# NuSMVの反例解析支援ツールの試作

大池 勇太郎[1,a)]　小形 真平[1,b)]　青木 善貴[2,c)]　中川 博之[3,d)]　岡野 浩三[1,e)]

**概要：**
モデル検査において，複雑・大規模なシステムのモデルの反例を手動で解析することは，非常に時間がかかる．NuSMV では反例情報として，状態遷移により変化した変数の値が各状態ごとに出力されるだけであるため，変数の多い大規模なモデルでは開発者による解析が困難になりやすい．本稿では NuSMV から得られた反例解析の効率を向上させるため，反例を自動で変数ごとの遷移を確認できるように, 表形式に整理し保存する．また，反例をグラフとして可視化するためのツールを試作し，セマフォのモデルに対して実行し，誤りのある箇所を絞り込むことに有効な見込みを得られた．

**キーワード：**モデル検査，NuSMV，可視化，解析，反例

# A Prototype Tool to Aid Analysis of Counterexamples Produced by NuSMV

## 1. はじめに

信頼性の高いソフトウェア開発支援をする有望な技術にモデル検査 [1] があり，具体的なツールとして NuSMV[2] がある．しかし，複雑・大規模なシステムのモデルを検査する場合，NuSMV から出力された反例を手動で解析することは非常に時間がかかる [3]．そのようなシステムのモデルは変数が多く存在し，その中で必要な変数だけを確認したい場合もある．しかし，図 1 に示すように NuSMV では反例情報として，状態遷移により変化した変数の値が各状態ごとに出力されるだけであるため，変数の多い大規模なモデルでは開発者による解析が困難になりやすい．複雑な反例から大規模なモデルの誤りを効率的に発見するためには，開発者が解析しやすいように，反例から必要な情報を簡便に得られる支援が必要となる．

[1] 信州大学
Shinshu University
[2] 日本ユニシス株式会社
Nihon Unisys, Ltd.
[3] 大阪大学
Osaka University
[a)] 15t5017b@shinshu-u.ne.jp
[b)] ogata@cs.shinshu-u.ne.jp
[c)] yoshitaka.aoki@unisys.co.jp
[d)] nakagawa@ist.osaka-u.ac.jp
[e)] okano@cs.shinshu-u.ne.jp

```
-> State: 1.1 <-
  semaphore = FALSE
  p1.state = idle
  p2.state = idle
-> Input: 1.2 <-
  _process_selector_ = p1
  running = FALSE
  p2.running = FALSE
  p1.running = TRUE
-- Loop starts here
-> State: 1.2 <-
  p1.state = entering
-> Input: 1.3 <-
```

**図 1**　NuSMV の反例出力

そこで本研究では反例の整理と可視化を行い，モデルの誤りを効率的に発見できる反例解析支援ツールの実現を目指す．本稿では，変数ごとの変化を確認しやすいように反例を表形式に整理し，また，誤りを発見しやすいように反例をグラフで可視化するために試作した支援ツールについて述べる．評価では試作ツールをセマフォのモデルに適用して，モデルの誤りのある箇所を絞り込むことに有効な見込みが得られた．

## 2. 例題

支援ツールを実行するモデルとして，セマフォのモデルを用いる．複数のプロセスがあり，ツールの試作段階で結果の分析が容易なモデルを例題として選んだ．2 つのプロセスが平行に動作しており，各プロセスにはクリティカル領域があるとする．両方のプロセスが同時にクリティカル領域に入れないようシステムを実現する排他制御の一つが

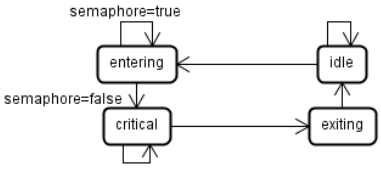



図 2　セマフォの状態遷移

セマフォである．モデルの各プロセスの状態遷移系を図 2 に示す．本例題ではこのプロセスを p1，p2 として 2 つ使用する．片方のプロセスがクリティカル領域に入ろうとしたときに，もう片方が使用していなければ入れる [4]．検査式は $\mathbb{AG}(p1.state = entering \rightarrow \mathbb{AF}p1.state = critical)$ を用いる．この式は，1 つのプロセスがリクエストを出したら必ずクリティカル領域に入ることを意味している [5]．

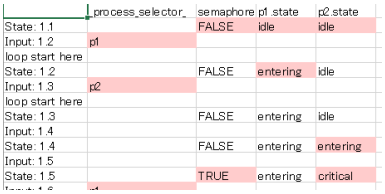
## 3.　支援ツールの試作

本研究では支援ツールを Python で試作した．本ツールには検査したいモデルに検査式を記述した smv コードのファイル名を入力し，図 3 に示すような表形式による反例の整理と，図 4 に示すようなグラフによる反例の可視化を行う．表形式では，行を状態，列を変数として注目することで，変数ごとの変化が確認できる．

