分散プログラムを形式的証明から抽出する (修正版)

平井 洋一

分散動作するプログラムのバグは，ひとたび作ってしまうと，スケジューリングに依存して顕在化したりしなかったりするために，テストによって発見することが困難である．モデル検査によっても，スケジューリングによる状態数の爆発により，大規模な分散プログラムのバグを素早く見付けることは困難である．従って，分散プログラムを作るときには，初めからバグを入れないことが重要である．プロセス間の同期が不可能なため特にスケジューリングへの依存性が高い wait-free 計算と呼ばれる分散計算のクラスに関して，形式的証明から仕様を満たすプログラムを抽出する機構を考案した．

1 はじめに

共有メモリ付き wait-free 計算では，プロセスが待つのは自プロセスが共有メモリに書き込むのを待つだけで，他のプロセスを待つことがない．この制限のためにできないことの例を挙げると，たとえば，複数のプロセスに与えた入力を，予め固定したあるプロセスに集約することができない．なぜならば，集約先のプロセスが他のプロセスを待つことができないからである．

この，wait-free という制約のもとで可能な計算が，どのようなクラスを成すかについて，Herlihy, M. と Shavit, N. [4] が，彩色単体的複体 (本稿第 2 節で定義する) を用いた美しい特徴付けを与えた．本稿の定義 4.5 で与えた wait-free protocol が，wait-free 計算で可能な計算である．彼ら [4] は，wait-free protocol から共有メモリを操作するプログラムたちを具体的に構成して，プロセスに割り当てている．

本稿では，第 3 節で，彩色単体的複体の上である様相論理の論理式に意味を与える．第 4 節で，形式的な証明体系を定義して，その証明体系で仕様が導出可能ならば，その仕様を満たす wait-free protocol が存在することを示す．仕様では，プロセスの知識について述べることができる．Wait-free protocol の存在証明を，形式的証明の構成に関して帰納的に，構成的に行うので，形式的証明から wait-free protocol を抽出できることが，わかる．

Extracting Distributed Programs from Formal Proofs.
Yoichi Hirai, 東京大学大学院情報理工学系研究科, Graduate School of Information Science and Technology, The University of Tokyo,

2 単体的複体

定義 2.1 (単体的複体)**.** 単体的複体 $X = (V, S)$ は，有限集合 V と $S \subset \mathcal{P}(V)$ の組で，

1. $\emptyset \notin S$.
2. 任意の $v \in V$ について，$\{v\} \in S$.
3. $s \in S$ かつ $\emptyset \neq s' \subset s$ ならば $s' \in S$.

を満たすもの．

記法 2.1. 単体的複体 $X = (V, S)$ について，V のことを $|X|$ と書いたり S のことを X と書いたりする．

定義 2.2 (単体的写像)**.** 単体的複体 A, B について，単体的写像 $f\colon A \to B$ とは，写像 $f\colon |A| \to |B|$ であって，任意の $a \in A$ について，$f(a) \in B$ を満たすもの．

定義 2.3 (次元を保つ単体的写像)**.** 次元を保つ単体的写像とは，単体的写像 $f\colon A \to B$ で，$|f(a)| = |a|$ を任意の $a \in A$ について満たすもの．

定義 2.4 (単体)．単体とは，単体的複体 $\langle V, S\rangle$ で，$S = \mathcal{P}(V) \setminus \{\emptyset\}$ であるもの．

定義 2.5 (順序付単体的複体)．順序付単体的複体 $\langle V, S, \preceq\rangle$ とは，$\langle V, S\rangle$ が単体的複体で，$\preceq$ が S 上の全順序であり $s \subset t$ ならば $s \preceq t$ を満たすもの．

定義 2.6 (順序付単体)．順序付単体とは，順序付単体的複体 $\langle V, S, \preceq\rangle$ で，$S = \mathcal{P}(V) \setminus \{\emptyset\}$ かつ $\preceq = S \times S$ であるもの．

