第4章　モデル検査ツールの利用

マルチコア環境における タスク設計検証

藤倉 俊幸

マルチタスクOSで動作するタスクは，割り込みなどの外的要因によってタスクの実行順序が変化し，それがバグの要因となることがある．タスクの実行順序を把握するためには，実行順序を全て洗い出し，ステート・マシンとして記述するという方法がある．従来は手動でこの作業を行っていたが，モデル検査ツールLTSAを使用することにより，ステート・マシンを自動出力できる．本稿では，形式検証を使ったマルチプロセッサ環境で動作するタスクの検証について解説する．（編集部）

モデル検査ツールを使用したタスク設計の検証については，CQ出版社から刊行されているTECH I vol. 34「組み込みソフトウェアの設計&検証」の 第22章以降で説明したことがあります．本稿は，その記事の内容を簡単におさらいし，マルチプロセッサ環境やマルチコア環境にどのように適用するのかなどを，モデル検査にあまりなじみのない人でも分かるように説明したいと思います．

1．モデル検査とは

● 数学的な手法をソフトウェア開発に取り入れる

形式手法（Formal Method）と呼ばれる手法があります．この形式手法は，「数学を積極的に使ってソフトウェアを開発していこう！」という心意気に対して付けられた名前です．手法と言うよりはアプローチあるいは手法群と言った方が良いかもしれません．歴史は古く，コンピュータが使われ始めた頃から研究されていました．研究はされていましたが，「難しすぎる」，「実際に使うにはコストが掛かりすぎる」などの理由から，ずっと日の目を見ない存在でした．しかし，この形式手法と呼ばれる一群の手法の中に，「モデル検査」と呼ばれる分野があり，最近になって開発現場で利用され始めています．

モデル検査では，検査対象になる要求仕様や設計仕様，実際のコードなどから動きや操作に関する情報を抽出してモデルを作ります．このモデルは，全ての可能な動きのパターンを生成します．全ての可能な動きのパターンが生成できたら，次に，一つ一つの動きを検査します．例えば，イベントの順番や特定のイベントが発生しているかなどです．

モデルと検査でモデル検査になるわけですが，要求や設計を対象とする場合には，要求分析を行う人や設計を行う人が全ての可能な動きを把握できることには重要な意味があります．つまり，検査なしでも有効な使い道があります．考えていることの全体を把握できることが重要なのです．そこで，ここでは検査にはあまり立ち入らずに，まず「モデルとはどんなものか」，「全ての可能な動きとは何か」について詳しく説明します．

● LTSAを使ってボールを取り出す問題を解く

非常に簡単なサンプルで考えてみましょう．高校などで習う順列組み合わせ問題です．

> つぼの中にAというボールが3個とBというボールが2個入っているとする．ここから3個のボールを取り出すときの取り方は何通りあるのか？

これは，順列組み合わせ問題の公式に当てはめれば，7通りであることが分かります．しかし，具体的にどのような取り出し方が可能なのかは，公式を見ても分かりません．これをモデル検査ツールであるLTSAを使って解くと，具体的な7通りの動作パターンを作り出すことができます．

図1に，実際にLTSAのモデルと生成した動作パターンを示します．動作パターンは，実際はつぼからAかBを取り出す取り出し順で示すべきですが，ここではその取り出し順を生成するステート・マシンで示します．モデルと言っているのは，通常このステート・マシンのことです．A=…，B=…と書いてあるのはLTSAに入力するソース・

