情報制御システムのモデル検査における状態爆発対策と課題

小 山 恭 平[†1]　小 飼　　敬[†2]　上 田 賀 一[†1]

モデル検査において，システムを抽象化せずにモデル化すると，多くの場合，状態爆発が生じる．本研究では，情報制御システムを対象としたモデル検査の状態爆発を防ぐため，cone of influence reduction を参考に，システムの状態空間から検査項目と関係する範囲のみを探索する手法を検討している．

Counterplan for state-explosion in model checking for Information Control System

Kyohei Oyama ,[†1] Kei Kogai [†2] and Yoshikazu Ueda[†1]

In order to prevent the state explosion of model checking in information control systems, By referencing cone of influence reduction, we has investigated a method of searching only the range associated with the check items in the state space of the system.

1. はじめに

モデル検査とはモデルを用いたシステムの振舞いシミュレーションによって，システムの状態空間を網羅的に調べる方法である．このとき，システムを抽象化せずに，モデルを作成すると状態爆発が発生する可能性が高い．そのため，状態爆発はモデル検査において解決すべき問題のひとつである．我々は現在，インフラ系の制御システムである情報制御システムに対してモデル検査を適用するため，状態爆発を防ぐ手法を検討している[3)]．

2. 情報制御システム

情報制御システムとはインフラ系の制御システムである．例として，列車の走行ルート制御や電気の送電経路制御に用いられている．情報制御システムはセンサから制御対象の情報を取得し，ルールベースの判断ロジックを基に制御内容を決定する．このとき，センサからの情報は実測値ではなく，抽象化された離散値として入力される．例えば，温度センタの場合，5 °C や 30 °C という具体的な値ではなく,「寒い」,「暑い」等の抽象的な値が入力値となる．

†1 茨城大学
Ibaraki University
†2 茨城工業高等専門学校
Ibaraki National College of Technology

図 1　本手法による探索

3. 手　　法

3.1 モデル検査の問題点

モデル検査において，モデルの状態は全属性の値の組み合わせから構成される．このため，属性数が増えると状態は爆発的に増加する．

状態数が爆発的に増加することを状態爆発[2)]と呼ぶ．状態爆発が発生すると実用時間での検査が不可能になったり，検査中に状態をメモリに記録できなくなる．

3.2 検討中の手法

状態爆発を防止するため，cone of influence reduction[4)] を参考にした検査手法を検討している．我々の手法では状態数が属性数に比例する点と検査項目と関係のある属性は一部である点に着目する．つまり，システムの状態空間のうち検査項目に関係のある部分だけを探索することによって，状態爆発を防ぐ (図 1 左)．

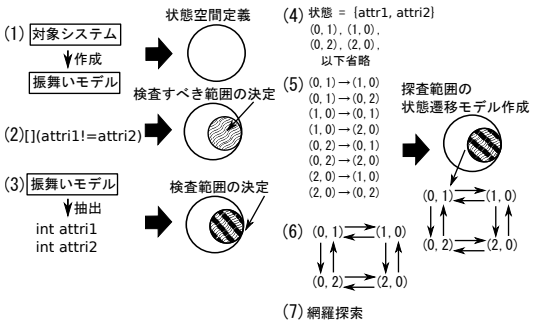

図 **2**　手法の具体例と状態空間

本手法を用いたモデル検査の流れを次に示す．

(1)　システムの振舞いモデルを作成する
(2)　検査項目を決める
(3)　検査項目に関係のある属性を抽出する
(4)　属性の全組み合わせ (検査状態) を生成する
(5)　振舞いモデルを用いて，検査状態間の遷移関係 (遷移履歴) を取得する
(6)　遷移履歴から状態遷移モデルを作成する
(7)　状態遷移モデルを網羅探索する

この流れと状態空間との関係を表したものを図 2 に示す．図 2 に示すように，まず (1) で，検査対象であるシステムの状態空間を決定する．次に (2) で検査項目を用いて，状態空間のうち探索すべき範囲を決定する．探索すべき範囲決定後，(3) で振舞いモデルの属性を抽出することで実際に探索する範囲を決定する．そして，(4)〜(6) で探索範囲の状態遷移モデルを作成する．最後に (7) で検査項目を満たしているか調べる．

3.3　課　　題

解決すべき課題として属性抽出の難しさがある．このため以下の 2 つの問題が存在する．

(1)　属性数の削減数がモデルに対する理解度に依存
(2)　属性抽出の正確さが検査結果の信頼性に影響

問題 (1) に関して，状態数は属性数に比例する関係にある．そのため，状態数を少なくするには抽出する属性を最低限にしなくてはならない．このとき，振舞いモデルに対する理解度によって属性抽出に大きな差が出る可能性が高い．理解度が高い場合，属性間の依存関係や検査項目との関係を把握しているため，必要最低限の属性を抽出することが容易である．それに対して理解度が低い場合，検査に必要かどうかの判断が困難になるため，必要以上の属性を抽出する可能性がある．この場合，状態爆発が発生する可能性が高い．

問題 (2) に関して，本手法で探索する状態空間の範囲は属性抽出の段階で決定される．そのため，抽出する属性に抜けが存在すると，探索範囲が狭くなり，振舞いモデルの不具合を発見できない可能性がある (図 1 右)．

3.4　解決アプローチ

問題 (1) に関して，松原ら[1] の手法を参考に LTL 式を用いたアプローチに着手している．彼ら[1] は変数依存グラフを用いて，振舞いモデルの抽象度を選択する手法を確立した．この手法を参考に，我々はまず検査項目を LTL 式で定式化する．このとき式中に存在する属性を抽出する．次に，振舞いモデルの変数依存グラフを用いて，式中の属性と他の属性の依存関係を可視化する．検査者はこのグラフを見て，追加で抽出する属性を選択する．これにより，検査者はモデル理解度に依存せずに，検査項目と関係のある属性を取得することができる．

4. ま　と　め

我々は現在，情報制御システムにモデル検査を適用するため，cone of influence reduction[4] を参考にした手法を検討している．検討中の手法ではシステムの状態空間のうち，検査項目と関係のある範囲だけを探索することで状態爆発を防止する．

本手法の課題として属性抽出の難しさがある．このため以下の 2 つの問題が存在する．

- 状態の削減量がモデル理解度に依存する
- 属性の抽出精度が探索の信頼性に影響する

このうち，問題 1 を解決する方法として，LTL 式とプログラム依存グラフを用いた関連属性の可視化によって，属性抽出を容易にする方法がある．

問題 2 に関しては今後，解決手法を検討していく．

謝辞　本研究を進めるにあたり，適切な助言をくださいました株式会社日立製作所　武澤隆之氏，山形知行氏に感謝致します．本研究は JSPS 科研費 25330075 の助成を受けたものである．

参　考　文　献

1) 松原正裕ら：ハードウェア異常に対応した組み込み制御ソフトウェア不具合のモデル検査手法，情報処理学会研究報告．2012-EMB-24(11)．pp.1-5(2012)．
2) 吉岡信和ら: SPIN による設計モデル検査, 近代科学社 (2008)．
3) 小山恭平ら：状態制御システムのモデル検査における状態空間分割による探索手法の提案，ソフトウェア工学の基礎 XIX，pp.39-44，近代科学社 (2012)．
4) Edmund M.Clarke Jr ら：Model Checking, The MIT Press(1999)．