定義 2.7 (順序付単体的写像)．順序付単体的複体 $\langle V, S, \preceq\rangle, \langle V', S', \preceq'\rangle$ について，順序付単体的写像 $f\colon \langle V, S, \preceq\rangle \to \langle V', S', \preceq'\rangle$ とは，単体的写像 $f\colon \langle V, S\rangle \to \langle V', S'\rangle$ であって，任意の $s, t \in S$ について，$s \preceq t \Leftarrow f(s) \preceq f(t)$ をみたすもの．

定義 2.8 (彩色単体的複体)．単体 C について，C-彩色単体的複体 $\langle S, \chi\rangle$ とは，

1. 単体的複体 S
2. 次元を保つ単体的写像 $\chi\colon S \to C$

の組である．

のちに，wait-free protocol を抽出するときに，$|C|$ の元をプロセスとみなす．

定義 2.9 (色保存単体的写像)．色保存単体的写像とは，単体的写像 $f : \langle S, \chi\rangle \to \langle S', \chi'\rangle$ であって，任意の $s \in S$ について，$\chi(s) = \chi'(f(s))$ を満たすもの．

補題 2.1. 色保存単体的写像 $f\colon \langle S, \chi\rangle \to \langle S', \chi'\rangle$ は，次元を保つ．

証明. 任意の $s \in S$ について $|s| = |f(s)|$ を示せばよい．彩色単体的複体の定義より，χ は次元を保つから，$|s| = |\chi(s)|$ である．f は色を保存するから，$\chi(s) = \chi(f(s))$ であり，したがって，$|\chi(s)| = |\chi(f(s))|$ である．彩色単体的複体の定義より，χ' も次元を保つから，$|s'| = |\chi'(s)|$ である．以上より，$|s| = |f(s)|$ である． □

定義 2.10 (彩色順序付単体的複体)．順序付単体 C について，順序付単体的写像 $\chi\colon \langle V, S, \preceq\rangle \to C$ があって，χ が次元を保つとき，$\langle V, S, \preceq, \chi\rangle$ を C 彩色順序付単体的複体と呼ぶ．

3 論理

命題記号の集合 $PVar$ を固定する．$P, Q, \ldots$ を，命題記号を走るメタ変数とする．

定義 3.1. 単体 C について，C-論理式 φ を BNF で定義する*:*

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

ただし，a は C の部分集合で，P は命題記号．曖昧でないときには括弧を省略することがある．

$\bot$ や $\supset$ はなく，のちに意味を定義するとわかるように，すべての論理式のすべての部分論理式が positive である．

定義 3.2 (付値)．順序付単体的複体上の付値 ρ とは，$\rho\colon PVar \to \mathcal{P}(S)$ で，$s \in \rho(P)$ かつ $s \preceq t$ ならば $t \in \rho(P)$ をみたすもののこと．

定義 3.3 (モデル)．$\langle V, S, \preceq, \chi, \rho\rangle$ は，

1. $\langle V, S, \preceq, \chi\rangle$ が順序付単体的複体である
2. $\preceq$ が反対称的である
3. ρ が $\langle V, S, \preceq, \chi\rangle$ 上の付値である

とき，モデルである．

定義 3.4. モデル $\langle V, S, \preceq, \chi, \rho\rangle$ の単体とは，S の元のこと．

定義 3.5 (充足関係)．モデル $\langle V, S, \preceq, \chi, \rho\rangle$ と，S の元 s と，論理式 φ についての関係 $\langle V, S, \preceq, \chi, \rho\rangle, s \models \varphi$ を，下記を満たす最小の $\models$ として定義する．ただし，以下，$\langle V, S, \preceq, \chi, \rho\rangle$ を固定して，$s \models \varphi$ と書くと，$\langle V, S, \preceq, \chi, \rho\rangle, s \models \varphi$ のことである．

- $s \models \varphi$ かつ $s \preceq t$ ならば $t \models \varphi$ である．
- $s \subset \rho(P)$ ならば $s \models P$ である．
- $s \models \psi_0$ かつ $s \models \psi_1$ ならば，$s \models \psi_0 \wedge \psi_1$ である．
- $s \models \psi_0$ または $s \models \psi_1$ ならば，$s \models \psi_0 \vee \psi_1$ である．
- $\chi(s) = a$ かつ $s \models \varphi$ ならば，$s \models \varphi$ ならば，$s \models K_a\varphi$ である．

