ソフトウェア工学 96−30
（1994．1．21）

拡張有限状態機械モデルの通信プロトコルのlivenessの検証法

須川 聡† 樋口 昌宏† 藤井 護‡

†大阪大学基礎工学部 ‡大阪大学教養部

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

筆者らは，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安全性の検証法を提案している．本稿では，同様にモデル化され，上記検証法により安全性が保証されているプロトコルのlivenessの検証法を提案する．まず，livenessを初期状態から到達可能な任意の状態からある性質Qを満たす状態に到達可能であるという性質(Q-live性)として定式化する．安全性の検証によりプロトコルΠの初期状態から到達可能な状態集合が部分集合$GS_1, GS_2, \cdots, GS_n$に分割されているとする．このとき，各頂点$v_1, v_2, \cdots, v_n$がそれぞれ$GS_1, GS_2, \cdots, GS_n$に対応し，v_iからv_jへの辺があるならば「$\forall gs \in GS_i \exists gs' \in GS_j${$gs$から$gs'$に到達可能}」であるような有向グラフ$DRG_\Pi$を作る．さらに，$DRG_\Pi$上を探索することにより，Πの$Q$-live性を示す．OSIセションプロトコルのデータ転送フェーズから抽出したプロトコルのQ-live性の検証を行った結果についても述べる．

A Method for Verifying Liveness of Communication Protocols Modeled as ECFSMs

Satoshi Sugawa† Masahiro Higuchi† Mamoru Fujii‡

†Faculty of Engineering Science, Osaka University
‡College of General Education, Osaka University

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

The authors of this paper proposed a method for verifying safety of communication protocols modeled as two ECFSMs with bilateral unbounded FIFO channels connecting them. This paper presents a method for verifying liveness of communication protocols which have been already verified to be safe by the above method. Liveness property can be formulated as Q-liveness which states "any state reachable from an initial state can reach a state which satisfies some property Q". In the proposing verification method, a set of states reachable from an initial state of a given protocol Π is divided into some subsets $GS_1, GS_2, \cdots, GS_n$. Our method constructs a directed graph DRG_Π whose vertex $v_i (1 \leq i \leq n)$ represents GS_i and whose edge from v_i to v_j expresses "$\forall gs \in GS_i \exists gs' \in GS_j${$gs'$ is reachable from gs}". By exploring DGR_Π, Π is showed to be Q-live. A sample protocol extracted from the data transfer phase of the OSI session protocol was verified by the proposing method.

1 まえがき

通信プロトコルなどの並行システムに求められる基本的な性質に安全性と liveness がある．安全性とはデッドロックなどの好ましくないことが起こらないという性質であるのに対して，liveness とは「興味のあるメッセージの送信が行なわれる」，「正常終了状態に到達する」などの好ましいことがいずれ起こるという性質である．プロトコル機械の状態数が有限で，通信路の有界性が保証されているならば，プロトコルの状態数は有限であり，有限の状態空間を探索することによって安全性と liveness は決定可能であることが知られている[1] [2]．しかし，実用プロトコルでは通信路の有界性が成り立たない場合や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 context variable を持つ拡張有限状態機械でモデル化される場合も多い．このような場合にはプロトコルの状態空間は無限集合となるので，文献 [1], [2] の方法は適用できない．状態空間が有限でないプロトコルの検証法については，プロトコル機械が有限状態機械でモデル化され，通信路が非有界であるプロトコルの安全性の検証法の研究がさかんに行なわれている[3] [4]．また，筆者らはプロトコル機械が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，通信路が長さに制限のない FIFO でモデル化された通信プロトコルの安全性の検証法を考案し，そのための検証システムを試作している[5]．

Finkel は liveness を初期状態から到達可能な任意の状態 s と任意の状態遷移 tr に対して，状態 s から到達可能なある状態で状態遷移 tr が実行可能であるという性質であると定義し，有限状態機械モデルで通信路が非有界のプロトコルの liveness の検証法を議論している．本稿では，Q-live 性を初期状態から到達可能な任意の状態からある性質 Q を満たす状態に到達可能であるという性質であると定義する．文献 [5] と同様にモデル化され，文献 [5] の検証法によって安全性が保証されている通信プロトコルに対する Q-live 性の検証法を提案する．安全性の検証によりプロトコルΠの初期状態から到達可能な状態の集合がいくつかの部分集合 $GS_1, GS_2, \cdots, GS_n$ に分割され，また性質 Q は $\bigcup_{i\in I_Q} GS_i$ $(I_Q \subseteq \{i \mid 1 \leq i \leq n\})$ の形の状態集合で指定されているものとする．各 $GS_i (1 \leq i \leq n)$ に対応して頂点 v_i を考え，$V = \{v_1, v_2, \cdots, v_n\}$ とする．以下のような性質を持つ縮退到達可能性グラフ $DRG_\Pi = (V, E)$ を生成する．

$(v_i,v_j)\in E$ ならば，$\forall gs\in GS_i \exists gs'\in GS_j \{gs$ から gs' に到達可能$\}$

以下が成立することを示すことにより，プロトコルΠが Q-live であることが示される．

$\forall i\ (1\leq i\leq n)\ \exists j \in I_Q \{DRG_\Pi$ 上で v_i から v_j への道がある$\}$

2 プロトコルモデル

本稿では，プロトコル機械を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し，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 でモデル化したプロトコルを取り扱う．形式的には以下のように定義する．

定義 1 プロトコル機械を以下のような拡張有限状態機械 (S, Σ, T, SI) として定義する．

(M1) $S = \langle SF, r\rangle$: プロトコル機械の状態集合を定義する 2 字組．SF 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の数を表す．プロトコル機械の取り得る状態の集合は $SF \times \mathcal{N}^r$ となる ($\mathcal{N}$ は非負整数の集合を表す)．

