通信プロトコルのフェーズ合成法とそのトークンパッシング制御を含むプロトコルの検証への適用

佐野 哲央† 樋口 昌宏† 関 浩之†‡ 嵩 忠雄‡†
†大阪大学基礎工学部情報工学科 ‡奈良先端科学技術大学院大学

順序機械としてモデル化されるプロトコルのフェーズと呼ばれるサブクラスを定義し, 規模の大きいプロトコルを複数のフェーズの合成として定義する合成法を提案する. その合成法を用いた拡張有限状態機械としてモデル化されたプロトコルの安全性の検証をフェーズごとの検証に帰着する手法についても述べる. さらにトークンパッシング制御を行うOSIセションプロトコルの一部に適用した結果についても述べる.

1 まえがき

筆者らはプロトコル機械が拡張有限状態機械としてモデル化され, 通信路が非有界FIFOとしてモデル化されるプロトコルの検証法を提案している[1][2]. 提案している検証法は (i) 検証者が初期状態から到達可能なあらゆる状態で成立すると考えられる条件を論理式の形で記述し, (ii) 記述された式が実際に初期状態から到達可能なあらゆる状態で成立することを帰納法により示す, というもので, (ii) の帰納段階の検証過程を自動化する検証システムを試作している. しかし、提案している検証法の実用プロトコルの検証への適用について考えると, 実用プロトコルの多くはさまざまな機能を提供しているため, その規模もかなり大きなものとなっており, 検証者による論理式の記述が実際上不可能になるという問題がある.

規模の大きなプロトコルの検証をより規模の小さなプロトコルの検証に帰着するための概念として, プロトコル機械の分解検証法[3], 射影検証法[4]などが知られている. 逆に, 複数のプロトコルの合成によって大規模プロトコルを定義する手法も知られている[5][6][7]. 文献[5]においてLinらは, 複数のフェーズと呼ばれるプロトコルを直列合成する手法を提案している. 但し, 彼らの合成法では合成のための条件として, プロトコル機械が有限状態機械としてモデル化されること, フェーズ終了時に双方向の通信路がともに空になっていることを仮定している.

本報告では上記の2つの制限を緩めた, より一般的なフェーズの合成手法を提案する. 本報告で提案する手法を用いることにより, たとえばトークンパッシングを行うプロトコルを, トークンが一方のプロトコル機械に固定されている2つのプロトコルの合成によって定義できる.

以下2.で基本的定義, 3.でフェーズと呼ばれるプロトコルのサブクラスとそれらの合成, 4.では拡張有限状態機械モデルのプロトコルの安全性の検証への適用法, 5.ではOSIセションプロトコルの一部の安全生の検証へ適用した結果について述べる.

An improved method for constructing multi-phase protocol and its application.
T. Sano†, M. Higuchi†, H. Seki†, T. Kasami‡
†Osaka University, ‡Advanced Institute of Science and Technology, Nara

2 準備

2.1 プロトコルモデル (CSMs)

本稿では, 2つのプロトコル機械が順序機械でモデル化され, 双方の通信路は非有界のFIFOでモデル化された, 2-Communicating Sequential Machines(2-CSMs) と呼ばれるプロトコルモデルを取り扱う.

定義 2.1 プロトコル機械 PM は以下のM1-M5を満たす5字組 (S, Σ, T, SI, SE) によって定義される.

M1: Sは状態の無限 (または有限) 集合.

M2: $\Sigma = \Sigma_- \cup \Sigma_+$はメッセージの無限 (または有限) 集合. Σ_-, Σ_+はそれぞれ送信メッセージ, 受信メッセージの集合を表す.

M3: $T \subseteq S \times \Sigma \times S$は状態遷移の無限 (または有限) 集合. $\langle s, e, s' \rangle \in T$ならば, プロトコル機械は状態 s においてメッセージ e を送信または受信し (e がΣ_-, Σ_+のどちらに属するかによる), 状態 s' に遷移できる. T により $S \times \Sigma$から 2^Sへの非決定性状態遷移関数δ は

$$\delta(s, e) = \{s' \mid \langle s, e, s' \rangle \in T\}$$

のように定まる. またδを $S \times \Sigma^*$から Sへの非決定性状態遷移関数に拡張して用いる場合もある.

M4: $SI \subseteq S$は初期状態の無限 (または有限) 集合.

M5: $SE \subseteq S$は終了状態の無限 (または有限) 集合. $s \in SE$ ならば あらゆる e, s' に対して $\langle s, e, s' \rangle$ なる状態遷移はT中に存在しないものとする. □

定義 2.2

プロトコル機械 $PM_A = (S_A, \Sigma_A, T_A, SI_A, SE_A)$ 及び $PM_B = (S_B, \Sigma_B, T_B, SI_B, SE_B)$ に対し, $\Sigma_{A-} = \Sigma_{B+}$かつ$\Sigma_{B-} = \Sigma_{A+}$ (それぞれ$\Sigma_{A\to B}, \Sigma_{B\to A}$と表記する) であるとき, $\Pi = (PM_A, PM_B, GSI(\subseteq SI_A \times SI_B \times \Sigma^*_{B\to A} \times \Sigma^*_{A\to B}))$ をプロトコルと呼ぶ. 4字組 $\langle s_A, s_B, ch_{B\to A}, ch_{A\to B} \rangle \in S_A \times S_B \times \Sigma^*_{B\to A} \times \Sigma^*_{A\to B}$ をプロトコルΠの系の状態と呼ぶ. GSIはΠの系の状態の部分集合でありΠの系の初期状態集合である.

ある $e \in \Sigma_{B\to A}$または $e \in \Sigma_{A\to B}$に対して, 以下の (1)〜(4) の少なくとも1つが成立するとき, $gs' = \langle s'_A, s'_B, ch'_{B\to A}, ch'_{A\to B} \rangle$ は, $gs = \langle s_A, s_B, ch_{B\to A}, ch_{A\to B} \rangle$ から遷移可能であるという ($gs \to gs'$で表す).

$$\langle s_A, e, s'_A \rangle \in T_A \ \wedge \ s'_B = s_B \ \wedge \ ch'_{B\to A} = ch_{B\to A} \ \wedge \ ch'_{A\to B} = ch_{A\to B} \cdot e; \quad (1)$$

$$\langle s_A, e, s'_A\rangle \in T_A \ \wedge\ s'_B = s_B \ \wedge \\ e\cdot ch'_{B\to A} = ch_{B\to A} \ \wedge\ ch'_{A\to B} = ch_{A\to B}; \quad (2)$$

$$s'_A = s_A \ \wedge\ \langle s_B, e, s'_B\rangle \in T_B \ \wedge \\ ch'_{B\to A} = ch_{B\to A}\cdot e \ \wedge\ ch'_{A\to B} = ch_{A\to B}; \quad (3)$$

$$s'_A = s_A \ \wedge\ \langle s_B, e, s'_B\rangle \in T_B \ \wedge \\ ch'_{B\to A} = ch_{B\to A} \ \wedge\ e\cdot ch'_{A\to B} = ch_{A\to B}. \quad (4)$$

上式の (1) または (2)((3) または (4)) の条件が成立するとき, PM_A (PM_B) はイベント e の実行者であるといい, これを $gs \xrightarrow[A]{e} gs'$ ($gs \xrightarrow[B]{e} gs'$) と表記する. また "$\to$" の反射推移閉包を "$\overset{*}{\to}$" で表し, $gs \overset{*}{\to} gs'$ ならば gs' は gs から到達可能であるという. □

定義 2.3 プロトコルΠに対して, 系の状態 gs が系の初期状態から到達可能ならば, gs はΠにおいて到達可能であるという. 到達可能な系の状態の集合をΠの可達集合と呼び, $RS(\Pi)$ と表す. $gs = \langle s_A, s_B, x, y\rangle$ は $s_A \in SE_A, s_B \in SE_B$ であるとき系の終了状態という. またΠの系の初期状態から到達可能な系の終了状態の集合を $EX(\Pi)$ で表す. Πの可達集合が以下の (P1), (P2) のような状態を含まないとき, かつそのときに限りΠは安全であるという.

(P1) 空チャネルデッドロック状態:
系の状態 $gs = \langle s_A, s_B, \epsilon, \epsilon\rangle$ は,
(1) $s_A \notin SE_A$ かつ $\forall_{e\in\Sigma_{A\to B}}\{\delta_A(s_A, e) = \phi\}$, かつ
(2) $s_B \notin SE_B$ かつ $\forall_{e\in\Sigma_{B\to A}}\{\delta_B(s_B, e) = \phi\}$
であるとき空チャネルデッドロック状態であるという.

(P2) 未定義受信状態:
系の状態 $gs = \langle s_A, s_B, x, y\rangle$ は,
(1) $s_A \notin SE_A$ かつ $\delta_A(s_A, \mathrm{first}(x)) = \phi$ または
(2) $s_B \notin SE_B$ かつ $\delta_B(s_B, \mathrm{first}(y)) = \phi$
(ここで $\mathrm{first}(x)$ は系列 x の先頭要素を表し, $\mathrm{first}(\epsilon) = \epsilon$とする.)
であるとき未定義受信状態であるという. □

2.2 ECFSMs モデル

プロトコル機械のクラスに制限を加えることにより, CSMs のサブクラスが定義できる. CSMs の重要なサブクラスの一つに Extended Communicating Finite State Machines(以下 ECFSMs) があり, このモデルに基づいて通信プロトコルの形式的記述言語である SDL[6] などが規定されている. 筆者らは用いるデータ型を非負整数に限定し, プロトコル機械の定義を以下のように定めたモデルのプロトコルの検証法を提案している[1][2].

定義 2.4 プロトコル機械 PM は以下の M1-M5 を満たす 5 字組 (S, Σ, T, SI, SE) によって定義される.

M1: $S = \langle S_F, r\rangle$ はプロトコル機械の状態集合を定義する 2 字組. S_F は有限制御部の取り得る状態の有限集合, rは非負整数値を保持するレジスタ数を表す. プロトコル機械の取り得る状態集合は $S_F \times \mathcal{N}^r$($\mathcal{N}$は非負整数の集合) となる.

M2: $\Sigma = \Sigma_- \cup \Sigma_+$は送受信するメッセージ型の有限集合. Σ_-, Σ_+はそれぞれ送信メッセージ型, 受信メッセージ型の集合を表す. メッセージはメッセージ型 d と非負整数値パラメータ n の 2 字組 $\langle d, n\rangle$ で表される.