指摘 3.1. 上の条件たちは，各条の前半に登場する $\models$ から，各条の後半に登場する $\models$ への，包含関係について単調な写像 F を与えているように読むことができる．したがって，*Tarski* の不動点定理より，上の条件たちを満たす包含関係について最小の $\models$ がある．

以下,「$\models$ の最小性によって，$\models$ は性質 R を満たす」と述べた箇所では,「関係としての $\emptyset$ は性質 R を満たし，かつ，関係 X が性質 R を満たすならば $F(X)$ も性質 R を満たす．よって F の最小不動点 $\models$ も，性質 R を満たす」という議論が可能である．

定義 3.6. C の部分集合 G について，$\langle V,S,\preceq,\chi,\rho\rangle \models_G \varphi$ とは，$\preceq$ の極大元 s で $\chi(s)=G$ なる任意の s について，$\langle V,S,\preceq,\chi,\rho\rangle, s \models \varphi$ であるということ．

定義 3.7. 証明図を図 *1* の推論規則によって定義する．

4 プログラム抽出

定義 4.1. 単体的複体 $\langle V,S\rangle$ の，頂点の集合 $V'\subset V$ への制限 $\langle V,S\rangle\restriction_{V'}$ とは，$\langle V',\{s\in S \mid s\subset V'\}\rangle$ のこと．

単体的複体の，頂点を制限すると，単体的複体になる．

定義 4.2 (順序付単体的複体の G 分割)**.** C の部分集合 G について，順序付き単体的複体 $\langle V,S,\preceq,\chi\rangle$ の G 分割という順序付き単体的複体 $\langle V',S',\preceq',\chi'\rangle$ を定義する．$S_G=\{s\in S \mid \chi(s)\subset G \textit{ and } s \textit{ is a maximal with respect to } \preceq'\}$ と定義し，$Vnew=\{\langle s,c\rangle\in S_G\times C \mid |s|>1 \textit{ and } c\in\chi(s)\}$ と定義した上で，$V'=V\sqcup Vnew$ とする．

$\langle s,t,g\rangle\in(S\cup\{\emptyset\})\times S\times\mathcal{P}(C)$ について，

$$\begin{aligned}(\!|s,t,g|\!) &= \{v\in V \mid v\in t \textit{ and } \chi(v)\notin g\}\\ &\cup \{\langle s_{new},c\rangle\in Vnew \mid s_{new}=s \textit{ and } c\in g\}\end{aligned}$$

と定義する．これを用いて，

$$\begin{aligned}S' = \{&(\!|s,t,g|\!)\in\mathcal{P}(V') \mid\\ &\langle s,t,g\rangle\in(S\cup\{\emptyset\})\times S\times\mathcal{P}(C)\\ &\textit{and}\quad \chi(s)\subset g\subset\chi(t)\}\end{aligned}$$

とする．

$v\in V$ について $\chi'(v)=\chi(v)$ とし，$\langle s,c\rangle\in Vnew$ について $\chi'(\langle s,c\rangle)=c$ とする†1.

関係 $\preceq^1\subset S'\times S'$ を，$(\!|s,t,g|\!)\preceq^1(\!|s',t',g'|\!)$ である必要十分条件を $t\preceq t'$ かつ $\chi'(t)\cap\chi'(t')\cap g=\chi'(t)\cap\chi'(t')\cap g'$ として定義する．

関係 $\preceq^2\subset S'\times S'$ を，$(\!|s,t,g|\!)\preceq^1(\!|s',t',g'|\!)$ である必要十分条件を $t'\subset t$ かつ $g=\emptyset$ として定義する．

関係 $\preceq'=(\preceq^1\cup\preceq^2)^*$ と定義する†2.

