オートマトンによるモデル化を用いたプロトコル検証法

吉田　裕　　野村　雅行　　田中　良和
（日本電信電話公社　武蔵野電気通信研究所）

1．まえがき

通信プロトコル（以下単にプロトコルと呼ぶ）は通信回線を介してデータ等を送受する信号形式や手順を定めた規則である。送信データが相手に正しく到達するためにはプロトコルがある意味で正しく規定されていなければならない。実際にはプロトコルの正しさの条件全部を列挙することは困難であり、むしろプロトコルの不適格性の条件を設定し，その条件のいずれをも満足しないことをもってプロトコルが正しいと定義する。デッドロック即ち「通信が先に進まなくなる」ことをプロトコルの不適格性の条件とする検証法が既に提案されている。これには、Danthineらによるcolloqyを用いたモデルに基づく方法[1],[2]及びMarlinによるペトリネットを用いる方法[3]，Zafiropuloらによる Duologue－Matrix 解析による方法[4][5]等がある。一方データの欠落，即ち送信データが相手によって受信されないこと，及びデータの重複，即ち同一の送信データが相手によって2度以上受信されることをプロトコルの不適格性の条件とする必要があることは既に述べられている[6]が，具体的な検証法にまで発展させた例は今のところ見当らない。

本報告では，デッドロック及びデータの欠落・重複をプロトコルの不適格性条件とし，伝送誤りも考慮したプロトコル検証法を提案する。なお手法としては有限オートマトンの合成を用いるものである。まず2章ではプロトコルのモデル化を行い，3章ではプロトコルの不適格性の条件とその条件の判定法を与える。4章ではJIS標準ベーシック伝送制御手順に本検証法を適用してみる。

2．プロトコルのモデル化

本章では、伝送路を介してある通信プロトコルに従い対向通信する2端末をモデル化し，オートマトンとして表現する。

2.1　端末オートマトン

端末の構成は図1に示されるように、キーボード／プリンタに代表されるマンマシンインタフェース及び伝送路に向うインタフェースを持っており，これら2つのインタフェースを通して外部との入・出力を行うオートマトンと見なせる。

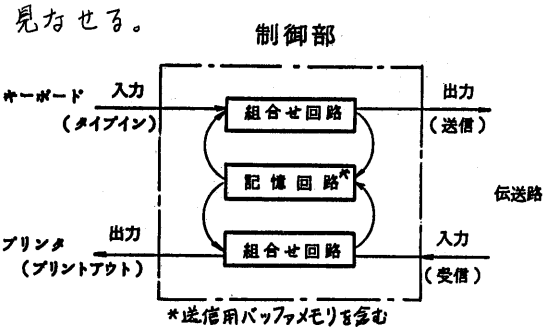


図1　端末モデル

図1に示す端末制御部の動作に注目し，端末の動作をMealy型の有限オートマトンとして表現し，端末オートマトンと呼ぶことにする。なお，ここで用いる端末モデルはプロトコル検証用であるため，一つの端末装置のキーボードからの入力が直ちにプリンタへ出力されることはないと仮定する。また後で考察する2端末間の通信モデルを組立てる都合のため，伝送路からの入力そのもの，またはその入力に応じる

出力が直ちに伝送路への出力として送信されることはないと仮定する。

【定義1】 端末オートマトンは次の形式で表現される。

$$M=\langle Q,\Sigma,\Gamma,\delta,\omega,q_0\rangle$$

ただし

① Q：端末の状態集合

② $\Sigma=I\times X$：入力集合，I：キーボードからの入力集合，X：伝送路からの入力集合

③ $\Gamma=O\times Y$：出力集合，O：プリンタへの出力集合，Y：伝送路への出力集合

④ $\delta: Q\times\Sigma\to Q$　状態遷移関数

⑤ $\omega\equiv\omega_1\times\omega_2: Q\times\Sigma\to\Gamma$　出力関数，ただし $\omega_1: Q\times\Sigma\to O$，$\omega_2: Q\times\Sigma\to Y$