(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である．Σ_-, Σ_+ は互いに素であるとする．各メッセージは非負整数値パラメータを一つ持つものとする．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．アクションは以下のような 5 字組 (sf, d, sf', C, R) である．$sf \in SF, d \in \Sigma, sf' \in SF$, C は状態遷移前のプロトコル機械のレジスタ値 $p_1, p_2, \cdots, p_r$ と送信または受信メッセージのパラメータ値 p が満たすべき連立線形不等式で，遷移条件と呼ばれる．R は状態遷移前のプロトコル機械のレジスタ値 $p_1, p_2, \cdots, p_r$ 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 $p_1, p_2, \cdots, p_r$ を定める $\mathcal{N}^{r+1}$ から $\mathcal{N}^r$ への部分関数で，レジスタ更新関数と呼ばれる．T によって，$SF \times \mathcal{N}^r \times \Sigma \times \mathcal{N}$ から $SF \times \mathcal{N}^r$ への非決定性状態遷移関数 δ_T は以下のように定義される．

$$\delta_T((sf, p_1, p_2, \cdots, p_r), \langle d, p\rangle) = \{(sf', R(p_1, p_2, \cdots, p_r, p)) \mid (sf, d, sf', C, R) \in T \text{かつ } p_1, p_2, \cdots, p_r, p \text{ は } C \text{を満たす}\}$$

(M4) $SI \subseteq SF \times \mathcal{N}^r$: 初期状態の集合． □

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 $gs = (s_A, s_B, ch_{BA}, ch_{AB})$ $(s_A \in SF_A \times \mathcal{N}^{r_A}, s_B \in SF_B \times \mathcal{N}^{r_B}, ch_{BA} \in (\Sigma_{BA} \times \mathcal{N})^*$, $ch_{AB} \in (\Sigma_{AB} \times \mathcal{N})^*)$ 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 PM_A, PM_B の状態を表し，ch_{BA}, ch_{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す．以下では，混乱のない限り系の状態を単に状態と呼ぶことがある．$gs_I = (si_A, si_B, \varepsilon, \varepsilon)$ $(si_A \in SI_A, si_B \in SI_B, \varepsilon$ は空系列) をΠの初期状態と呼ぶ． □

定義 3 プロトコル $\Pi = (PM_A, PM_B)$ の任意の状態 $gs = (s_A, s_B, u_{BA}, u_{AB})$ および $gs' = (s'_A, s'_B, u'_{BA}, u'_{AB})$ に対して，ある $d \in \Sigma_{AB}, p \in \mathcal{N}$ が存在して次の (TA1) または (TA4) が成立するとき，またはある $d \in \Sigma_{BA}, p \in \mathcal{N}$ が存在して次の (TA2) または (TA3) が成立するとき gs から gs' に遷移可能であるといい，$gs \rightarrow gs'$ と書く．

(TA1) $s'_A \in \delta_{T_A}(s_A, \langle d, p\rangle)$, $s'_B = s_B$, $u'_{BA} = u_{BA}$, $u'_{AB} = u_{AB} \cdot \langle d, p\rangle$

(TA2) $s'_A \in \delta_{T_A}(s_A, \langle d, p\rangle)$, $s'_B = s_B$, $\langle d, p\rangle \cdot u'_{BA} = u_{BA}$, $u'_{AB} = u_{AB}$

(TA3) $s'_A = s_A$, $s'_B \in \delta_{T_B}(s_B, \langle d, p\rangle)$, $u'_{BA} = u_{BA} \cdot \langle d, p\rangle$, $u'_{AB} = u_{AB}$

(TA4) $s'_A = s_A$, $s'_B \in \delta_{T_B}(s_B, \langle d, p\rangle)$, $u'_{BA} = u_{BA}$, $\langle d, p\rangle \cdot u'_{AB} = u_{AB}$

関係 $\rightarrow$ の反射推移閉包を $\stackrel{*}{\rightarrow}$ と書く．$gs \stackrel{*}{\rightarrow} gs'$ のとき，gs から gs' に到達可能であるという．プロトコルΠにおいて初期状態から到達可能である状態の集合を RGS_Π と書く． □

3 安全性の検証法

2で述べたモデルのプロトコルの安全性 (3.1 参照) を不変式を用いて検証する方法[5] について説明する.

プロトコルΠの初期状態から到達可能な任意の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 Pを満たす系の状態の集合を $GS(P)$ と書く. 文献 [5] で提案している検証法では, (a) 検証者の記述した論理式 Fが不変式, すなわち $GS(F) \supseteq RGS_{\Pi}$であること, (b) $GS(F)$ が安全でない状態を含まないこと, を証明する. (a) と (b) が示されれば, Πは安全であると結論できる.

3.1 安全性

プロトコル$\Pi = (PM_A, PM_B)$ の安全性を以下のように定義する.

定義 4 状態 $gs = (s_A, s_B, \varepsilon, \varepsilon)$ において, 任意の $d \in \Sigma_{AB}$, $p \in \mathcal{N}$に対して$\delta_{T_A}(s_A, \langle d, p\rangle) = \phi$, かつ任意の $d \in \Sigma_{BA}$, $p \in \mathcal{N}$に対して$\delta_{T_B}(s_B, \langle d, p\rangle) = \phi$ であるとき, gs は (空チャネル) デッドロック状態であるという. 空でないメッセージ系列αに対して, $head(\alpha)$ はαの先頭のメッセージを表すとする. 状態 $gs = (s_A, s_B, ch_{BA}, ch_{AB})$ に対して, $ch_{BA} \neq \varepsilon$かつ$\delta_{T_A}(s_A, head(ch_{BA})) = \phi$, または $ch_{AB} \neq \varepsilon$ かつ$\delta_{T_B}(s_B, head(ch_{AB})) = \phi$ であるとき, gs は未定義受信状態であるという. プロトコルΠの初期状態からデッドロック状態および未定義受信状態に到達可能でないとき, プロトコルΠは安全であるという. □

3.2 不変式の記述

検証者は, プロトコルΠ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プロトコル機械の状態と通信路上のメッセージ系列を考慮して, 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). さらに, 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 $(i = 1, 2, \cdots, n)$ として記述し, $F = P_1 \vee P_2 \vee \cdots \vee P_n$とする.

(AF1) PM_A, PM_Bの有限制御部の状態の 2 字組 $\langle sf_A, sf_B\rangle$: PM_A, PM_Bの有限制御部の状態がそれぞれ sf_A, sf_B であることを表す.

(AF2) Σ_{BA}上の正規表現とΣ_{AB}上の正規表現の 2 字組 $\langle R_{BA}, R_{AB}\rangle$: 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型系列 $type(ch_{BA})$, $type(ch_{AB})$ に対し, $type(ch_{BA}) \in \mathcal{L}(R_{BA}), type(ch_{AB}) \in \mathcal{L}(R_{AB})$ 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, メッセージ型系列 $type(\alpha)$ はメッセージ系列αからメッセージ型のみを取り出した系列である. 例えば, $\langle \varepsilon, \text{MIP}^+\rangle$ は, PM_Bから PM_Aへの通信路上にはメッセージが無く, PM_Aから PM_Bへの通信路上のメッセージ型系列が 1 個以上の MIP から成る系列であることを表す.