M3: Tはアクションの集合. 各アクション $t(\in T)$ は状態遷移の集合を定義する 5 字組 $(s_{F1_t}, d_t, s_{F2_t}\ C_t, R_t)$. $s_{F1_t} \in S_F, d_t \in \Sigma, s_{F2_t} \in S_F$. C_tは送受信されるメッセージのパラメータ値 n とプロトコル機械のレジスタ値 $p_1, p_2, \ldots, p_r$に関する連立不等式で, t が実行できるための条件を表す. R_tは遷移後のレジスタ値を定義するための $\mathcal{N}^r \times \mathcal{N}$から $\mathcal{N}^r$への部分関数. 状態 $s = (s_F, p_1, p_2, \ldots, p_r)$ において, あるアクション $t = (s_{F1_t}, d_t, s_{F2_t}, C_t, R_t)$ に対して, $s_F = s_{F1_t}$かつ $p_1, p_2, \ldots, p_r, n$ が C_tを満たすならば, メッセージ $\langle d_t, n\rangle$ の送信または受信が可能であり, 状態 $s' = (s_{F2_t}, R_t(p_1, p_2, \ldots, p_r, n))$ に遷移する. Tにより, $S_F \times \mathcal{N}^r \times \langle\Sigma \times \mathcal{N}\rangle$ から $S_F \times \mathcal{N}^r$への非決定性状態遷移関数δは以下のように定まる.

$$\delta((s_F, p_1, p_2, \ldots, p_r), \langle d, n\rangle) = \\ \{(s'_F, R(p_1, p_2, \ldots, p_r, n)) \mid \\ (s_F, d, s'_F, C, R) \in T \ \wedge \\ (p_1, p_2, \ldots, p_r, n \text{ は } C\text{を満たす})\}$$

M4: $SI \subseteq S_F$はプロトコル機械の初期状態集合.

M5: $SE \subseteq S_F$は終了状態集合を定義するプロトコル機械の有限制御部の集合. $s_F \in SE$ ならば, あらゆる $p_1, p_2, \ldots, p_r$ に対して $(s_F, p_1, p_2, \ldots, p_r)$ は終了状態であると定義する. 但し d, s'_F, C, R に対して (s_F, d, s'_F, C, R) なるアクションは T中に存在しないものとする. □

2.3 プロトコル系列

2-CSMs の動作を記述するために, 系の状態遷移系列とプロトコル系列[7]を導入する. なお補題 2.1, 補題 2.2 の証明については文献 [7] を参照. 以下では系列 F, F'に関して次のような表記法を用いる. F'が Fの接頭語であることを $F' \sqsubseteq F$ によって表す. $F' \backslash F$は, $F' \sqsubseteq F$ならば Fから接頭語 F'を取り除くことによって得られる Fの接尾語を表す. また Fの i 番目の要素を $F[i]$ で表し, $F[i, j]$ は Fの i 番目の要素から j番目の要素までからなる Fの連続する部分系列を表す. さらに Xのスーパーセット上の系列 Fに対して $sub_X(F)$ 及び $\mathcal{O}_X(F)$ は, それぞれ, Xの要素のみからなる Fの部分列, インデックスの集合 $\{i \mid F[i] \in X\}$ を表す. $i, j \in \mathcal{O}_X(F)$ に対して, $i < j$ かつ $i < h < j$であるような整数 $h \in \mathcal{O}_X(F)$ が存在しないとき, "$i \lessdot_{(F,X)} j$" と表記する.

2.3.1 系の状態遷移系列

定義 2.5 プロトコル機械 $PM = (S, \Sigma, T, SI, SE)$ に対して, $t_1 \cdot \ldots \cdot t_n \in T^*$は, $\forall_{1\le i\le n-1}\{s'_i = s_{i+1}\}$(ここで $t_k = \langle s_k, e_k, s'_k\rangle$) ならば, PMの s_1-状態遷移系列という. 状態遷移系列 $Q = t_1 \cdot \ldots \cdot t_n$(ここで $t_k = \langle s_k, e_k, s'_k\rangle$) に対して, $s(Q)$ は Q の状態部分の系列 $s'_1 \cdot \ldots \cdot s'_n$を, $e(Q)$ は Q のイベント部分の系列 $e_1 \cdot \ldots \cdot e_n$をそれぞれ表す. □

定義 2.6 プロトコルΠ $= (PM_A, PM_B, GSI)$ に対して, 系の状態の系列 $G = gs_0 \cdot \ldots \cdot gs_n$は, $gs_0 \in GSI$ かつ $\forall_{1 \le i \le n}\{gs_{i-1} \rightarrow gs_i\}$ ならば Π の系の状態遷移系列という. またある gs_jに対して $G_j = gs_j \cdot \ldots \cdot gs_n$は, $\forall_{j<i \le n}\{gs_{i-1} \rightarrow gs_i\}$ ならば Π の gs_j-系の状態遷移系列という. 以下各 i に対して $gs_i = \langle s_{A,i}, s_{B,i}, ch_{B\to A,i}, ch_{A\to B,i}\rangle$ とする. 系の状態遷移系列 $G = gs_0 \cdot \ldots \cdot gs_n$に対して, $gs_{i-1} \xrightarrow[p_i]{e_i} gs_i$となる G の i 番目のイベント e_i及び i 番目の実行者 p_iは一意に定まる. G の状態遷移系列を $\langle s_{p_1,0}, e_1, s_{p_1,1}\rangle \cdot \ldots \cdot \langle s_{p_n,n-1}, e_n, s_{p_n,n}\rangle$ と定義し $Q(G)$ で表す.

$P = A$(または B) に対して, $Q_P(G)$ は $sub_P(Q(G))$ を表す. $Q_P(G)$ は $Q(G)$ の P上への射影という. 定義より $Q_P(G)$ は PM_Pの $s_{P,0}$-状態遷移系列である. □

以下の補題は系の状態遷移系列の基本的な性質を表す.

補題 2.1 $G = gs_0 \cdot \ldots \cdot gs_n$をプロトコルΠ $= (PM_A, PM_B, GSI)$ の系の状態遷移系列, $Q_A = Q_A(G)$, $Q_B = Q_B(G)$, $\bar{e}_A = ch_{A\to B,0} \cdot e(Q_A)$, $\bar{e}_B = ch_{B\to A,0} \cdot e(Q_B)$ とする.

(i) 以下の関係が成立する.

CH1: $sub_{\Sigma_{B\to A}}(\bar{e}_A) \sqsubseteq sub_{\Sigma_{B\to A}}(\bar{e}_B)$ かつ
$ch_{B\to A,n} = sub_{\Sigma_{B\to A}}(\bar{e}_A) \backslash sub_{\Sigma_{B\to A}}(\bar{e}_B)$,

CH2: $sub_{\Sigma_{A\to B}}(\bar{e}_B) \sqsubseteq sub_{\Sigma_{A\to B}}(\bar{e}_A)$ かつ
$ch_{A\to B,n} = sub_{\Sigma_{A\to B}}(\bar{e}_B) \backslash sub_{\Sigma_{A\to B}}(\bar{e}_A)$.

(ii) $i \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_A)$ $(\mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_B))$ に対して, 以下の PS1 から PS3 を満たすただ 1 つの正整数$\varphi_{B\to A}(i)$ $(\varphi_{A\to B}(i)) \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_B)$ $(\mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_A))$ が存在する

PS1: $i \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_A)$ $(\mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_B))$ ならば
$\bar{e}_A(i) = \bar{e}_B(\varphi_{B\to A}(i))$
$(\bar{e}_B(i) = \bar{e}_A(\varphi_{A\to B}(i)))$.

PS2: $i,j \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_A)$ $(\mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_B))$ かつ
$i \leqslant_{(\bar{e}_A, \Sigma_{B\to A})} j$ $(i \leqslant_{(\bar{e}_B, \Sigma_{A\to B})} j)$ ならば
$\varphi_{B\to A}(i) \leqslant_{(\bar{e}_B, \Sigma_{B\to A})} \varphi_{B\to A}(j)$
$(\varphi_{A\to B}(i) \leqslant_{(\bar{e}_A, \Sigma_{A\to B})} \varphi_{A\to B}(j))$.

PS3: $i \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_A)$, $h \in \mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_B)$ かつ
$i < \varphi_{A\to B}(h)$ $(h < \varphi_{B\to A}(i))$ ならば
$\varphi_{B\to A}(i) < h$ $(\varphi_{A\to B}(h) < i)$. □

2.3.2 プロトコル系列

以下では, 可達集合の解析を行う上で有用な手段となるプロトコル系列の概念を導入する.

定義 2.7 PM_Aの s_A-状態遷移系列 Q_A, PM_Bの s_B-状態遷移系列 Q_B, $ch_{B\to A} \in \Sigma^*_{B\to A}$, $ch_{A\to B} \in \Sigma^*_{A\to B}$ に対して, $ch_{B\to A,0} = ch_{B\to A}$, $ch_{A\to B,0} = ch_{A\to B}$ とすることによって Q_A及び Q_Bが補題 2.1(ii) を満たすならば, $\langle Q_A, Q_B\rangle$ はΠ $= (PM_A, PM_B, GSI)$ の $\langle s_A, s_B, ch_{B\to A}, ch_{A\to B}\rangle$-プロトコル系列と呼ぶ. 以下では, $\langle Q_A, Q_B\rangle$ がある系の状態 gs に対する gs-プロトコル系列ならば, $\langle Q_A, Q_B\rangle$ を単にプロトコル系列という. □

補題 2.2 $\langle Q_A, Q_B\rangle$ をΠの gs-プロトコル系列とする. $Q_A(G) = Q_A$かつ $Q_B(G) = Q_B$なる gs-系の状態遷移系列 G が存在する. □

$\langle s_A, s_B, x, y\rangle$-プロトコル系列 $\langle Q_A, Q_B\rangle$(ここで $Q_A = t_{A,1} \cdot \ldots \cdot t_{A,l}$, $Q_B = t_{B,1} \cdot \ldots \cdot t_{B,m}$) に対して, 補題 2.1(i) 及び補題 2.2から, 系の状態遷移系列

$\langle s_A, s_B, x, y\rangle \cdot \ldots \cdot \langle s'_{A,l}, s'_{B,m}, ch_{B\to A}, ch_{A\to B}\rangle$

が存在する. 但し

$ch_{B\to A} = sub_{\Sigma_{B\to A}}(e(Q_A)) \backslash sub_{\Sigma_{B\to A}}(x \cdot e(Q_B))$

$ch_{A\to B} = sub_{\Sigma_{A\to B}}(e(Q_B)) \backslash sub_{\Sigma_{A\to B}}(y \cdot e(Q_A))$

このとき系の状態 $\langle s'_{A,l}, s'_{B,m}, ch_{B\to A}, ch_{A\to B}\rangle$ は $\langle s_A, s_B, x, y\rangle$ から $\langle Q_A, Q_B\rangle$ の実行によって到達可能であるといい, $GS(\langle Q_A, Q_B\rangle, \langle s_A, s_B, x, y\rangle)$ と表す. $GS(\langle Q_A, Q_B\rangle, gs_0)$(ここで $gs_0 \in GSI$) を単に $GS(\langle Q_A, Q_B\rangle)$ と表記することもある.

