \supset \psi\text{かつ } SC(\pi, k) \vdash \varphi \restriction_{\pi,k} \supset K_{\pi_k}\psi,$$

を，ψ についての帰納法を使って示す．

(ψ が原子論理式であるとき) $R(\varphi, \pi), w_{k'} \models \psi$ または $I_{\pi_k} = \psi$ の少なくとも片方は成立する．最初の場合には，帰納法の仮定による．二番目の場合には，$k = 0$ の場合と同様である．

(ψ の最上位の論理結合子が $\vee$ か $\wedge$ であるとき) 帰納法の仮定を素直に使える．

($\psi = K_p\psi'$ のとき) 場合分けをする．$\pi_k \neq p$ の場合には，$f_{\pi_k}(w_k) \models K_p\psi'$ は $w_{k'} \models K_p\psi'$ を含意する．外側の帰納法の仮定より，$SC(\pi, k') \vdash \varphi \restriction_{\pi,k'} \supset K_p\psi'$ が成立し，かつ $SC(\pi, k') \vdash \varphi \restriction_{\pi,k'} \supset K_p\psi'$ が成立する．$SC(\pi, k)$ は $SC(\pi, k')$ を包含し，かつ，$\varphi \restriction_{\pi,k}$ は $\varphi \restriction_{\pi,k'}$ よりも強いので，これらの命題は，k' を k に置き換えてもやはり成り立つ．一方で $\pi_k = p$ の場合には，$w_k \models K_p\psi'$ は $w_k \models \psi'$ を含意する．内側の帰納法の仮定により，$SC(\pi, k) \vdash \varphi \restriction_{\pi,k} \supset K_p\psi'$ を得る．さらにこれにより，$SC(\pi, k) \vdash \varphi \restriction_{\pi,k} \supset K_pK_p\psi'$ を得る． ∎

3.6 定理の例

逐次一貫性のもとで，通信に沿ってあらゆる知識が伝達されると仮定すると，

- p が m に φ であると伝える通信をし，m から p に返事があった．
- q が m に ψ であると伝える通信をし，m から q に返事があった．

この二つの前提から，q から p に ψ が伝わったか，p から q に φ が伝わったかどちらかであるということが言える．これを意味するのが，$\vdash_{\mathrm{SC}}$ で導出可能な $K_pK_{\mathsf{m}}K_p\varphi, K_qK_{\mathsf{m}}K_q\psi \vdash_{\mathrm{SC}} K_pK_q\psi \vee K_qK_p\varphi$ である．この判断の証明図を図 3 に示す．

Part A

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{K_q K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vdash_{\mathrm{sc}} K_q K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi)}\,(\text{axiom})}{K_q K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vdash K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi)}\,(\mathrm{T})}{K_q K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi), K_p K_\mathsf{m} K_p\varphi \vdash_{\mathrm{sc}} K_p K_\mathsf{m} K_q\psi}\,(\supset\text{-E})}{K_q K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vdash_{\mathrm{sc}} K_p K_\mathsf{m} K_p\varphi \supset K_p K_\mathsf{m} K_q\psi}\,(\supset\text{-I})}{K_q K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vdash_{\mathrm{sc}} (K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vee (K_\mathsf{m} K_q\psi \supset K_\mathsf{m} K_p\varphi)}\,(\vee\text{-I})$$

$$\dfrac{\dfrac{}{K_\mathsf{m} K_p\varphi \vdash_{\mathrm{sc}} K_\mathsf{m} K_p\varphi}\,(\text{axiom})}{K_\mathsf{m} K_p\varphi, K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi \vdash_{\mathrm{sc}} K_\mathsf{m} K_q\psi}\,(\supset\text{-E})$$

$$\dfrac{\dfrac{}{K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi \vdash_{\mathrm{sc}} K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi}\,(\text{axiom})}{K_p K_\mathsf{m} K_p\varphi, K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vdash_{\mathrm{sc}} K_p K_\mathsf{m} K_q\psi}\,(\supset\text{-I})$$

