マルチメディア通信と分散処理 79－11
（1996. 11. 15）

EFSMモデル通信プロトコルの時制に関する性質の一検証法

原 圭吾 樋口 昌宏 藤井 護

大阪大学基礎工学部

e-mail: {hara, higuchi, fujii}@ics.es.osaka-u.ac.jp

あらまし　プロトコル機械が拡張有限状態機械でモデル化され，通信路が非有界FIFOでモデル化された通信プロトコルの時制に関する性質のうち，「性質Pが成立する任意の状態から，有限時間内に性質Qが成立する状態に遷移する」という性質(leads-to性)の検証法を提案する．ここで，性質P,QはPQ変数と呼ばれる共通の整数値パラメータを用いた連立不等式として与えられる．本手法では，性質Pが成立する状態から性質Qが成立する状態に遷移する過程で成立するいくつかの性質を求め，それに従って，プロトコルが初期状態から到達可能な状態の集合を部分集合$RS_1, RS_2, \ldots, RS_n$に分割する．さらに，これらの$RS_1, RS_2, \ldots, RS_n$の間の遷移関係を表すグラフ(leads-to到達可能性グラフ)を構成し，それを探索することによって，性質Pが成立する状態から始まる無限長の状態遷移系列で性質Qが成立する状態への遷移が存在しないようなものがないことを示す．

キーワード　通信プロトコル，拡張有限状態機械，不変式，論理検証，leads-to性

A Verification Method for Temporal Properties of Communication Protocols modeled as EFSMs

Keigo Hara, Masahiro Higuchi, and Mamoru Fujii

Faculty of Engineering Science,
Osaka University

Abstract In this paper, a verification method for leads-to property of communication protocols modeled as EFSMs is proposed. A leads-to property "$GS(P) \rightsquigarrow GS(Q)$" represents that " if a global state satisfies the property P, then the protocol eventually transits to the global states satisfying the property Q". Property P and Q are described as simultaneous inequalities using several integral parameters (called PQ-parameter). In our method, intermediate properties between P and Q are generated. Using these intermediate properties, the set of reachable global states RS is divided into $RS_1, RS_2, \ldots$, and RS_n, and a leads-to reachability graph (LRG) which represents the relation between those subsets is constructed. By exploring such a LRG, "$GS(P) \rightsquigarrow GS(Q)$" can be shown to hold.

Keyword communication protocol, extended finite-state machine, invariant, logical verification, leads-to property

1　まえがき

通信ソフトウェアの信頼性向上のためには，通信プロトコルの設計段階での論理検証が重要である．検証の対象となる性質に，"ある性質がいずれ成立する"，"ある性質が常に成り立つ"といった時制に関するものがある．通常，二者間の通信を規定するプロトコルは順序機械でモデル化される二つのプロトコル機械と，それらを接続する双方向のFIFOでモデル化される通信路からなる系としてモデル化される．実用レベルの通信プロトコルはプロトコル機械が有限制御部の他に整数値などの値を取る変数を持つ拡張有限状態機械（以下，EFSMと呼ぶ）でモデル化される場合が多い．そのような通信プロトコルでは，プロトコル機械は整数値パラメータを持つメッセージを送受信することで状態遷移を行なうが，プロトコル機械の送信するメッセージ系列のパラメータ系列は，狭義単調増加，増分1の増加等のプロトコル固有の単調な性質を持つ場合が多い．筆者らは，この点に着目して通信路上に現れるメッセージ系列のパラメータ系列の単調性を表す述語とそれらに関する補題を用いたEFSMモデルプロトコルの安全性，生存性の検証法を提案してきた[1] [2]．それらに基づき，本稿ではプロトコルの時制に関する次のような性質(leads-to性)を検証する手法を提案する．ある性質P,Qを満たす状態の集合をそれぞれ$GS(P), GS(Q)$とするとき，$\forall gs' \in GS(P) \exists gs \in GS(Q)\{gs'$から$gs$へ有限時間内に到達する$\}$．

提案する検証法では，示すべき性質とプロトコルの動作の定義に応じて，$GS(P)$に属する状態から$GS(Q)$に属する状態へ到達する過程で成立するいくつかの性質$Q_0, Q_1, \cdots, Q_m$を生成し，これらの性

質を基に状態集合の分割を行ない，分割した状態集合間の遷移関係を調べて有限の leads-to 到達可能性グラフ LRG を構成する．さらに LRG を解析することにより，$GS(P)$ に属する状態から始まる状態遷移系列で $GS(Q)$ に属する状態への遷移が存在しないようなものがないことを示す．

2 プロトコルモデル

プロトコル機械を有限個の非負整数値レジスタを持つ拡張有限状態機械，二つのプロトコル機械を接続する双方向の通信路を長さに制限のない FIFO でモデル化する．形式的には以下のように定義する．

定義 1 プロトコル機械を 4 字組 (S, Σ, T, SI) で定義する．
(M1) $S = \langle SF, rg\rangle$: SFは有限制御部の値の有限集合，rgは非負整数値を保持するレジスタの数を表す．
(M2) $\Sigma = \Sigma_- \cup \Sigma_+$: 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有限集合を表し，Σ_-とΣ_+は互いに素であるとする．各メッセージはメッセージ型に加えて非負整数値パラメータを一つ持つものとし，パラメータ $p \in \mathcal{N}$を持つ型 $d \in \Sigma$のメッセージを $\langle d, p\rangle$ と書く．
(M3) T : アクションの有限集合．アクションは5字組 (u, d, v, C, R) で定義される．$u \in SF, d \in \Sigma, v \in SF$．$C$は状態遷移前のプロトコル機械のレジスタ値 $r_1, r_2, \ldots, r_{rg}$ と送信または受信メッセージ $\langle d, p\rangle$ のパラメータ値 p が満たすべき連立線形不等式であり，遷移条件と呼ぶ．Rは状態遷移前のプロトコル機械のレジスタ値 $r_1, r_2, \ldots, r_{rg}$ と送信または受信メッセージのパラメータ値 p から状態遷移後のプロトコル機械のレジスタ値 $r_1, r_2, \ldots, r_{rg}$を定める $\mathcal{N}^{rg+1}$から $\mathcal{N}^{rg}$ への線形演算により定義される部分関数であり，レジスタ更新関数と呼ぶ．

