代数的に記述されたプロトコルの検証に関する一考察

5T-3

神長 裕明　白鳥 則郎　野口 正一

(東北大学　電気通信研究所)

1. はじめに

代数的に記述されたプロトコルにおいては、プロトコルが満たすべき様々な性質は定理として、同じ代数の枠組みの中で証明が行われる(1),(3)。

本稿では、プロトコル・プロジェクション(2)の概念を基に、与えられたプロトコルの代数的仕様から、証明すべき命題に関して等価なより簡単な代数を定義して、証明の手続きを簡単にする方法について述べる。

2. プロトコルの代数的記述

【定義1】 プロトコルの仕様を4項組<S,Σ,E,G>で定義する。

Gはプロトコルのグローバル状態の集合で、グローバル状態は各ステーションやチャネルの状態を表す状態変数の組として表され、各状態変数はそのデータタイプが既に代数的に定義されているものとする。また、集合Gのソートをstateとする。

Sはソートの集合でS={state,message}とする。messageは各ステーション間でやり取りするメッセージの集合のソート名である。

Σはプロトコルのアクション(メッセージの送・受信等の動作)を表す関数記号の集合で、

Σ=Σε,state∪Σstate,state∪Σstste message,state

Σε,state={*INITIAL*}(*INITIAL*はプロトコルの初期状態を表す定数関数)とする。

Eは関数の定義を与える公理系で、公理 $l \approx r \in E$ に対して、lはα(s)またはα(s,m)である。rはGの元あるいはGの元を表す変数とif_then_elseから構成される条件式で、アクションが可能な条件とその結果の状態の変化を表す。プロトコルで許されない動作に対しては同じ値を返すことにする。ここで、α∈Σでありsは Gの元を表す変数でmはメッセージを表す。また *INITIAL*≈s0 ∈E(s0はGの元でグローバル初期状態)である。

シグニチャ<S,Σ>の上の変数を含まない項の集合族をT[Σ]と書き、T[Σ]の元をΣ項という。

【定義2】 各Σ項t∈T[Σ]に対して、Gの元gを次のように対応させ、それをtに対応するグローバル状態と呼ぶ。

$$g=\begin{cases} s0 & t=INITIAL\text{のとき} \\ \alpha(g1,\cdots,gn) & t=\alpha(t1,\cdots,tn)\text{のとき} \end{cases}$$

ここで、α∈Σstate,state∪Σstste message,state でgiはtiに対応するグローバル状態である。また、(、)は記号としての括弧を表す。

全てのΣ項に対して、対応するグローバル状態の集合をR⊂Gとする。

【定義3】 シグニチャ<S,Σ(G)>を、

Σ(G)ε,state=G∪Σε,state

Σ(G)w,s=Σw,s (その他のとき)

で定義し、Σ(G)項の集合族をT[Σ(G)]と書く。

【定義4】 各Σ(G)項t∈T[Σ(G)]に対して、Gの元gを次のように対応させ、それをtに対応するグローバル状態と呼ぶ。

$$g=\begin{cases} s0 & t=INITIAL\text{のとき} \\ s & t=s\in G\text{ のとき} \\ \alpha(g1,\cdots,gn) & t=\alpha(t1,\cdots,tn)\text{ のとき} \end{cases}$$

ここで、α∈Σstate,state∪Σstste message,state でgiはtiに対応するグローバル状態である。

全てのΣ(R)項t∈T[Σ(R)]に対応するグローバル状態の集合はRになる。

【定義5】 T[Σ(G)]上の合同関係≡を

$$t\equiv t' \Leftrightarrow g=g'$$

で定義する。ここでg、g'はそれぞれt、t'に対応するグローバル状態である。

【定義6】 プロトコルの仕様<S,Σ,E,G>の意味する抽象データタイプは、商代数T[Σ(G)]/≡で定義される。

仕様は、無矛盾かつ完全で、項書き換え系として有限停止性、Church-Rosser性が保証されているものとする。

3. 像プロトコル

G={(p,q)}とし、pをGの元(p,q)の第1要素と呼ぶ。但し、qはpの値によって影響されないものとする。

A Consideration on Verification of Protocol by Algebraic Specification Method

Hiroaki KAMINAGA, Norio SHIRATORI and Shoichi NOGUCHI

Tohoku University

【定義7】 プロトコルの仕様<S,Σ,E,G>に対して、4項組<S,Σ',E',G'>を次のように定義しこれを像プロトコルの仕様と呼ぶ。

G'={p|(p,q)∈G}

Σ',E'は次の条件を満たす。

INITIAL∈Σε,state で *INITIAL*≈(p0,q0) ∈Eなら

INITIAL'∈Σ'ε,state で *INITIAL'*≈p0 ∈E'