プロトコル系列に関して以下の性質が成り立つ.

補題 2.3 $\langle Q_A, Q_B\rangle$ を $gs_0(= \langle s_A, s_B, x, y\rangle)$-プロトコル系列とする. このとき以下の性質及びそれらの A, Bを入れ換えた性質が成り立つ.

(1) Q''_Aが受信遷移のみからなる状態遷移系列であり, $Q_A = Q'_A \cdot Q''_A$ならば, $\langle Q'_A, Q_B\rangle$ も gs_0-プロトコル系列である.

(2) 補題 2.1と同様の$\bar{e}_A, \varphi_{B\to A}$に対して
$i \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_A)$ ならば $\langle Q_A[1, (i - |y|) - 1], Q_B[1, (\varphi_{B\to A}(i) - |x|) - 1]\rangle$ も gs_0-プロトコル系列である. ここで i は Q_A系列中の $i - |y|$ 番目の受信イベントを, $\varphi_{B\to A}(i)$ は Q_A系列中の $i - |y|$ 番目の送信イベントを表している.

[略証] ともに補題 2.1の (ii) において, $\langle Q_A, Q_B\rangle$ の $\varphi_{B\to A}, \varphi_{A\to B}$の定義域を縮小した関数を考えることにより PS2,PS3 の成立は明らか. $\langle Q'_A, Q_B\rangle$ については PS1 も $\langle Q_A, Q_B\rangle$ の PS1 の必要条件となっているので gs_0-プロトコル系列である. $\langle Q_A[1, i-1-|y|], Q_B[1, \varphi_{B\to A}(i) - 1 - |x|]\rangle$ の PS1 は, $\langle Q_A, Q_B\rangle$ の PS3 より $j < \varphi_{B\to A}(i)$ ならば$\varphi_{A\to B}(j) < i$ が成り立つことより示される. □

3 フェーズ

3.1 フェーズの定義とその合成

ここではフェーズと呼ばれるプロトコルのクラスを定義する. さらに 2 つのフェーズを合成して得られるプロトコルを定義し, 合成されたプロトコルがフェーズとなるための十分条件を示す.

定義 3.1 Π $= (PM_A, PM_B, GSI)$ は以下の条件を満たすときフェーズであるという.

(1) Πの任意の gs_0-プロトコル系列 $\langle Q_A, Q_B\rangle$(但し $GS(\langle Q_A, Q_B\rangle) = \langle s_A, s_B, ch_{B\to A}, ch_{A\to B}\rangle$ とする) に対して,

$s_A \in SE_A$ならば, $GS(\langle Q_A, Q_B \cdot Q'_B\rangle) \in EX(\Pi)$ なる Q'_B が存在する.

$s_B \in SE_B$ならば, $GS(\langle Q_A \cdot Q'_A, Q_B\rangle) \in EX(\Pi)$ なる Q'_A が存在する.

(2) $s_A \in SE_A$ かつ $\langle s_A, s_B, ch_{B\to A}, \varepsilon\rangle \in RS(\Pi)$
ならば $s_B \in SE_B$
$s_B \in SE_B$ かつ $\langle s_A, s_B, \varepsilon, ch_{A\to B}\rangle \in RS(\Pi)$
ならば $s_A \in SE_A$
($EX(\Pi)$, $RS(\Pi)$ については定義 2.3参照) □

定義 3.2 $\Pi_1 = (PM_{1_A}, PM_{1_B}, GSI_1)$, $\Pi_2 = (PM_{2_A}, PM_{2_B}, GSI_2)$ をプロトコル, $\sigma = \langle\sigma_A, \sigma_B\rangle$ を SE_{1_A} から SI_{2_A} への部分関数σ_Aと SE_{1_B} から SI_{2_B} への部分関数σ_Bの2字組とする. Π_1, Π_2をσによって合成した$\Pi = \langle\Pi_1, \sigma, \Pi_2\rangle = (PM_A, PM_B, GSI)$ を以下のように定義する. (ここで $S_{1_P} \cap S_{2_P} = \phi$とする)
$PM_P = (S_P, \Sigma, T_P, SI_P, SE_P)(P \in \{A, B\})$ を以下のように定める.

$S_P = (S_{1_P} - \{s \in SE_{1_P} \mid \sigma_P(s)$ が定義されている $\})$
$\cup\, S_{2_P}$

$\Sigma = \Sigma_1 \cup \Sigma_2$

$T_P = \{\langle s, e, s'\rangle \in T_{1_P} \mid (s' \notin SE_{1_P}$ または$\sigma_P(s')$ が未定義)$\}\cup$
$\{\langle s, e, \sigma_P(s')\rangle \mid \langle s, e, s'\rangle \in T_{1_P}$かつ$\sigma_P(s')$ が定義されている $\} \cup T_{2_P}$

$SI_P = SI_{1_P}$

$SE_P = (SE_{1_P} - \{s' \in SE_{1_P} \mid \langle s, e, s'\rangle \in T_{1_P}$かつ
$\sigma(s')$ が定義されている $\}) \cup SE_{2_P}$

また, Πの系の初期状態集合は $GSI = GSI_1$とする. □

以下では$\sigma = \langle\sigma_A, \sigma_B\rangle$ を以下のように拡張して用いる. 系の状態 $\langle s_A, s_B, x, y\rangle$ に対して$\sigma(\langle s_A, s_B, x, y\rangle)$ は
$\sigma(\langle s_A, s_B, x, y\rangle)$

$$= \begin{cases} \langle\sigma_A(s_A), \sigma_B(s_B), x, y\rangle & (\sigma_A(s_A), \sigma_B(s_B) \text{ ともに} \\ & \text{定義されている場合}) \\ \text{未定義} & (\text{それ以外の場合}) \end{cases}$$

と定義する. また系の状態集合 Sに対して$\sigma(S)$ を
$\sigma(S) = \{\sigma(s) | s \in S$ かつ$\sigma(s)$ が定義されている $\}$
と定義する.

次の補題 3.1は, PM_A(または PM_B) がΠ_2の状態で送信したメッセージを, PM_B(または PM_A) はΠ_1の状態で受信することがないことを表している.

補題 3.1 $\Pi_1 = (PM_{1_A}, PM_{1_B}, GSI_1)$, $\Pi_2 = (PM_{2_A}, PM_{2_B}, GSI_2)$, $\sigma = \langle\sigma_A, \sigma_B\rangle$ に対して, $\langle s_A, s_B, x, y\rangle \in EX(\Pi_1)$ かつ$\sigma_A(s_A)$,$\sigma_B(s_B)$ の少なくとも一方が定義されているならば他方も定義されており, $\sigma(\langle s_A, s_B, x, y\rangle) \in GSI_2$であるとする.

このとき$\Pi = \langle\Pi_1, \sigma, \Pi_2\rangle = (PM_A, PM_B, GSI)$ の任意の $gs_0(\in GSI)$-プロトコル系列 $\langle Q_A, Q_B\rangle$ について以下が成り立つ.

(1) $i \in \mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_B)$ かつ $s_{B,i-1} \in S_{1_B}$ならば
$s_{A,\varphi_{A\to B}(i)-1} \in S_{1_A}$
(2) $i \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_A)$ かつ $s_{A,i-1} \in S_{1_A}$ならば
$s_{B,\varphi_{B\to A}(i)-1} \in S_{1_B}$

ここで,
$gs_0 = \langle s_{A,0}, s_{B,0}, ch_{B\to A,0}, ch_{A\to B,0}\rangle \in GSI$,
$\bar{e}_A = ch_{A\to B,0} \cdot e(Q_A)$,
$\bar{e}_B = ch_{B\to A,0} \cdot e(Q_B)$,
$\varphi_{A\to B}, \varphi_{B\to A}$ は補題 2.1(ii) を満たす関数
とする.

[証明] $|ch_{A\to B,0}| = a, |ch_{B\to A,0}| = b$ とする. $i \in \mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_B)$, $s_{B,i-1} \in S_{1_B}$かつ $s_{A,\varphi_{A\to B}(i)-1} \in S_{2_A}$を満たす最小の iが存在すると仮定し, $j = \varphi_{A\to B}(i) - 1$ とする. このとき補題 2.3の (1) より $\langle Q_A[1, j-a], Q_B[1, i-1-b]\rangle$ もまた gs_0-プロトコル系列である. さらに $s_{A,j} \in S_{2_A}$であることと PM_Aの定義より, $s_{A,k-1} \in S_{1_A}$かつ $s_{A,k} \in S_{2_A}$であるような $k(\leq j)$ がただ一つ存在する. iの最小性と$\varphi_{A\to B}$についての補題 2.1PS2 より, $k < k' \leq j$に対して $k' \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_A)$ なので, 特に $k' = k+1$ の場合を考えると, 補題 2.3の (2) より $\langle Q_A[1, k-a], Q_B[1, i-1-b]\rangle$ もまた gs_0-プロトコル系列であることが分かる.

ここで $k \leq j = \varphi_{A\to B}(i) - 1$ より $sub_{\Sigma_{A\to B}}(\bar{e}_A[1,k]) \sqsubseteq sub_{\Sigma_{A\to B}}(\bar{e}_A[1,j]) = sub_{\Sigma_{A\to B}}(\bar{e}_B[1,i-1])$. 一方 $\langle Q_A[1,k-a], Q_B[1,i-1-b]\rangle$ が gs_0-プロトコル系列であることより $sub_{\Sigma_{A\to B}}(\bar{e}_B[1,i-1]) \sqsubseteq, sub_{\Sigma_{A\to B}}(\bar{e}_A[1,k])$ なので $sub_{\Sigma_{A\to B}}(\bar{e}_A[1,k]) = sub_{\Sigma_{A\to B}}(\bar{e}_B[1,i-1])$ となる. よってある $x \in \Sigma^*_{B\to A}$を用いて $GS(\langle Q_A[1,k-a], Q_B[1,i-1-b]\rangle, gs_0) = \langle s_{A,k-a}, s_{B,i-1-b}, x, \varepsilon\rangle$ と書ける. Πの定め方より $\langle\sigma^{-1}(s_{A,k-a}), s_{B,i-1-b}, x, \varepsilon\rangle \in RS(\Pi)$ かつ$\sigma^{-1}(s_{A,k-a}) \in SE_{1_A}$及び $s_{B,i-1-b} \notin SE_B$ が成り立つので, フェーズとしての条件 2. を満たさず, Π_1がフェーズであるという前提に反する.