Tにより $\langle SF \times \mathcal{N}^{rg}\rangle \times \langle \Sigma \times \mathcal{N}\rangle$ から $SF \times \mathcal{N}^{rg}$ への非決定性状態遷移関数 δ は以下のように定まる．
$\delta(\langle u, r_1, r_2, \ldots, r_{rg}\rangle, \langle d, p\rangle) =$
$\{\langle v, R(r_1, r_2, \ldots, r_{rg}, p)\rangle \mid (u, d, v, C, R) \in T$かつ $r_1, r_2, \ldots, r_{rg}, p$ は Cを満たす$\}$
(M4) $SI \subseteq SF \times \mathcal{N}^{rg}$: 初期状態の集合． □

本稿では，解析の効率を考慮して，アクションの定義の中で遷移条件を構成する各不等式を "$x - y \leq c$" という形 (差分制約と呼ぶ) に限定し，レジスタ更新関数を "$r := x + c$" という形に限定する．ここで x, y はレジスタまたは送受信するメッセージのパラメータ値，cは整定数 (差分と呼ぶ)，r'は変更前のレジスタ rの値である．また，"$(x - y \leq c) \wedge (y - x \leq -c)$" を略して "$x - y = c$" と書く．

定義 2 二つのプロトコル機械 $PM_A = (\langle SF_A, r_A\rangle, \Sigma_A, T_A, SI_A)$, $PM_B = (\langle SF_B, r_B\rangle, \Sigma_B, T_B, SI_B)$ について，$\Sigma_{B-} = \Sigma_{A+}$ (Σ_{BA}と書く)，$\Sigma_{A-} = \Sigma_{B+}$ (Σ_{AB}と書く) であるとき，2 字組 $\Pi = (PM_A, PM_B)$ をプロトコルと呼ぶ．4字組 $gs = \langle s_A, s_B, u_{BA}, u_{AB}\rangle \in \langle SF_A \times \mathcal{N}^{rg_A}, SF_B \times \mathcal{N}^{rg_B}, \langle \Sigma_{BA} \times \mathcal{N}\rangle^*, \langle \Sigma_{AB} \times \mathcal{N}\rangle^*\rangle$ をプロトコルΠの系の状態と呼ぶ．ここで，s_A,s_Bはそれぞれ gs におけるプロトコル機械 PM_A, PM_Bの状態を表し，u_{BA}, u_{AB}はそれぞれ gs における PM_Bから PM_Aへの通信路，PM_Aから PM_B への通信路上のメッセージ系列を表している．以下では，混乱のない限り，系の状態を単に状態と呼ぶ．$s_A \in SI_A, s_B \in SI_B$であるとき，状態 $\langle s_A, s_B, \varepsilon, \varepsilon\rangle$ (εは空系列を表す) をΠの初期状態と呼ぶ． □

プロトコルΠの状態遷移は通常の非同期通信の定義に従う．プロトコルが状態 gs'から gs に遷移可能であることを $gs' \rightarrow gs$ と書く．また，関係 "$\rightarrow$" の反射推移閉包を "$\overset{*}{\rightarrow}$" と書く．$gs' \overset{*}{\rightarrow} gs$ のとき，gs'から gs に到達可能であるという．プロトコルΠの初期状態から到達可能である状態を可達状態と呼ぶ．また，その集合をΠの可達集合と呼び，RS_Πと書く．

定義 3 アクション t による，gs'から gs への状態遷移を 3 字組 (gs', t, gs) で表す．以下，遷移 (gs_{i-1}, t_i, gs_i) をτ_iで表す．また，プロトコルΠにおいて $\forall i\{gs_i \rightarrow gs_{i+1}\}$ であるとき，状態遷移系列 $ts = \tau_1 \tau_2 \tau_3 \ldots \tau_n$ はプロトコルΠにおいて実行可能であるという．プロトコルΠにおいて実行可能な状態遷移系列の集合を TS_Πと書く．さらに，Πにおける無限長の状態遷移系列の集合を TS_Π^∞と書く．

状態集合 GS', GSについて，
$\neg\exists \tau_1 \tau_2 \tau_3 \ldots \in TS_\Pi^\infty \{gs_0 \in GS' \wedge \forall i\{gs_i \notin GS\}\}$
であるとき，$GS' \rightsquigarrow GS$と書く． □

$GS' \rightsquigarrow GS$であるとき，Πは GS'に属する任意の状態から GSに属する状態へ有限時間内に遷移する．定義より，関係 "$\rightsquigarrow$" は推移律を満たす．

3 不変式に基づく安全性の検証法

プロトコル Π の任意の可達状態において論理式 F が成立するとき，Fは Π の不変式であるという．論理式 F を満たす状態の集合を $GS(F)$ と書く．

検証者は，プロトコル$\Pi = (PM_A, PM_B)$ の初期状態から到達可能であると想定している状態の集合を，それぞれの状態における各プロトコル機械の状態，各通信路上のメッセージ系列により，いくつかの互いに素な部分集合に分割する (以下ではその分割数を n とする)．それぞれの状態集合に対して，その集合中のすべての状態で成立する条件を以下の (AF1)-(AF4) の 4 種類の原子式の積項 P_i $(i = 1, 2, \ldots, n)$ として記述し，$F = P_1 \vee P_2 \vee \cdots \vee P_n$とする．

(AF1) $\langle sf_A, sf_B\rangle$ $(sf_A \in SF_A, sf_B \in SF_B)$: PM_A, PM_Bの有限制御部の値がそれぞれ sf_A, sf_B であることを表す．

(AF2) 通信路上のメッセージ系列の型系列が満たすべき性質を正規表現を用いて記述した式．例えば，AF2 型原子式 $u_{AB} \in \mathcal{L}(\text{MIP}^+)$ は，PM_Aから PM_Bへの通信路上の型系列が正規表現 "MIP^+" の表す系列集合の要素である，すなわち 1 個以上の MIP から成る系列であることを表す．ここで，$\mathcal{L}(R)$ は正規表現 Rの表す系列集合である．