気分を説明する．単体 $(\!|s,t,g|\!)$ は，もともと t であったものが，s が分割されたために，分割され，g 色たちの頂点は V_{new} から，それ以外の頂点は V からとった，そういう単体である．

例 4.1. $C=\{a,b\}$, $G=\{a,b\}$, $V=\{v,w\}$, $S=\{\{v\},\{w\},\{v,w\}\}$, $\chi(v)=a$, $\chi(w)=b$,

$$\begin{aligned}\preceq = \{&(\{v\},\{v,w\}),(\{w\},\{v,w\}),(\{v\},\{v\}),\\ &(\{w\},\{w\}),(\{v,w\},\{v,w\})\}\end{aligned}$$

とする．このとき，$\langle V,S,\preceq,\chi\rangle$ の G 分割 $\langle V',S',\preceq',\phi'\rangle$ はどんなものか，定義に従って構成してみる．

$S_G=\{\{v,w\}\}$ である．$V_{new}=\{(\{v,w\},a),(\{v,w\},b)\}$ である．$V'=V\cup V_{new}=\{v,w,(\{v,w\},a),(\{v,w\},b)\}$ である．

S' を定義するために，$\langle s,t,g\rangle\in(S\cup\{\emptyset\})\times S\times\mathcal{P}(C)$ で，$s\cap t\neq\emptyset$ かつ $g\subset\chi(t)$ かつ $\chi(s)=G$ なる組を挙げる．すなわち，$\langle\{v,w\},\{v\},\emptyset\rangle$, $\langle\{v,w\},\{v\},\{v\}\rangle$, $\langle\{v,w\},\{w\},\emptyset\rangle$, $\langle\{v,w\},\{w\},\{w\}\rangle$, $\langle\{v,w\},\{v,w\},\emptyset\rangle$, $\langle\{v,w\},\{v,w\},\{v\}\rangle$, $\langle\{v,w\},\{v,w\},\{w\}\rangle$, $\langle\{v,w\},\{v,w\},\{v,w\}\rangle$ の 8つである．

定義 4.3 (G 分割についての *carrier*)**.** $\langle V,S,\preceq,\chi\rangle$ の G 分割 $\langle V',S',\preceq',\chi'\rangle$ について，$carrier_G\colon S'\to S$ を，$(\!|s,t,g|\!)\mapsto t$ と定義する．

定義 4.4 (モデルの G 分割)**.** モデル $M=\langle V,S,\preceq,\chi,\rho\rangle$ の G 分割 GM とは，$\langle V,S,\preceq,\chi\rangle$ の G 分割 $\langle V',S',\preceq',\chi'\rangle$ について，$\langle V',S',\preceq',\chi',\rho'\rangle$ のことである．ただし ρ' は，

- $s\in\rho(P)$ かつ $carrier(s')=s$ ならば $s'\in\rho'(P)$ である．
- $s'\preceq' s''$ かつ $s'\in\rho'(P)$ ならば $s''\in\rho'(P)$ である

を満たす，関係として包含関係について最小の，付値．

定義 4.5 (G-wait-free protocol)**.** *G-wait-free protocol* とは，G の空でない部分集合の列 $(g_i)_{i\in I}$ のことである．

†1 すると，$\chi'((\!|s,t,g|\!))=\chi(t)$ となる．

†2 r^* は r の反射的推移的閉包である．

$$\text{(axiom)}\ \frac{}{\varphi \vdash_G \varphi} \qquad \text{(cut)}\ \frac{\Gamma \vdash_G \Delta, \varphi \qquad \varphi, \Gamma' \vdash_G \Delta'}{\Gamma, \Gamma' \vdash_G \Delta, \Delta'} \qquad \text{(K)}\ \frac{}{K_a\varphi \vdash_{\{a\}\cup G} \varphi}$$

$$\text{(comm)}\ \frac{}{K_a\varphi, K_b\psi \vdash_{\{a,b\}\cup G} K_aK_b\psi, K_bK_a\varphi}$$

$$\text{(nec)}\ \frac{\Delta \vdash_G \Gamma}{K_a(\bigwedge\!\!\bigwedge \Gamma) \vdash_{G\cup\{a\}} K_a(\bigvee\!\!\bigvee \Delta)}\ \text{(上のほうに comm が無い)}$$