$i \in \mathcal{O}_{\Sigma_{B\to A}}(\bar{e}_A)$, $s_{A,i-1} \in S_{1_A}$かつ $s_{B,\varphi_{B\to A}(i)-1} \in S_{2_B}$を満たす最小の iが存在すると仮定した場合も同様にして矛盾が導かれる. □

補題 3.2 $\Pi_1 = (PM_{1_A}, PM_{1_B}, GSI_1)$, $\Pi_2 = (PM_{2_A}, PM_{2_B}, GSI_2)$ をフェーズ, $\sigma = \langle\sigma_A, \sigma_B\rangle$ は補題 3.1の条件を満たすものとする.

$\langle Q_A, Q_B\rangle$ をΠの任意の gs_0-プロトコル系列とし,
$gs_0 = \langle s_{A,0}, s_{B,0}, ch_{B\to A,0}, ch_{A\to B,0}\rangle \in GSI$
$Q_A = \langle s_{A,0}, e_{A,1}, s_{A,1}\rangle \cdot \ldots \cdot \langle s_{A,m-1}, e_{A,m}, s_{A,m}\rangle$
$Q_B = \langle s_{B,0}, e_{B,1}, s_{B,1}\rangle \cdot \ldots \cdot \langle s_{B,n-1}, e_{B,n}, s_{B,n}\rangle$
$\bar{e}_A = ch_{A\to B,0} \cdot e(Q_A)$
$\bar{e}_B = ch_{B\to A,0} \cdot e(Q_B)$
とする. このとき $s_{A,m} \in S_{2_A}$, $s_{B,n} \in S_{2_B}$ならば, $\sigma_A^{-1}(s_{A,i}) \in SE_{1_A}$, $\sigma_B^{-1}(s_{B,j}) \in SE_{1_B}$ かつ $GS(\langle Q_A[1,i], Q_B[1,j]\rangle, gs_0) \in GSI_2$なる (i,j) がただ1つ存在する.

[証明] Πの定義から, $s(Q_A), s(Q_B)$ それぞれの系列中に $\sigma_A^{-1}(s_{A,i}) \in SE_{1_A}$, $\sigma_B^{-1}(s_{B,j}) \in SE_{1_B}$ なる $s_{A,i}, s_{B,j}$がそれぞれただ1つずつ存在する. $\langle Q_A[1,i], Q_B[1,j]\rangle$ が gs_0-プロトコル系列であるための条件補題 2.1(ii) の中で PS2,PS3 の成立は $\langle Q_A, Q_B\rangle$ の$\varphi_{B\to A}, \varphi_{A\to B}$の定義域を縮小した関数を考えることにより明らか.

補題 3.1より, $j' \in \mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_B)$ かつ $s_{B,j'-1} \in S_{1_B}$ ならば $s_{A,\varphi_{A\to B}(j')-1} \in S_{1_A}$である. i,jの一意性より, $j' \in \mathcal{O}_{\Sigma_{A\to B}}(\bar{e}_B)$ かつ $j' \le j + |ch_{BA,0}|$ ならば$\varphi_{A\to B}(j') \le i + |ch_{AB,0}|$ (A を Bと入れ換えた場合も同様) が成り立つ. このことよりPS1も成立し, $\langle Q_A[1,i], Q_B[1,j]\rangle$ が gs_0-プロトコル系列であることがわかる.

$GS(\langle Q_A[1,i], Q_B[1,j]\rangle, gs_0) = \langle s_{A,i}, s_{B,j}, x, y\rangle$ とおくと, Πの定義から $(\sigma^{-1}(s_{A,i}), \sigma^{-1}(s_{B,j}), x, y) \in RS(\Pi_1)$ なので, σに関する条件より $\langle s_{A,i}, s_{B,j}, x, y\rangle \in GSI_2$. □

定理 3.1 $\Pi_1 = (PM_{1_A}, PM_{1_B}, GSI_1)$, $\Pi_2 = (PM_{2_A}, PM_{2_B}, GSI_2)$ をフェーズとし, $\sigma = \langle \sigma_A, \sigma_B\rangle$ は補題 3.1の条件を満たすものとする. このとき$\Pi = \langle \Pi_1, \sigma, \Pi_2\rangle = (PM_A, PM_B, GSI)$ はフェーズである.

[証明] 定義 3.1の (1),(2) が成立することを個々に示す.

[A: 定義 3.1の (1) が成立することの証明]

$gs_0 \in GSI$, $GS(\langle Q_A, Q_B\rangle, gs_0) = \langle s_A, s_B, ch_{B\to A}, ch_{A\to B}\rangle$, $s_A \in SE_A, s_B \notin SE_B$である任意の$\Pi$ の gs_0-プロトコル系列 $\langle Q_A, Q_B\rangle$ に対して, $GS(\langle Q_A, Q_B \cdot Q'_B\rangle, gs_0) \in EX(\Pi)$ なる状態遷移系列 Q'_Bが存在することを示す. ($s_B \in SE_B, s_A \notin SE_A$の場合においても所期の Q'_Aが存在することを同様に示せる.)

$gs_0 = \langle s_{A,0}, s_{B,0}, ch_{B\to A,0}, ch_{A\to B,0}\rangle$,

$Q_A = \langle s_{A,0}, e_{A,1}, s_{A,1}\rangle \cdot \ldots \cdot \langle s_{A,m-1}, e_{A,m}, s_A\rangle$,

$Q_B = \langle s_{B,0}, e_{B,1}, s_{B,1}\rangle \cdot \ldots \cdot \langle s_{B,n-1}, e_{B,n}, s_B\rangle$,

s_Aが SE_{1_A}, SE_{2_A}, s_Bが S_{1_B}, S_{2_B}のそれぞれどちらに属するかによって以下の4通りの場合が考えられる.

(A1) $s_A \in SE_{1_A}, s_B \in S_{1_B}$である場合

Πの定義から $s_A \in SE_{1_A}$であるのは, $\sigma_A(s_A)$ が未定義のときかつそのときに限る. $\langle Q_A, Q_B\rangle$ はΠ_1 の gs_0-プロトコル系列でもあるから $GS(\langle Q_A, Q_B \cdot Q'_B\rangle, gs_0) = \langle s_A, s'_B, x, y\rangle \in EX(\Pi_1)$ なる Q'_Bが存在する. 補題 3.1のσの条件と$\sigma_A(s_A)$ が未定義であることよりσ$_B(s'_B)$ も未定義となり, $GS(\langle Q_A, Q_B \cdot Q'_B\rangle, gs_0) \in EX(\Pi)$ が成り立つ.

(A2) $s_A \in SE_{1_A}, s_B \in S_{2_B}$である場合

Πの定義から, $s(Q_B)$ の系列中に$\sigma_B^{-1}(s_{B,j}) \in SE_{1_B}$ なる $s_{B,j}$がただ1つ存在する. このときσの条件から$\sigma(s_A) \in SI_{2_A}$であり, $s_A \in SE_{1_A}$であることに反する. よってこのような場合は存在しない.

(A3) $s_A \in SE_{2_A}, s_B \in S_{1_B}$である場合

Πの定義から, $s(Q_A)$ の系列中に$\sigma_A^{-1}(s_{A,i}) \in SE_{1_A}$ なる $s_{A,i}$がただ1つ存在する. まず $\langle Q_A[1,i], Q_B\rangle$ が gs_0-プロトコル系列であることを示す. 補題 2.1の (ii) において $\langle Q_A, Q_B\rangle$ の$\varphi_{B\to A}, \varphi_{A\to B}$の定義域を縮小した関数を考えることにより PS2,PS3 の成立は明らか. 補題 3.1より, $j \in \mathcal{O}_{\Sigma_{A\to B}}(ch_{A\to B,0} \cdot e(Q_B))$ に対して, $\varphi_{A\to B}(j) \le i + |ch_{B\to A,0}|$ であるからPS1 を満たし, $\langle Q_A[1,i], Q_B\rangle$ は gs_0-プロトコル系列である. Π_1はフェーズであるので, σの条件から $\langle Q_A[1,i], Q_B \cdot Q'_B\rangle = gs' \in GSI_2$なる Q'_Bが存在する.

次に $\langle Q_A, Q_B \cdot Q'_B\rangle$ を考えると $\langle Q_A, Q_B\rangle$ が gs_0-プロトコル系列であるから, $e(Q'_B)$ 系列中の送信イベントに対する受信イベントは $e(Q_A[i+1,m])$ 系列中に存在せず, $\langle Q_A, Q_B \cdot Q'_B\rangle$ は gs_0- プロトコル系列であることが示される. よって $\langle Q_A[i+1,m], \varepsilon\rangle$ はΠ_2の gs'-プロトコル系列であり, Π_2はフェーズであるから $GS(\langle Q_A[i+1,m], Q''_B\rangle, gs') \in EX(\Pi_2)$ である Q''_Bが存在し, そのような Q''_Bに対しては $GS(\langle Q_A, Q_B \cdot (Q'_B \cdot Q''_B)\rangle, gs_0) \in EX(\Pi)$ となる.

(A4) $s_A \in SE_{2_A}, s_B \in S_{2_A}$である場合

補題 3.2より$\sigma_A^{-1}(s_{A,i}) \in SE_{1_A}, \sigma_B^{-1}(s_{B,j}) \in SE_{1_B}$ かつ $GS(\langle Q_A[1,i], Q_B[1,j]\rangle, gs_0) = gs' \in GSI_2$ なる i,jがそれぞれただ1つずつ存在する.

Π_2はフェーズであるから gs'-プロトコル系列 $\langle Q_A[i+1,m], Q_B[j+1,n]\rangle$ に対して $GS(\langle Q_A[i+1,m], Q_B[j+1,n] \cdot Q'_B\rangle, gs') \in EX(\Pi_2)$ なる Q'_Bが存在する. Πの定義から, そのような Q'_Bに対しては, $GS(\langle Q_A, Q_B \cdot Q'_B\rangle, gs') \in EX(\Pi)$ となる.

[B: 定義 3.1の (2) が成立することの証明]

$gs = \langle s_A, s_B, x, \varepsilon\rangle \in RS(\Pi)$, $s_A \in SE_A$, $s_B \notin SE_B, x \in \Sigma^*_{B\to A}$である系の状態 gs が存在すると仮定する. ($gs = \langle s_A, s_B, \varepsilon, y\rangle \in RS(\Pi)$, $s_B \in SE_B$, $s_A \notin SE_A, y \in \Sigma^*_{A\to B}$である系の状態 gs を仮定した場合も同様にして示される.)