Part B

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash_{\mathrm{sc}} (K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vee (K_\mathsf{m} K_q\psi \supset K_\mathsf{m} K_p\varphi)}\,(\mathrm{SC})}{\vdash_{\mathrm{sc}} K_p\left((K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vee (K_\mathsf{m} K_q\psi \supset K_\mathsf{m} K_p\varphi)\right)}\,(\mathrm{nec})}{\vdash_{\mathrm{sc}} K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vee K_p(K_\mathsf{m} K_q\psi \supset K_\mathsf{m} K_p\varphi)}\,(\vee K)}{\vdash_{\mathrm{sc}} K_q\left(K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vee K_p(K_\mathsf{m} K_q\psi \supset K_\mathsf{m} K_p\varphi)\right)}\,(\mathrm{nec})}{\vdash_{\mathrm{sc}} K_q K_p(K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi) \vee K_q K_p(K_\mathsf{m} K_q\psi \supset K_\mathsf{m} K_p\varphi)}\,(\vee K)$$

$\vdots$ Part A

$\vdots$ (同左．p と q とを，φ と ψ とを入れ替える．)

$$\dfrac{}{\vdash_{\mathrm{sc}} (K_p K_\mathsf{m} K_p\varphi \supset K_p K_\mathsf{m} K_q\psi) \vee (K_q K_\mathsf{m} K_q\psi \supset K_q K_\mathsf{m} K_p\varphi)}\,(\vee\mathrm{E})$$

Part C

$$\dfrac{\dfrac{\dfrac{}{K_p K_\mathsf{m} K_p\varphi \vdash_{\mathrm{sc}} K_p K_\mathsf{m} K_p\varphi}\,(\text{axiom})}{K_p K_\mathsf{m} K_p\varphi \supset K_p K_\mathsf{m} K_q\psi, K_p K_\mathsf{m} K_p\varphi \vdash_{\mathrm{sc}} K_p K_\mathsf{m} K_q\psi}\,(\supset\text{-E})}{K_p K_\mathsf{m} K_p\varphi \supset K_p K_\mathsf{m} K_p\psi, K_p K_\mathsf{m} K_p\varphi \vdash_{\mathrm{sc}} K_p K_q\psi}$$

$$\dfrac{\dfrac{\dfrac{}{K_\mathsf{m} K_q\psi \vdash_{\mathrm{sc}} K_\mathsf{m} K_q\psi}\,(\text{axiom})}{K_\mathsf{m} K_q\psi \vdash_{\mathrm{sc}} K_q\psi}\,(\mathrm{T})}{K_p K_\mathsf{m} K_q\psi \vdash_{\mathrm{sc}} K_p K_q\psi}\,(\mathrm{nec})}{\vdash_{\mathrm{sc}} K_p K_\mathsf{m} K_q\psi \supset K_p K_q\psi}\,(\supset\text{-I})$$

Main Part

$$\dfrac{\dfrac{\dfrac{\dfrac{}{(K_p K_\mathsf{m} K_p\varphi \supset K_p K_\mathsf{m} K_q\psi) \vee (K_q K_\mathsf{m} K_q\psi \supset K_q K_\mathsf{m} K_p\varphi)}}{K_p K_\mathsf{m} K_p\varphi, K_q K_\mathsf{m} K_q\psi \vdash_{\mathrm{sc}} K_p K_q\psi \vee K_q K_p\varphi}\,\vee\mathrm{E}}$$

$\vdots$ Part B

$$\dfrac{\dfrac{}{K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi,\ K_p K_\mathsf{m} K_p\varphi \vdash_{\mathrm{sc}} K_p K_q\psi}}{K_\mathsf{m} K_p\varphi \supset K_\mathsf{m} K_q\psi,\ K_p K_\mathsf{m} K_p\varphi \vdash_{\mathrm{sc}} K_p K_q\psi \vee K_q K_p\varphi}$$

$\vdots$ Part C

$\vdots$ (同左．p と q とを，φ と ψ とを入れ替える．)