⑥ $q_0\in Q$：初期状態

Q，Σ，Γはいずれも有限集合とする。

上述の定義1に関連して若干の補足説明を行う。

i) 入力集合 $\Sigma=I\times X$ の要素

以下の要素も入力集合に含めることとする。

① 零要素 $\lambda\in I$，X：キーボードからのタイプインなし，及び伝送路から受信信号なしに相当する。

② 伝送誤り $e\in X$：伝送路上における伝送誤りは端末においてパリティ誤りあるいはブロック誤りとして検出されるが，モデルを簡単化するためにこれらの検出結果を一種の入力とみなす。

③ タイムアウト $t_0\in I$：例えばキーボードからの入力に基づき伝送路へデータを送信後，応答を受信するまでのタイミングを取り，タイムアウト時同じデータを再送することがある。この場合のタイムアウトは本来端末内部で発生する要因であるが，これも外部からの入力とみなしてモデル化する。

④ リトライアウト $r\in I$：上述③のタイムアウト後の再送を規定回数繰返すと，以後再送を中断する。このリトライアウトの契機も入力とみなすことにより端末オートマトンの状態数を減らすこととする。

ii) 出力集合 $\Gamma=O\times Y$ の要素

上述i)の②，③，④はΓに含まれないし，キーボードからの入力符号とプリンタへの出力符号が一般には異なるが，これらの点を除いてΓはΣと同じである。

iii) 状態及び出力系列

定義1で用いた各集合の要素を対応する小文字で表わすこととし，時刻τにおける状態，入力，出力を$q(\tau)$，$i(\tau)$，$x(\tau)$，$o(\tau)$，$y(\tau)$等と書けば，

$$\left.\begin{aligned} q(\tau+1)&=\delta(q(\tau),i(\tau),x(\tau))\\ \gamma(\tau)&\equiv(o(\tau),y(\tau))\\ &=(\omega_1(q(\tau),x(\tau)),\omega_2(q(\tau),i(\tau)))\end{aligned}\right\}(1)$$

となる。これらの関係式が端末オートマトンの動作を表現する。(1)式中，$\gamma(\tau)$のω_1，ω_2にそれぞれ$i(\tau)$，$x(\tau)$が含まれていないのは，図1の端末モデルにおいて，キーボードからの入力が直ちにプリンタへ出力されないこと，及び伝送路からの入力はその時点の伝送路への出力に影響しないためである。また，端末は自動的なデータ再送等のために送信用バッファを持つと仮定する。

2.2 通信オートマトン

伝送路を介して対向通信する2端末

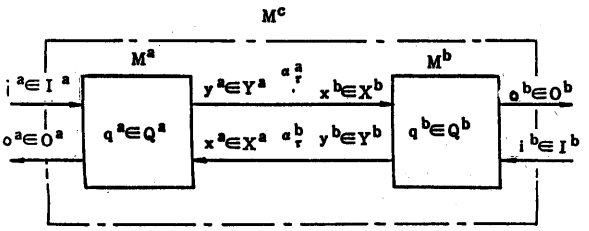


図2　通信オートマトン

から成る通信システムを前節で述べた端末オートマトン2台に伝送路上における伝送誤りを考慮して合成されるオートマトンとして表現し，通信オートマトンと呼ぶ（図2）。

【定義2】 通信オートマトン $M^c = \langle Q^c, \Sigma^c, \Gamma^c, \alpha_\tau, \delta^c, \omega^c, q_0^c \rangle$ は，2台の端末オートマトン $M^a = \langle Q^a, \Sigma^a, \Gamma^a, \delta^a, \omega^a, q_0^a \rangle$，$M^b = \langle Q^b, \Sigma^b, \Gamma^b, \delta^b, \omega^b, q_0^b \rangle$ 及び伝送路の特性を考慮し，次の様に合成して得られる。ここでとくに断らない限り，用いる記号は上肩の添字を除いて前節と同じ意味を持つこととする。