$gs_0 \in GSI$

$Q_A = \langle s_{A,0}, e_{A,1}, s_{A,1}\rangle \cdot \ldots \cdot \langle s_{A,m-1}, e_{A,m}, s_A\rangle$

$Q_B = \langle s_{B,0}, e_{B,1}, s_{B,1}\rangle \cdot \ldots \cdot \langle s_{B,n-1}, e_{B,n}, s_B\rangle$

$GS(\langle Q_A, Q_B\rangle, gs_0) = gs$

とする. A:と同様に以下の4通りの場合が考えられる.

(B1) $s_A \in SE_{1_A}, s_B \in S_{1_B}$である場合

Π_1はフェーズであるから, 定義 3.1の (2) より $s_B \in SE_{1_B}$である. このとき補題 3.1のσの条件から $\sigma_B(s_B)$ は未定義であり, Πにおける SE_Bの定義から $s_B \in SE_B$である. しかしながら, これは $s_B \notin SE_B$ であるという仮定に反する.

(B2) $s_A \in SE_{1_A}, s_B \in S_{2_B}$である場合

(A2) よりこのような場合は存在しない.

(B3) $s_A \in SE_{2_A}, s_B \in S_{1_B}$である場合

Πの定義から, $s(Q_A)$ の系列中に$\sigma_A^{-1}(s_{A,i}) \in SE_{1_A}$ なる $s_{A,i}$がただ1つ存在する. 補題 3.1及び gs において PM_Aから PM_Bへの通信路が空であることから $e(Q_A[i+1,m]) \in \Sigma^*_{B\to A}$である. よって補題 2.3の 1. より $\langle Q[1,i], Q_B\rangle$ も gs_0-プロトコル系列であり, $GS(\langle Q[1,i], Q_B\rangle, gs_0) = \langle s_{A,i}, s_{B,n}, x', \varepsilon\rangle$ に対して $\langle \sigma^{-1}(s_{A,i}), s_{B,n}, x', \varepsilon\rangle$ を考えると, Π_1はフェーズであるから $s_{B,n} \in SE_{1_B}$でなければならず, $s_{B,n} \notin SE_{1_B}$であることに反する.

(B4) $s_A \in SE_{2_A}, s_B \in S_{2_B}$である場合

補題 3.2より $GS(\langle Q_A[1,i], Q_B[1,j]\rangle, gs_0) = gs' \in$

GSI_2 なる i,j がそれぞれただ 1 つずつ存在する．このとき $GS(\langle Q_A, Q_B\rangle, gs_0) = GS(\langle Q_A[i+1,m], Q_B[j+1,m]\rangle, gs')$ であり，Π_2 はフェーズであることから，$s_B \in SE_{2_B}$ でなければならず，$s_B \notin SE_{2_B}$ に反する．

以上により Π がフェーズであることが示された． □

定理 3.2 $\Pi_1 = (PM_{1_A}, PM_{1_B}, GSI_1), \Pi_2 = (PM_{2_A}, PM_{2_B}, GSI_2)$ をフェーズ，$\sigma = \langle \sigma_A, \sigma_B\rangle$ は補題 3.1の条件を満たすものとする．このとき Π_1, Π_2 が安全であるならば，$\Pi = \langle \Pi_1, \sigma, \Pi_2\rangle$ も安全である．

[証明] $gs = \langle s_A, s_B, ch_{B\to A}, ch_{A\to B}\rangle \in RS(\Pi)$ であるような安全でない状態 (未定義受信状態またはデッドロック状態) gs が存在すると仮定する．

$gs_0 = \langle s_{A,0}, s_{B,0}, ch_{B\to A,0}, ch_{A\to B,0}\rangle \in GSI$,

$Q_A = \langle s_{A,0}, e_{A,1}, s_{A,1}\rangle \cdot \cdots \cdot \langle s_{A,m-1}, e_{A,m}, s_A\rangle$,

$Q_B = \langle s_{B,0}, e_{B,1}, s_{B,1}\rangle \cdot \cdots \cdot \langle s_{B,n-1}, e_{B,n}, s_B\rangle$,

$GS(\langle Q_A, Q_B\rangle, gs_0) = gs$ とする．

s_A が S_{1_A}, S_{2_A}, s_B が S_{1_B}, S_{2_B} のそれぞれどちらに属するかによって以下の 4 通りの場合が考えられる．

(1) $s_A \in S_{1_A}, s_B \in S_{1_B}$ である場合

$gs \in RS(\Pi_1)$ であり，Π_1 は安全であるから gs が安全でない状態という仮定に反する．

(2) $s_A \in S_{2_A}, s_B \in S_{1_B}$ である場合

Π の定義から，$s(Q_A)$ の系列中に $\sigma_A^{-1}(s_{A,i}) \in SE_{1_A}$ なる $s_{A,i}$ がただ 1 つ存在し，定理 3.1の証明の (A2) と同様の理由から $s_B \in SE_{1_B}$ でない．ここで定理 3.1の証明の (A3) と同様にして $\langle Q_A[1,i], Q_B\rangle$ が Π の gs_0-プロトコル系列であること，$GS(\langle Q_A[1,i], Q_B \cdot Q'_B\rangle, gs_0) = gs' \in GSI_2$ なる Q'_B が存在し，$GS(\langle Q_A, Q_B \cdot Q'_B\rangle, gs_0) = gs' \in RS(\Pi)$ であることが示される．よって $gs \xrightarrow{+} gs'$ であり gs はデッドロック状態でない．

次に，$\widehat{gs} = GS(\langle Q_A[1,i], Q_B\rangle, gs_0)$ とすると，ある $\widehat{x}, \widehat{y}$ が存在して，

$\widehat{gs} = \langle s_{A,i}, s_B, \widehat{x}, \widehat{y}\rangle \in RS(\Pi_1)$, ここで，

$ch_{A\to B} = \widehat{y} \cdot sub_{\Sigma_{A\to B}} e(Q_A[i+1,m])$

Π_1 は安全であるから $\widehat{gs}$ は未定義受信状態ではなく，

$\delta_B(s_B, \mathrm{first}(\widehat{y})) = \delta_B(s_B, \mathrm{first}(ch_{A\to B})) \neq \phi$

である．また gs' に対して，ある x', y' が存在して，

$gs' = \langle s_A, s'_B, x', y'\rangle \in RS(\Pi_2)$, ここで，

$x' = ch_{B\to A} \cdot sub_{\Sigma_{B\to A}} e(Q'_B)$

Π_2 は安全であるから gs' は未定義受信状態ではなく，$s_A \notin SE_A$ ならば

$\delta_A(s_A, \mathrm{first}(x')) = \delta_A(s_A, \mathrm{first}(ch_{B\to A})) \neq \phi$

が成り立つ．以上から gs は未定義受信状態でない．よって gs が安全でないという仮定に反する．

(3) $s_A \in S_{1_A}, s_B \in S_{2_B}$ である場合

(2) と同様．

(4) $s_A \in S_{2_A}, s_B \in S_{2_B}$ である場合

補題 3.2より $GS(\langle Q_A[1,i], Q_B[1,j]\rangle, gs_0) = gs' \in GSI_2$ なる i,j がそれぞれただ 1 つずつ存在する．このとき $GS(\langle Q_A[i+1,m], Q_B[j+1,m]\rangle, gs') = gs \in RS(\Pi_2)$ であり，Π_2 は安全であるから，gs が安全でない状態であるという仮定に反する． □

3.2 終了状態と初期状態の結合

ここでは，1 つのフェーズの終了状態と初期状態を結合したプロトコルについて議論する．

定義 3.3 $\Pi = (PM_A, PM_B, GSI)$ をプロトコル，σ を SE_A から SI_A への部分関数 σ_A と SE_B から SI_B への部分関数 σ_B の 2 字組 $\langle \sigma_A, \sigma_B\rangle$ とする．このとき，$\langle \sigma, \Pi\rangle = (PM'_A, PM'_B, GSI)$ を，以下のように定義する．

$PM'_P = (S'_P, \Sigma, T'_P, SI_P, SE'_P)(P \in \{A,B\})$ を以下のように定める．

$S'_P = S_P - \{s \in SE_P \mid \sigma_P(s)$ が定義されている $\}$

$T'_P = \{\langle s,e,s'\rangle \in T_P \mid s' \notin SE_P$ または $\sigma_P(s')$ が未定義 $\}$

$\cup \{\langle s,e,\sigma_P(s')\rangle \mid \langle s,e,s'\rangle \in T_P$ かつ $\sigma_P(s')$ が定義されている $\}$

$SE'_P = (SE_P - \{s' \in SE_P \mid \langle s,e,s'\rangle \in T_P$ かつ $\sigma(s')$ が定義されている $\})$

□

定理 3.3 $\Pi = (PM_A, PM_B, GSI)$ をフェーズ，$\sigma = \langle \sigma_A, \sigma_B\rangle$ を以下の条件を満たす SE_A から SI_A への部分関数 σ_A と SE_B から SI_B への部分関数 σ_B とする．

$\langle s_A, s_B, x, y\rangle \in EX(\Pi)$ かつ $\sigma_A(s_A), \sigma_B(s_B)$ の少なくとも一方が定義されているならば

$\langle \sigma_A(s_A), \sigma_B(s_B), x, y\rangle \in GSI$

このとき $\langle \sigma, \Pi\rangle = (PM'_A, PM'_B, GSI)$ はフェーズである．

[証明] Π に対して $\Pi_n = (PM_{n_A}, PM_{n_B}, GSI)$ $(n \geq 1)$ とする．ここで，

プロトコル機械 $PM_{n_P} = (S_{n_P}, \Sigma, T_{n_P}, SE_{n_P}, SI_{n_P})$, GSI_n $(P \in \{A,B\})$ を以下のように定義する．

$S_{n_P} = \{s_{n_P} \mid s_P \in S_P\}$

$T_{n_P} = \{\langle s_{n_P}, e, s'_{n_P}\rangle \mid \langle s_P, e, s'_P\rangle \in T_P\}$

$SE_{n_P} = \{s_{n_P} \mid s_P \in SE_P\}$

$SI_{n_P} = \{s_{n_P} \mid s_P \in SI_P\}$

$GSI_n = \{\langle s_{n_A}, s_{n_B}, x, y\rangle \mid \langle s_A, s_B, x, y\rangle \in GSI\}$

また $\sigma = \langle \sigma_A, \sigma_B\rangle$ に対して $\sigma^n = \langle \sigma_A^n, \sigma_B^n\rangle$ $(n \geq 1)$ を以下のように定義する．

$$\sigma_P^n(s_{n_P}) = \begin{cases} s'_{n+1_P} & (\sigma_P(s_P) = s'_P) \\ \text{未定義} & (\sigma_P(s_P) \text{ が未定義}) \end{cases}$$

$\langle Q_A, Q_B\rangle$ を $\langle \sigma, \Pi\rangle$ の gs_0-プロトコル系列とし，

$gs'_0 = \langle s_{A,0}, s_{B,0}, ch_{B\to A,0}, ch_{A\to B,0}\rangle \in GSI$,

$Q_A = \langle s_{A,0}, e_{A,1}, s_{A,1}\rangle \cdot \cdots \cdot \langle s_{A,m-1}, e_{A,m}, s_A\rangle$,

$Q_B = \langle s_{B,0}, e_{B,1}, s_{B,1}\rangle \cdot \cdots \cdot \langle s_{B,n-1}, e_{B,n}, s_B\rangle$,

$GS(\langle Q_A, Q_B\rangle, gs_0) = \langle s_A, s_B, x, y\rangle = gs$,

$\overline{T}_A = \{\langle s,e,\sigma_A(s')\rangle \in T'_A \mid \sigma_A(s')$ が定義されている $\}$,

$\overline{T}_B = \{\langle s,e,\sigma_B(s')\rangle \in T'_B \mid \sigma_B(s')$ が定義されている $\}$,

$i = |sub_{\overline{T}_A}(Q_A)|, j = |sub_{\overline{T}_B}(Q_B)|$,

$k = max(i,j) + 1$ とする．

このとき定義 3.1の (1),(2) が成立することを示す.