図 3. 逐次一貫性下での判断の例の証明図．対称性により補完できる部分を省略した．

4　関連研究

4.1　Wait-free 計算の幾何的特徴付けとの関連

2004 年のゲーデル賞は，Herlihy と Shavit と [11] と，Saks と Zaharoglou と [23] とに与えられた．本研究は，これらの研究を道標として進んだ．

Helihy と Shavit [11] は，彩色単体的複体の分割を用いて，wait-free 計算を特徴づけた．彩色単体的複体とは，単体的複体の各頂点に主体が割り振られていて，各単体には主体が相異なる頂点たちが属しているようなもののことである．さらに彩色単体的複体の分割とは，彩色単体的複体であり，頂点にはときどき，carrier と呼ばれる先祖の単体が指定されているようなものである．今回提案した論理 $\mathbf{K}\vee$ のモデルに現れる f_a という関数は，carrier 関数からヒントを得た．単体を状態とみなすと，彩色単体的複体の分割を，情報を失わずに，$\mathbf{K}\vee$ のモデルとみなすこともできる．

Saks と Zaharoglou [23] は，wait-free プロトコルの中でも特に完全情報 [28] なものに特化して特徴付けを行った．共有変数でさえもが，代入された値の履歴全体をリストとして保持している．すべての部品の知識が，時間の経過に従って，増えつづけるのである．このことは，wait-free 計算を特徴づけるために，単調に知識が増え続ける，直観主義論理の意味論に登場する主体を用いることが適していることを示唆している．また，Saks と Zaharoglou [23] は，“We believe that it will be worthwhile to explore the connection with the formal theory of distributed knowledge” (我々は，分散知識の形式的理論との関連を探求することにそれなりの価値があろうと信じる) と述べている．本研究は，wait-free 計算における知識伝達の形式的な取り扱いをすることによって，彼らが示唆した方向の研究の足掛りとなるものである．

4.2　類似の論理

Majer の Relevant Epistemic Logic [18] は，論理結合子の意味が古典論理と異なる論理に知識様相をつけたという点で，本研究の $\mathbf{K}\vee$ と類似している．しかし，彼らの論理には知識様相は一種類しか入っていない．つまり，単一の主体しか扱わないので，コミュニケーションを扱えるわけではない．

時相様相と知識様相を両方使う論理はたくさんある．また，Ewald [7] は，時相のついた直観主義論理を考案している．統語論的にプロセスが現れるが時間が現れない点では，小林・米澤 [14] の体系は $\mathbf{K}\vee$ に類似している．しかし統語論的にも，この体系は線形論理をもとにしている点で $\mathbf{K}\vee$ と大きく異なり，使い方も論理プログラミングなので，本研究の論理の使い方と異なる．この体系で論理式がプロセスを表すのに対して，$\mathbf{K}\vee$ では様相がプロセスを名指す．

5　議論

5.1　レイテンシの分析により適している

今回提案した論理 $\mathbf{K}\vee$ が分析に適しているコミュニケーションとは，スループットよりもレイテンシが重要である場面であると考える．なぜならば，論理を単純にする目的から直観主義論理の Kripke モデルの半順序を時間の進行と同一視しているために，あらゆる知識が，時間の進行に沿って保たれることを暗黙に仮定しているからである．特に，通信に沿って時間が進むために，通信は，完全情報 [28] として扱わざるを得ない．完全情報プロトコルから実装可能なプロトコルを抽出する研究は盛んに行われている [8–10, 28]．けれども，今回提案した論理がより向いている状況が，レイテンシがスループットに比べてきつい制約になっていて，課題を解くために何通のメッセージが必要か推論するような場面であることに変わりはない．