(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によって記述した式. ここで, パラメータ系列とはメッセージ系列からパラメータ値のみを取り出した系列である. 例えば, $step1(ch_{AB})$ は, PM_Aから PM_Bへの通信路上のメッセージ系列 ch_{AB}のパラメータ系列が, 述語 $step1$ について定義された性質を満たしていることを表す. ここで, $step1$ は表 1のように定義される述語である.

(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からなる線形方程式または線形不等式. 例えば, $VM_A = last(ch_{AB}) + 1$ は, PM_Aのレジスタ VM_Aの値が PM_Aから PM_Bへの通信路上のメッセージ系列 ch_{AB}の末尾の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. ここで, $last(\alpha)$ はメッセージ系列α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.

以下では, 各 P_iにおいて AF1 型原子式, AF2 型原子式はそれぞれちょうど一つずつ記述されているものとする. P_i中の PM_A(または PM_B) に関する AF1 型原子式で指定された PM_A(または PM_B) の有限制御部の状態を $sf_A(P_i)$(または $sf_B(P_i)$) と書く.

【例】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$\Pi_{EX} = (PM_A, PM_B)$ とΠ_{EX}に関する論理式 F_{EX}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設定を行なう. PM_Aは MIP を送信するごとに同期点番号を 1 ずつ増加する. PM_Bは受信した MIP 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 PM_Aに送信することにより同期点応答を行なう. PM_Bは必ずしもすべての MIP に応答する必要はなく, 対応する MIA を送信しないこともある. しかし, PM_Bが MIA 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をパラメータ値とする MIA 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番号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の有限状態部はそれぞれ 1 状態 "STA713" のみからなるとする. PM_A,PM_Bはそれぞれ表 2に記されたような 2 つのレジスタ VM_Aと VA_A,VM_Bと VA_Bを持つ.
- Σ_{AB}={MIP}, Σ_{BA}={MIA}.
- PM_A, PM_Bのアクションは表 3で定義する. $tb1$ は, PM_Bについて有限制御部の状態が "STA713" で, レジスタ VM_B, VA_Bの値が $VM_B > VA_B$を満たすとき, $VM_B = sn + 1, sn \geq VA_B$を満たすような sn をパラメータ値とする型 MIA のメッセージ $\langle$MIA, $sn\rangle$ を送信するアクションであり, 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 (1)PM_Aから PM_Bへの通信路上に MIP があるかないか, (2)PM_Bから PM_Aへの通信路上に MIA があ

るかないか, (3)PM_BがMIA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. その一つである図 1のような状態集合について考える. この集合中の任意の状態で成立する論理式を表 4の式P_4のように記述する. ここで, 定義述語, 定義関数としてそれぞれ表 1, 表 5に記したものを用いている. 同様にして, 残りの状態集合についてもその集合中の任意の状態で成立する論理式 $P_i(1 \leq i \leq 8)$ を表 4のように記述する. $F_{EX} = P_1 \vee P_2 \vee \cdots \vee P_8$とする.

3.3 安全性の検証手続き

論理式 $F = P_1 \vee P_2 \vee \cdots\cdots \vee P_n$ がプロトコルΠの不変式であることを, 系の状態遷移系列に関する構造的帰納法を用いて以下のように証明する.

- 初期段階 : Πの各初期状態において, ある $P_i(1 \leq i \leq n)$ が成立することを示す.
- 帰納段階 : 各 $P_i(1 \leq i \leq n)$ について, P_iを満たす任意の状態から遷移可能な任意の状態で論理式 Fが成立することを以下の手順で証明する.
  - (i) 各アクション$t \in T_A$(または$t \in T_B$)について, P_iを満たすある状態でtが実行可能であるかどうかを調べる.
  - (ii) (i)で求めた アクションtごとに, 次を示す. アクションtが実行可能な任意の状態 $gs \in GS(P_i)$ からtによる状態遷移によって遷移可能な状態において成立する P_jが少なくとも一つは存在する, すなわち P_j中のすべての原子式が成立する. P_j中の AF3 型原子式の成立は項書換え系上での項の書き換えによって示す. P_j中の AF4 型原子式の成立は連立線形不等式を解くことによって判定できる.

論理式 Fが不変式であることが示され, さらに不変式 Fを満たす状態集合 $GS(F)$ がデッドロック状態および未定義受信状態を含まないことが示されれば, Πが安全であると結論できる. Fが不変式であることの上記証明法の帰納段階の証明過程, および $GS(F)$ がデッドロック状態または未定義受信状態を含むかどうかの判定を自動化する検証システムが試作されている[5].

4 livenessの検証法

ここでは, 3で述べた検証法により安全性が保証されているプロトコルの livenessの検証法について述べる.

4.1 Q-live性

livenessを以下の Q-live 性として定式化する.

定義 5 プロトコルΠにおいて性質 Q を満たす状態集合をGS_Qとする. 以下が成立するとき, Πは Q-liveであるという.

$$\forall gs \in RGS_\Pi\ \exists gs' \in GS_Q\ \{gs \xrightarrow{*} gs'\} \qquad \square$$

例えば, Q を興味のあるアクション t が実行可能であるという性質とすると, Q-live 性は, 初期状態から到達可能な任意の状態から t がいずれ実行可能になるという性質になる. また, Q を正常終了状態であるという性質とすると, Q-live 性は常に正常終了状態に到達可能であるという性質になる.

プロトコルΠにおいて, 有向グラフ $RG_\Pi = (RGS_\Pi, \{(gs, gs') \mid gs \rightarrow gs'\})$ をΠの到達可能性グラフという. RGS_Π が有限集合となる場合には RG_Πも有限であるので, RG_Π上を model checking[2]等の手法によって探索することにより, 時制論理の式として表された Q-live 性を検証することができる.

