

最短試験系列を多項式時間で計算可能なプロトコルのクラスについて

4 V - 3

行友 英記

角田 良明

菊野 亨

大阪大学基礎工学部情報工学科

1 まえがき

通信プロトコルがその仕様通りに実装されているか否かを試験することは実用上極めて重要な問題である。実装されたプロトコルの内部状態を外部から直接識別することはできないので、一般にメッセージの入出力によって内部状態を同定する方法が用いられる。この状態の同定と、状態での入力に対する正しい出力の確認に必要なメッセージ系列をプロトコルの試験系列と言う。試験のコストを削減するためには試験系列の長さを短くすることが要求される。一般に任意のプロトコルに対して、最短試験系列を多項式時間で求めることはできないと予想されている。本稿では、最短試験系列を多項式時間で計算可能なプロトコルのクラスについて議論し、従来の研究で報告されていたプロトコルのクラスを真に含む、実用的なプロトコルのクラスを新しく提案する。

2 プロトコルの試験

通信プロトコルは有限状態機械でモデル化されていると仮定する。このとき、プロトコルの内部状態を同定する従来の手法として、UIO 系列, W 手法, DS 系列などが知られている [1, 2, 3]。プロトコルの試験は、プロトコルの各遷移が仕様通りに実装されているかどうかを確認することである。そのためには、(1) 遷移先の状態と (2) 遷移の入力に対する出力、を調べなければならない。

文献 [4] では、全ての遷移を試験する最短の試験系列を求める問題を、いわゆる Rural Chinese Postman 問題 (以下 RCP 問題と略す) に帰着させて効率よく解いている。但し、有限状態機械は次の3つの条件を満たしていることが仮定されている。

- (1) 決定性動作をする。
- (2) グラフで表現した時その有向グラフは強連結である。
- (3) 状態数が最小である (等価な状態はない)。

更に、文献 [4] では最短試験系列を多項式時間で求めるための条件、及び、その条件を満たす十分条件が2つあげられている。

本稿では、その2つの十分条件を覆う新しい条件を満たすプロトコルのクラスを提案する。

3 試験系列

ここではプロトコルを表す有限状態機械 FSM を  $M$  とし、そのグラフ表現を  $G$  とする。  $G$  中の頂点と辺はそれぞれ  $M$  の状態、状態遷移に等しく、辺のラベルとして、状態遷移の入力/出力がつけられる。図1にその例を示す。以降、  $M$  は前節であげた3つの条件を満たしているものとする。UIO 系列は、  $M$  中の各状態に固有の入出力系列であって、ある状態に固有な入力系列を  $M$  中のその状態において与えた時得られる出力系列は、その入力系列を  $M$  中の

他のどんな状態において与えても、決して同じ出力系列が得られないものである [1]。状態  $S$  の UIO 系列を  $UIO_S$  と表す。図1においては、系列の接続を  $'|'$  で表すと、  $UIO_1$  は  $x/a, UIO_2$  は  $y/b; z/c$  である。

試験したい遷移を  $test$  とし、その遷移先の状態を  $D$  とする。このとき、試験部分系列を  $test; UIO_D$  とする。例えば、図1で、  $test$  を状態1から状態2への遷移  $x/a$  とする。  $UIO_2$  は  $y/b; z/c$  なので、状態1から状態2への遷移の試験部分系列は  $x/a; y/b; z/c$  となる。試験部分系列の実行前の状態と実行後の状態を結ぶ辺を  $TS_{test}$  と表す。  $G$  の全ての頂点と、全ての  $TS_{test}$  から構成される有向グラフを  $\hat{G}$  と表す。試験系列は全ての試験部分系列を含む系列である。  $\hat{G}$  は有向グラフであるが、以降では辺の向きをなくした無向グラフとみなす。

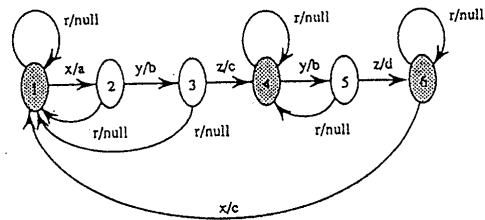


図1 プロトコルのグラフ表現の例

$M$  がリセット機能を持つとは、対応するグラフ表現  $G$  上の全ての状態から初期状態に遷移が定義されていることを表す。  $M$  中の状態がセルフープを持つとは、対応するグラフ表現  $G$  上でその状態からの遷移のうち、遷移先が自分自身であるものが含まれていることである。

4 試験容易なプロトコルのクラス

4.1 従来の結果

文献 [4] では補題1に示す最短試験系列を多項式時間で求めるための条件が与えられ、補題1を満たす十分条件として補題2、補題3が証明されている。

補題1  $G$  から導かれるグラフ  $\hat{G}$  が弱連結であれば最短試験系列を多項式時間で求めることができる。

補題2 有限状態機械  $M$  がリセット機能をもっていれば、  $\hat{G}$  は弱連結である。

補題3 有限状態機械  $M$ 中の全ての状態にセルフループがあれば、 $\hat{G}$ は弱連結である。

4.2 チェックポイントリスタート機能

チェックポイントリスタート機能とはプロトコルがプロセス間の同期のずれなどにより異常が生じた時、それ以前に通過した、チェックポイント状態と呼ばれる特定の状態に戻る事ができる機能である。異常時にチェックポイント状態へ戻る遷移をリスタート遷移と呼び、それ以外の遷移を正常遷移と呼ぶ。ある状態  $S$  からチェックポイント状態  $CP$  にリスタート遷移が記述されている時、 $S$  は  $CP$  に属するという。