① $Q^c = Q^a \times Q^b$ ：状態集合

② $\Sigma^c = I^a \times I^b$ ：入力集合

③ $\Gamma^c = O^a \times O^b$ ：出力集合

④ 伝送特性関数 $\alpha_\tau = \alpha_\tau^a \times \alpha_\tau^b : Y^b \times Y^a \to X^a \times X^b$，$\alpha_\tau^a : Y^b \to X^a$，$\alpha_\tau^b : Y^a \to X^b$

α_τ，α_τ^a，α_τ^b は時刻により変化する関数であり，次の形式である。

$$x^a(\tau) = \alpha_\tau^a(y^b(\tau)) = y^b(\tau),\ \lambda,\ e \text{ または } \overline{y^b(\tau)}$$

$$x^b(\tau) = \alpha_\tau^b(y^a(\tau)) = y^a(\tau),\ \lambda,\ e \text{ または } \overline{y^a(\tau)}$$

ここで $\overline{y^b(\tau)}$ は $y^b(\tau)$，λ，e 以外の Y^b の要素であり，伝送誤りで他の信号に化けることに相当する。$y^a(\tau)$ も同様である。

⑤ 状態遷移関数 $\delta^c : Q^c \times \Sigma^c \to Q^c$

δ^c は次の様にして得られる。

$$\left.\begin{aligned} q^c(\tau+1) &\equiv (q^a(\tau+1), q^b(\tau+1)) \\ &= \delta^c(q^a(\tau), q^b(\tau), i^a(\tau), i^b(\tau)) \\ q^a(\tau+1) &= \delta^a(q^a(\tau), \sigma^a(\tau)) \\ &= \delta^a(q^a(\tau), i^a(\tau), x^a(\tau)) \\ &= \delta^a(q^a(\tau), i^a(\tau), \alpha_\tau^a(\omega_2^b(q^b(\tau), i^b(\tau)))) \\ q^b(\tau+1) &= \delta^b(q^b(\tau), i^b(\tau), \alpha_\tau^b(\omega_2^a(q^a(\tau), i^a(\tau)))) \end{aligned}\right\} (2)$$

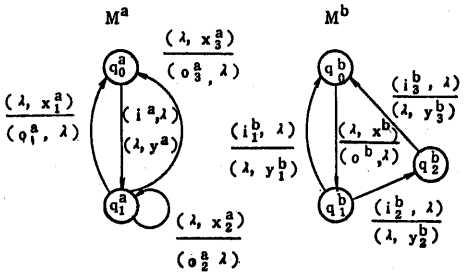
⑥ 出力関数 $\omega^c = \omega_1^a \times \omega_1^b : Q^c \times \Sigma^c \to \Gamma^c$

$$\left.\begin{aligned} \sigma^c(\tau) &\equiv (o^a(\tau), o^b(\tau)) \\ &= \omega^c(q^a(\tau), q^b(\tau), i^a(\tau), i^b(\tau)) \end{aligned}\right\}$$

$$\left.\begin{aligned} o^a(\tau) &= \omega_1^a(q^a(\tau), \alpha_\tau^a(\omega_2^b(q^b(\tau), i^b(\tau)))) \\ o^b(\tau) &= \omega_1^b(q^b(\tau), \alpha_\tau^b(\omega_2^a(q^a(\tau), i^a(\tau)))) \end{aligned}\right\} (3)$$

⑦ 初期状態 $q_0^c = (q_0^a, q_0^b)$

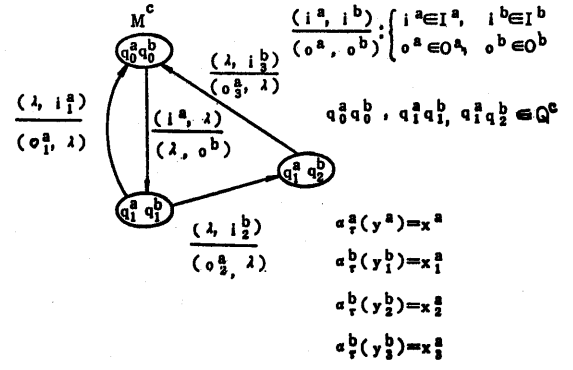
端末オートマトン及び通信オートマトンは状態遷移図によって記述できる。簡単な端末オートマトンの例と，その端末オートマトン2台が伝送誤りのない伝送路を介して通信する通信オートマトンの例を図3に示す。いずれもMealy型のオートマトンであるので，状態遷移図中の点（vertex）はオートマトンの状態を表示し，枝（edge）は状態間の遷移を表示する。枝に付与されるラベルは，キーボード／プリンタの