$$\text{(K}\wedge\text{)}\ \frac{}{K_a\varphi, K_a\psi \vdash_G K_a(\varphi\wedge\psi)} \quad \text{(K}\vee\text{)}\ \frac{}{K_a(\varphi\vee\psi) \vdash_G K_a\varphi, K_a\psi} \quad (\vee\ \text{左})\ \frac{\Gamma, \varphi \vdash_G \Delta \qquad \Gamma', \varphi' \vdash_G \Delta'}{\Gamma, \Gamma', \varphi\vee\varphi' \vdash \Delta, \Delta'}$$

$$(\vee\ \text{右})\ \frac{\Gamma \vdash_G \Delta, \varphi, \varphi'}{\Gamma \vdash_G \Delta, \varphi\vee\varphi'} \qquad (\wedge\ \text{左})\ \frac{\Gamma, \varphi, \varphi' \vdash_G \Delta}{\Gamma, \varphi\wedge\varphi' \vdash_G \Delta} \qquad (\wedge\ \text{右})\ \frac{\Gamma \vdash_G \Delta, \varphi \qquad \Gamma' \vdash_G \Delta', \varphi'}{\Gamma, \Gamma' \vdash_G \Delta, \Delta', \varphi\wedge\varphi'}$$

図 1　推論規則たち．ただし，G は C の部分集合．φ, ψ は C-論理式であり，さらに weakening と contraction と exchange は古典命題論理と同じルールがある．

定義 4.6 (wait-free protocol の適用)．モデル M に *wait-free protocol* $p = (g_i)_{0\le i<n}$ を適用したモデル pM を，$(g_0(g_1(\cdots g_{n-1}M)))$ と定義する．

定義 4.7 (wait-free protocol についての carrier)．*Wait-free ptorocol* p とモデル $M = \langle V, S, \preceq, \chi, \rho\rangle$ について，$pM = \langle V', S', \preceq', \chi', \rho'\rangle$ として，$carrier_p\colon S' \to S$ を，$carrier_{g_{n-1}} \circ \cdots \circ carrier_{g_0}$ と定義する．

定義 4.8. *Wait-free protocol* p について，$p\colon \varphi \rightsquigarrow_G \psi$ とは，$M \models_G \varphi$ なる任意のモデル M について，$pM \models_G \psi$ であること．

補題 4.1. 任意の *wait-free protocol* p について，$M, s \models \varphi$ かつ $carrier_p(s') = s$ ならば，$pM, s' \models \varphi$ である．

証明. p の長さに関する数学的帰納法で証明する．p の長さが 0 のとき，$carrier_p$ は恒等関数である．$carrier_p(s') = s$ ならば $s = s'$ であり，かつ $pM = M$ だから $M, s \models \varphi$ ならば $pM, s' \models \varphi$ である．

p の長さが $k+1$ とする．色の集合 g を用いて，$p = g \circ p'$ とおく．$M, s \models \varphi$ かつ $carrier_{p'}(s') = s$ ならば，帰納法の仮定より，$p'M, s' \models \varphi$ である．$carrier_g(s'') = s'$ と仮定して，$gp'M, s'' \models \varphi$ を示せばよい．$gp'M = \langle V'', S'', \preceq'', \chi'', \rho''\rangle$ とおくと，S'' の元を $(\!|\emptyset, x, \emptyset|\!)$ という形の元だけに制限すると，色付単体的複体として $p'M$ と同型になり，$\rho'' \supseteq \rho'$ である．よって特に $gp'M, (\!|\emptyset, s'\emptyset|\!) \models \varphi$ である．$carrier_g(s'') = s'$ より，$s'' = (\!|s'_0, s', g'|\!)$ という形をしている．よって，$(\!|\emptyset, s', \emptyset|\!) \preceq^1 s''$ である．以上より，$gp'M, s'' \models \varphi$ である．　□

系 4.1. 任意のモデル M と *wait-free protocolp* について，$M \models_G \varphi$ ならば $pM \models_G \varphi$ である．

補題 4.2. $: \psi \rightsquigarrow_G \varphi$ かつ $\chi(s') = G$ かつ $M, carrier_p(s') \models \psi$ ならば，$pM, s' \models \varphi$ である．