(AF3) 通信路上のメッセージ系列のパラメータ系列が満たすべき性質を検証者が定義した述語を用いて記述した式．例えば，$step1(u_{AB})$ は，PM_A から PM_Bへの通信路上のパラメータ系列が述語 $step1$ として定義された性質を満たしていることを表す．ここで，$step1(\alpha)$ はメッセージ系列 α のパラメータ系列が増分 1 の増加列であることを表す検証者の定義した述語である．

(AF4) プロトコル機械のレジスタ値，および通信路上のメッセージ系列の特定位置のメッセージのパラメータ値に関する差分制約式．例えば，$VM_A - firstp(u_{BA}, \{MIP\}) = 1$ は，PM_Aのレジスタ VM_Aの値が PM_Bから PM_Aへの通信路上の型 MIPのメッセージのみからなるメッセージ系

列 u_{BA}の先頭メッセージのパラメータ値に1を加えたものに等しいことを表す.

【例 1】OSI セションプロトコルのデータ転送フェーズに基づく以下のようなプロトコル$\Pi_{EX} = (PM_A, PM_B)$を考える. PM_Aは同期点番号 sn をパラメータ値とするメッセージ $\langle$MIP, $sn\rangle$ を PM_Bに送信することにより同期点 sn の設定を行なう. PM_A は型 MIP のメッセージを送信するごとに送信する同期点番号を1ずつ増加させる. PM_Bは受信したメッセージ $\langle$MIP, $sn\rangle$ に対してメッセージ $\langle$MIA, $sn\rangle$ を PM_Aに送信することにより同期点 sn への応答を行なう. PM_Bは必ずしも受信したすべてのメッセージ $\langle$MIP, $sn\rangle$ に応答する必要はなく, 対応するメッセージ $\langle$MIA, $sn\rangle$ を送信しないこともある. しかし, PM_Bが型 MIA のメッセージを送信するときには, PM_Bがそのときまでに受け取った最大の同期点番号 sn をパラメータ値とするメッセージ$\langle$MIA, $sn\rangle$を送信するものとする. PM_Aは $\langle$MIA, $sn\rangle$ を受信したとき, PM_Bが sn 以下のすべての同期点に応答したとみなす. プロトコル機械 PM_A, PM_Bを次のように定義する.

- PM_A, PM_Bの有限制御部の取り得る値はそれぞれ "ST_A", "ST_B" のみとする. PM_A,PM_B は表 1の 2 つのレジスタを持つ.
- Σ_{AB}={MIP}, Σ_{BA}={MIA}.
- PM_A, PM_Bのアクション $t_{a,1}, t_{a,2} \in T_A$, $t_{b,1}, t_{b,2} \in T_B$の定義を表 2に示す. 例えば, アクション$t_{b,1}$はPM_Bについて有限制御部の値が ST_Bで, $VM_B > VA_B$を満たすとき, $VM_B = sn+1$ を満たすメッセージ $\langle$MIA, $sn\rangle$ を送信することができ, 状態遷移後の VA_Bの値を $sn+1$ にすると定義している.
- PM_A, PM_Bの初期状態では, すべてのレジスタの値が 0 であるとする.

プロトコルΠ_{EX}の初期状態から到達可能であると想定している状態の集合を (a)PM_Aから PM_Bへの通信路上に型MIP のメッセージがあるかないか, (b)PM_B から PM_Aへの通信路上に型 MIA のメッセージがあるかないか, (c)PM_Bが型 MIA のメッセージを送信できる ($VM_B > VA_B$) か送信できない ($VM_B = VA_B$) かによって, 8 個の部分集合に分割する. 各集合中の任意の状態で成立する論理式として表 3の式 $F_i (1 \le i \le 8)$ が記述できる. 表 3では定義述語, 定義関数として表 4 に記したものを用いている. $F_{EX} = F_1 \vee F_2 \vee \cdots \vee F_8$とする. □

文献 [1] では, プロトコルの不変式を用いた安全性の検証法が提案され, それに基づく検証システムが試作されている.

4 leads-to 性の検証法

ここでは, 文献 [1] で述べられている検証法により安全性が保証されているプロトコルの leads-to 性と呼ばれる性質 $GS(P) \rightsquigarrow GS(Q)$ の検証法について述べる. ここで, 性質 P, Q は PQ 変数と呼ばれる共通の整数値パラメータを用いた連立不等式として与えられる. 例えば, 対象となるプロトコルをΠ_{EX}, 性質 Pを $VM_A = k$, Q を $VA_A \ge k$ (kは PQ 変数) とする. このとき, $GS(P) \rightsquigarrow GS(Q)$ は PQ 変数で表されるパラメータ値 kを持つ同期点設定要求が送信されているならば, いつかは k 以上のパラメータ値を持つ同期点応答が受信されることを表す. 以下, 簡単のために $GS(P) \rightsquigarrow GS(Q)$ を $P \rightsquigarrow Q$ と書く.

表 1: プロトコルΠ_{EX}のプロトコル機械のレジスタ

レジスタ	意味
VM_A	次に送信する MIP の同期点番号
VA_A	応答が返っていない最小の同期点番号
VM_B	次に受信すべき MIP の同期点番号
VA_B	応答を返していない最小の同期点番号