$$\frac{(i^a, x^a)}{(o^a, y^a)} : \begin{cases} i^a \in I^a, & x^a \in X^a \\ o^a \in O^a & y^a \in Y^a \end{cases} \qquad \frac{(i^b, x^b)}{(o^b, y^b)} : \begin{cases} i^b \in I^b, & x^b \in X^b \\ o^b \in O^b & y^b \in Y^b \end{cases}$$

$q_0^a,\ q_1^a \in Q^a$ $\qquad$ $q_0^b,\ q_1^b,\ q_2^b \in Q^b$

(a) 2台の端末オートマトン



(b) 通信オートマトン

図3　端末オートマトンと通信オートマトン

入力，出力ばかりでなく，伝送路からノへの入力，出力も含むのに対し，通信オートマトンの入力，出力は伝送路からノへの入力，出力を含まない。

3. プロトコル不適格性の条件とその判定法

本章では，プロトコル不適格性の条件として，デッドロック，データの欠落，データの重複を挙げ，通信オートマトンがそれらの条件を満足するか否かの判定法を与える。さらに状態遷移行列により検査する方法を与え，プロトコル検証の自動化への可能性を探る。

3.1 デッドロック

デッドロックとは，対向通信中の両端末のキーボードから如何なる入力をしても両端末が初期状態に戻れない状態をいう。

〔判定法1〕 通信オートマトンM^cにおいてデッドロックの起る条件は，初期状態s_0^cから到達可能な状態のうち，s_0^cに到達不可能な状態が存在することである。

状態数nの通信オートマトンM^cの状態遷移図の隣接行列$A(M^c)$に対応する到達可能性行列$R(M^c)$

$$R(M^c)=I+A(M^c)+A(M^c)^2+\cdots+A(M^c)^{n-1} \quad (4)$$

を計算する。ここで，$A(M^c)$の(i,j)要素は，状態$s_0^c, s_1^c \cdots$について，s_i^cからs_j^cへ隣接すれば1，それ以外は0とする。$R(M^c)$の第1行及び第1列の要素が1となる状態の集合をそれぞれQ_r^c，Q_c^cとするとき，デッドロックが生じる条件は次の関係が成立しないことである。

$$Q_r^c \subseteq Q_c^c \quad (5)$$

3.2 データの欠落．重複

データの欠落とは，一方の端末のキーボードから入力されたデータが相手端末のプリンタに出力されないで初期状態に戻ってしまうことである。またデータの重複とは，初期状態に戻るまでに，入力されたデータが2度以上相手端末のプリンタに出力されるか，キーボードから入力されないデータが相手端末のプリンタに出力されることである。

データの欠落，重複の発生する状況をもう少し詳しくみると，次のようになる。

現在対象としている端末モデルでは，実質的にデータを保持できるのは送信バッファのみである。もし送信バッファがキーボードからの次の入力により書き換えられると，元の内容は通信オートマトンの中から完全に失われてしまう。したがって，データがキーボードから入力されたものの，もしそのデータが相手側に出力されないうちに次のデータ入力により送信バッファの内容が書き換えられてしまうと，前に入力されたデータは相手側に出力され得ない。一方，重複は次のように生じる。キーボードから送信バッファに入力されたデータが相手プリンタへ既に1度出力されたとする。もし次の入力により送信バッファが書き換えられないうちに，送信バッファの内容が再送されて相手プリンタへ再度出力されると重複となる。