図1はチェックポイントリスタート機能を持つプロトコルの例となっている。網線の引いてある状態がチェックポイント状態を、白い状態は非チェックポイント状態を表している。この図のように非チェックポイント状態にはそれ以前に通過した最も近いチェックポイント状態への遷移があり、チェックポイント状態には自分自身への遷移がある。

チェックポイント状態が初期状態しかない時は補題2の  $M$  に、全ての状態がチェックポイント状態の時は補題3の  $M$  に等しいことから、次の補題が導かれる。

補題4 チェックポイントリスタート機能を持つプロトコルのクラスは補題2、補題3を満たすプロトコルのクラスを含む。

チェックポイントリスタート機能、リセット機能、セルフループそれぞれを持つプロトコルのクラスの包含関係を図2に示す。

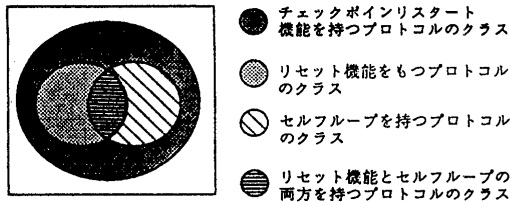


図2 包含関係

定理1 チェックポイントリスタート機能を持つプロトコルのグラフ表現  $G$  から得られるグラフ  $\hat{G}$  は弱連結である。

(証明)

まず、(ステップ1)であるチェックポイント状態に属するもの同士が  $\hat{G}$  中で連結であることを示し、次に(ステップ2)で異なるチェックポイント状態に属する状態の集合が  $\hat{G}$  中で連結であることを示す。

(ステップ1)

図3において、 $T, U$  は  $CP$  に属する任意の状態を表している。 $T, U$  が  $CP$  に属するので、 $T, U$  から  $CP$  へのリスタート遷移が存在する。今、それらを  $t, u$  とする。すると、試験部分系列はそれぞれ、 $t; UIO_{CP}$ 、 $u; UIO_{CP}$  となる。各々の試験部分系列に対応する辺  $TS_t, TS_u$  が  $\hat{G}$  に含まれ、両辺の行き先が同じであることから、 $T, U$  は連結である。よってグラフ  $\hat{G}$  中の  $CP$  に属する任意の2つの状態は連結である。

(ステップ2)

$G$  の強連結性とチェックポイントリスタート機能の定義より、 $CP$  への正常遷移  $a$  を持ち、かつ  $CP$  に属さない状態  $S'$  が必ず存在する。 $CP$  にはセルフループ  $b$  が存在するため、 $\hat{G}$  中には  $TS_a$ 、 $TS_b$  により、 $CP$  と  $S'$  の連結性が保証される。一方、 $S'$  は自分が属するチェックポイントと連結なのでチェックポイント状態同士が連結される。よって隣接するチェックポイント状態同士が弱連結となる。 $G$  が強連結であることより、全てのチェックポイント状態同士も弱連結となり、 $\hat{G}$  全体は弱連結となる。

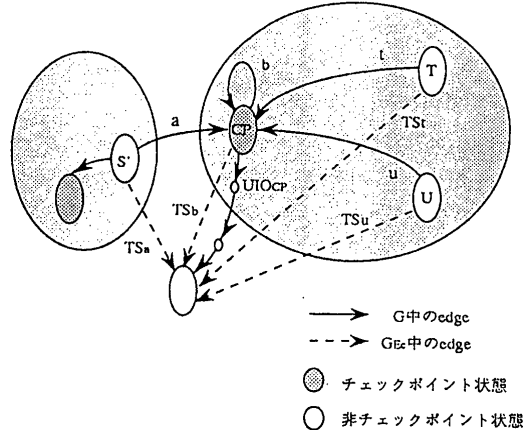


図3 チェックポイントリスタート機能

先の定理1と補題1より、次の系が得られる。

系1 チェックポイントリスタート機能を持つプロトコルの最短試験系列は多項式時間で計算可能である。

5' あとがき

チェックポイントリスタート機能を含むプロトコルのクラスに対しては ROP 問題の解法を応用すれば最短試験系列を多項式時間で解くことが可能であることを示した。今後の課題としては最短試験系列を多項式時間で解くためのプロトコルのクラスの必要十分条件を求めることがある。

文献

- [1] K. K. Sabnani and A. T. Dahbura: "A new technique for generating protocol tests", Proc. of 9th Data Communications Symp., pp. 36-43, Sept. 1985.
- [2] D. Sidhu and T. Leung: "Fault coverage of protocol test methods", Proc. of INFOCOM'88, pp. 80-85, March 1988.
- [3] T. Chow: "Testing software design modeled by finite-state machines", IEEE Trans. Software Eng., SE-4, pp. 178-187, March 1978.
- [4] A. V. Aho, A. T. Dahbura, D. Lee and M. U. Uyar: "An optimization technique for protocol conformance test generation based on UIO sequences and rural chinese postman tours", Proc. of the 9th Int'l. Symp. on Protocol Specification Testing and Verification, pp. 75-86, 1988.