表 2: プロトコルΠ_{EX}のプロトコル機械のアクションの定義

$t_{a,1} = (\mathrm{ST}_A, \langle\mathrm{MIP}, sn\rangle, \mathrm{ST}_A, C_{t_{a,1}}, R_{t_{a,1}})$ $C_{t_{a,1}} = \{sn = VM_A\}$ $R_{t_{a,1}}(VM_A, VA_A) = (VM'_A + 1, VA'_A)$
$t_{a,2} = (\mathrm{ST}_A, \langle\mathrm{MIA}, sn\rangle, \mathrm{ST}_A, C_{t_{a,2}}, R_{t_{a,2}})$ $C_{t_{b,1}} = \{VM_A \ge sn+1, sn \ge VA_A\}$ $R_{t_{a,2}}(VM_A, VA_A) = (VM'_A, sn+1)$
$t_{b,1} = (\mathrm{ST}_B, \langle\mathrm{MIA}, sn\rangle, \mathrm{ST}_B, C_{t_{b,1}}, R_{t_{b,1}})$ $C_{t_{b,1}} = \{VM_B > VA_B, VM_B = sn+1\}$ $R_{t_{b,1}}(VM_B, VA_B) = (VM'_B, sn+1)$
$t_{b,2} = (\mathrm{ST}_B, \langle\mathrm{MIP}, sn\rangle\ \mathrm{ST}_B, C_{t_{b,2}}, R_{t_{b,2}})$ $C_{t_{b,2}} = \{VM_B = sn\}$ $R_{t_{b,2}}(VM_B, VA_B) = (VM'_B + 1, VA'_B)$

4.1 中間性質

プロトコルが性質 Pを満たす状態から性質 Q を満たす状態に到達する過程で成立するいくつかの性質 (中間性質) を生成し, それらが満たされているかどうかによって RS_Πを分割することを考える.

各中間性質はあるメッセージ $\langle d, p\rangle$ が通信路上 u に存在することを表す原子式 $\langle d, p\rangle$ on u と, AF4 型原子式の積からなる.

以下の 1–3. の手続きによって生成される各性質 $Q_i (\in \mathcal{Q}_{P,Q})$ を始点性質 P, 目標性質 Q の中間性質と呼ぶ. 手続き中で扱う連立不等式が不等式 $x - y \le c$, $y - z \le c'$を含む場合, 二つの不等式から導かれる不等式 $x - z \le c + c'$も含むものとする. q', sn, op, k はそれぞれアクション実行前のあるレジスタ値, アクションによって送信 (受信) されるメッセージのパラメータ値, 比較演算子$\ge$または$\le$, PQ 変数を表すものとする. また, c は整定数とする. $Q_i (\in \mathcal{Q}_{P,Q})$ の不等式の集合を C_{Q_i}, Q_iの連立不等式に現れるレジスタと PQ 変数の集合を RV_{Q_i}と書く.

1. $\mathcal{Q}_{P,Q} \leftarrow \{Q\}$.
2. ある $Q_i (\in \mathcal{Q}_{P,Q})$ に着目し, 集合 $\mathcal{Q}_{Q_i}$の初期値を$\emptyset$ として次の操作 (a)–(c) を行なう.

(a) Q_iが連立不等式 (AF4 型原子式の積) のみからなる場合: アクション tによって値が変更される可能性があるようなレジスタの集合を $R_t = \{r \mid t$ の rに関するレジスタ更新関数が $r := r'$でない $\}$ とする. $R_t \cap RV_{Q_i} \ne \emptyset$ であるすべての $t (\in T_A \cup T_B)$ に対し, 以下の手続き (a-1)–(a-3) を実行する.

(a-1) C_{Q_i}と t のレジスタ更新関数と遷移条件から, tの実行後の状態で Q_iが成り立つための条件を表す t 実行前後のレジスタ値, パラメータ値,

表 3: プロトコルΠ_{EX}に関する論理式 F_{EX}

$P_1 = \langle \mathrm{ST}_A, \mathrm{ST}_B \rangle$	$P_2 = \langle \mathrm{ST}_A, \mathrm{ST}_B \rangle$
$\wedge \langle \varepsilon, \varepsilon \rangle$	$\wedge \langle \varepsilon, \varepsilon \rangle$
$\wedge VM_A = VM_B$	$\wedge VM_A = VM_B$
$\wedge VA_A = VA_B$	$\wedge VA_A = VA_B$
$\wedge VM_A = VA_A$	$\wedge VM_A > VA_A$
$\wedge VM_B = VA_B$	$\wedge VM_B > VA_B$
$P_3 = \langle \mathrm{ST}_A, \mathrm{ST}_B \rangle$	$P_4 = \langle \mathrm{ST}_A, \mathrm{ST}_B \rangle$
$\wedge \langle \varepsilon, \mathrm{MIP}^+ \rangle$	$\wedge \langle \varepsilon, \mathrm{MIP}^+ \rangle$
$\wedge\ step1(u_{AB})$	$\wedge\ step1(u_{AB})$
$\wedge VM_A = lastp(u_{AB}) + 1$	$\wedge VM_A = lastp(u_{AB}) + 1$
$\wedge VM_B = firstp(u_{AB})$	$\wedge VM_B = firstp(u_{AB})$
$\wedge VA_A = VA_B$	$\wedge VA_A = VA_B$
$\wedge VM_A > VA_A$	$\wedge VM_A > VA_A$
$\wedge VM_B = VA_B$	$\wedge VM_B > VA_B$
$P_5 = \langle \mathrm{ST}_A, \mathrm{ST}_B \rangle$	$P_6 = \langle \mathrm{ST}_A, \mathrm{ST}_B \rangle$
$\wedge \langle \mathrm{MIA}^+, \varepsilon \rangle$	$\wedge \langle \mathrm{MIA}^+, \varepsilon \rangle$
$\wedge\ st\text{-}inc(u_{BA})$	$\wedge\ st\text{-}inc(u_{BA})$
$\wedge VM_A = VM_B$	$\wedge VM_A = VM_B$
$\wedge VA_B = lastp(u_{BA}) + 1$	$\wedge VA_B = lastp(u_{BA}) + 1$
$\wedge VA_A \leq firstp(u_{BA})$	$\wedge VA_A \leq firstp(u_{BA})$
$\wedge VM_A > VA_A$	$\wedge VM_A > VA_A$
$\wedge VM_B = VA_B$	$\wedge VM_B > VA_B$
$P_7 = \langle \mathrm{ST}_A, \mathrm{ST}_B \rangle$	$P_8 = \langle \mathrm{ST}_A, \mathrm{ST}_B \rangle$
$\wedge \langle \mathrm{MIA}^+, \mathrm{MIP}^+ \rangle$	$\wedge \langle \mathrm{MIA}^+, \mathrm{MIP}^+ \rangle$
$\wedge\ step1(u_{AB})$	$\wedge\ step1(u_{AB})$
$\wedge\ st\text{-}inc(u_{BA})$	$\wedge\ st\text{-}inc(u_{BA})$
$\wedge VM_A = lastp(u_{AB}) + 1$	$\wedge VM_A = lastp(u_{AB}) + 1$
$\wedge VM_B = firstp(u_{AB})$	$\wedge VM_B = firstp(u_{AB})$
$\wedge VA_B = lastp(u_{BA}) + 1$	$\wedge VA_B = lastp(u_{BA}) + 1$
$\wedge VA_A \leq firstp(u_{BA})$	$\wedge VA_A \leq firstp(u_{BA})$
$\wedge VM_A > VA_A$	$\wedge VM_A > VA_A$
$\wedge VM_B = VA_B$	$\wedge VM_B > VA_B$

