

状態遷移に基づく設計支援システムについて

4 N-1

鷲澤正英

菅野文友

東京理科大学 工学研究科

1. はじめに

ソフトウェアに対する需要が高まるにつれて、その信頼性と生産性の向上を求める声も高まっている。これに対して、開発現場レベルでは、開発手順の標準化、体系的開発技法の採用、各種ソフトウェアツールの導入などの試みを行なっているようである。

本報告では、既に研究レベルで有効性が確認されている技術を評価し、現場レベルで使用が可能になるように適用するアプローチとして、状態遷移に基づき、仕様を記述する際の支援システムを試作した。

2. システム化の背景

最近では、パーソナルコンピュータやワークステーションが低価格化しており、これによって、それらをネットワークとして接続したいという要求が増加している。そして、必然的に、既存のプロトコル以外に独自に開発していきたいと考えるユーザが増えることが考えられる。

その際、設計したプロトコルを検証し、論理的矛盾をなくすことが重要である。こうした、プロトコルを検証するという研究は、数多くなされているが、ソフトウェアによる支援システムは少ないのが現状である。

そこで、パーソナルコンピュータ上で実行可能なプロトコル検証機能を備えた設計支援システムを、試作した。

3. 検証項目と内容

プロトコル検証で、代表的なものとしては、以下のものがある。

- ① デュオログマトリックス (DM) 検証法
(Zafiropulo:1977)
- ② パータバージョン (PB) 解析法
(West.et.al:1978)

また、これらを基に、逆パータバージョン解析やプロセス状態遷移の一括処理を行なう効率良い検証法等が、研究されている。

本システムでは、まず、代表的な検証法である上記①、②の検証を行なえるものを意図した。

DM検証法およびPB検証法の検証項目を、それぞれ表1および表2に示す。

表1 DM検証法の検証項目

| 項番 | 検証項目 | 説明 |
|----|-------------|-----------------------------------|
| 1 | 個々のユニログ | 状態0で始まり、状態0で終わるが、途中で状態0を通過しないパス |
| 2 | デュオログマトリックス | -1:誤りを含む 0:発生できない 1:うまく動作する |

表2 PB検証法の検証項目

| 項番 | 検証項目 | 説明 |
|----|-------------|--|
| 1 | システム状態集合 | システムの動的な遷移状態集合 |
| 2 | デッドロック状態集合 | それ以上遷移先のない"すくみ"の状態集合 |
| 3 | オーバーフロー状態集合 | 設定したバッファ容量を超えるイベント受信時状態 |
| 4 | 受信不能状態集合 | 受信バッファ内のイベントの相手プロセスでその送信イベントがないときの状態集合 |

4. システムの開発

試作した状態遷移に基づく設計支援システムの概要を、説明する。

4.1 システムの目的

本システムは、プロトコル設計の流れで、その一部をパーソナルコンピュータに行なわせようというものである。つまり、通常、プロトコルを設計していく過程は、試行錯誤しながら状態遷移図を作成し、これを、図から行列に変換

する。そして、複数の状態遷移行列に、論理的矛盾がないかどうかを検証する。

これによって、より誤りの少ないプロトコル仕様を作成することが可能になる。ここでは、この設計過程の一部を支援し、設計の効率化を目指すことを目的としている。

4.2 システムの概要

本システムでは、パーソナルコンピュータで実行することも、特徴の一つである。つまり、手軽に、このシステムを利用することが可能である。本システムの動作環境を表3に示す。

表3 動作/開発環境

| 項番 | 種別 | 環境 |
|----|-----|--------------------------------------|
| 1 | H/W | NEC PC-9800シリーズ or 互換機 |
| 2 | S/W | ・MS-DOS Ver.3.3 |
| | | ・Lattice C Ver.3.1 ・Mifes Ver.4.0 |

本システムでは、状態遷移図を作成し、それらを自動検証することが基本である。このモジュール構成を図1に示す。

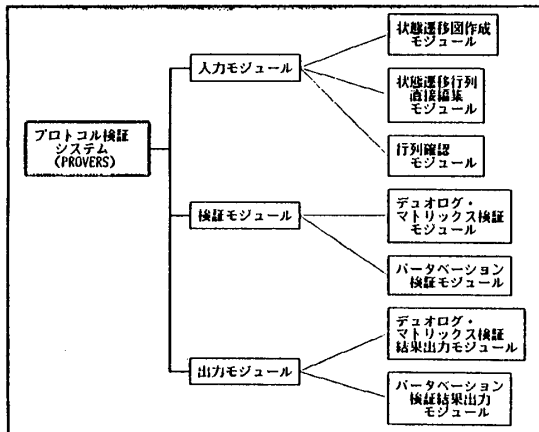


図1 システムのモジュール構成

さらに、本システムのメニュー画面を図2に、状態遷移図作成の画面例を図3に、それぞれ示す。

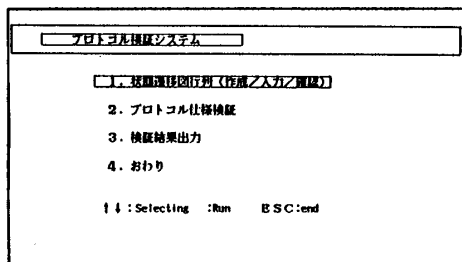


図2 システムのメニュー画面

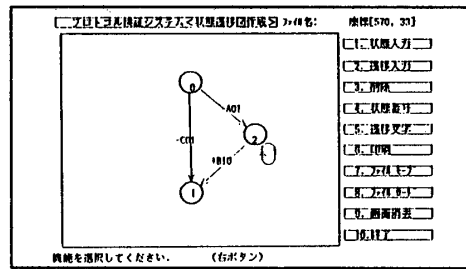


図3 状態遷移図作成の画面(例)

4.3 実施事例

システムの実施事例として、DM検証法およびPB検証法の検証結果出力例を、図4に示す。

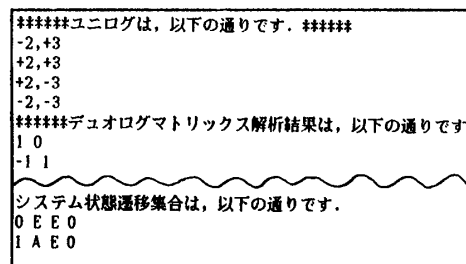


図4 検証結果出力画面(例)

5. おわりに

状態遷移による記述の欠点としては、状態数が増えすぎることによる理解性や解析性の低下がある。実際、本システムについて、プロセス数および状態数を、本システム最大の大きさに記述し、その解析を行なうと、かなりの量の情報が出力され、かつ時間もかかった。

しかし、まったくの手作業による検証に比べれば効率が上がることは期待できる。さらに、これをパーソナルコンピュータ上で実現していることから、手軽に利用することが可能である。

【参考/引用文献】

[1]片岡雅憲:「ソフトウェア・モデリング」, 日科技連出版,(1988).
 [2]C.H.West:”General Technique for Communications Protocol Validation”,IBM J.Res. Develop.,Vol.22,pp.393-404,(July.1978).
 [3]Vijay Ahuja,池野信一 訳:「コンピュータ通信ネットワーク -設計と解析-」, 近代科学社,(1983).
 [4]Pitro Zafiropuro:”Protocol Validation by Duologue-Matrix Analysis”,IEEE Trans.Commun.,Vol.COM-26,No.8, pp.1187-1194,(Aug.1978).