自動検証システムＡＴＶＳの拡張

2R－6

田中誠一郎　宮崎義弘　手島文彰　井上勝博　三原幸博
株式会社　東芝　システム・ソフトウェア技術研究所

１．はじめに

システム開発において、その仕様を形式的に記述することにより、実現されたシステムと仕様の間に論理的矛盾がないかどうかを検証することができる。

我々は、このような検証をオートマトンを用いて機械的に行うシステム ＡＴＶＳ（Automated Testing and Verification System）を開発している[1]。ＡＴＶＳで対象としている仕様はシステムの設計仕様であり、それは有限状態機械（Finite State Machine 以下、ＦＳＭと略す）により表現される。しかし、実際の製品仕様をＦＳＭで記述しようとすると、記述性や理解性の点で問題がある。また、ＡＴＶＳの検証能力自体も改良の余地がある。

本稿では、まずＡＴＶＳにおける検証の概要について述べ、次に仕様記述の拡張と検証機能の追加、その実現に伴うＡＴＶＳの拡張について述べる。

なお、このＡＴＶＳは一貫ソフト開発支援システムＩＭＡＰ[2]の一環として開発している。

２．検証手法

本手法は、オートマトンの概念に基づいている。すなわち、システムの設計仕様をＦＳＭを用いてモデル化し、そのＦＳＭを表現するオートマトンに、実際のシステムの振舞いをモニタしたときのデータを入力として与え、それが受理されるか否かにより検証を行うのである。この概念図を図１に示す。

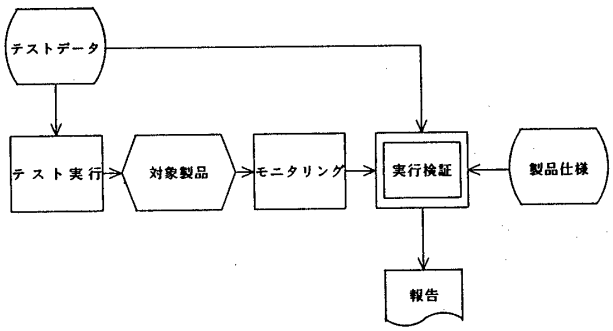

図１．検証手法の概念図

ＡＴＶＳでは、対象システムへの内界や外界からの入力をイベント、それに対するシステムの出力動作をアクションとしてとらえている。まず発生したイベントやアクションとＦＳＭにより表現された仕様との対応付けを行う。もしうまく対応付けられれば、その状態に遷移した時刻とイベントやアクションの発生時刻とが時間的に矛盾していないかどうかを調べる。

このようなことから、ＡＴＶＳでは、「仕様と実際の動作との矛盾」を検出できる。

３．仕様記述の拡張

対象となるシステムの大規模化、複雑化により、状態や遷移の数が指数関数的に増大する傾向にある。この傾向は、仕様記述の容易性、理解性を著しく妨げる。

これを解決するため、ＦＳＭの階層記述を可能にした。階層化したＦＳＭを用いてシステムの仕様を機能的に分割すれば、仕様記述の容易性、理解性を向上させることができる。

また、次に述べる検証機能を用いることにより、階層レベルの記述の検証を可能にする。この機能を用いて階層単位の仕様を組み上げることにより、より厳密な仕様の記述が可能になる。

４．表明による検証

検証能力の向上を図るため表明による検証を考える。

表明とは、設計者の意図したことを宣言的に表現したものであり、その正当性を調べることにより、検証を行うことができる[3]。

我々は、次のような２つのことを表明として与えることを提案する。

（１）要求仕様によって与えられた各機能の入出力条件

設計仕様が機能別に分割され記述されると、図２に示すように個々の機能は、ある入力に対し出力を行う関数のようなものとみすことができ、この表明により機能レベルの検証を行うことができる。

An extension of automated testing and verification system 'ATVS'
Seiichiro TANAKA, Yoshihiro MIYAZAKI, Fumiaki TESHIMA, Katsuhiro INOUE, Yukihiro MIHARA
TOSHIBA Corporation