[A: 定義 3.1の (1) が成立することの証明]

$s_A \in SE'_A, s_B \notin SE'_B$とする. このとき $GS(\langle Q_A, Q_B \cdot Q'_B\rangle) \in EX(\langle \sigma, \Pi\rangle)$ なる Q'_B が存在することを示す. ($s_A \notin SE'_A, s_B \in SE'_B$の場合も同様)

$\Pi_n (n \geq 1)$ の定義及びΠがフェーズであることよりΠ_nはフェーズである. このとき

$\Pi^k = \langle\langle \ldots \langle\langle \Pi_1, \sigma^1, \Pi_2\rangle, \sigma^2, \Pi_3\rangle, \ldots,\rangle, \sigma^{k-1}, \Pi_k\rangle$

は, σの条件とσ^nの定義及び定理 3.1を繰り返し用いることによって, フェーズであることが示される.

$Q_A = Q_{1_A} \cdot Q_{2_A} \cdot \ldots \cdot Q_{i+1_A}$

$Q_B = Q_{1_B} \cdot Q_{2_B} \cdot \ldots \cdot Q_{j+1_B}$

(ここで

Q_{1_A}は Q_Aの先頭から $sub_{\overline{T}_A}(Q_A)[1]$ までの系列

Q_{2_A}は $Q_{1_A} \backslash Q_A$の先頭から $sub_{\overline{T}_A}(Q_A)[2]$ までの系列

$\vdots$

Q_{i_A}は $Q_{1_A} \cdots Q_{i-1_A} \backslash Q_A$の先頭から $sub_{\overline{T}_A}(Q_A)[i]$ までの系列

Q_{i+1_A}は $Q_{1_A} \cdots Q_{i_A} \backslash Q_A$の先頭から末尾までの系列

($Q_{l_B} (1 \leq l \leq j+1)$ についても同様)

を表す)

と表したとき, $\widehat{Q}_A, \widehat{Q}_B$を次のように定める.

$\widehat{Q}_A = \widehat{Q}_{1_A} \cdot \widehat{Q}_{2_A} \cdot \ldots \cdot \widehat{Q}_{i+1_A}$

$\widehat{Q}_B = \widehat{Q}_{1_B} \cdot \widehat{Q}_{2_B} \cdot \ldots \cdot \widehat{Q}_{j+1_B}$

ここで各 $l (1 \leq l \leq i+1)$ について,

$Q_{l_A} = \langle s_A, e, s'_A\rangle \cdot \ldots \cdot \langle \bar{s}_A, \bar{e}, \bar{s}'_A\rangle$ のとき,

$\widehat{Q}_{l_A} = \langle s_{l_A}, e, s'_{l_A}\rangle \cdot \ldots \cdot \langle \bar{s}'_{l_A}, \bar{e}, \bar{s}'_{l+1_A}\rangle \ (1 \leq l \leq i)$

$\widehat{Q}_{l_A} = \langle s_{l_A}, e, s'_{l_A}\rangle \cdot \ldots \cdot \langle \bar{s}'_{l_A}, \bar{e}, \bar{s}'_{l_A}\rangle \quad (l = i+1)$

と定義する (Q_{l_B}についても同様).

このとき, $\langle \widehat{Q}_A, \widehat{Q}_B\rangle$ はΠ^kのプロトコル系列であり, Π^kはフェーズであるから $GS(\langle \widehat{Q}_A, \widehat{Q}_B \cdot \widehat{Q}'_B\rangle) \in EX(\Pi^k)$ なる$\widehat{Q}'_B$が存在する. このとき, $\widehat{Q}'_B$に対して上述と逆の操作にを行うことによって得られる系列 Q'_Bによって $GS(\langle Q_A, Q_B \cdot Q'_B\rangle) \in EX(\langle \sigma, \Pi\rangle)$ となる.

[B: 定義 3.1の (2) が成立することの証明]

$gs = \langle s_A, s_B, x, \varepsilon\rangle \in RS(\langle \sigma, \Pi\rangle)$, $s_A \in SE'_A$, $s_B \notin SE'_B, x \in \Sigma^*_{B \to A}$である系の状態 gs が存在すると仮定する. ($gs = \langle s_A, s_B, \epsilon, y\rangle \in RS(\langle \sigma, \Pi\rangle)$, $s_B \in SE'_B$, $s_A \notin SE'_A, y \in \Sigma^*_{A \to B}$である系の状態 gs を仮定した場合も同様にして示される.)

$GS(\langle Q_A, Q_B\rangle) = gs$ なるプロトコル系列 $\langle Q_A, Q_B\rangle$ を考える. このとき Q_A, Q_Bに対して上と同様にして得られる$\widehat{Q}_A$, $\widehat{Q}_B$はΠ^kのプロトコル系列であり,$GS(\langle \widehat{Q}_A, \widehat{Q}_B\rangle) = \langle s'_A, s'_B, x', y'\rangle \in RS(\Pi^k)$ である. $\langle \widehat{Q}_A, \widehat{Q}_B\rangle$ の作り方及び各 $T_{l_A} (1 \leq l \leq i), T_{h_B} (1 \leq h \leq j)$ の定義の仕方から, $x' = x$, $y' = \epsilon$である. これはΠ^kがフェーズであることに反する. よってそのような gs は存在しない.

以上より, $\langle \sigma, \Pi\rangle$ は定義 3.1の (1),(2) をともに満たしフェーズであることが証明された. □

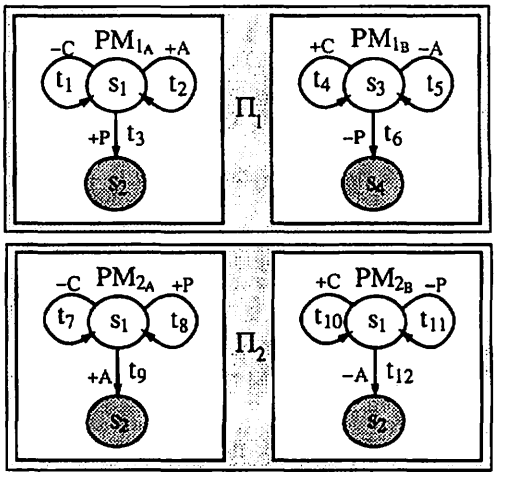

図 1: Π_1, Π_2の状態遷移図

定理 3.4 $\Pi = (PM_A, PM_B, GSI)$ をフェーズ, $\sigma = \langle \sigma_A, \sigma_B\rangle$ は定理 3.3の条件を満たすものとする. このときΠが安全性ならば $\langle \sigma, \Pi\rangle$ は安全である.

[証明] $GS(\langle Q_A, Q_B\rangle, gs_0) = gs$, $gs \notin EX(\langle \sigma, \Pi\rangle)$ であるような $\langle \sigma, \Pi\rangle$ の任意のプロトコル系列 $\langle Q_A, Q_B\rangle$ に対して, 定理 3.3から $\langle Q_A, Q_B\rangle$ に対応するΠ^kのプロトコル系列 $\langle \widehat{Q}_A, \widehat{Q}_B\rangle$ が存在し, Π^kは安全であることから容易に示すことができる. □

3.3 ECFSMs モデルにおけるフェーズとその合成例

定理 3.1において, 補題 3.1の条件を満たすσが存在すれば, 2つのフェーズをσによって合成したプロトコルもフェーズであることを示した. 以下は EFSMs でモデル化された 2 つのプロトコルΠ_1, Π_2をσによって合成したフェーズ合成の例である. このプロトコルでは, 一連番号 n の処理要求を表す $\langle C, n\rangle$, 一連番号 n までの処理要求完了の通知を表す $\langle A, n\rangle$, 一連番号 n の処理要求の受付を許可を表す $\langle P, n\rangle$ の 3 つのメッセージを用いる. Π_1, Π_2は $\langle P, n\rangle, \langle A, n\rangle$ の送受信で終了する. また以下の 3 つのレジスタを用いる.

Rc: 最大の処理要求の一連番号を保持する.

Ra: 受信確認された最大の一連番号を保持する.

Rp: 要求を許可された最大の一連番号を保持する.

[Π_1の説明]: PM_{1_A}は $Rc+1 \leq n \leq Ra+4$ の連続した連続した一連番号 n の処理要求 $\langle C, n\rangle$ を PM_{1_B}に送信する. PM_{1_B}は処理の完了した n に対して $\langle A, n\rangle$ の送信によって応答を返す. [Π_2の説明]: PM_{2_A}は $Rc+1 \leq n \leq Rp$ の連続した一連番号 n をもつ $\langle C, n\rangle$ を送信する. PM_{2_B}は $\langle P, n\rangle$ の送信により PM_{2_A}に一連番号 n までの処理要

求を許可する.

表 1,2,3 にΠ_1, Π_2の形式的定義を示す. なおΠ_1, Π_2の系の初期状態集合GSI_1, GSI_2は以下のものとする.

$GSI_1 = \{\langle (s_1, Rc_A, Ra_A, Rp_A), (s_3, Rc_B, Ra_B, Rp_B), \varepsilon, C^* \rangle \mid Ra_A = Ra_B, Rc_B \geq Ra_B, Rc_A = Rc_B + |ch_{A\to B}|\}$

$GSI_2 = \{\langle (s_6, Rc_A, Ra_A, Rp_A), (s_7, Rc_B, Ra_B, Rp_B), \varepsilon, C^* \rangle \mid Rp_A = Rp_B, Rc_B \geq Ra_B, Rc_A = Rc_B + |ch_{A\to B}|\}$

$\sigma = \langle \sigma_A, \sigma_B \rangle$ を$\sigma_A(s_2) = s_5$, $\sigma_B(s_4) = s_7$とすると, $\Pi = \langle \Pi_1, \sigma, \Pi_2 \rangle$ のアクションの集合は $T_A = \{t_1, t_2, t_3', t_7, t_8, t_9\}$, $T_B = \{t_4, t_5, t_6', t_{10}, t_{11}, t_{12}\}$ となる.