グラフによる反例の可視化では，検査式を途中まで満たす反例が出た際に，どこで検査式を満たさなくなるのかを発見できるよう，可視化を行う．本ツールではグラフで反例を可視化する際に，それぞれの変数の値などの多量な情報を一度に表示してしまうと確認が困難になるため，GUI アプリケーションで必要に応じた情報を出力するように作成した．グラフには検査式内の変数の条件を示す式がそれぞれの状態で満たしているか否かを出力する．具体的には，本稿の例題モデルの検査式では $p1.state = entering$ と $p1.state = critical$ がそれぞれの状態で満たしているのかを色分けして出力する．横軸は状態変数を表す．具体的には横軸の 0-1 の部分が図 1 に示す NuSMV からの出力の “State 1. 1” に相当する．縦軸は検査式内に登場する式を自動で分解し，出力する．各状態で，縦軸の式を満たすならば淡緑，満たさなければ淡赤で棒グラフを出力する．また，ループの開始点は赤線，変数の値の変化点は白線で区別した．棒グラフを選択すると参照している変数に対して，選択した変数の値と状態変数を追加で右上に表示する．

## 4.　結果

図 3 に excel，図 4 に GUI の出力を示す．excel の出力は NuSMV の出力を表形式に整理できた．GUI の出力は $p1.state = entering$ を満たした後に $p1.state = critical$ を満たさないことが分かるため，$p1.state = critical$ を満たさない原因を調べればよいと見当がつく．また，見当をつけた箇所を選択することで変数の値を調べることができた．



| | process_selector_ | semaphore | p1.state | p2.state |
|---|---|---|---|---|
| State: 1.1 | | FALSE | idle | idle |
| Input: 1.2 | p1 | | | |
| loop start here | | | | |
| State: 1.2 | | FALSE | entering | idle |
| Input: 1.3 | p2 | | | |
| loop start here | | | | |
| State: 1.3 | | FALSE | entering | idle |
| Input: 1.4 | | | | |
| State: 1.4 | | FALSE | entering | entering |
| Input: 1.5 | | | | |
| State: 1.5 | | TRUE | entering | critical |

図 3　excel の出力

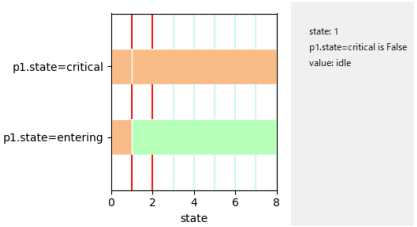



図 4　GUI の出力

## 5.　考察

表形式の出力に関しては，必要な変数だけを確認したい場合に，NuSMV の出力形式に比べて効果的であるといえる．また，GUI による可視化は NuSMV からの出力より直感的にモデルの誤りのある箇所を絞り込めたといえるであろう．この可視化は検査式を途中まで満たす反例の誤りのある箇所を絞ることを目的として作成したため，検査式内の変数の条件を表す式が複数かつそれが階層的になっている検査式にしか有効でないだろう．そのため，多くの検査式に適用できるよう，出力する内容を再考する必要がある．

## 6.　まとめ

本稿では，反例の解析支援ツールを作成した．その結果，NuSMV からの出力を直接確認するより効率的に反例解析を行えるという見込みが得られた．今後の課題としては，GUI で何を出力したら反例をより効率よく解析できるのかを調査し，検査式に出てくる式だけでなく，より重要性の高いものを出力できるようにする必要がある．

### 参考文献

[1] E. Clarke, O. Grumberg, and D. Peled: *Model Cheking,* MIT Press (2000).
[2] A. Cimatti, E. Clarke, E. Giunchiglia, F. Giunchiglita, and M. Roveri: *NuSMV: A New Symbolic Model Verifier,* Proc. of CAV’99, LNCS 1633, pp.495–499, Springer Verlag (1999).
[3] 佐藤　友昭，岡本 圭史: *RBAC* モデルの検証における反例解析手法の提案，平成 26 年度電気関係学会東北支部連合大会 (2014).
[4] 産業技術総合研究所システム検証研究センター: モデル検査　初級編 —基礎から実践まで 4 日で学べる—，ナノオプト・メディア (2009).
[5] 産業技術総合研究所システム検証研究センター: モデル検査　上級編 —実践のための三つの技法—，ナノオプト・メディア (2009).