表 4: 検証に用いたメッセージ系列に関する定義述語, 定義関数

名前	意味
$step1(\alpha)$	αが増分 1 の増加列である.
$st\text{-}inc(\alpha)$	αが狭義単調増加列である
$firstp(\alpha)$	αの先頭メッセージのパラメータ値
$lastp(\alpha)$	αの末尾メッセージのパラメータ値

PQ 変数に関する連立不等式を構成し，$C_{Q_i,t}$とする．

(a-2) tが送信アクションの場合，$C_{Q_i,t}$中の $q'\ op\ k+c$ の形の不等式を抽出し，それらからなる連立不等式を Q'とする．tが受信アクションの場合，$C_{Q_i,t}$中の $sn\ op\ k+c$ の形の不等式を抽出し，それらからなる連立不等式と $\langle d, sn\rangle$ on u_{AB} (または u_{BA})(d は t で受信されるメッセージの型) の論理積を Q'とする．

(a-3) $GS(Q') \subseteq GS(Q_l)$ となる $Q_l \in \mathcal{Q}_{P,Q} \cup \mathcal{Q}_{Q_i}$ が存在しなければ，$\mathcal{Q}_{Q_i} \leftarrow \mathcal{Q}_{Q_i} \cup \{Q'\}$．また，$GS(Q_l) \subseteq GS(Q')$ となる $Q_l \in \mathcal{Q}_{P,Q} \cup \mathcal{Q}_{Q_i}$が存在すれば，$Q_l$を除去する．

(b) Q_iが連立不等式 (AF4 型原子式の積) と $\langle d, sn\rangle$ on u の形の原子式からなる場合: すべての $t(\in T = \{t \mid t$ はメッセージ型 d の送信アクション$\})$ に対し，手続き (b-1)–(b-3) を実行する．

(b-1) C_{Q_i}と t のレジスタ更新関数と遷移条件から，t の実行後の状態で Q_iが成り立つための条件を表す t 実行前後のレジスタ値，パラメータ値，PQ 変数らの間の連立不等式を構成し，$C_{Q_i,t}$とする．

(b-2) $C_{Q_i,t}$中の $q'\ op\ k+c$ の形の不等式を抽出し，それらからなる連立不等式を Q'とする．

(b-3) $GS(Q') \subseteq GS(Q_l)$ となる $Q_l \in \mathcal{Q}_{P,Q} \cup \mathcal{Q}_{Q_i}$ が存在しなければ，$\mathcal{Q}_{Q_i} \leftarrow \mathcal{Q}_{Q_i} \cup \{Q'\}$．また，$GS(Q_l) \subseteq GS(Q')$ となる $Q_l \in \mathcal{Q}_{P,Q} \cup \mathcal{Q}_{Q_i}$が存在すれば，$Q_l$を除去する．

(c) $\mathcal{Q}_{P,Q} \leftarrow \mathcal{Q}_{P,Q} \cup \mathcal{Q}_{Q_i}$.

3. $GS(P) \subseteq \bigcup_{Q_k \in \mathcal{Q}_{P,Q}} GS(Q_k)$ となった場合手続きは終了し，$\mathcal{Q}_{P,Q}$を中間性質の集合とする．そうでない場合，2. へ．

ただし，手続き 2. において $\forall Q_i (\in \mathcal{Q}_{P,Q})\{|\mathcal{Q}_{Q_i}| = 0\}$ となった場合にも手続きは終了する．

【例 2】例 1 で用いたプロトコル$\Pi_{EX} = (PM_A, PM_B)$ と始点性質 $P = (VM_A = k)$，目標性質 $Q = (VA_A \geq k)$ について，集合 $\mathcal{Q}_{P,Q}$を求める．

1. $\mathcal{Q}_{P,Q} \rightarrow \{Q\}$.

2. $Q = (VA_A \geq k)$ に着目する．このとき，$C_Q = (VA_A \geq k)$，$RV_Q = \{VA_A\}$ である．Q は連立不等式 (AF4 型原子式の積) のみからなるので，操作 (a),(c) を行なう．

(a) $R_t \cap RV_Q \neq \emptyset$ であるのは，$t = t_{a,2}$の場合のみである．$t_{a,2}$に対して手続き (a-1) を実行した結果，$C_{Q,t_{a,2}} = \{(VA_A \geq k) \wedge (VM'_A \geq sn + 1) \wedge (sn \geq VA'_A) \wedge (VM_A = VM'_A) \wedge (VA_A = sn + 1) \wedge (VM'_A \geq sn + 1) \wedge (VM_A \geq VA'_A + 1) \wedge (VM_A \geq VA_A) \wedge (VM_A \geq k) \wedge (VM'_A \geq VA'_A + 1) \wedge (VM'_A \geq VA_A) \wedge (VM'_A \geq k) \wedge (sn + 1 \geq k)\}$ が得られる．$C_{Q,t_{a,2}}$に対して (a-2) を実行した結果，$Q' = ((\langle \mathrm{MIA}, sn\rangle \text{ on } u_{BA}) \wedge (sn \geq k - 1))$ が得られる．さらに (a-3) を実行した結果，$\mathcal{Q}_Q = \{Q'\}$ が得られる．

(c) $\mathcal{Q}_{P,Q} \leftarrow \{Q\} \cup \{Q'\})$.