しかし, 本稿で扱うプロトコルモデルのように RGS_Πが無限集合となる場合には, その到達可能性グラフ RG_Πも有限でなくなるので, 上記の方法を適用できない. 以下では, RGS_Π が無限集合となる場合の Q-live 性の検証法について考える. RGS_Πを有限個の部分集合 $GS_1, GS_2, \cdots, GS_n$に分割する. 各 GS_iに対応して頂点 v_iを考え, $V = \{v_1, v_2, \cdots, v_n\}$ とする. 以下のような有向グラフ $G = (V, E)$ を考える.

$$\forall gs \in GS_i \exists gs' \in GS_j \{gs \rightarrow gs'\} \Leftrightarrow (v_i, v_j) \in E \qquad (1)$$

ただし, $\Leftrightarrow$ は同値関係を表す. このとき, ある $i(1 \leq i \leq n)$ に対して $GS_Q = GS_i$とすると, G 上を探索することによりプロトコルΠの Q-live 性を示すという方法が考えられる. しかしながら, (1) の条件が強すぎるため, 適用できる場合が極めて限定されたものになる. そこで, 4.2では以下のような性質を持つ有向グラフ $G' = (V, E')$ を生成し, G'上を探索することにより, Πの Q-live 性を示す方法を考える.

$$\forall gs \in GS_i \exists gs' \in GS_j \{gs \xrightarrow{*} gs'\} \Leftrightarrow (v_i, v_j) \in E' \qquad (2)$$

4.2 縮退到達可能性グラフと Q-live性

安全性の検証によって不変式であること, 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 $F = P_1 \vee P_2 \vee \cdots \vee P_n$とする. 以下では$\bigvee_{i \in I_Q} P_i$ ($I_Q \subseteq \{i \mid 1 \leq i \leq n\}$ とする) の形で記述された性質 Q に対して Q-live 性を示すことを考える. $GS_Q = \bigcup_{i \in I_Q} GS(P_i)$ であるので, 以下が成立するならばプロトコルΠは Q-live である.

$$\forall i (1 \leq i \leq n)\, \forall gs \in GS(P_i) \exists j \in I_Q \exists gs' \in GS(P_j) \{gs \xrightarrow{*} gs'\} \quad (3)$$

以下では, PM_A(または PM_B) の送信によって gs から gs' に遷移可能であるとき, $gs \xrightarrow{\overrightarrow{A \cdot s}} gs'$(または $gs \xrightarrow{\overrightarrow{B \cdot s}} gs'$) と書く. また, PM_A(または PM_B) の受信によって gs から gs' に遷移可能であるとき, $gs \xrightarrow{\overrightarrow{A \cdot r}} gs'$(または $gs \xrightarrow{\overrightarrow{B \cdot r}} gs'$) と書く. 関係$\xrightarrow{\overrightarrow{A \cdot r}}, \xrightarrow{\overrightarrow{B \cdot r}}$の推移閉包をそれぞれ$\xrightarrow{+}_{\overrightarrow{A \cdot r}}, \xrightarrow{+}_{\overrightarrow{B \cdot r}}$と書く.

定義 6 プロトコルΠと不変式 $F = P_1 \vee P_2 \vee \cdots \vee P_n$に対して, 以下のような有向グラフ $DRG_\Pi = (V, E_S \cup E_R)$ を縮退到達可能性グラフと呼ぶ.

$$V = \{v_i \mid 1 \leq i \leq n\}$$
$$E_S = \{(v_i, v_j) \mid \forall gs \in GS(P_i)\, \exists gs' \in GS(P_j)\, \{gs \xrightarrow{\overrightarrow{A \cdot s}} gs'\}\} \cup \{(v_i, v_j) \mid \forall gs \in GS(P_i)\, \exists gs' \in GS(P_j)\, \{gs \xrightarrow{\overrightarrow{B \cdot s}} gs'\}\}$$
$$E_R = \{(v_i, v_j) \mid \forall gs \in GS(P_i)\, \exists gs' \in GS(P_j)\, \{gs \xrightarrow{+}_{\overrightarrow{A \cdot r}} gs'\}\} \cup \{(v_i, v_j) \mid \forall gs \in GS(P_i)\, \exists gs' \in GS(P_j)\, \{gs \xrightarrow{+}_{\overrightarrow{B \cdot r}} gs'\}\}$$

□

DRG_Π上で v_iから v_jへの道があるならば, $\forall gs \in GS(P_i)$ $\exists gs' \in GS(P_j)\{gs \xrightarrow{*} gs'\}$ が成り立つ. このことより, (3) の成立を示すためには, 以下を示せば十分である.

$$\forall i (1 \leq i \leq n)\, \exists j \in I_Q \{DRG_\Pi \text{上で } v_i \text{から } v_j \text{への道がある}\} \quad (4)$$

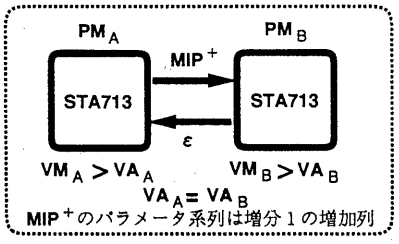

図 1: プロトコルΠ_{EX}の状態集合の例

表 1: 検証に用いたメッセージ系列に関する定義述語

述語名	意味
*step*1	パラメータ系列が増分 1 の増加列である
st-inc	パラメータ系列が狭義単調増加列である

表 2: プロトコル機械のレジスタ

レジスタ名	意味
PM_A VM_A	次に送信する MIP の同期点番号
VA_A	応答が返ってきていない最小の同期点番号
PM_B 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 3: プロトコル機械のアクションの定義

$ta1$ = (STA713, ⟨MIP, sn⟩,STA713,C_{ta1}, R_{ta1}) $\in T_A$ $C_{ta1} = \{sn = VM_A\}$ $R_{ta1}(VM_A, VA_A) = (VM_A + 1, VA_A)$
$ta2$ = (STA713, ⟨MIA, sn⟩,STA713,ϕ, R_{ta2}) $\in T_A$ $R_{ta2}(VM_A, VA_A) = (VM_A, sn + 1)$
$tb1$ = (STA713, ⟨MIA, sn⟩,STA713,C_{tb1}, R_{tb1}) $\in T_B$ $C_{tb1} = \{VM_B > VA_B, VM_B = sn + 1, sn \geq VA_B\}$ $R_{tb1}(VM_B, VA_B) = (VM_B, sn + 1)$
$tb2$ = (STA713, ⟨MIP, sn⟩ STA713,ϕ, R_{tb2}) $\in T_B$ $R_{tb2}(VM_B, VA_B) = (VM_B + 1, VA_B)$