以上からわかるように，基本的には，2度の入力の間に1度も相手側への出力がなければデータの欠落が起り，2度の出力の間に1度も相手側への入力がなければデータの重複が起るといえる。

以上の考察に基づいて，データの欠落・重複の判定法を述べる。そのために先ず通信オートマトンを表現する状態遷移図の変形を行う。

〔定義3〕 通信オートマトンM^cの検証用状態図は，一方の端末オートマトンのキーボードからのデータ入力σ^c及び相手プリンタへのデータ出力μ^cを表示するラベルσ^c/μ^cが付いた枝すべてについて，図4に示す様に2つの枝（ラベルσ^c/λ及びλ/μ^c）と補助状態（q^c_{ij}）により変形して得られる状態遷移図である。

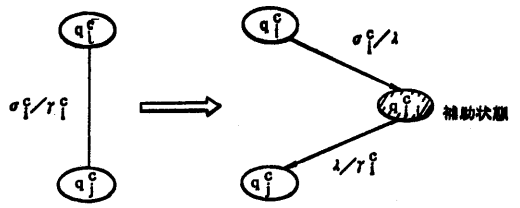


図4　検証用状態図への変形

定義3は，以下に述べる2つの判定法の中で枝を取り除く操作を行う際に，入力と出力とを分離しておく必要があるために導入する。

〔判定法2〕 デッドロックのない通信オートマトンM^cにおいてデータの欠落が生じる条件は，検証用状態図から一方の端末オートマトンのプリンタへのデータ出力を表示するラベルの付いた枝全部を取り除いて得られる状態遷移図の中に，他方の端末オートマトンのキーボードからのデータ入力を表示するラベルが付いた枝同士を結ぶ枝のシーケンス（枝の向きに従う）が1つでも存在することである。

〔判定法3〕 デッドロックのない通信オートマトンM^cにおいてデータの重複が生じる条件は，検証用状態図から一方の端末オートマトンのキーボードからのデータ入力を表示するラベルの付いた枝全部を取り除いて得られる状態遷移図の中に，他方の端末オートマトンのプリンタへのデータ出力を表示するラベルが付いた枝同士を結ぶ枝のシーケンス（枝の向きに従う）が1つでも存在することである。

判定法2，3の正当性の詳細な証明は省略する。なお，これらの判定法は判定法1と同様に到達可能性行列を用いた形式にすることができる。例えば判定法2の場合には，出力表示ラベル付きの枝全部を取り除いたあと，到達可能性行列を計算し，入力表示ラベル付きの枝の終端にある状態から入力表示ラベル付きの枝の始端にある状態へのあらゆる組み合わせについて到達可能性（対応する要素が1）を検査すればよい。

4. JIS標準ベーシック伝送制御手順への適用例

本報告で提案するモデル及び検証法をJIS標準ベーシック伝送制御手順に適用してみる。なお，説明に不要なシーケンスについては簡単のため省略する。

ベーシック手順では，図5(a)に示すようにデータリンク確立後通信状態となり，相手からの肯定応答受信後に次のデータの送信が可能となる。さらに

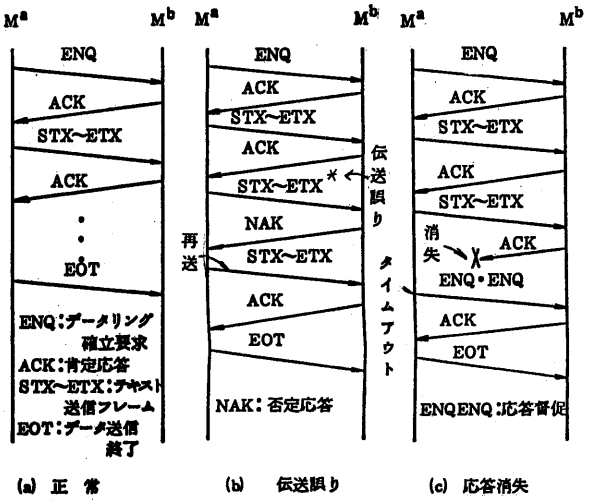


図5　ベーシック手順の通信シーケンス例

図5(b)に示すように，伝送誤りを検出した場合は否定応答を返し，送信側は否定応答受信後に直前のデータを再送する。また図5(c)のように，データ送信後応答が返ってこないとタイムアウトし，応答督促を送信できる。