以下，同様に手続きを続行し，

$$\mathcal{Q}_{P,Q} = \{(VA_A \geq k),\ ((\langle \mathrm{MIA}, sn\rangle \text{ on } u_{BA}) \wedge (sn \geq k - 1)),\ (VM_B \geq k),\ ((\langle \mathrm{MIP}, sn\rangle \text{ on } u_{AB}) \wedge (sn \geq k - 1)),\ (VM_A \geq k - 1)\}$$

$(GS(P) \subseteq \bigcup_{Q_l \in \mathcal{Q}_{P,Q}} GS(Q_l))$ が得られる． □

$Q_j\ (\in \mathcal{Q}_i)$ の連立不等式は，プロトコルがあるアクションを実行して Q_iが成立する状態へ遷移することの必要条件の一つになっている．また，状態遷移の定義より，あるメッセージの受信アクションが実行されるためには，通信路上にそのメッセージが存在している必要がある．さらに，文献 [1] の検証法によってプロトコルΠが未定義受信状態を含まないことが保証されているため，通信路上のメッセージはいずれ必ず受信される．従って，条件 $\langle d, p\rangle$ on u を満たす状態を経由することは，メッセージ $\langle d, p\rangle$ の受信アクションが実行されるための必要十分条件である．従って，各 $Q_j\ (\in \mathcal{Q}_i)$ はそれぞれプロトコルがアクション t を実行して Q_iが成立する状態へ遷移する

ことの必要条件であり，また$\bigvee_{Q_j \in \mathcal{Q}_{\cdot}} Q_j$は$Q_i$が成立する状態へ遷移することの必要条件である．従って，$\bigvee_{Q_j \in \mathcal{Q}_{P,Q}} Q_j$は，プロトコルΠが性質$Q$が成り立つ状態に到達することの必要条件になっている．従って，$\forall Q_i (\in \mathcal{Q}_{P,Q})\{|\mathcal{Q}_{Q_i}| = 0\}$となって手続きが終了した場合，$P \rightsquigarrow Q$は成立しない．また，$P \rightsquigarrow Q$であっても手続きが停止せず，検証に失敗する場合も考えられる．

こうして求めた各中間性質によって，可達状態集合RS_Πを分割することを考える．文献[1]の安全性の検証法によってプロトコルΠの不変式であること，およびいかなるデッドロック状態，未定義受信状態でも成立しないことが証明された論理式を$F = F_1 \vee F_2 \vee \cdots \vee F_{n_F}$とする．ただし，$GS(F_i)$と$GS(F_j)\,(i \neq j)$は互いに素であり，$GS(F_i)$に属する全ての状態が各アクション$t \in T_A \cup T_B$の遷移条件を満たすか満たさないかのどちらかに定まるものとする．この論理式の各積項F_iを，$GS(F_{i,j})$に属する全ての状態が各中間性質$Q_k\,(\in \mathcal{Q}_{P,Q})$を満たすか満たさないかのどちらかに定まるような$F_{i,j}\,(1 \leq j \leq n_i)$に分割する．

以下，この条件を満たさないような積項F_iを分割する手法について述べる．(i) 連立不等式のみからなる$Q_k\,(\in \mathcal{Q}_{P,Q})$については，$Q_k$の不等式それぞれについて満たされる場合と満たされない場合に場合分けを行なう．これらすべての場合の積項を生成し，分割後の積項とする．(ii)(i) 以外の場合，$Q_k\,(\in \mathcal{Q}_{P,Q})$は$\langle d, sn\rangle$ on uの形の原子式とsnに関する連立不等式からなる．この場合には (i) の手法をそのまま適用することはできない．このとき，不変式記述の際に定義述語を用いて表したパラメータ系列の単調性を利用してQ_kと等価な連立不等式を求め，それについて積項を分割することを考える．この連立不等式は，検証者によって与えられた単調系列の性質に関する補題を用いて導出する．例として，増分1の増加数列の性質に関する補題を示す．

【例3】増分1の増加数列に関する補題として，以下のようなものを用いる．以下，数列αのi番目の要素をα_iと表す．また，"⇒" は含意を表す．

[増分1の増加数列の性質に関する補題1]

$\forall k\ \forall \alpha \in \mathcal{N}^*\{step1(\alpha) \Rightarrow (\exists i\{\alpha_i \geq k\} \Leftrightarrow \alpha_n \geq k)\}$

すなわち，メッセージ型dに関して$step1(u, \{d\})$が成り立っている場合，条件$\exists sn\{(\langle d, sn\rangle \text{ on } u) \wedge (sn \geq k)\}$は$lastp(u, \{d\}) \geq k$という条件と等価である．□

以下，すべての$F_{i,j}\,(1 \leq i \leq n_F, 1 \leq j \leq n_i)$の論理和からなる式を$D = D_1 \vee D_2 \vee \cdots \vee D_n$とする．こうして分割を行なった結果，各中間性質$Q_j\,(\in \mathcal{Q}_{P,Q})$を満たす可達状態の集合は$GS(D_1), GS(D_2), \ldots, GS(D_n)$の中のいくつかの和集合，すなわち$(GS(Q_j) \wedge GS(F)) = \bigcup_{i \in I_{Q_j}} GS(D_i)$ $(I_{Q_j} \subseteq \{i \mid 1 \leq i \leq n\})$の形で表すことができる．

4.2 leads-to 到達可能性グラフ

定義 4 論理式$D_\Pi = D_1 \vee D_2 \vee \cdots \vee D_n$の各$D_i\,(1 \leq i \leq n)$に対応する頂点を$v_i$とし，$V = \{v_1, v_2, \cdots, v_n\}$とする．有向グラフ$G = (V, E_1 \cup E_2)$が以下の性質を満たすとき，$G$をΠの leads-to 到達可能性グラフという．

$(v_i, v_j) \in E_1 \Rightarrow \exists gs' \in GS(D_i)\ \exists gs \in GS(D_j)\{gs' \rightarrow gs\}$