表 4: 3.3 のプロトコルΠ_{EX}に関する論理式 F_{EX}

P_1 = ⟨ STA713, STA713 ⟩
$\wedge \langle \varepsilon, \varepsilon \rangle$
$\wedge VM_A = VM_B$
$\wedge VA_A = VA_B$
$\wedge VM_A = VA_A$
$\wedge VM_B = VA_B$

P_2 = ⟨ STA713, STA713 ⟩
$\wedge \langle \varepsilon, \varepsilon \rangle$
$\wedge VM_A = VM_B$
$\wedge VA_A = VA_B$
$\wedge VM_A > VA_A$
$\wedge VM_B > VA_B$

P_3 = ⟨ STA713, STA713 ⟩
$\wedge \langle \varepsilon,$ MIP$^+\rangle$
$\wedge step1(ch_{AB})$
$\wedge VM_A = last(ch_{AB})+1$
$\wedge VM_B = first(ch_{AB})$
$\wedge VA_A = VA_B$
$\wedge VM_A > VA_A$
$\wedge VM_B = VA_B$

P_4 = ⟨ STA713, STA713 ⟩
$\wedge \langle \varepsilon,$ MIP$^+\rangle$
$\wedge step1(ch_{AB})$
$\wedge VM_A = last(ch_{AB})+1$
$\wedge VM_B = first(ch_{AB})$
$\wedge VA_A = VA_B$
$\wedge VM_A > VA_A$
$\wedge VM_B > VA_B$

P_5 = ⟨ STA713, STA713 ⟩
$\wedge \langle$ MIA$^+, \varepsilon\rangle$
$\wedge st\text{-}inc(ch_{BA})$
$\wedge VM_A = VM_B$
$\wedge VA_B = last(ch_{BA})+1$
$\wedge VA_A \leq first(ch_{BA})$
$\wedge VM_A > VA_A$
$\wedge VM_B = VA_B$

P_6 = ⟨ STA713, STA713 ⟩
$\wedge \langle$ MIA$^+, \varepsilon\rangle$
$\wedge st\text{-}inc(ch_{BA})$
$\wedge VM_A = VM_B$
$\wedge VA_B = last(ch_{BA})+1$
$\wedge VA_A \leq first(ch_{BA})$
$\wedge VM_A > VA_A$
$\wedge VM_B > VA_B$

P_7 = ⟨ STA713, STA713 ⟩
$\wedge \langle$ MIA$^+$, MIP$^+\rangle$
$\wedge step1(ch_{AB})$
$\wedge st\text{-}inc(ch_{BA})$
$\wedge VM_A = last(ch_{AB})+1$
$\wedge VM_B = first(ch_{AB})$
$\wedge VA_B = last(ch_{BA})+1$
$\wedge VA_A \leq first(ch_{BA})$
$\wedge VM_A > VA_A$
$\wedge VM_B = VA_B$

P_8 = ⟨ STA713, STA713 ⟩
$\wedge \langle$ MIA$^+$, MIP$^+\rangle$
$\wedge step1(ch_{AB})$
$\wedge st\text{-}inc(ch_{BA})$
$\wedge VM_A = last(ch_{AB})+1$
$\wedge VM_B = first(ch_{AB})$
$\wedge VA_B = last(ch_{BA})+1$
$\wedge VA_A \leq first(ch_{BA})$
$\wedge VM_A > VA_A$
$\wedge VM_B > VA_B$

表 5: 検証に用いた定義関数

関数名	意味
$first(\alpha)$	αの先頭メッセージのパラメータ値
$last(\alpha)$	αの末尾メッセージのパラメータ値

4.3 縮退到達可能性グラフの構成法

以下では, 縮退到達可能性グラフ $DRG_\Pi = (V, E_S \cup E_R)$ の構成法について説明する.

4.3.1 E_Sの求め方

P_i, P_j $(1 \leq i,j \leq n)$ と PM_Aのある送信アクション $t = (sf, d, sf', C, R)$ に対して, 以下の (a), (b) が成り立つならば $(v_i, v_j) \in E_S$である.

(a) 任意の状態 $gs = (s_A, s_B, ch_{BA}, ch_{AB}) \in GS(P_i)$ に対して, あるパラメータ値 p が存在して, $\langle d, p\rangle$ が送信可能である. すなわち以下の (ES1)-(ES3) が成立する. ただし, C_iを P_i中の AF4 型原子式からなる連立線形不等式とし, $C_p, C_{\overline{p}}$をそれぞれ送信メッセージのパラメータ値を表す変数 p を含む C中の線形不等式の部分集合, 変数 p を含まない C中の線形不等式の部分集合とする.

(ES1) $sf_A(P_i) = sf$.

(ES2) C_iを満たすPM_Aの任意のレジスタ値$\langle p_1, p_2, \cdots, p_r\rangle$は $C_{\overline{p}}$中の任意の線形不等式を満たす.

(ES3) C_iを満たすPM_Aの任意のレジスタ値$\langle p_1, p_2, \cdots, p_r\rangle$について, $\langle p_1, p_2, \cdots, p_r, p\rangle$ が C_pを満たすような p が存在する.

(b) 任意の状態 $gs \in GS(P_i)$ から Cを満たす任意のパラメータ値 p を持つメッセージ $\langle d, p\rangle$ の送信を PM_Aが行なった後の状態 gs'で P_jが成立する.

(b) は安全性の検証手続きと同様の手法を用いて調べることができる. (ES1) は t と P_iからただちに判定可能である. (ES2) と (ES3) の判定法については 4.4で述べる. P_i, P_j $(1 \leq i,j \leq n)$ と PM_Bのある送信アクション t に対して, (a), (b) と同様の条件が成り立つならば $(v_i, v_j) \in E_S$ である. 以上の手順によって求まった辺集合を E'_Sとする. このとき $E'_S \subseteq E_S$が成り立つ.

4.3.2 E_Rの求め方

各 P_i $(1 \leq i \leq n)$ において, AF2 型原子式 $\langle R_{BA}, R_{AB}\rangle$ について $R_{BA} = \varepsilon$であるか, $\mathcal{L}(R_{BA}) \cap \{\varepsilon\} = \phi$であるとする. R_{AB}についても同様とする. この制約を満たすように P_iを記述することは容易である.

定義 7 プロトコルΠと不変式 $F = P_1 \vee P_2 \vee \cdots \vee P_n$に対して, 以下のような有向グラフ $G_A = (V, E_A)$, $G_B = (V, E_B)$ をそれぞれ PM_A, PM_Bの受信到達可能性グラフと呼ぶ.