このときΠ_1, Π_2はフェーズであること, σが補題 3.1の条件を満たすこと及びΠもフェーズであることは簡単に確認できる. さらに$\widehat{\sigma} = \langle \widehat{\sigma}_A, \widehat{\sigma}_B \rangle$ を$\widehat{\sigma}_A(s_6) = s_1$, $\widehat{\sigma}_B(s_8) = s_3$とすると, $\langle \widehat{\sigma}, \langle \Pi_1, \sigma, \Pi_2 \rangle \rangle$ も同様にフェーズとなる.

表 1: Π_1, Π_2の定義

	Π_1	
	PM_{1_A}	PM_{1_B}
S_F	s_1, s_2	s_3, s_4
Σ	$-C, +A, +P$	$+C, -A, -P$
T	t_1, t_2, t_3	t_4, t_5, t_6
SI	s_1	s_3
SE	s_2	s_4
	Π_2	
	PM_{2_A}	PM_{2_B}
S_F	s_5, s_6	s_7, s_8
Σ	$-C, +P, +A$	$+C, -P, -A$
T	t_7, t_8, t_9	t_{10}, t_{11}, t_{12}
SI	s_5	s_7
SE	s_6	s_8

表 2: アクションの定義

T	s_{F1}	d_t	s_{F2}	C	R (更新されるレジスタへの操作, 他は不変)
t_1	s_1	$-C$	s_1	C_1	$Rc \leftarrow Rc+1$
t_2	s_1	$+A$	s_1	ε	$Ra \leftarrow n$
t_3	s_1	$+P$	s_2	ε	$Rp \leftarrow n$
t_3'	s_1	$+P$	s_5	ε	$Rp \leftarrow n$
t_4	s_3	$+C$	s_3	ε	$Rc \leftarrow Rc+1$
t_5	s_3	$-A$	s_3	C_5	$Ra \leftarrow n$
t_6	s_3	$-P$	s_4	C_6	$Rp \leftarrow n$
t_6'	s_3	$-P$	s_7	C_6	$Rp \leftarrow n$
t_7	s_5	$-C$	s_5	C_7	$Rc \leftarrow Rc+1$
t_8	s_5	$+P$	s_5	ε	$Rp \leftarrow n$
t_9	s_5	$+A$	s_6	ε	$Ra \leftarrow n$
t_{10}	s_7	$+C$	s_7	ε	$Rc \leftarrow Rc+1$
t_{11}	s_7	$-P$	s_7	C_{11}	$Rp \leftarrow n$
t_{12}	s_7	$-A$	s_8	C_{12}	$Ra \leftarrow n$

表 3: 条件 Cの定義

C_i	条件
C_1	$(n = Rc+1) \wedge (n \leq Ra+4)$
C_5	$(Ra+1 \leq n \leq Rc)$
C_6	$(n \geq Ra+1)$
C_7	$(n = Rc+1) \wedge (n \leq Rp)$
C_{11}	$(n \geq Rp+1)$
C_{12}	$(Ra \leq Rc) \wedge (n \geq Ra+1)$

4 フェーズ合成に基づく ECFSMs の検証法

ここでは ECFSMs でモデル化されたプロトコルに対する不変式を用いた安全性の検証法について述べる.

4.1 ECFSMs の不変式を用いた検証法[1]

ECFSMs でモデル化されたプロトコルの系の状態に関する条件を表現するために, 以下のような 4 つの型の原子式を導入する.

(AF1) プロトコル機械の有限制御部の状態が指定した値をもつかどうかを表す式. "(STA713A, STA10B)" は PM_Aの有限制御部の状態が STA713A, PM_Bの有限制御部の状態が STA10B であることをそれぞれ表している.

(AF2) PM_Bから PM_Aへの通信路 $ch_{B\to A}$または PM_Aから PM_Bへの通信路 $ch_{A\to B}$上のメッセージ系列内のメッセージ型の系列が, 指定した系列集合に属するかどうかを表す式. "$ch_{A\to B} \in$ MIP$^*\cdot$MAP" は, PM_Aから PM_Bへの通信路 $ch_{A\to B}$上に 0 個以上のメッセージ型 MIP のメッセージに続いてメッセージ型 MAP のメッセージが 1 つ存在することを表している.

(AF3) PM_Bから PM_Aへの通信路 $ch_{B\to A}$または PM_Aから PM_Bへの通信路 $ch_{A\to B}$上のメッセージ系列に含まれるパラメータ列についての述語. 例えば "step1($subseq(AB, \{\text{MIP}\})$)" は PM_Aから PM_Bへの通信路上のメッセージ型が MIP であるメッセージ列のパラメータの系列が増分 1 の増加列である場合に真となるような述語である. 述語に関する諸性質は, 書き換え規則及び関係式からなる基底代数の性質として別に与える.

(AF4) 通信路内のメッセージのパラメータと, プロトコル機械のレジスタとの関係を表す線形の等式・不等式. 例えば "Vm(A) == last($subseq(AB, \{\text{MIP}\})$) + 1" は, PM_Aのレジスタ Vm の値が PM_Aから PM_Bへの通信路上のメッセージ型が MIP である末尾のメッセージのパラメータ値に正定数値 1 を加算したものに等しいことを表す. ここで last はメッセージ系列の末尾のメッセージのパラメータ値を表す定義関数である.

以上を原子式とする論理式 Fに対して, Fを満たす系の状態の集合を $GSF(F)$ で表す. 系の初期状態の集合の満たすべき条件を原子式を用いて F_{init}として記述することで, $GSI = GSF(F_{init})$ としてプロトコルの系の初期状態集合を指定することができる.

プロトコルΠの可達集合 $RS(\Pi)$ に属するすべての系の状態において論理式 Fが満たされるとき, FをΠの不変式という.

提案している検証法は, 検証者が不変式と思われる積和形論理式 $F = \bigvee_{1\leq i\leq n} F_i$を記述し, Fが実際にΠの不変式であることを送受信イベントに関する構造的帰納法によっ

て示し, $GSF(F)$ が未定義受信及びデッドロック状態を含まないことを示すことにより, プロトコルΠが安全性であると結論するものである.

提案している検証法に基づき帰納段階の証明過程を自動化する検証系が作成されている.

4.2 不変式によるフェーズの検証と合成

以下では 4.1の検証法を用いて安全であることが保証されたプロトコルΠがフェーズであることを示す方法について述べる. また安全なフェーズであることが示された2つのフェーズΠ_1, Π_2と$\sigma = \langle \sigma_A, \sigma_B \rangle$ が与えられるとき, $\langle \Pi_1, \sigma, \Pi_2 \rangle$ に対してσが補題 3.1の条件を満たしていることを示す方法についても述べる.

[フェーズであることの証明法]

$F = \bigvee_{1 \le i \le n} F_i$をΠ $= (PM_A, PM_B, GSI)$ の不変式とする.

以下のような関数, 集合を考える.

fc は状態から有限制御部を取り出す関数であり, $fc((s_F, p_1, \ldots, p_r)) = s_F$

$EX_{A\overline{B}} = \{\langle s_A, s_B, x, y \rangle \in RS(\Pi) \mid fc(s_A) \in SE_A$かつ $fc(s_B) \notin SE_B\}$

$GS_{EX_{A\overline{B}}}(F) = \{\langle s_A, s_B, x, y \rangle \in GSF(F) \mid s_A$が終了状態であり s_Bが終了状態でない $\}$

$GS_{EX}(F) = \{\langle s_A, s_B, x, y \rangle \in GSF(F) \mid s_A, s_B$がともに終了状態である $\}$

$GS_{EI}(F) = \{\langle s_A, s_B, x, y \rangle \in GSF(F) \mid s_A, s_B$がともに終了状態であり, $\sigma_A(s_A), \sigma_B(s_B)$ がともに定義されている $\}$

このとき Fが不変式であることより $GS_{EX_{A\overline{B}}}(F) \supseteq EX_{A\overline{B}}$及び $GS_{EX}(F) \supseteq EX(\Pi)$ が成立する.

Πがフェーズであること, つまり定義 3.1の条件 (1), (2) を満たすことを以下のようにして示す.

(1) Πの任意の gs_0-プロトコル系列 $\langle Q_A, Q_B \rangle$(但し $GS(\langle Q_A, Q_B \rangle) = \langle s_A, s_B, ch_{B\to A}, ch_{A\to B} \rangle$ とする) に対して,

$s_A \in SE_A$ならば, $GS(\langle Q_A, Q_B \cdot Q'_B \rangle) \in EX(\Pi)$ なる Q'_B が存在する.

$s_B \in SE_B$ならば, $GS(\langle Q_A \cdot Q'_A, Q_B \rangle) \in EX(\Pi)$ なる Q'_A が存在する.

以下では上記の条件の前者の証明法のみを述べる (後者についても同様).

$GS_{EX_{A\overline{B}}}(F) \supseteq EX_{A\overline{B}}$及び $GS_{EX}(F) \supseteq EX(\Pi)$ より

$\forall_{gs \in GS_{EX_{A\overline{B}}}(F)} \exists_{gs \doteq gs'} \{gs' \in GS_{EX}(F)\}$ $\cdots$(I)

を示せば十分である. ここで $gs = \langle s_A, s_B, x, y \rangle \in GS_{EX_{A\overline{B}}}(F)$, $fc(s_A) \in SE_A$とすると, $GSF(F)$ の安全性は保証されていることより $GS_{EX_{A\overline{B}}}(F)$ に属するすべての系の状態は未定義受信でないから, $GS(\langle \varepsilon, Q_B \rangle, gs) = gs'' = \langle s_A, s''_B, x'', \varepsilon \rangle$ を満たす PM_Bのある状態遷移系列 Q_Bが存在する.

ここで補題 3.1の条件 (2) が成り立つならば $fc(s''_B) \in SE_B$が成立し $gs'' \in EX(\Pi)$ である. よって (I) を示すには次の条件 (2) の成立を示せば十分である.

(2) $s_A \in SE_A$かつ $\langle s_A, s_B, ch_{B\to A}, \varepsilon \rangle \in RS(\Pi)$ ならば $s_B \in SE_B$

$s_B \in SE_B$かつ $\langle s_A, s_B, \varepsilon, ch_{A\to B} \rangle \in RS(\Pi)$ ならば $s_A \in SE_A$

上記の条件の前者の証明法のみを述べる (後者についても同様).

