状態遷移表モデル検査ツールGarakabu2の設計と開発

白石知弘†，孔維強†　　松本充広‡　　片山徹郎§　　福田晃¶
水島祐紀†，片平典幸†　　渡辺政彦‡
†福岡県産業・科学技術振興財団　　‡キャッツ株式会社　　§宮崎大学 工学部 情報システム工学科
¶九州大学 大学院システム情報科学研究院

1　はじめに

ソフトウェアの信頼性向上のための一手法としてモデル検査技術が注目されており，適用事例も数多くある．しかしシステム開発においてモデル検査を導入する際，モデル検査用のモデルを新たに作成したり，ユーザが反例を解析するために経験を要する等の課題がある．

そこで我々は，設計フェーズで有用な状態遷移表を検査対象としたモデル検査ツールGarakabu2 [1]を設計開発した．Garakabu2は商用のCASEツールであるZIPC [2, 5]と連動しており，実際の開発現場において使用されている状態遷移表がそのまま検査可能である．また反例を検出した際，ZIPCと連動してシミュレーションすることができるため反例解析コストを削減できる特徴がある．本稿はGarakabu2を使用した検査の流れ，検査対象である状態遷移表の説明，Garakabu2の構成と機能，検査可能な性質に関して述べる．

2　Garakabu2の特徴

本ツールは状態遷移表で設計したモデルに対してモデル検査を行うツールである．以下に本ツールの特徴について具体的に説明する．

2.1　Garakabu2を使用した検査の流れ

本ツールを使用した検査の流れを図1に示す．本ツールは検査対象のモデルとしてZIPCで設計した状態遷移表を読込み，ユーザが性質を設定し，モデル検査を実行する．もしツールが反例を発見した場合，ユーザが本ツールとZIPCが提供するシミュレーション機能を活用しながら設計モデルを修正し，再度モデルを検査する．反例を発見しなかった場合，次の開発工程へ進む．本ツールが反例を発見しなくなるまでこれらの手順を繰り返すことで設計モデルのバグの早期発見と信頼性向上を実現する．

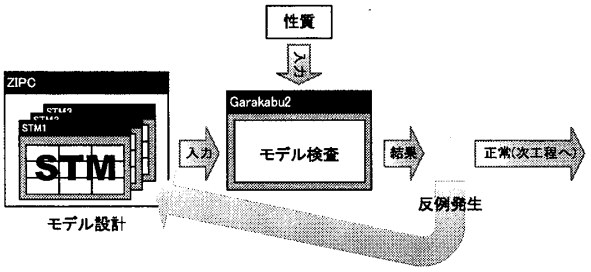

図1: Garakabu2の検査フロー

2.2　状態遷移表

本ツールで検査対象としているモデルは状態遷移表であり，表の記述方法や意味はZIPCを基準としている．代表的な機能を図2を例に以下に説明する．

状態遷移表Tは，縦軸にシステムに対する事象(xE1, E2,E3)，横軸にシステムの状態(S1,S2,S3)，事象と状態が交わる各セル内にアクション(処理)を記述する．例えば，事象xE1と状態S1が交差するセルのアクションは，「システムの状態がS1で事象xE1が発生した場合，action1を実行して状態S2へ遷移する」ことを表す．事象xE1と状態S2の交差するセルに記述している”／”マークのセルは”無視セル”と呼び，「状態がS2の時に事象xE1が発生してもアクションを実行しない」ことを表す．事象E2と状態S1の交差するセルに記述している”×”マークのセルは”不可セル”と呼び，「状態がS1の時に事象E2は発生しない」ことを表す．また，事象名の先頭に”x”のある”xE1”は”能動的イベント”と呼び，「システムのあらゆる状態で発生し得る事象」を表し，”E2,E3”は”受動的イベント”と呼び，「セル中のアクションによって発生する事象」を表す．

2.3　Garakabu2の構成と機能

本ツールは図3で示す機能で構成されている．

モデル変換機能はZIPCの状態遷移表モデルから検査に必要なデータを抽出し，本ツール専用の有限デー

Design and development of state transition matrix model checking tool Garakabu2.
†T.Shiraishi, W.Kong, Y.Mizushima, N.Katahira
†Fukuoka Industry, Science & Technology Foundation
‡M.Matsumoto, M.Watanabe
‡CATS Co., Ltd.
§T.Katayama
§Department of Computer Science and Systems Engineering, Faculty of Engineering, Miyazaki University
¶A.Fukuda
¶Graduate School of Information Science and Electrical Engineering, Kyushu University