$V = \{v_i \mid 1 \leq i \leq n\}$

$E_A = \{(v_i, v_j) \mid \exists gs \in GS(P_i)\, \exists gs' \in GS(P_j) \{gs \xrightarrow[A\cdot r]{} gs'\}\}$

$E_B = \{(v_i, v_j) \mid \exists gs \in GS(P_i)\, \exists gs' \in GS(P_j) \{gs \xrightarrow[B\cdot r]{} gs'\}\}$ロ

P_i, P_j $(1 \leq i,j \leq n)$ と PM_Aのある受信アクション $t = (sf, d, sf', C, R)$ に対して, 以下の (a), (b) が成り立つならば $(v_i, v_j) \in E_A$である.

(a) ある状態 $gs = (s_A, s_B, ch_{BA}, ch_{AB}) \in GS(P_i)$ に対して, $\langle d, p\rangle$ が受信可能である. すなわち以下の (EA1)-(EA3) が成立する. ただし, C_iを P_i中の AF4 型原子式からなる連立線形不等式, $\langle R_{BA}, R_{AB}\rangle$ を P_i中の AF2 型原子式とする.

(EA1) $sf_A(P_i) = sf$.

(EA2) $\exists u \in \Sigma^*_{BA}$ $\{d \cdot u \in \mathcal{L}(R_{BA})\}$.

(EA3) C_iと Cからなる連立線形不等式を満たす PM_Aのレジスタ値 $p_1, p_2, \cdots, p_r$ と受信メッセージのパラメータ値 p が存在する.

(b) ある状態 $gs \in GS(P_i)$ から Cを満たすあるパラメータ値 pを持つメッセージ $\langle d, p\rangle$ の受信を PM_Aが行なった後の状態 gs'で P_jが成立する.

(EA2) および (b) は安全性の検証手続きと同様の手法を用いて調べることができる. また, (EA1) は t と P_iからただちに判定可能である. (EA3) の判定法については 4.4で述べる. P_i, P_j $(1 \leq i,j \leq n)$とPM_Bのある受信アクション t に対して, (a),(b)と同様の条件が成り立つならば $(v_i, v_j) \in E_B$である.

$V_{BA=\varepsilon} = \{v_i \mid P_i$中の $AF2$ 型原子式で $R_{BA} = \varepsilon\}$,

$V_{AB=\varepsilon} = \{v_i \mid P_i$中の $AF2$ 型原子式で $R_{AB} = \varepsilon\}$,

とする. ここで $v_i \in V$に対して,

$RS_A(v_i) = \{v_j \mid \forall v_k \in V_{BA=\varepsilon} \forall G_A$上の道 $p = (v_i, \cdots, v_k)$ $\{v_j$は p 上の頂点$\}\}$

$RS_B(v_i) = \{v_j \mid \forall v_k \in V_{AB=\varepsilon} \forall G_B$上の道 $p = (v_i, \cdots, v_k)$ $\{v_j$は p 上の頂点$\}\}$

とする. グラフ G_Aからある頂点 v_jとそれに接続するすべての辺を取り除いたグラフを G^j_Aとすると, $\{v_k | G_A$上で v_i から $v_k \in V_{BA=\varepsilon}$への道がある $\} - \{v_k | G^j_A$上で v_iから $v_k \in V_{BA=\varepsilon}$への道がある $\} \neq \phi$であるとき, かつそのときのみ $v_j \in RS_A(v_i)$ である. $RS_B(v_i)$ についても同様である.

$v_j \in RS_A(v_i)$ であると仮定すると, 任意の $gs \in GS(P_i)$ から PM_Bから PM_Aへの通信路が空であるような状態 gs''へ PM_Aの受信遷移のみによって到達可能ならば, 必ず $gs' \in GS(P_j)$ なる状態を経由する. 一方, 安全性が保証されているという前提より $GS(F)$ は未定義受信状態を含まず, 任意の $gs \in GS(P_i)$ は PM_Aの受信遷移のみによって PM_Bから PM_Aへの通信路が空であるような状態に到達可能である. したがって, $v_j \in RS_A(v_i)$ ならば,

$\forall gs \in GS(P_i),\ \exists gs' \in GS(P_j)\ \{gs \xrightarrow[A\cdot r]{+} gs'\}$

が成り立ち, $(v_i, v_j) \in E_R$である. $v_j \in RS_B(v_i)$ についても同様である. 以上によって求まった辺集合を E'_Rとする. このとき $E'_R \subseteq E_R$が成り立つ.

4.3.3 $DRG'_\Pi = (V, E'_S \cup E'_R)$ の探索

$E'_S \subseteq E_S, E'_R \subseteq E_R$より, $DRG'_\Pi = (V, E'_S \cup E'_R)$ 上で以下が成り立つならば縮退到達可能性グラフ $DRG = (V, E_S \cup E_R)$ で (4) が成り立ち, Q-live 性が成立する.

$\forall i (1 \leq i \leq n)\, \exists j \in I_Q \{DRG'_\Pi$上で v_iから v_jへの道がある $\}$ (5)

(5) は深さ優先探索などによって判定可能である.

【例】 3.2 のプロトコルΠ_{EX}と不変式 F_{EX}に対する DRG'_Π は図 2のようになる. この場合, DRG'_Π上で任意の頂点 v_iから v_1への道があるので, Π_{EX}は P_1-live であるといえる.

4.4 プレスブルガー文の真偽判定

m 個の変数 $x_1, x_2, \cdots, x_m$を含む l個の線形不等式からなる連立不等式を Cとする. また, $X = (x_1, x_2, \cdots, x_m)$ とする. 4.3 の (EA3), (ES2), (ES3) はそれぞれ以下の (S1), (S2), (S3) のように表現することができる.

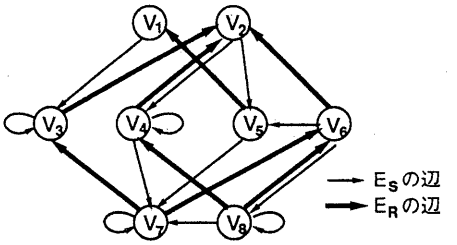

図 2: 3.2 のΠ_{EX}と F_{EX}に対する DRG'_{Π}

(S1) 連立線形不等式 Cの非負整数解 Xが存在する.

(S2) 連立線形不等式 Cの任意の非負整数解 Xは新たな制約を表す線形不等式 c を満たす.

