

モデル検査ツールについて



1. いろいろなモデル検査ツール

代表的なモデル検査ツールを3つご紹介します。

□SMV系（NuSMV, CadenceSMVなど）**お勧めです。**

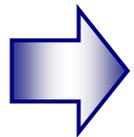
- データ構造としてBDD(Binary Decision Diagram)を採用しています。
大きな状態のモデルを検査することができます。
専用言語の構文がとても簡単で**処理が高速**です。

□SPIN

- モデルを記述する専用言語としてPromelaを採用しています。
PromelaはC言語に似ているため取っ付きやすいです。

□UPPAAL

- 画面上で状態遷移図の記述ができます。GUIがあります。
状態遷移図からモデルを自動生成する機能があります。



フォーマルテックでは**NuSMV**を使用しています。

- **大きな状態（大規模システム）**を**高速**で検査するためです。

2. モデル検査ツールSMVについて

4つの種類のSMVが公開されています。

名称	開発元	特徴	GUI	商用利用
CMU-SMV	米カーネギーメロン大学	下記3つのSMVの大元	無	×
CadenceSMV	ケーデンス社	汎用向けチューニング済	有	×
NuSMV	NuSMV開発チーム	LGPLライセンス	無	○
nuXmv	同上	NuSMVにGUIを付加	有	×

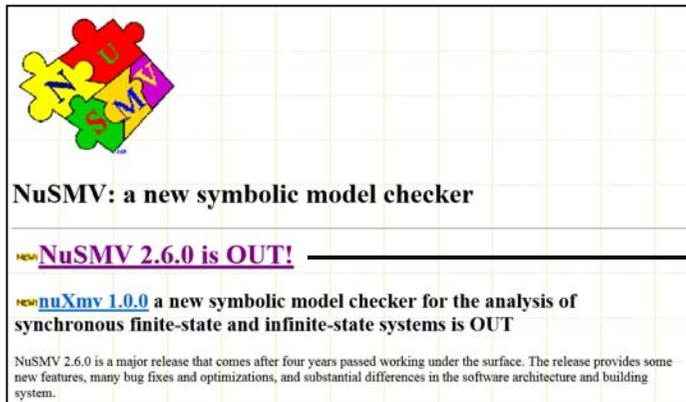
商用利用：企業等の営利団体での利用

例) 自社や他社のシステムにモデル検査を適用する等

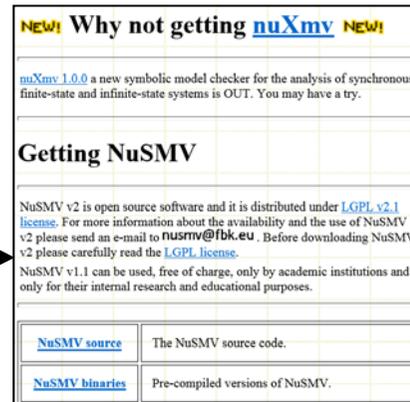
商用利用可能なSMVは「NuSMV」だけなので注意が必要です。

3. NuSMVの入手方法

NuSMVは以下のサイトでダウンロードできます。無料です。
<http://nusmv.fbk.eu/>



NuSMV 2.6.0 is OUT! をクリック



NuSMV binaries をクリック

必要事項を入力

NuSMV-2.6.0-win64.zip (Windows 64bit版) を入手できます。

4. NuSMVについて

NuSMVは研究用（プロユース）を目的に開発されているので、使いこなすのに、ノウハウが必要です。

（様々なオプションがあります）

うまく使いこなすと？

■ 大規模なシステムを

数億～数兆の状態を持つシステムを検査した実績があります

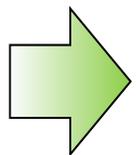
■ 限られたメモリで

オプションによって、メモリ使用量を数分の1に削減できる場合があります

■ 非常に高速に

オプションによって、検査時間を数分の1～数百分の1に削減できる場合があります

モデル検査することができます。



弊社のモデル検査の技術者育成（導入コンサルティング）サービスではNuSMVを使いこなすノウハウをご提供します

5. ご参考 (BDDについて)

SMVはシンボリックモデル検査のアルゴリズムが実装されています。

BDD (Binary Decision Diagram : 二分決定グラフ) をデータ構造として、
論理学の集合理論等を用いて記号的にモデル検査を行うアルゴリズムです
単純な総当り検査より非常に効率的です

BDDによるのメモリ効率化の例 $f() = a \ \& \ b \ \& \ c \ \& \ d \ \& \ e$

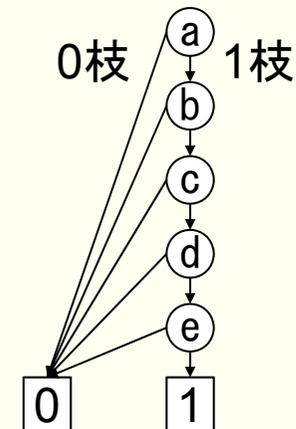
[真偽値表]

f	a	b	c	d	e
0	0	0	0	0	0
0	1	0	0	0	0
.
.
.
1	1	1	1	1	1

32行 (160セル)

5ノード

[BDD]



論理式 $f()$ をメモリ上に展開する場合 → 真偽値表では160個のセルが必要です
→ BDDでは5個のノードで表現できます