証明. $s = carrier_p(s')$ とおく．M の単体を $s' \preceq s$ な s' たちだけに制限したものを $M \restriction_s$ と書く．$M \restriction_s \models_G \psi$ である．$\rightsquigarrow$ の定義より $p(M \restriction_s) \models_G \varphi$ である．$p(M \restriction_s)$ の pM への自然な埋め込みは $\models$ を保存し像に s' が属するので，$pM, s' \models \varphi$ である．　□

補題 4.3. $p\colon \psi \rightsquigarrow_G \varphi$ ならば，$p\colon \psi\vee\psi' \rightsquigarrow_G \varphi\vee\psi'$ である．

証明. $p\colon \psi \rightsquigarrow_G \varphi$ と仮定する．$M \models_G \psi$ なる任意のモデル M について，$pM \models_G \varphi$ である．$M' \models_G \psi\vee\psi'$ と仮定する．$M'' = pM'$ と仮定する ($\chi(s'') = G$ なる $s'' \in S''$ を任意にとる．$M'', s'' \models \varphi\vee\psi$ を示せばよい)．

$M', carrier_p(s'') \models \psi\vee\psi'$ であるから，$M', carrier_p(s'') \models \psi$ であるか，または，$M', carrier_p(s'' \models \psi')$ である．$M', carrier_p(s'') \models \psi$ であるとき，補題 4.2 より，$M'', s'' \models \psi'$ であるか

ら $M'', s'' \models \varphi \vee \psi'$ である．$M', carrier_p(s'' \models \psi')$ であるとき，補題 4.1 より，$M'', s'' \models \varphi$ であるから，$M'', s'' \models \varphi \vee \psi'$ である． □

補題 4.4. $p\colon \psi \rightsquigarrow_G \varphi$ ならば，$p\colon \psi \wedge \psi' \rightsquigarrow_G \varphi \wedge \psi'$ である．

証明. $p\colon \psi \rightsquigarrow_G \varphi$ と仮定する．$M \models_G \psi \wedge \psi'$ と仮定すると，$M \models_G \psi$ である．よって $pM \models_G \varphi$ である．$M \models_G \psi'$ かつ系 4.1 より，$pM \models_G \psi'$ である．以上より，$pM \models_G \varphi \wedge \psi'$ である． □

補題 4.5. *Wait-free protocol* p, p' について

1. $p\colon \bigwedge\!\!\bigwedge \Gamma \rightsquigarrow_G \bigvee\!\!\bigvee \Delta \vee \varphi$
2. $p'\colon \bigwedge\!\!\bigwedge \Gamma' \rightsquigarrow_G \bigvee\!\!\bigvee \Delta' \vee \varphi'$

の両方を仮定すると，$p'p\colon \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \rightsquigarrow_G \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta' \vee (\varphi \wedge \varphi')$ が成り立つ．

証明. $M \models_G \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma'$ と仮定する．$p'pM \models_G \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta' \vee (\varphi \wedge \varphi')$ を示せばよい．補題 4.4 と $p\colon \bigwedge\!\!\bigwedge \Delta \rightsquigarrow_G \bigvee\!\!\bigvee \Delta \vee \varphi$ を適用すると，$pM \models_G (\bigvee\!\!\bigvee \Delta \varphi) \wedge \bigwedge\!\!\bigwedge \Delta'$ である．$p'\colon \bigwedge\!\!\bigwedge \vee \Delta' \rightsquigarrow_G \bigvee\!\!\bigvee \Delta' \vee \varphi'$ と補題 4.4 とを適用すると，$p'pM \models_G \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta' \vee (\varphi \wedge \varphi')$ である．すなわち，$p'pM \models_G \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta' \vee (\varphi \wedge \varphi')$ である． □

補題 4.6. *Wait-free protocol* p, p' について

1. $p\colon \bigwedge\!\!\bigwedge \Gamma \wedge \varphi \rightsquigarrow_G \bigvee\!\!\bigvee \Delta$
2. $p'\colon \bigwedge\!\!\bigwedge \Gamma' \wedge \varphi' \rightsquigarrow_G \bigvee\!\!\bigvee \Delta'$

の両方を仮定すると，
$p'p\colon \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \wedge (\varphi \vee \varphi') \rightsquigarrow_G \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta'$
が成り立つ．