(S3) 連立線形不等式 Cの任意の非負整数解 Xについて, 新たな変数 yを含む連立線形不等式 C_y と Cからなる連立線形不等式の非負整数解 (X,y) が存在する.

これらはプレスブルガー文とみなすことができ, 判定可能であることが知られている[6]. しかし, 例えば (S1) は NP 完全であることが知られている整数線形計画問題の一般形そのものであり, 一般には効率よく解けないと考えられる. 以下では, (S1)-(S3) が効率よく解ける場合について考える.

定義 8 変数 x,y, 整定数値 qに対して, 以下のような形の線形不等式を差分制約と呼ぶ.

$$x-y \le q \qquad \square$$

AF4 型原子式とプロトコル機械のアクションの遷移条件 C **がすべて差分制約であるとき**, (EA3), (ES2), (ES3) の線形不等式もすべて差分制約である. 差分制約のみからなる連立線形不等式の充足性について以下のような判定法が知られている[7].

[差分制約の充足性判定] 差分制約のみからなる連立線形不等式 Cに対して, 以下のような重みつき有向グラフ $G_C=(V_C,E_C)$ を作る.

$V_C=\{v_1,v_2,\cdots,v_m\}$ (各 v_iはそれぞれ x_iに対応)

$E_C=\{(v_i,v_j)\mid x_j-x_i\le q$は C中の差分制約 $\}$

($x_j-x_i\le q$が C中の差分制約ならば, 辺 (v_i,v_j) の重み $w(v_i,v_j)=q$とする.)

G_Cが負の重みの閉路を持たないとき, かつそのときのみ連立線形不等式 Cは非負整数解 Xを持つ. また, G_C上で v_iから v_jへの道があるとき, かつそのときのみ x_j-x_iは有界であり, v_iから v_jへの重み最小の経路の重みを $d(v_i,v_j)$ とすると, 以下の性質が成り立つ.

$$x_i,x_j \text{は } C\text{を満たす} \Leftrightarrow x_j-x_i\le d(v_i,v_j) \qquad (6)$$

G_Cが負の重みの閉路を持つかどうかは Bellman-Ford のアルゴリズムにより $O(|V_C|\cdot|E_C|)$ で判定可能である[7]. $\square$

(S1) は上記の手法により, $O(lm)$ で判定可能である. (S2) についても Cと新たな制約「$x_j-x_i\le q$」の否定「$x_i-x_j\le -q-1$」からなる連立線形不等式の非負整数解 Xが存在しないかどうかに帰着することができるので, 上記の手法により $O((l+1)m)$ で判定可能である. (S3) の判定法については, まず Cの非負整数解 Xが存在することを Bellman-Ford のアルゴリズムを用いて調べる. Cの非負整数解 Xが存在しないならば,(S3) は直ちに成立する. C_y中の差分制約の中で yの系数が-1である差分制約 $x_j-y\le q'$の集合を C'_y, C_y中の差分制約の中で yの系数が 1 である差分制約 $y-x_i\le q''$の集合を C''_yとする. $c'\in C'_y, c''\in C''_y$に対して, $E_y(C,c',c'')$ は, Cを満たす任意の非負整数解 Xに対して c'と c''を同時に満たす非負整数 yが存在することを表すものとする. このとき以下の性質が成り立つ.

[性質] 任意の $c'\in C'_y, c''\in C''_y$に対して $E_y(C,c',c'')$ が成立するとき, かつそのときのみ (S3) は成立する.

[証明] 必要性は明らか. 以下では十分性についてその対偶を考えることにより議論する. (S3) が成立しないとすると,

$$\neg\exists y\{(X,y) \text{ は } C\text{と } C_y\text{を同時に満たす}\} \qquad (7)$$

が成立するような Cの非負整数解 $X=(a_1,a_2,\cdots,a_n)$ が存在する. $X=(a_1,a_2,\cdots,a_n)$ に対して, C'_yの不等式 $x_j-y\le q'$ の中で yに関するもっとも強い制約を与える不等式, すなわち a_j-q'が最大である不等式を c'とする. C''_yの不等式 $y-x_i\le q''$ の中で yに関するもっとも強い制約を与える不等式, すなわち a_i+q''が最小である不等式を c''とする. このとき (7) は以下と等価である.

$$\neg\exists y\{(X,y) \text{ は } C\text{と } c',c''\text{を同時に満たす}\} \qquad (8)$$

これは, $E_y(C,c',c'')$ が成立しないことを表しており, 以上により十分性が証明された. $\square$

$c':x_j-y\le q', c'':y-x_i\le q''$に対して $E_y(C,c',c'')$ の真偽は以下のようにして判定できる.

[$E_y(C,c',c'')$ の判定]

(a) G_C上で v_iから v_jへの道がないならば, 偽である.

(b) G_C上で v_iから v_jへの道があるならば,

(b-i) $d(v_i,v_j)>q'+q''$ならば, 偽である.

(b-ii) $d(v_i,v_j)\le q'+q''$ならば, 真である.

上記判定法の正当性について以下で述べる. $x_j-y\le q'$, $y-x_i\le q''$に対して, 明らかに以下が成り立つ.

$$x_j-x_i\le q'+q'' \Leftrightarrow \exists y\{x_j-y\le q'\wedge y-x_i\le q''\} \qquad (9)$$

(a) の場合には, 任意の整数 qに対して $x_j-x_i=q$と Cを満たす非負整数 x_i,x_jが存在するので, $x_j-x_i\le q'+q''$を満たさない Cの非負整数解 $x_i=a_i, x_j=a_j$が存在する. すなわち, $a_j-a_i>q'+q''$. (9) より, $a_j-y\le q', y-a_i\le q''$ を満たす yは存在しないことがわかる. よって, $E_y(C,c',c'')$ は偽である. (b-i) の場合には, $d(v_i,v_j)>q'+q''$と (6) より $x_j-x_i\le q'+q''$ を満たさない Cの非負整数解 $x_i=a_i,x_j=a_j$が存在する. すなわち, $a_j-a_i>q'+q''$. (9) より, $a_j-y\le q', y-a_i\le q''$ を満たす yは存在しないことがわかる. よって, $E_y(C,c',c'')$ は偽である. (b-ii) の場合には, $d(v_i,v_j)\le q'+q''$と (6) より Cの任意の非負整数解 x_i,x_jに対して $x_j-x_i\le q'+q''$が成り立つ. よって, (9) より Cの任意の非負整数解 x_i,x_jに対して $x_j-y\le q', y-x_i\le q''$ を満たす非負整数 yは存在する. したがって, $E_y(C,c',c'')$ は真である. G_C上で v_iから v_jへの道があり, $d(v_i,v_j)\le q'+q''$であることは Bellman-Ford のアルゴリズムによって $O(lm)$ で判定可能である.