その他のα∈Σに対しては、第1要素がpであるGの元の集合をGpとするとき、

∃(p,q)∈Gp,α(p,q)=(p',q') (p≠p') が公理系Eで定義されている

⇔

∃α'∈Σ',α'(p)=p' が公理系E'で定義されている

像プロトコルの仕様に対して、次の命題が成り立つ。

【命題1】 T[Σ'(G')]に対応するグローバル状態の集合はG'であり、T[Σ'(R')]に対応するグローバル状態の集合はR'である。ここで、R'={p|(p,q)∈R}。

命題1により、次の定理が成り立つ。

【定理2】

(1) プロトコルの仕様<S,Σ,E,G>において

∀(p,q)∈R, 命題 *p*(p)≡*TRUE*

⇔

像プロトコルの仕様<S,Σ',E',G'>において

∀p∈R', 命題 *p*(p)≡*TRUE*

(2) プロトコルの仕様<S,Σ,E,G>において

∃(p,q)∈R, 命題 *p*(p)≡*TRUE*

⇔

像プロトコルの仕様<S,Σ',E',G'>において

∃p∈R', 命題 *p*(p)≡*TRUE*

4. 像プロトコルによる検証例

プロトコルの仕様記述の例として、Alternating Bit Protocol(AB Protocol) の代数的記述(1)の主要な公理を示す。

[AB Protocol]

```
Initial≈(NQM,NQP,T,NQP,NQP,T,NQP,NQM)
Send((st,pd,sn,sr,rs,rn,rb,rd),m)≈
    if  pd=NQP  then
        (Add(st,m),Make(m,sn),sn,Make(m,sn),rs,rn,rb,rd)
    else    (st,pd,sn,sr,rs,rn,rb,rd)
ReceivePacket(st,pd,sn,sr,rs,rn,rb,rd)≈
    if  rn=Seq(sr) and sr≠NQP and rb=NQP  then
        (st,pd,sn,NQP,rs,~rn,sr,rd)
  else
    if  rn≠Seq(sr) and sr≠NQP and rb=NQP  then
        (st,pd,sn,NQP,NQP,rn,rb,rd)
    else    (st,pd,sn,sr,rs,rn,rb,rd)
Deliver(st,pd,sn,sr,rs,rn,rb,rd)≈
    if  rb=NQP  then
        (st,pd,sn,sr,rs,rn,rb,rd)
    else    (st,pd,sn,sr,rb,rn,NQP,Add(rd,rb))
ReceiveAck(st,pd,sn,sr,rs,rn,rb,rd)≈
    if  sn=Seq(rs) and rs≠NQP  then
        (st,NQP,~sn,sr,NQP,rn,rb,rd)
    else    (st,pd,sn,NQP,rs,rn,rb,rd)
Retransmit(st,pd,sn,sr,rs,rn,rb,rd)≈
    if  pd≠NQP  and  sr=NQP and rb=NQP  then
        (st,pd,sn,pd,rs,rn,rb,rd)
    else    (st,pd,sn,sr,rs,rn,rb,rd)
LoseAck(st,pd,sn,sr,rs,rn,rb,rd)≈
                    (st,pd,sn,sr,NQP,rn,rb,rd)
LosePacket(st,pd,sn,sr,rs,rn,rb,rd)≈
                    (st,pd,sn,NQP,rs,rn,rb,rd)
```

このプロトコルに対して、命題

∀(st,pd,sn,sr,rs,rn,rb,rd)∈R,

st=rd OR st=rd join pd

(受信側で受け取ったメッセージは、転送途中の物を除いて、送信側の送ったメッセージと順序も含めて等しい)

を証明する場合、

p=(st,pd,rd)、q=(sn,sr,rs,rn,rb) として、像プロトコルの公理は、次のようになる。

[AB Protocol']

```
Initial'≈(NQM,NQP,NQM)
Send'((st,pd,rd),m)≈
            if pd=NQP then (Add(st,m),m,rd)
            else (st,pd,rd)
Deliver'(st,pd,rd)≈
            if pd≠NQP then (st,NQP,Add(rd,pd))
            else (st,pd,rd)
```

命題の証明は、項の長さに関する帰納法を用いて行われるので、像プロトコルの仕様上での証明のほうがはるかに簡単であることがわかる。

5. むすび

命題の証明に直接関係する状態変数の数が、全状態変数の数に比べて少ない時には、像プロトコルの仕様は非常に簡単になる。また、命題の証明に直接関係する状態変数と、他の状態変数との独立性が強い場合には、像プロトコルの仕様は容易に得られる。プロトコルの代数的仕様から、像プロトコルの仕様を生成する手続きについて、現在検討中である。

[参考文献]

(1) C.A.SUNSHINE *et al.*, 'Specification and Verification of Communication Protocols in AFFIRM Using State Transition Models', IEEE Trans. S.E.(1982)

(2) S.S.LAM and A.U.SHANKER, 'Protocol Verification via Projections', IEEE Trans. S.E. (1984)

(3) 稲垣、坂部, '抽象データタイプの代数的仕様記述法の基礎', 情報処理(1984)