証明. $M \models_G \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \wedge (\varphi \vee \varphi')$ と仮定する．$p'pM$ の単体 s' について，$carrier_{p'p}(s') = s$ とすると，$M, s \models \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \wedge (\varphi \vee \varphi')$ である．$\models$ の定義 (最小性) より，$s, M \models \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \wedge \varphi$ または $s, M \models \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \wedge \varphi'$ である．$s, M \models \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \wedge \varphi$ のとき，$\rightsquigarrow$ の定義より，$pM, carrier_{p'}(s') \models \bigvee\!\!\bigvee \Delta$ であるから，$p'pM, s' \models \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta'$ である．$s, M \models \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \wedge \varphi'$ のとき，系 4.1 より，$pM, carrier_{p'}(s') \models \bigwedge\!\!\bigwedge \Gamma' \wedge \varphi'$ である．よって，$\rightsquigarrow$ の定義より，$p'pM, s' \models \bigvee\!\!\bigvee \Delta'$ であるから，$p'pM, s' \models \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta'$ である． □

補題 4.7.
1. $p\colon \bigwedge\!\!\bigwedge \Gamma \rightsquigarrow_G \bigvee\!\!\bigvee \Delta \vee \varphi$
2. $p'\colon \varphi \wedge \bigwedge\!\!\bigwedge \Gamma' \rightsquigarrow_G \bigvee\!\!\bigvee \Delta'$

の両方を仮定すると，$p'p\colon \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma' \rightsquigarrow_G \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta'$ が成り立つ．

証明. $M \models_G \bigwedge\!\!\bigwedge \Gamma \wedge \bigwedge\!\!\bigwedge \Gamma'$ と仮定する．補題 4.4 より，$pM \models_G (\bigvee\!\!\bigvee \Delta \vee \varphi) \wedge \bigwedge\!\!\bigwedge \Gamma'$ である．すなわち，$pM \models_G \bigvee\!\!\bigvee \Delta \vee (\varphi \wedge \Delta')$ でもある．よって補題 4.3 より $p'pM \models_G \bigvee\!\!\bigvee \Delta \vee \bigvee\!\!\bigvee \Delta'$ である． □

定理 4.1. 判断 $\Gamma \vdash_G \Delta$ が導出可能とする．ある G-*wait-free protocol* p が存在して，$p\colon \bigwedge\!\!\bigwedge \Gamma \rightsquigarrow_G \bigvee\!\!\bigvee \Delta$ である．

証明. 証明図の構成に関する帰納法で示す．以下で，長さ 0 の wait-free protocol を ϵ と表記する．

(axiom) 任意の論理式 φ と任意の G について，$\epsilon\colon \varphi \rightsquigarrow_G \varphi$ である．

(cut) 補題 4.7 を用いると，帰納法の仮定の wait-free protocol たちの連接を p とすればよいことがわかる．

(K) $M, s \models K_a\varphi$ ならば $M, s \models \varphi$ が $\models$ の定義から成立する．従って $\epsilon\colon K_a\varphi \rightsquigarrow_G \varphi$ である．

(comm) 長さ 1 で，$p_0 = \{a, b\}$ である wait-free protocol p について，$p\colon (K_a\varphi) \vee (K_b\psi) \rightsquigarrow_{\{a,b\} \cup G} (K_aK_b\psi) \vee (K_bK_a\varphi)$ である．

(nec) 任意のモデル M と，M の単体 s について $M, s \models \bigwedge\!\!\bigwedge \Gamma$ ならば $M, s \models \bigvee\!\!\bigvee \Delta$ であるとする．このとき，$M, s \models K_a(\bigwedge\!\!\bigwedge \Gamma)$ ならば $M, s \models K_a(\bigvee\!\!\bigvee \Delta)$ であることが，$\models$ の定義からわかる．

(K$\wedge$) $\models$ の定義より，$p = \epsilon$ として成り立つ．

(K$\vee$) $\models$ の定義 (最小性) より，$p = \epsilon$ として成り立つ．

($\vee$ 左) 補題 4.6 より，帰納法の仮定の wait-free protocol たちの連接を p とすればよいことがわかる．

($\wedge$ 左) $\bigwedge\!\!\bigwedge(\varphi, \varphi') = \varphi \wedge \varphi'$ より成り立つ．