$(v_i, v_j) \in E_2 \Rightarrow \neg\exists \tau_1 \tau_2 \tau_3 \ldots \in TS^{\infty}_{\Pi}\ \{(|\{gs_k \mid gs_k \in GS(D_i)\}| = \infty) \wedge \forall l\{gs_l \notin GS(D_j)\}\}$ □

4.3 leads-to 到達可能性グラフの構成法

以下では，leads-to 到達可能性グラフ$LRG_{\Pi,F} = (V, E_1 \cup E_2)$の構成法のうち，辺集合$E_1, E_2$を求める手法について説明する．

4.3.1 E_1の辺の求め方

すべての頂点$v_i, v_j \in V$について，$(v_i, v_j) \in E_1$であるような辺を次のように求める．

(i) D_iを満たすある状態で実行可能なアクション$t \in T_A \cup T_B$をすべて求める．

(ii) (i) で求めたアクションtごとに，tが実行可能なある状態$gs' \in GS(D_i)$からtによる状態遷移により遷移可能な状態gsにおいて積項D_jが成立する，すなわちD_j中のすべての原子式が成立するとき，$(v_i, v_j) \in E_1$であるとする．

積項D_jの成立を示す部分は，文献[1]で述べられている手法を用いることができる．

4.3.2 E_2の辺の求め方

$(v_i, v_j) \in E_2$であるのは，以下の (E2a)-(E2c) の条件のいずれかが成り立つ場合である．

(E2a) $\forall gs' \in GS(D_i)\ \exists gs \in GS(D_j)\{gs' \rightarrow gs\}$

(E2b) $\exists \langle d, sn\rangle\{(GS(D_i) \subseteq GS(\langle d, sn\rangle \text{ on } u)) \wedge \forall gs' \in GS(D_i)\ \exists gs \in GS(D_j)\{gs'$で$\langle d, sn\rangle$を受信した場合の遷移先が$gs\}\}$

(E2c) ある送信アクションtが存在し，
$\neg\exists \tau_1 \tau_2 \tau_3 \ldots \in TS^{\infty}_{\Pi}\{(|\{gs_k \mid gs_k \in GS(D_i)\}| = \infty) \wedge \forall gs \in GS(D_i)\{gs$ で t が実行可能 $\} \wedge \neg\exists (gs_{k-1}, t, gs_k)\{(gs_{k-1} \in D_i) \wedge (gs_k \in D_j)\}\}$

(E2a) の条件のうち，AF4 型原子式の成立を以下のように示す．ある$gs'\,(\in GS(D_i))$で実行されることで$gs\,(\in GS(D_j))$へ遷移するようなアクションtについて，tの遷移条件，レジスタ更新関数，D_iのAF4 型原子式から，t実行後のレジスタ値に関する連立方程式C_tを構成する．この連立方程式とD_jのAF4 型原子式C'について$C_t \Rightarrow C'$であれば，D_iから遷移する任意の状態でD_jのAF4 型原子式が成立する．これは，連立不等式の解の存在判定に帰着できる．AF1–3 型原子式はE_1と同様の方法で行なう．

(E2b) について，$\exists \langle d, sn\rangle\{GS(D_i) \subseteq GS(\langle d, sn\rangle \text{ on } u)\}$であることは，$\exists Q_k \in \mathcal{Q}_{P,Q}\{(Q_k$が原子式$\langle d, sn\rangle$ on uを含む$) \wedge (GS(D_i) \subseteq GS(Q_k))\}$であることを示せばよい．受信を行なった際の遷移先についての条件は，(E2a) と同様の方法により示せる．

(E2c) の成立は$\forall gs \in GS(D_i)\{gs$ で t が実行可能 $\}$であるような各アクションtに対して以下のような手続きを適用し，十分条件の判定を行う．以下，遷移trで送信されるメッセージのパラメータ値を$prm(tr)$，遷移系列ts中のアクションtによる遷移で送信 (受信) されるメッセージ系列のパラメータ系列を$prm(t, ts)$で表す．

1. 不変式記述の際に定義述語を用いて表した単調数列の性質pについて，$GS(D_i)$に属する状態から始まる任意の状態遷移系列tsが$p(prm(t, ts))$を満たすことを示す．例えば$step1(prm(t, ts))$を満たすことを示す．

2. tの遷移条件，レジスタ更新関数，D_iのAF4型原子式から，D_iを満たす状態でのアクションtによる遷移の実行前後のレジスタ値に関する連立不等式を構成する．この連立不等式とD_jのAF4型原子式からなる連立不等式より，送信されるメッセージのパラメータ値とPQ変数との間の連立不等式を構成し，$C_{t,sn}$とする．このとき，$C_{t,sn}$の不等式 $sn\ op\ k+c$ (snは送信されるメッセージのパラメータ値，opは比較演算子$\geq, \leq$のいずれか，kはPQ変数，cは整定数) それぞれに対して$prm(t,ts)$で成立するある性質pが存在し，$op_p = op$であることを示す．ここで，op_pは検証者がpに対して与える比較演算子である．例えば，$C_{t,sn} = (sn \geq k-1)$ (kはPQ変数) であり，さらに状態遷移系列tsである性質pが成立して$op_p =$ "$\geq$"であればよい．