KEYWORD ―形式手法，モデル検査，RTOS，タスク設計，タスクの動作モデル，LTSA，ステート・マシン

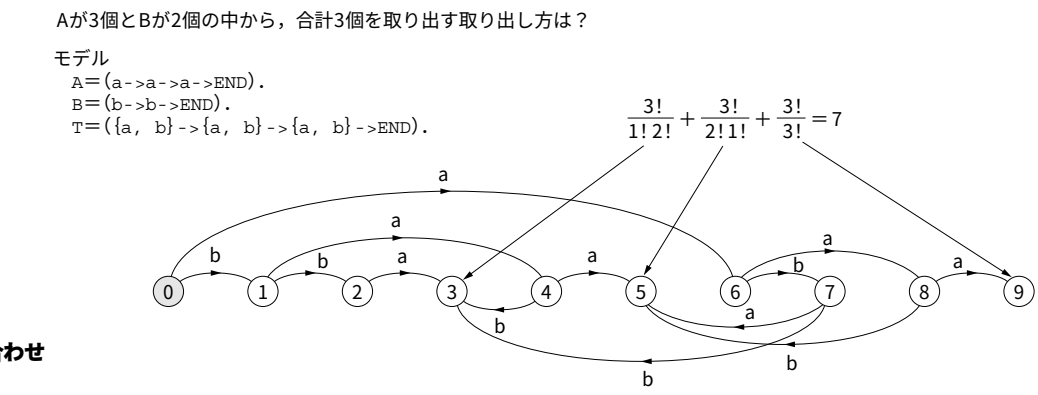
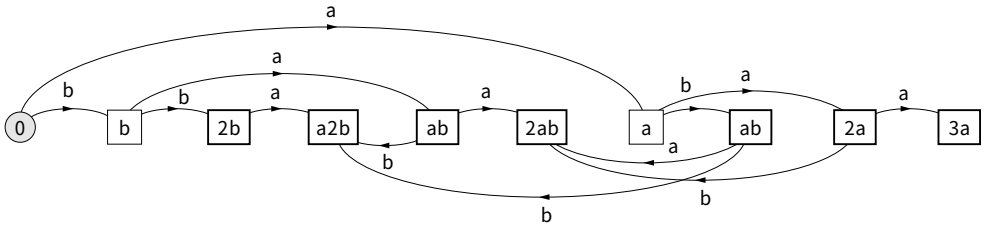


図1
モデル検査ツールで組み合わせ問題を解く



各状態は組み合わせに対応している
1個取る　組み合わせは2通り　a, b
2個取る　組み合わせは4通り　2b, ab, ba, 2a
3個取る　組み合わせは3通り　a2b, 2ab, 3a

その状態に到達する経路の数が取り出し方の数
a2b　b→b→a, b→a→b, a→b→b
2ab　b→a→a, a→b→a, b→a→a
3a　a→a→a

図2
状態分析

コードに当たりますが，これをモデルと呼ぶこともあります．それぞれ一つのモデルのテキスト表現とグラフィックス表現だと思えば良いでしょう．

モデルの，

```
A = (a->a->a->END).
```

の意味は，「3個あるAを一つ取り出す動作をaで表して，それを3回行ったら終了する」，つまりなくなるという意味です．

```
B = (b->b->END).
```

も同じような意味です．これで，AとBだけをモデルにすると，合計5個あるボールを5個とも取り出す取り出し方を生成するモデルになります．ここでは，合計3個取り出す取り出し方が問われているので

```
T = ({a,b}->{a,b}->{a,b}->END).
```

を制約としてモデルに追加します．{a,b}は「aかbを実行する」という意味です．従って，Tはaかbを実行することを3回行うという意味になります．bは3回繰り返すことはできないのですが，その条件はBに記述してあるので，Tはこのままで良いのです．このようにして作ったA，B，Tはプロセス式と呼ばれています．これらを合成して一つにすることで，**図1**に示すようなステート・マシンが生成されます．このステート・マシンを分析することで，いろいろなことが分かってきます．

LTSAが生成するステート・マシンの各状態は組み合わせに対応し，初期状態から各状態に到達する経路が具体的な取り出し動作列に対応します．**図2**に書き込んだコメントのような，状態や経路の意味を日本語だけで記述するのは効率が悪く，正しく伝わるかどうか，そもそもまじめに読んでもらえるのかどうか怪しいものです．モデル化してあれば，グラフィカルに表現できるだけでなく，シミュレーションすることなども可能になります．こちらの方が成果物としても優れています．

ステート・マシンから生成される動作列が「動作パターン」となります．モデル検査ツールを使用すると，いろいろなことが網羅的に分かるということが重要です．この性質は，タスク設計だけでなくテスト・ケースの生成などにも応用できます．

つぼからボールを取り出す方法ではタスク設計との関連

News Flash――日立，人の動きや脈拍などのデータを24時間測定する腕時計型センサ・ネット端末を試作
日立製作所は，人の動きや脈拍などのデータを24時間測定する腕時計型センサ・ネット端末を試作した．3軸加速度センサや脈波形センサ，温度センサ，マイコン，無線モジュール，電池などを内蔵する．毎秒20回の頻度で，10日間連続して測定できる．