2E−2

ECFSMモデルの通信プロトコルの検証のための不変式の自動生成システムの開発

原 圭吾† 佐野 順子‡ 樋口 昌宏† 藤井 護†

†大阪大学 基礎工学部 情報工学科 ‡(株)リコー

1 はじめに

信頼性の高い通信ソフトウェアの設計には，プロトコルを形式的に記述し，検証を行なうことが重要である．我々の研究グループでは，拡張有限状態機械(以下，ECFSMと呼ぶ)でモデル化された通信プロトコルの検証法を提案している．この検証法は，検証者の記述した積和形の不変式を用いて，プロトコルの安全性，生存性を示すものである．しかしながら，手作業による不変式の記述に多大の作業量を必要とするという問題がある．これに対し，文献[1]において不変式の記述を支援する手法を提案した．本稿ではこの手法に基づいて作成した不変式自動生成システムと，そのOSIセションプロトコルより抽出した例プロトコルに対する適用結果について述べる．

2 プロトコルのモデル

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，プロトコルを非有界FIFOでモデル化された双方向の通信路で接続された二つのプロトコル機械からなる系とする．プロトコル機械PMを4字組(S,Σ,T,SI)で定義する．ここで$S=\langle SF,r\rangle$は状態集合を定義する2字組で，SFは有限制御部の状態集合，rは非負整数値を保持するレジスタの数を表す．$\Sigma=\Sigma_-\cup\Sigma_+$は送受信するメッセージ型の有限集合であり，$\Sigma_-(\Sigma_+)$は送信（受信）メッセージ型の集合である．各メッセージは整数値パラメータを一つ持つものとする．Tはアクションの集合で，アクションtは5字組$(sf1_t,d_t,sf2_t,C_t,R_t)$で表される．ここで$sf1_t,sf2_t\in SF,d_t\in\Sigma,C_t$は送信または受信メッセージのパラメータ$p$と状態遷移前のプロトコル機械のレジスタ値$p_1,p_2,\cdots,p_r$に関する連立不等式であり，$R_t$は状態遷移によるレジスタ値の変化を表す関数である．非決定性状態遷移関数δは次のように定義される．$\delta((sf,p_1,\cdots,p_r),\langle d,n\rangle)=\{(sf',R(n,p_1,\cdots,p_r))\mid(sf,d,sf',C,R)\in T$かつ$n,p_1,\cdots,p_r,$は$C$を満たす$\}$．$SI\subseteq SF\times\mathcal{N}^r$は初期状態の集合である．

このとき，二つのプロトコル機械PM_A,PM_BからなるプロトコルΠを二字組(PM_A,PM_B)で表す．また，プロトコルの状態は4字組$gs=(s_A,s_B,ch_{BA},ch_{AB})\in(SF_A\times\mathcal{N}^{r_A},SF_B\times\mathcal{N}^{r_B},\langle\Sigma_{A+},\mathcal{N}\rangle^*,\langle\Sigma_{B+},\mathcal{N}\rangle^*)$で与えられる．その他，プロトコルに関する定義は文献[1]に従う．

3 安全性の検証法

文献[2]の安全性の検証法の概略を述べる．プロトコルが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が不変式であるという．不変式を記述するにあたって，以下の(AF1)〜(AF4)の4種類の原子式を導入する．

(AF1) 各プロトコル機械の有限制御部が指定された状態にあることを表す式，

(AF2) 通信路上のメッセージ型の系列が正規表現で記述された系列集合に属することを表す述語．

(AF3) 通信路上のメッセージ系列の部分列の整数値パラメータ列の性質に関して検証者の定義した述語．

(AF4) プロトコル機械のレジスタ値と通信路上のメッセージのパラメータ値の関係を表す等式・不等式．

検証者は，初期状態から到達可能であると想定している状態集合をいくつかの部分集合に分割し(分割数をnとする)，それぞれの状態集合で成立する条件を原子式の積項$P_i(i=1,2,\cdots,n)$として記述する．提案している検証法は，論理式$F=P_1\vee P_2\vee\cdots\vee P_n$が不変式であることを状態遷移系列に関する構造的帰納法を用いて示す．Fが不変式であり，さらにFを満たす状態の集合がデッドロック状態，未定義受信状態といった安全でない状態を含まないことを示すことにより，プロトコルが安全であると結論できる．筆者らの研究グループではこの検証法に基づく検証システムを試作している[2]．

An implementation of invariant formula generator system for verifying ECFSM communication protocols

Keigo HARA†, Junko SANO‡, Masahiro HIGUCHI† and Mamoru FUJII†

†Deperment of Information and Computer Sciences, Faculty of Engineering Science, Osaka University Toyonaka-shi, Osaka 560 Japan

‡RICOH CO. LTD.