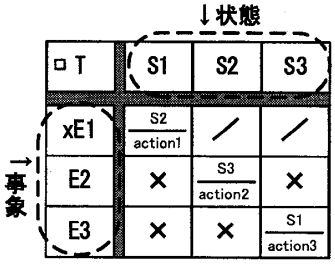

図 2: 状態遷移表の例

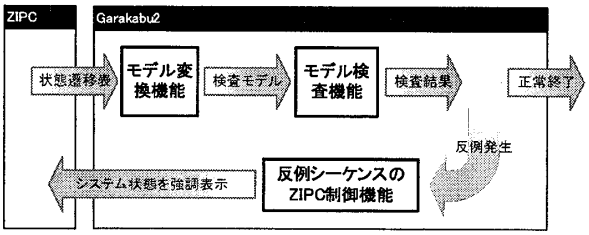

図 3: Garakabu2 の構成

タを対象とした検査モデルを生成する機能である．本機能を有することにより，ユーザはモデル検査用に新たなモデルを作成する必要がなく状態遷移表を直接検査することができるため，検査の効率化に効果がある．

モデル検査機能はモデル変換機能が生成したモデルを対象としてモデル検査する機能であり，explicit-state 検査アルゴリズムで実装している．

反例シーケンスの ZIPC 制御機能はモデル検査機能が反例を検出した際に，反例の各システム状態を状態遷移表のセルに対応させ，強調表示させる機能である．この機能により，初期システム状態から異常システム状態に至るまでの各ステップを状態遷移表上で確認することができるため，反例の解析コストを削減することができる．

2.4 検査可能な性質

本ツールで検査可能な性質は安全性であり，以下に具体的な内容を示す．

- システム状態変数制約チェック
- 不可セル到達チェック
- 変数型に対する最大・最小値超過チェック

システム状態変数制約チェックは，ユーザが設定したシステム状態を構成する変数の制約，またはそれらの組合せ (論理式) が常に" 真" であることを検査する．

不可セル到達チェックは，システム状態が状態遷移表の不可セルに到達しないことを検査する．

変数型に対する最大・最小値超過チェックは，システムで定義している全変数の値がそれぞれの変数型の値の範囲内であることを検査する．

システムが各性質に対して" 偽" となるシステム状態を発見した場合，本ツールは反例を出力する．

3 おわりに

本稿では我々が設計開発した Garakabu2 の構成や機能の説明，検査可能な性質に関して述べた．状態遷移系の設計は UML のステートチャート図や状態遷移図が知られているが，本ツールが検査対象としている状態遷移表は設計漏れのチェックができることが一番の特徴である．また本ツールは SPIN [4] のようにモデル検査するために新たにモデルを作成する必要が無く，商用ツールと連動することで反例解析コストを低減することができる．「操作が極めて単純で導入コストが極小」と本ツールを評価するユーザもおり，実際の開発現場においてソフトウェアの品質向上に有用であると考えている．

本ツールのパフォーマンスに関しては，他ツールとの比較を含めて今後の課題である．またモデル検査を実施する際，一般的に困難な作業の一つである性質 (本ツールではシステム状態変数制約チェック) の設定は，ユーザが設定する必要があり，性質の設定を支援する機能等ユーザビリティの向上も今後の課題である．

参考文献

[1] Garakabu2，http://garakabu2.lab-ist.jp

[2] ZIPC，http://www.zipc.com/product/zipc

[3] Edmund M.Clarke,jr.，Orna Grumberg，and Doron A.Peled，“Model Checking”，The MIT Press，1999.

[4] Gerard J.Holzmann，“The SPIN Model Checker - Primer and Reference Manual”，Addison-Wesley，2008.

[5] 渡辺政彦，“拡張階層化状態遷移表設計手法 ver.2.0”，東銀座出版社，2006 年.

[6] 松本充広，穴田啓樹，上島大輔，渡辺政彦，福田晃，“状態遷移表のモデル検査”，第二回システム検証の科学技術シンポジウム，産総研テクニカルレポート PS-2005-017，pp.2-11，2005 年.

[7] 穴田啓樹，松本充広，“モデル検査ツール「Garakabu」を開発”，日経 BP 社“モデルに基づく開発方法論のすべて”，pp.161-169，2006 年.