5.2 逐次一貫性か，整列可能性か

Attiya と Welch [2] は，逐次一貫性 [16] と整列可能性 [12] との定義が類似しているために，よく取り違えられることを指摘した．簡単に，演繹体系 $\vdash_{SC}$ が整列可能性を特徴づけるわけではないことを確認する．整列可能性を定義した Herlihy [12] によると，整列可能性の特徴は局所的な性質である: つまり，各メモリオブジェクトが整列可能性を満たすときに，それらのメモリオブジェクトを並べて大きなメモリオブジェクトとみなしても，整列可能性を満たすというのだ．しかし，我々の公理型は，局所的ではない．メモリオブジェクト m と m' とがあるとする．我々の公理型は，それぞれのメモリオブジェクトについて，$(K_{\mathsf{m}}\varphi \supset K_{\mathsf{m}}\psi) \vee (K_{\mathsf{m}}\psi \supset K_{\mathsf{m}}\varphi)$ と $(K_{\mathsf{m}'}\varphi \supset K_{\mathsf{m}'}\psi) \vee (K_{\mathsf{m}'}\psi \supset K_{\mathsf{m}'}\varphi)$ という形の論理式から成る．両方の形の公理型を認めたところで，両方のメモリオブジェクトにまたがる性質 $(K_{\mathsf{m}}\varphi \supset K_{\mathsf{m}'}\psi) \vee (K_{\mathsf{m}'}\psi \supset K_{\mathsf{m}}\varphi)$ を証明することはできない．このことは，$\vdash_{\mathrm{sc}}$ が表す性質が局所的な性質ではなく，特に整列可能性ではないことを示している．

5.3 他の共有メモリ一貫性

Steinke と Nutt [24] は，共有メモリの一貫性たちから成る束を定義した．そのなかには，名前がついているだけでも，逐次一貫性，因果一貫性，プロセッサ一貫性，PRAM 一貫性，キャッシュ一貫性，遅い一貫性，局所一貫性という一貫性が属する．逐次一貫性以外の一貫性を論理的に特徴づけることは，今後の課題である．

5.4 選言 $\vee$ を知識様相 K が分配すること

Kripke モデル上で，様相の意味が関数であることから，選言を様相が分配する．小島・五十嵐 [15] は，Kripke モデル上の関数で様相を意味づけることを避けて，選言を様相が分配することを避けている．一方本研究の $\mathbf{K}\vee$ では，様相の意味を状態集合上の関数にして，選言を様相に分配させている．彼らの様相の使い方では様相の内側は未来を指すのに対して，本研究の $\mathbf{K}\vee$ の使い方では様相の内側が過去を指すという違いによって，この選択の違いがうまれているのであろう．

鈴木 [25] の翻訳によって，$\mathbf{K}\vee$ の主体が 1 つだけの場合のモデルは，任意の状態 w について対応する領域が単元集合であるような直観主義述語論理のモデル (Kripke バンドル) に対応する[7]．このことは，$\mathbf{K}\vee$ の意味論が，主体が 1 つだけの場合には極めて単純であることを示唆している．できるだけ単純な論理を用いたかったという目的に叶っている．

5.5 著者の以前の研究との関係

著者は，平井 [29] でも論理を定義して，wait-free な知識の伝達を特徴づけることを目標としたが，健全性は示したけれども，いかなる意味でも完全性を示さなかった．そこ [29] で扱った体系は，今回の $\vdash_{\mathrm{sc}}$ と目標が似ているが，論理結合子 $\supset$ も無いし公理も異なるし古典論理なので，異なる．

謝辞 以前の関連する研究について発表 [29] した際，議論してくださった方々に，謝意を表する．匿名査読者たちに学ぶべき点は多大である．感謝する．

参考文献

[1] N. Alechina, M. Mendler, and V. Paiva. Categorical and Kripke semantics for constructive S4 modal logic. 2001.

[2] H. Attiya and J.L. Welch. Sequential consistency versus linearizability. *ACM Transactions on Computer Systems (TOCS)*, 12(2):122, 1994.

[7] 対応するというのは，小野 [19] にある論理 L_3 のモデルが定領域の直観主義述語論理のモデルに対応するのと同様に対応するという意味である．

[3] P. Balbiani, A. Baltag, H.V.A.N. Ditmarsch, A. Herzig, T. Hoshi, and T. de Lima. ‘Knowable’ as ‘known after an announcement’. *The Review of Symbolic Logic*, 1(03):305–334, 2008.

[4] A. Baltag, B. Coecke, and M. Sadrzadeh. Epistemic actions as resources. *Journal of Logic and Computation*, 17(3):555, 2007.