この手続きにおいて，op_pは任意のlについて
$\neg\exists ts = \tau_1\tau_2\tau_3\ldots \in TS^{\infty}_{\Pi}\{p(prm(t,ts))\wedge$
$(prm(t,ts)$が無限系列$)\wedge\neg\exists m\ \forall n\{(n\geq m)\wedge(tr_n$は$t$による遷移$)\wedge(sn = prm(tr_n))\Rightarrow(sn\ op_p\ l)\}\}$
が成り立つような，検証者によって与えられた比較演算子である．例えば，性質$step1$に関しては，以下のような性質より，$op_{step1} =$ "$\geq$"という条件が得られる．
[増分1の増加数列の性質に関する補題2]
任意のlについて$\neg\exists\alpha\in\mathcal{N}^*\{step1(\alpha)\wedge\neg\exists m\ \forall n\{(n\geq m)\Rightarrow(\alpha_n\geq l)\}\}$ □
1,2.により，
$\neg\exists ts = \tau_1\tau_2\tau_3\ldots \in TS^{\infty}_{\Pi}\{p(prm(t,ts))\wedge$
$(prm(t,ts)$が無限系列$)\wedge\neg\exists m\ \forall n\{(n\geq m)\wedge(tr_n$は$t$による遷移$)\wedge(sn = prm(tr_n))\Rightarrow(sn$は$C_{t,sn}$を満たす$)\}\}$
が示される．ここで，$C_{t,sn}$はD_iが成り立つ状態からtを実行したときにD_jが成り立つ状態へ遷移するための必要十分条件になっている．従って，
$\neg\exists ts = \tau_1\tau_2\tau_3\ldots \in TS^{\infty}_{\Pi}\{p(prm(t,ts))\wedge$
$(prm(t,ts)$が無限系列$)\wedge\neg\exists(gs_{l-1},t,gs_l)\{(gs_{l-1}\in D_i)\wedge(gs_l\in D_j)\}\}$
が得られる．さらに，遷移系列tr中に現れるgs_lのうちD_iを満たすものの数が無限であれば，以下のような状態遷移の公平性によって$prm(t,ts)$が無限系列となることが導かれ，(E2c)の成立が示される．
[状態遷移の公平性]
$\neg\exists\tau_1\tau_2\tau_3\ldots \in TS^{\infty}_{\Pi}\{\forall t\in T_A\cup T_B\{(|\{gs_i\,|\,gs_i$で$t$が実行可能$\}| = \infty)\wedge(t_j$のうち$t_j = t$であるものの数が有限$)\}\}$ □

次に，上記の1.が成立することを示す手法について述べる．ここでは，例としてpが増分1の増加数列であるという性質の場合を挙げる．ある状態遷移系列tsにおいてアクション$t1$によって送信されるメッセージ系列のパラメータ系列が増分1の増加数列であることの十分条件として，検証者が次のような条件を記述する．ここで，アクションtの遷移関数とレジスタ更新関数から構成したアクション実行前後のレジスタ値，パラメータ値の間で満たされるべき条件を表す関係式の集合をC_tと書く．
$\exists r$(プロトコル機械のレジスタ)$\{\exists c\in\mathcal{Z}\{(C_{t1}\Rightarrow((sn = r'+c)\wedge(r = r'+1))\}\wedge\forall t2\in T_A\cup T_B\{(t2\neq t1)\wedge(C_{t2}\Rightarrow r\neq r')\Rightarrow\{ts$は$t2$による遷移を含まない$\}$

この条件のうち，アクション$t1, t2$実行前後のレジスタ値，パラメータ値に関する条件は，C_{t1}, C_{t2}について(E2a)のAF4型原子式の判定と同様の手法を用いて示すことができる．また，tsが$t2$による遷移を含まないという条件は，$t2$の遷移条件を満たすような状態集合に到達可能でないことを示せば良い．他の単調性についても，適当な条件を与えてやることで同様の手法が適用可能である．

4.4 leads-to 到達可能性グラフ $LRG_{\Pi,F}$の解析

leads-to到達可能性グラフ$LRG_{\Pi,F} = (V, E_1\cup E_2)$が得られたとする．ここで，$LRG_{\Pi,F}$によって定義される条件$GS(D_i)\rightsquigarrow_G GS(D_j)$を次のように定義する．

定義 5 以下の条件が成立するとき，$GS(D_i)\rightsquigarrow_G GS(D_j)$が成立する．
$\exists D_k\{((v_i,v_k)\in E_2)\wedge(GS(D_k)\rightsquigarrow_G GS(D_j))\}\vee$
$\forall D_k\{((v_i,v_k)\in E_1)\Rightarrow(GS(D_k)\rightsquigarrow_G GS(D_j))\}$ □

$GS(D'_l)\rightsquigarrow GS(D_l)$を示す際に，ある積項の集合$\mathcal{D}$が存在して$GS(D'_l)\subseteq\bigcup_{D_k\in\mathcal{D}}GS(D_k)\}$であるとすると，十分条件$\forall D_k\in\mathcal{D}\{GS(D_k)\rightsquigarrow GS(D_l)\}$であることを示しても良い．このとき，$LRG_{\Pi,F}$を探索し，$\exists gs\in GS(D_i)\{gs\in GS(P)\}$であるような$v_i$から到達可能な頂点$v_k$すべてについて$\exists D_l\{(GS(D_k)\rightsquigarrow_G GS(D_l))\wedge(GS(D_l)\subseteq GS(Q))\}$の成立が示されたならば，$P\rightsquigarrow Q$であることが示される．

5 検証システム

文献[1]の安全性の検証システムを基にして，leads-to性の検証手続きを実行する検証システムを試作中である．この検証システムは，プロトコルΠの定義，Πの不変式であることが示されている論理式F，検証手続きに用いる検証者が導入した定義述語および定義関数の性質を表す補題，そして検証したい性質$P\rightsquigarrow Q$を入力として，4の検証手続きを実行する．

中間性質の集合を求めるのに失敗したと判定した場合，その時点での$\mathcal{Q}_{P,Q}$を検証者に示し，手続きを終了する．また，$LRG_{\Pi,F}$を探索した結果$P\rightsquigarrow Q$が示せなかった場合，$LRG_{\Pi,F}$と失敗の原因となった積項を検証者に示し，手続きを終了する．

6 まとめ

本論文では，プロトコル機械が有限制御部と有限個の非負整数値レジスタを持つ拡張有限状態機械でモデル化され，通信路が非有界FIFOでモデル化された通信プロトコルの時制に関する性質のうち，関係"$\rightsquigarrow$"で表される性質の検証法を提案した．

参考文献

[1] Higuchi M. et al. : "A Verification Method via Invariant for Communication Protocols Modeled as Extended Communicating Finite-State Machines", *IEICE Trans. Commun.* vol.E-76B, no.11, pp.1363–1372 (1993-11).

[2] 須川他 : "拡張有限状態機械でモデル化された通信プロトコルの生存性の検証法", 信学論 (B-I), vol.J78-B-I, no.1, pp.17–28 (1995-01).