以上のようなベーシック手順を，2台の端末オートマトンM^a（送信側），M^b（受信側）の状態遷移図で記述すると図6のようになる。図6のM^aで枝②→③はキーボードからのデータ入力により伝送路へデータを送出する遷移に相当し，ラベル中の信号Dがデータ入力を表示する。図6のM^bで枝②→③及び⑥→③は伝送路からのデータ受信によりプリンタへデータを出力する遷移に相当し，各ラベル中の信号Dがデータ出力を表示する。

図6の端末オートマトンM^a, M^bから定義2にしたがって通信オートマトンを作ったものが図7(a)である。ここで，伝送特性関数$\alpha_\tau = \alpha_\tau^a \times \alpha_\tau^b$は，データ以外の信号の伝送に関して$x^a(\tau)=\alpha_\tau^a(y^b(\tau))=y^b(\tau)$, $x^b(\tau)=\alpha_\tau^b(y^a(\tau))=y^a(\tau)$ とした。

ただしデータの伝送に関しては，これ以外に伝送誤り，消失を考慮して$\alpha_\tau^b(y^a(\tau))=e$，および$\alpha_\tau^b(y^a(\tau))=\lambda$となる場合のシーケンスも含めた（図7(a)）。

図7(a)で，枝(2,2)→(3,2)，(2,2)→(3,5)は共にデータ入力表示のある枝である。また枝(2,2)→(3,3)はデータ入力表示とデータ出力表示をもつラベル(D, λ)／(λ, D)をもつ。そこで，枝(2,2)→(3,3)の間に補助状態を追加し検証用状態図に変形したものが図7(b)である。

図7(b)から，データ出力を表示するラベルをもつ枝 ▨ →(3,3)及び(4,6)→(3,3)を除くと図7(c)の状態図になる。図7(c)中には波線で示したように，データ入力表示のある枝(2,2)→(3,2)自身を結ぶ枝のシーケンス(3,2)→(3,4)→(2,2)が存在し，判定法2によりデータ欠落の発生する条件を満足している。この状況を通信シーケンス例として表わすと，図8のように，応答督促に対する肯定応答は送信側にとっては直前に送信したデータD_2に対する肯定