($\wedge$ 右) 補題 4.5 より，帰納法の仮定の wait-free protocol たちの連接を p とすればよいことがわかる． □

以上の証明で，wait-free protocol を証明図から具

体的に構成していることが，プログラム抽出のために重要である．Herlihy と Shavit [4] に従うと，本稿の wait-free protocol を，実際のプログラミング言語の分散プログラムに翻訳することができる．すなわち，長さ 0 の wait-free protocol をなにもしないプログラムに翻訳できる．長さ $k+1$ の wait-free protocol gp は，p から抽出したプログラムの処理を各プロセスが行ってから，自プロセスが g の元である場合には，共有メモリへの書き込みを行い，然る後に g の他の元であるプロセスたちの書いた書きこみを読み込むという処理を行うような，プログラムに翻訳できる．

5 関連研究

形式的証明から wait-free protocol を抽出する既存研究を発見することができなかった．

Cattani と Winskell らの，並列計算の presheaf モデル [1] の枠組全般に応用できないか，関連を調べたい．線形論理 [3] のモデルである，整合空間は，単体的複体の特殊なものとみなせる．関連を調べたい．動的知識論理 [2] や，Concurrent common knowledge [5] など，通信を扱う様相論理が多数考案されているので，関連を調べたい．

6 まとめと今後の課題

以上のように，導出可能な判断について，導出可能性の定義について帰納的に，wait-free protocol を抽出できることがわかった．

今後の課題を挙げる:

- 完全性も示したい．
- 導出可能性が決定可能であることを示したい．
- Timothy Porter [6] による，Kripke 構造から単体的複体への変換との関係を，調べたい．
- より実用的にするために，たとえばロックや compare-and-swap というような同期機構を使うプログラムも抽出できるように体系を変更したい．
- 実際に動作するプログラムを抽出できる機構を実装したい．
- 分散計算の本質を掴むために，今回考えた wait-free protocol よりもさらに計算を制限して，sequencial consistency が成立しない場合を考えたい．
- 通信プリミティブを細かくしたい．本研究のプリミティブである (n 者通信) は，participating-set problem である．Participating-set problem は，分散計算のプリミティブとして通常用いられる，共有メモリへの読み書きやメッセージの授受と比較して，大きく複雑な問題である．
- カットを除去できるような，本研究の導出可能性と等価な体系を作りたい．
- 同じ仕様に対して同じプログラムをチェックするためにかかる時間を，本研究の枠組みとモデル検査とで比較する実験をしたい．
- 本研究の議論全体の形式化をして，wait-free protocol 抽出器をプログラム抽出したい．

謝辞 煩瑣な議論に付き合ってくださった，萩谷昌己先生と角谷良彦氏と木村大輔氏とに，感謝する．

参 考 文 献

[1] Cattani, G. L. and Winskel, G.: Presheaf Models for Concurrency, *Selected Papers From the 10th International Workshop on Computer Science Logic, LNCS*, Vol. 1258. Springer-Verlag, London, 1996, pp. 58–75.

[2] Ditmarsch, H. v., Hoek, W. v. d. and Kooi, B.: *Dynamic Epistemic Logic*, Springer, Dordrecht, 2007.

[3] Girard, J.: Linear logic, *Theor. Comput. Sci.* Vol. 50, No. 1, 1987, pp. 1–102.

[4] Herlihy, M. and Shavit, N.: The Topological Structure of Asynchronous Computability, *J. ACM*, Vol. 46, No. 6, 1999, pp. 858–923.

[5] Panangaden, P. and Taylor, K.: Concurrent common knowledge: defining agreement for asynchronous systems, *Distrib. Comput.*, Vol. 6, No. 2, 1992, pp. 73–93.

[6] Porter, T: Interpreted systems and Kripke models for multiagent systems from a categorical perspective, *Theor. Comput. Sci*, Vol. 323, No. 1–3, 2004, pp. 235–266.