$GS_{EX_{A\overline{B}}}(F) \supseteq EX_{A\overline{B}}$より, (AF1) 型原子式において PM_Aの有限制御部が終了状態を指定しており, PM_Bの有限制御部が終了状態を指定していない各積項 $F_i (1 \le i \le n)$ に対して, F_iの (AF2) 型原子式が, PM_Aから PM_Bへの通信路のメッセージ系列を表す系列集合が空系列を含んでいないことを確認することによって示される.

[σが補題 3.1の条件を満たすことの証明]

$\Pi_1 = (PM_{1_A}, PM_{1_B}, GSI_1)$, $\Pi_2 = (PM_{2_A}, PM_{2_B}, GSI_2)$ を安全なフェーズとする. また$\sigma = \langle \sigma_A, \sigma_B \rangle$ においてσ_Aは SE_{1_A}から SI_{2_A}への部分関数σ_{F_A}によって以下のように指定されるものとする. (σ_Bについても同様.)

$$\sigma_A((s_F, p_1, \ldots, p_r)) = \begin{cases} (\sigma_{F_A}(s_F), p_1, \ldots, p_r) & (\sigma_{F_A}(s_F) \text{が定義されている}) \\ \text{未定義} & (\sigma_{F_A}(s_F) \text{が未定義}) \end{cases}$$

このとき $\langle \Pi_1, \sigma, \Pi_2 \rangle$ に対して$\sigma = \langle \sigma_A, \sigma_B \rangle$ が補題 3.1の条件

$\langle s_A, s_B, x, y \rangle \in EX(\Pi_1)$ かつ$\sigma_A(s_A)$,$\sigma_B(s_B)$ の少なくとも一方が定義されているならば

$\langle \sigma_A(s_A), \sigma_B(s_B), x, y \rangle \in GSI_2$

を満たしていることを示す方法について述べる.

Π_1に対する不変式を $F = \bigvee_{1 \le i \le n} F_i$とする.

まず $\langle s_A, s_B, x, y \rangle \in EX(\Pi_1)$ に対して$\sigma_A(s_A)$ が定義されているとき, $\sigma_B(s_B)$ が定義されていることを以下のようにして示す. ($\sigma_B(s_B)$ が定義されているときについても同様にして示せる.)

$GS_{EX}(F) \supseteq EX(\Pi_1)$ より, (AF1) 型原子式において PM_{1_A}, PM_{1_B}の有限制御部の状態を表す式がそれぞれ終了状態 s_A, s_Bを指定しているような積項 $F_i (1 \le i \le n)$ に対して, PM_{1_A}(または PM_{1_B}) の有限制御部の状態に対して$\sigma_A(s_A)$ が定義されているならば$\sigma_B(s_B)$ が定義されてことを確認する.

次に $\langle s_A, s_B, x, y \rangle \in EX(\Pi_1)$ に対して, $\sigma_A(s_A)$, $\sigma_B(s_B)$ がともに定義されているとき, $\langle \sigma_A(s_A), \sigma_B(s_B), x, y \rangle \in GSI_2$であること, つまり$\sigma(EX(\Pi_1)) \subseteq GSI_2$であることを示す.

$GS_{EI}(F)$の定義より $GS_{EI}(F) \supseteq EX(\Pi_1)$, また$\sigma$についての条件より$\sigma(GS_{EI}(F)) \supseteq \sigma(EX(\Pi_1))$ が成立する. 従って, Π_2の系の初期状態集合の指定する論理式 $F_{2_{init}}$ に対して $GSF(F_{2_{init}}) \supseteq \sigma(GS_{EI}(F))$ であること示せば

よい. これは次のように示される.

(AF1) 型原子式において PM_{1_A}, PM_{1_B} の有限制御部の状態を表す式がともに終了状態を示しており, それら有限制御部の状態に対して $\sigma_{F_A}, \sigma_{F_B}$ がともに定義されているようなすべての積項 $F_i (1 \leq i \leq n)$ に対して以下を行う. 各 F_i において PM_{1_A}, PM_{1_B} の有限制御部の状態 s_{F_A}, s_{F_B} を $\sigma_{F_A}(s_{F_A}), \sigma_{F_B}(s_{F_B})$ によって置き換えた積項を F_i' とする. このとき F_i' を満たす系の状態の集合が $F_{2,\ldots,i} = \bigvee_{1 \leq j \leq k} \overline{F}_j$ (ここで各 $\overline{F}_k$ は (AF1) から (AF4) を原子式とする積項) を満たす系の状態の集合に含まれることを, 例えば各 $\overline{F}_j$ と F_i' の (AF1) から (AF4) までの原子式を比較することによって確認する.

5 OSI セションプロトコルの検証への適用例

ここでは, 4で述べた不変式を用いたプロトコルの安全性及びフェーズであることの検証法とフェーズ合成に関する性質を, トークンパッシング制御を含むプロトコル Π_{DATA} の安全性の検証に適用した例を示す. ここでトークンとは, あるサービスの起動などの権利を表すもので, 初期状態においては, どちらか一方に配置され, トークン譲渡メッセージの送受信により権利が移動する.

OSI セションプロトコル[9]のデータ転送フェーズのカーネル・全二重・大同期・小同期機能単位を抽出したプロトコルを Π_{DATA} とする. 但し OSI セションプロトコルはデータ転送フェーズにおいて, Major, Minor, Release の 3 つのトークンを使用しているが, 簡単のため Π_{DATA} では Major, Minor の 2 つのトークンの使用に限定した.

$\Pi_{DATA1} = (PM_{1_A}, PM_{1_B}, GSI_1)$, $\Pi_{DATA2} = (PM_{2_A}, PM_{2_B}, GSI_2)$ を Π_{DATA} と同じ機能を持つ以下のようなプロトコルとする.

Π_{DATA1} では, PM_A が Major トークンを所有しており, $PM_A(PM_B)$ は Major トークンの送信 (受信) によって終了状態に遷移する. Π_{DATA2} は Π_{DATA1} においてのプロトコル機械 PM_A と PM_B を入れ換えることで定義される Π_{DATA1} と対称なプロトコルである. $\sigma_{F_A}, \sigma_{F_B}$ は全単射である.

Π_{DATA1} 及び Π_{DATA2} の対称性から両者の安全性の検証は Π_{DATA1} に対して行えば十分である. Π_{DATA1} が安全なプロトコルであることを 4.1の検証法により確認した. さらに Π_{DATA1} と Π_{DATA2} がともにフェーズであること, 及び $\langle \Pi_{DATA1}, \sigma, \Pi_{DATA2} \rangle$ に対して σ が補題 3.1の条件を満たしていることを 4.2に述べた方法で確認した.

以上, 及び定理 3.2より $\langle \Pi_{DATA1}, \sigma, \Pi_{DATA2} \rangle$ は安全なフェーズであると結論できる. さらに

$$\overline{\sigma}_A((s_F, p_1, \ldots, p_r)) = (\sigma_{F_A}^{-1}(s_F), p_1, \ldots, p_r)$$

$$\overline{\sigma}_B((s_F, p_1, \ldots, p_r)) = (\sigma_{F_B}^{-1}(s_F), p_1, \ldots, p_r)$$

と定義した $\overline{\sigma} = \langle \overline{\sigma}_A, \overline{\sigma}_B \rangle$ と $\langle \Pi_{DATA1}, \sigma, \Pi_{DATA2} \rangle$ に対して定理 3.3の条件を満たしていることを 4.2に述べた方法と同様にして確認した. また以上のように合成したプロトコル $\langle \overline{\sigma}, \langle \Pi_{DATA1}, \sigma, \Pi_{DATA2} \rangle \rangle$ が先に定義した Π_{DATA} と一致することを確認した.

表 1: Π_{DATA}, Π_{DATA1} の検証結果

	不変式の積項数	CPU 時間 (sec)	メモリ使用量 (MByte)
(1) Π_{DATA}	306	3.27	24
(2) Π_{DATA1}	108	0.73	6
(1)/(2)	2.83	3.94	4

検証作業は UNIX ワークステーション (SONY NWS-5000VX) 上で行った.

比較のために Π_{DATA} の 4で述べた手法により直接検証した. Π_{DATA} 及び Π_{DATA1} の検証時に記述した不変式の積項数及び, 検証系実行時の CPU 時間, メモリ最大使用量を表 4 に示す.

Π_{DATA1} の検証の場合, Π_{DATA} を直接検証した場合に比べて検証時に必要な不変式の積項数が約 1/3 に, 検証系の実行時に必要となる最大メモリ使用量, 及び CPU 時間がともに約 1/4 に削減され, そのフェーズ合成の性質を利用して検証を行うことの有効性が確認された.

6 今後の予定

今後, フェーズ合成を利用した検証法を適用して OSI セションプロトコル全体の安全性の検証作業を行う予定である. さらにフェーズの諸性質を liveness の検証にも適用できると考えられ, 現在検討中の liveness の検証法[2]と併せて検討する予定である.

参考文献

[1] Higuchi et al.: "A Verification Method via Invariant for Communication Protocols Modeled as Extended Communicating Finite-State Machines", *IEICE Trans. Commun.*, vol.E-76-B, no.11(1993 年 11 月掲載予定).

[2] 須川, 樋口, 藤井: "拡張有限状態でモデル化された通信プロトコルの liveness の検証法", 情報処理学会第 4 7 回全国大会 (鳥取), 2F-2(1993 年 10 月).

[3] Choi T.Y., and Miller R.E.: "A Decomposition Method for the Analysis and Design of Finite State Protocols", in *Proc. of 8th ACM/IEEE Data Comm. Symp.*, pp.167-176(1983 年 10 月).

[4] Lam S.S., and Shankar A.U.: "Protocol Verification via Projections", *IEEE Trans. Software Eng.*, vol.10, no.7, pp.325-342 (1984 年 7 月).

[5] Chow et al: "A Discipline for Constructing Multiphase Communication Protocols", *ACM Trans. Comput. Systems*, vol.3, no.11, pp.315-343(1985 年 11 月).

[6] Lin H.: "Constructing Protocols with Alternative Functions", *IEEE Trans. Comput.*, vol.40, no.4, pp.376-386(1991 年 4 月).

[7] Higuchi et al: "A Method of Composing Communication Protocols with Priority Service", *IEICE Trans. Commun.*, vol.E75-B, no.10, pp.1032-1042(1992 年 10 月).

[8] CCITT: "Specification and Description Language (SDL)", Recommendation Z100, 1989.

[9] ISO: "Basic Connection Oriented Session Protocol Specification", ISO 8327.