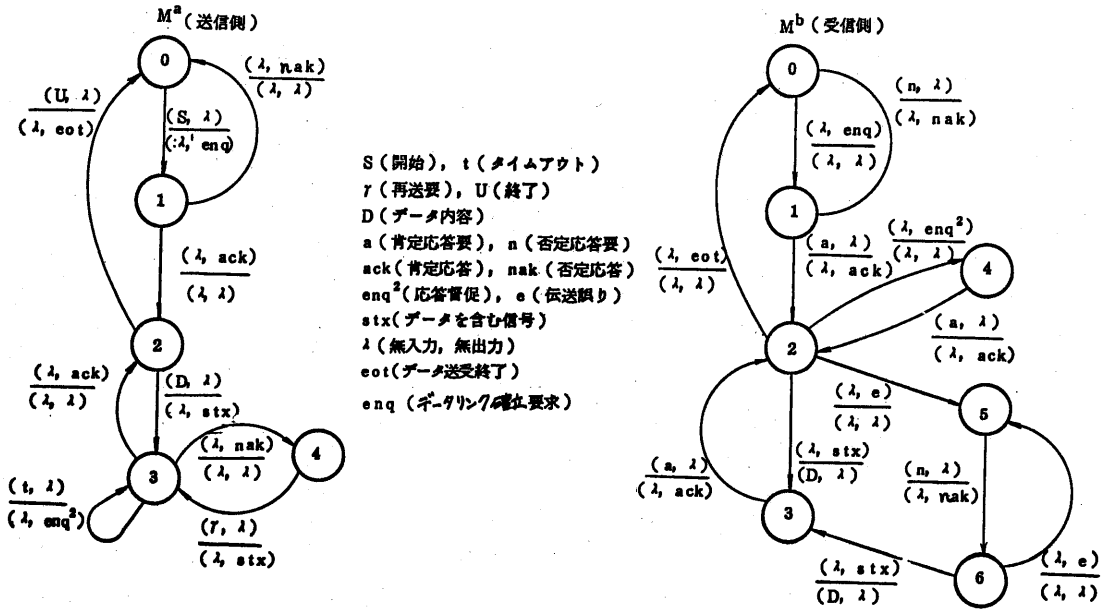
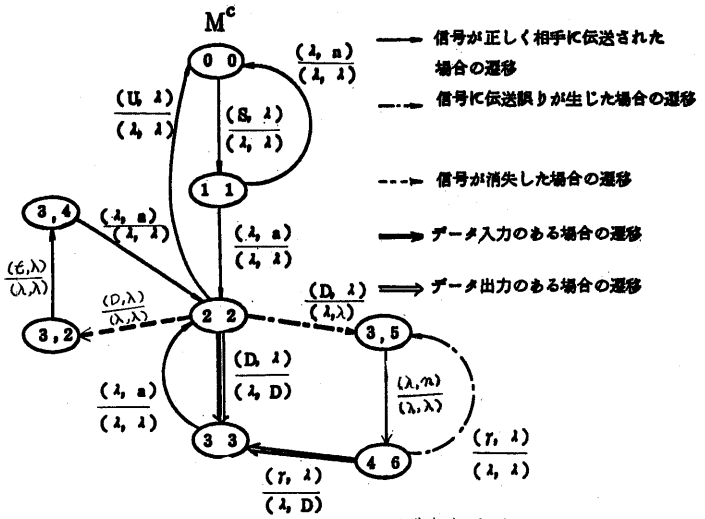


図6　ベーシック手順の端末オートマトン

応答となり次のデータD3を送信する。結局データD2は受信側には受けとられないことになる。

以上の例は，図6のようなベーシック手順の誤り検出能力が欠落発生に対しては不足していることを示している。また，無応答時にタイムアウトすると送信側は直前のデータを再送することも規定上許されている。この場合は，重複の可能性があることがISOの規定[7]では明示されており，本検証法の判定法ろによっても確認している。[8] 上記ベーシック手順を実際のシステムで使用する場合は，欠落・重複の可能性を前