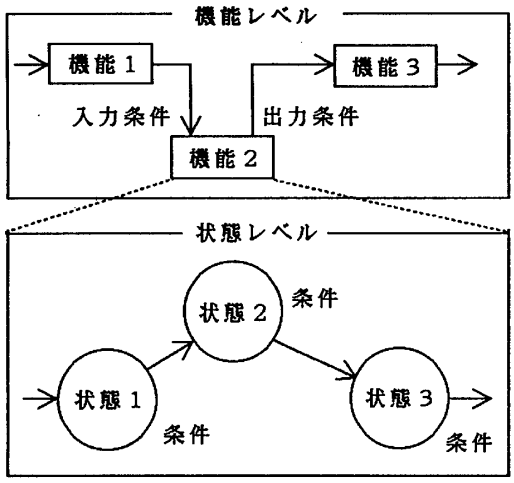

図２．表明として与える条件

（２）設計時に考えられた各状態においてシステムが満たしていなければならない条件

図２に示すように機能の詳細は、状態と遷移から構成されており、この表明により、より詳細なレベルの検証が行える。

表明を用いて検証を行うとき、具体的にはシステムの状態を変数として実現し、その変数に関する論理式を表明として与える。その論理式が成立するかどうかを調べることにより検証を行う。

５．二つの検証手法の併用の有効性

これまでの検証手法では、機能を実現する手続きについて仕様と対象システムとの間に矛盾がないかどうかを調べることができる。しかし、このような方法では、その機能を実行した後の結果に対して保証するものではない。それに対し、表明による検証では、その機能への入力や出力結果が要求仕様を満たしているかどうかを調べることができる。

例えば冷蔵庫で、霜取りを行った後、庫内の温度があるレベルを越えていなければならないという要求仕様があったとする。これまでの検証手法では、霜取りを行うときの手続きが正しく行われているかどうかは検証することができるが、その結果である庫内の温度については何も保証していない。これに対し、表明による検証では、この条件を表明として示しておけば、この機能の実行結果が要求仕様を満たしているかどうかを検証することができる。

このようにこの２つの検証手法では、違った観点から検証を行っているので、その対象としているエラー空間も異なっている。このため、この２つの検証手法を併用することにより、異なるエラーを検出することができ、より厳密な検証が可能となる。

６．システム構成

以上のような拡張を行うために、ＡＴＶＳを図３のような構成で実現を考える。網掛け部分が新たに追加されたものである。これによりＦＳＭの階層化と表明を用いた検証に対応することができる。

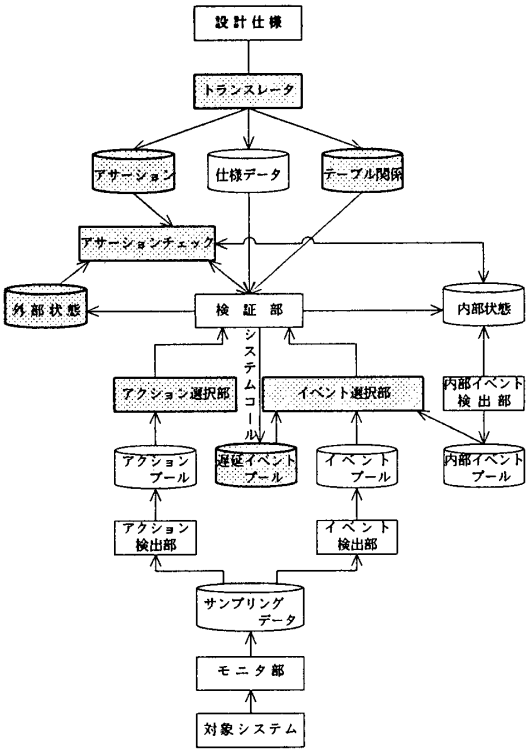

図３．システムの構成

７．おわりに

本稿では、仕様とシステムの動作の間に論理的矛盾がないかどうかを自動的に検証するシステムＡＴＶＳの概要とその拡張について述べた。この拡張により大規模なシステムや複雑な仕様への適用が可能になった。また、表明による検証を併用することにより、これまでの検証手法では検出できなかったエラーを検出することができ、より厳密なチェックが実現できるようになる。

今後、次の項目について検討していく予定である。

（１）仕様記述自体の矛盾の検出

（２）ＦＳＭに基づく設計方法論

参考文献

［１］手島他，「システム設計における仕様検証の一手法」，情処研報Vol.89,No.52,89-SE-66,1989

［２］大筆　豊他，「ＩＭＡＰシステム(1)-(10)」，情報処理学会，第31回全国大会予稿集，p489-508

［３］L.G.Stucki,"New Direction in Automated Tools for Improving Software Quality",in R.T.Yeh(ed) Current Trends in Programming Methodology, Vol.2,Prentice Hall,Englewood Cliffs,1978.