5 検証システム

文献 [5] の安全性の検証システムは, プロトコル機械の定義, 不変式の記述のために検証者が導入した定義述語および定義関数の性質, 不変式であることを示そうとする論理式 Fを入力として, 3.3で述べた安全性の検証手続きを実行する. ただし, 検証を効率よく行なうためにプロトコル機械のアクションの遷移条件 Cと F中の AF4 型原子式はすべて差分制約であるとしている. 入力される論理式 Fは必ずしも積和形をしている必要はなく, Fが積和形をしていない場合には, 検証システムが入力された Fを積和形に展開する. 文献 [5] の安全性の検証システムに, 4.3. で述べた縮退到達可能性グラフ DRG_Πの部分グラフである DRG'_Πの生成および DRG'_Π上の探索を行なう手続きを追加した. これにより, 検証システムは, 上記の入力に加えて, 性質 Q を入力として安全性および Q-live 性の検証を行なうことができる. 検証システムは C 言語, lex, yacc で記述されており, UNIX 環境下で動作している. Q-live 性の検証のために新たに記述した部分は約 6000 行である.

6 例プロトコルの検証実験の結果

本検証法の有効性を確認するために, 試作した検証システムを用いて, 文献 [8] で規定される OSI セションプロトコルのカーネル, 全二重, 大同期, 小同期機能単位のデータ転送フェーズを抽出したプロトコル $\Pi_{session} = (PM_A, PM_B)$ が P_i-live$(1 \leq i \leq n)$ であることを検証した. プロトコルの抽出にあたっては, 大同期および小同期設定用のトークンを一つのトークンで共用するなどの簡単化を施している. PM_Aと PM_Bは初期状態でトークンを持っているか持っていないかが異なる点を除いては同型である. プロトコル機械の有限制御部の状態数は 10, レジスタは 2 本, 送受信するメッセージ型は 12 種類, アクションの数は 22 である. プロトコル機械のアクションの遷移条件 Cはすべて差分制約である. まず, $\Pi_{session}$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 144 個の部分集合に分割して, $\Pi_{session}$の不変式であると思われる論理式を記述し, 文献 [5] の検証システムを用いて$\Pi_{session}$の安全性を検証した. Q-live の検証時には, これらの状態集合をその集合中の各状態において (1)PM_B から PM_Aへの通信路が空であるかどうか, (2)PM_Aから PM_Bへの通信路が空であるかどうか, (3)PM_Aが MIA を送信できる $(VM_A > VA_A)$ か, 送信できない $(VM_A = VA_A)$ (4)PM_Bが MIA を送信できる $(VM_B > VA_B)$ か, 送信できない $(VM_B = VA_B)$ かによってさらに分割したため, 状態集合の数は 480 に増加した. これらの状態集合に基づいて記述した論理式 F中の AF4 型原子式はすべて差分制約であり, F中の AF1–AF4 型原子式は積和形に展開される前ではそれぞれ 30, 30, 46, 471 個である. 定義述語および定義関数の性質は 10 個の条件付き書換え規則, 7 個の条件付き関係式からなる[5]. 検証システムを用いて$\Pi_{session}$の安全性および P_i-live 性の検証を UNIX ワークステーション (NWS-5000, 64MB) 上で行なった. $\Pi_{session}$の P_i-live 性 $(1 \leq i \leq n)$ が示され, $\Pi_{session}$の初期状態から到達可能な任意の状態から $P_i(1 \leq i \leq n)$ を満たす状態へ到達可能であることが検証できた. $\Pi_{session}$の安全性, P_i-live 性の検証に要した CPU 時間はそれぞれ約 40 秒, 約 60 秒, 使用したメモリはそれぞれ約 6MB, 約 7MB であった. 検証時に生成されたグラフ $DRG'_\Pi = (V, E'_S \cup E'_R)$ の規模は $|V| = 480, |E'_S| = 1566, |E'_R| = 1300$ であった. P_i-live 性の検証時に成立を判定した AF2 型, AF3 型原子式の数はそれぞれ 96157, 2432, Bellman-Ford のアルゴリズムを呼び出した回数は 27628 回であった.

7 あとがき

本報告では, liveness を Q-live 性として定式化し, 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 Q-live 性の検証法を提案した. さらに, 提案した検証法に基づく検証システムを試作した. また, 試作した検証システムを用いて, OSI セションプロトコルの一部の機能単位を抽出したプロトコルに対して, Q-live 性の検証を行なった. 試作した検証システムでは検証を効率よく行なうためにプロトコル機械のアクションの遷移条件 Cと不変式 F中の AF4 型原子式はすべて差分制約であるとしているが, 実用プロトコルに対しては十分に検証を行なうことができる. 今後は, OSI セションプロトコル全体の検証作業に本検証法を適用していく予定である.

参考文献

[1] Brand D. and Zafiropulo P.: "On Communicating Finite-State Machines", Journal of ACM, vol.30, no.2, pp.323–342(1983).

[2] Clarke E.M. , Emerson E.A.and Sistla A.P.: "Automatic Verification of Finite-State Concurrent System Using Temporal Logic Specification", ACM Trans. Program. Lang. Syst., vol.8, no.2, pp.244–263 (1986).

[3] Finkel A.: "A New Class of Analyzable CFSMs with Unbounded FIFO Channels", Proc. 8th Intern. Symp. on PSTV, pp.283–294 (1988).

[4] Pachl J.: "Protocol Description and Analysis Based on a State Transition Model with Channel Expressions", *Proc. 7th Int'l Workshop on PSTV*, pp.207–219, (1987).

[5] Higuchi M., Shirakawa O., Seki H., Fujii M. and Kasami T.: "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).

[6] 東野, 北道, 谷口: "整数上の線形制約の処理と応用", コンピュータソフトウェア, vol.9, no.6, pp.31–39 (1992).

[7] Cormen T., Leiserson C. and Rivest R. : "Introduction to Algorithms", The MIT Press, pp.539–543 (1990).

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