(a) 図6の端末オートマトンから合成される通信オートマトン

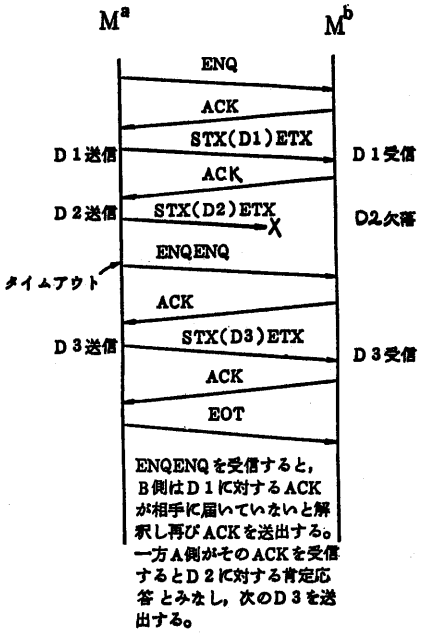
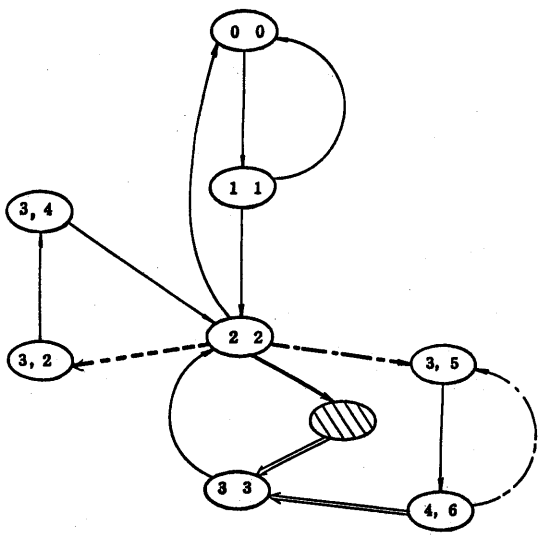
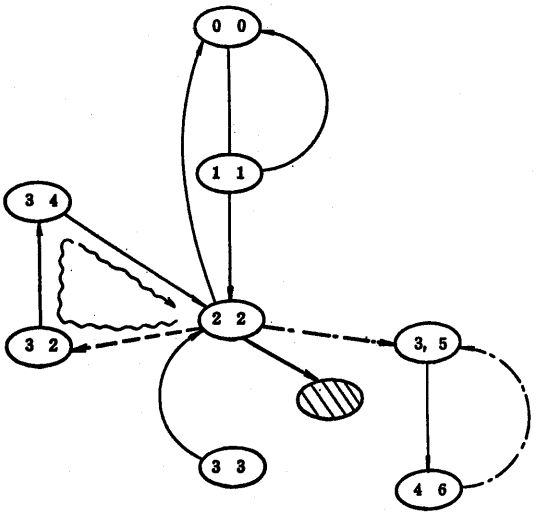


図8 ベーシック手順における欠落発生例



(b) 検証用状態図への変形



(c) データ欠落のある枝のシーケンス例

図7 データ欠落の検証例

提として使用する必要がある。

5. むすび

対向通信する端末を有限オートマトンでモデル化し，2台のオートマトンから通信オートマトンを合成し，デッドロック及びデータの欠落・重複に関してプロトコルの検証を行う手段を述べ，この検証法をJIS標準ベーシック伝送制御手順に適用してみた。

通信オートマトンを合成する方法は，かなり一般的なものであり，ほとんど制限条件がないが，3章で述べた検証法は制限条件が付いているので，この制限条件の緩和が今後の課題である。具体的には以下のような項目である。

i) 端末内の送信バッファの複数化、及びデータブロックを連続転送可能とするプロトコルもあるので，その取扱いを可能にすること。

ii) 上述に伴い，データブロックの順序誤りに関する検討も必要である。

また、プロトコル検証の自動化に当って，行列演算による方法は有効と思われるが，状態数の増加に伴い計算量がぼう大になるので，実用的な立場からは次の課題も重要である。

iii) 状態数と計算量の関係の推定及び計算量を削減する手段。

謝辞

本検討にあたって御協力いただいた関係各位に深く感謝いたします。

参考文献

(1) Danthine, A and Bremer, J. : "Axiomatic Description of the Transport Protocol of Cyclades", Proc. Processional Conf. on Computer Networks and Teleprocessing, Aachen, p. 259 (1975).

(2) Danthine, A. and Bremer, J. : "Specification and Verification of End-to-End Protocols", Proc. 4th ICCC, Kyoto, p. 811 (1978).

(3) Marlin, P.M. : "A Study of the Recoverability of Computing Systems", Ph. D. Univ. of California (1975).

(4) Zafiropulo, P. : "A New Approach to Protocol Validation", Proc. 13th ICC, Chicago, p. 259 (1977).

(5) West, C.H. and Zafiropulo, P. : "Automated Validation of Communications Protocol : CCITT X.21 Recommendation", IBM J. Res. & Dev., 22, 1, p. 60 (1978).

(6) Sunshine, C.A. : "Interprocess Communication Protocols for Computer Networks", Technical Report No. 105, Stanford Univ. (1975).

(7) ISO 1745-1975(E), Information Processing — Basic mode d Procedures for Data communication Systems.

(8) 野村，田中："通信プロトコルの検証について"，昭54信学情報・システム部門全大，251.