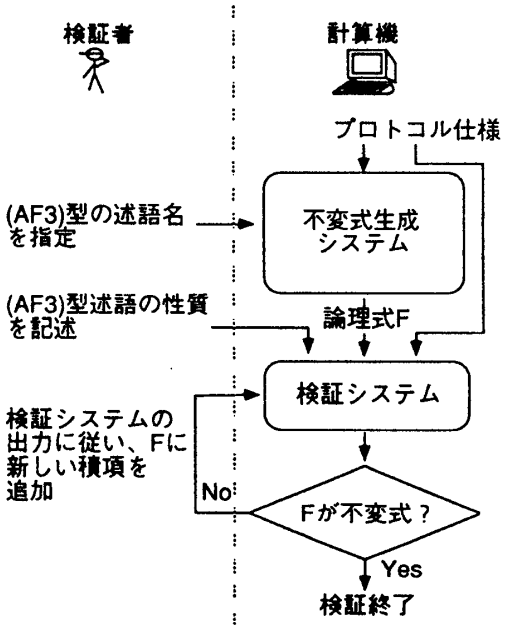

図1：不変式生成システムを導入した検証の手順

4 不変式生成システム

3. で述べた検証法の問題点として，検証作業において論理式 F の記述に費やす労力が大きいことがあげられる．いくつかの検証実験の結果，プロトコルの到達可能な状態のうち，二つのプロトコル機械の複雑な相互干渉によって到達可能となる状態はほとんどなく，不変式を構成する積項の大部分については単純な作業の繰り返しで導出できるであろうという知見が得られた．文献[1]では，不変式の積項のうち，次の(i),(ii)の状態集合に関する積項を自動生成する手法を提案している．

(i) 一方のプロトコル機械のメッセージの送信に同期して，他方のプロトコル機械がメッセージの受信を行なう，同期型の通信によって到達可能な状態集合．

(ii) (i)の状態から，双方のプロトコル機械のメッセージの送信のみによって到達可能な状態集合．

通常，プロトコルが到達可能な状態を求めるには，二つのプロトコル機械と双方向の通信路を考慮しなければならない．しかし，(i)の状態集合を求める場合にはプロトコル機械間の通信路を考慮する必要がなく，(ii)の状態集合を求める場合には片側のプロトコル機械と一方向の通信路のみ考慮すれば良い．従って，上記の(i),(ii)の状態集合を求める場合は通常に比べて解析が容易となる．この手法に基づいて，不変式を構成する積項を自動生成するシステムを試作した．このシステムと文献[2]の検証システムにより，図1のような手順で検証を行なうことができる．この場合，(i),(ii)の状態に関する積項をシステムによって生成できるため，検証者はそれに含まれない積項を追加する作業を行なうだけで良い．更に，積項を追加する作業を行なう際には検証システムの出力を参照することが可能である．

試作した不変式生成システムはC,yacc,lexで記述されており，規模は全体で約18,000行で，このうち約12,000行については，既存の検証システムより流用できた．

5 検証実験

5.1 例プロトコル

OSIセションプロトコルからカーネル，全2重，小同期，大同期機能単位のデータ転送フェーズを抽出したものを例プロトコルとした．このプロトコルは各プロトコル機械の有限制御部の状態数が3，レジスタ数が2，送受信するメッセージ型が12種類，アクションの数が22というものである．以前，手作業によりプロトコルの不変式記述を行ない，この例プロトコルについては積項数60の不変式を得ている．このときの作業時間は約120時間であった．

5.2 実験結果

上記の例プロトコルに対し，試作した不変式生成システムを用いて積項の自動生成を行なった．プログラムの実行はUNIXワークステーション(NWS-5000, 64MB)上で行ない，積項632個を生成することができた．この実行の際にCPU時間約75秒を要した．次に不変式生成システムによって生成された積項からなる論理式Fに対して既存の検証システムを適用したところ，Fは不変式でありかつ安全でない状態の積項を含まないことが示された．すなわち，この例では試作したシステムによって不変式を完全に自動生成することができた．しかし手作業で記述した不変式と比較して，システムの生成した不変式は状態の分割数 n がかなり大きくなっており，不変式の規模はかなり大きなものとなった．今後，この点の改善を検討する予定である．

参考文献

[1] 樋口他:“ECFSMモデル通信プロトコルの検証システムにおける不変式の自動生成”, 情処研報 DPS70-18(1995年5月).

[2] M. HIGUCHI, et al.: “A Verification Method via Invariant for Communication Protocols Modeled as Extended Finite-State Machines”, *IEICE Trans. Commun.*E76-B,11,pp,1363-1302,(1993年11月).