[5] P. Bieber and T. Onera-Cert. A logic of communication in hostile environment. In *Computer Security Foundations Workshop III, 1990. Proceedings*, pages 14–22, 1990.

[6] V. Costa and M. Benevides. Formalizing Concurrent Common Knowledge as Product of Modal Logics. *Logic Journal of IGPL*, 13(6):665, 2005.

[7] W.B. Ewald. Intuitionistic tense and modal logic. *The Journal of Symbolic Logic*, 51(1):166–179, 1986.

[8] J.Y. Halpern. Using reasoning about knowledge to analyze distributed systems. *Annual Review of Computer Science*, 2(1):37–68, 1987.

[9] J.Y. Halpern and R. Fagin. A formal model of knowledge, action, and communication in distributed systems: preliminary report. In *Proceedings of the fourth annual ACM symposium on Principles of distributed computing*, pages 224–236. ACM New York, NY, USA, 1985.

[10] J.Y. Halpern and Y. Moses. Knowledge and common knowledge in a distributed environment. *Journal of the ACM (JACM)*, 37(3):549–587, 1990.

[11] M. Herlihy and N. Shavit. The topological structure of asynchronous computability. *Journal of the ACM (JACM)*, 46(6):858–923, 1999.

[12] M. Herlihy and J.M. Wing. Linearizability: A correctness condition for concurrent objects. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 12(3):463–492, 1990.

[13] L. Jia and D. Walker. Modal proofs as distributed programs. *Lecture notes in computer science*, pages 219–233, 2004.

[14] N. Kobayashi and A. Yonezawa. Asynchronous communication model based on linear logic. *Formal Aspects of Computing*, 7(2):113–149, 1995.

[15] K. Kojima and A. Igarashi. On constructive linear-time temporal logic. *Proc. of IMLA*, 8, 2008.

[16] L. Lamport. How to make a multiprocessor computer that correctly executes multiprocess progranm. *IEEE transactions on computers*, 100(28):690–691, 1979.

[17] C.J. Liau. Belief, information acquisition, and trust in multi-agent systems—A modal logic formulation. *Artificial Intelligence*, 149(1):31–60, 2003.

[18] O. Majer and M. Peliš. Epistemic Logic with Relevant Agents.

[19] H. Ono. On some intuitionistic modal logics. *Publ. Res. Inst. Math. Sci.*, 13(3):687–722, 1977.

[20] D. Peleg. Communication in concurrent dynamic logic. *J. COMP. SYST. SCI.*, 35(1):23–58, 1987.

[21] J. Plaza. Logics of public communications. *Synthese*, 158(2):165–179, 2007.

[22] G. Plotkin and C Stirling. A framework for intuitionistic modal logics: extended abstract. In *TARK '86: Proceedings of the 1986 conference on Theoretical aspects of reasoning about knowledge*, pages 399–406, San Francisco, CA, USA, 1986. Morgan Kaufmann Publishers Inc.

[23] M. Saks and F. Zaharoglou. Wait-free k-set agreement is impossible: The topology of public knowledge. *SIAM journal on computing(Print)*, 29(5):1449–1483, 2000.

[24] R.C. Steinke and G.J. Nutt. A unified theory of shared memory consistency. *Journal of the ACM (JACM)*, 51(5):800–849, 2004.

[25] N.Y. Suzuki. Kripke bundles for intermediate predicate logics and Kripke frames for intuitionistic modal logics. *Studia Logica*, 49(3):289–306, 1990.

[26] A.S. Troelstra and D. Van Dalen. *Constructivism in Mathematics: An Introduction: Vol.: 1*. North-Holland, 1988.

[27] J. van Benthem. The information in intuitionistic logic. *Synthese*, 167(2):251–270, 2009.

[28] Thomas Y.C. Woo and Simon S. Lam. A lesson on authentication protocol design. *SIGOPS Oper. Syst. Rev.*, 28(3):24–37, 1994.

[29] 平井洋一. 「分散プログラムを形式的証明から抽出する」. 日本ソフトウェア科学会第 *26* 回大会, 2009.