リアルタイム・システム開発者に必須の時間制約検証作業に使える

モデル検査ツールで時間仕様を検証する

藤倉 俊幸

組み込みシステムでは制限時間内に処理を終了させるリアルタイム処理が要求される．完成したシステムが時間制約を満たせるかどうか，実際にシステムを作り上げてからでないと分からないという場合が多いため，経験や勘でクロック周波数を決めるといった丼勘定も多い．そこで設計段階で時間仕様を満たしていること検証するのがモデル検査ツールだ．本稿ではUPPAALとNuSMVを使い，時間仕様を検証する．（編集部）

応答時間やスループットなどに関わる時間仕様の検証に使える技術として時間オートマタがある．ツールとしてはUPPAAL[1]が有名である．組み込みシステムでは時間を含んだ仕様の検証は重要でUPPAALを使用すればそれが可能になる．しかし，UPPAALのアカデミック版[3]はフリーであるが商用ライセンスは有償である[2]．そこで，フリーのモデル検査機であるNuSMVを使用してUPPAALと同じことができるかどうか調べてみた．同じことができるのであればNuSMVを使ってみて効果があればUPPAALを検討するということも可能だろう．ここで説明する内容を自分で試してみるには，学生でない場合は参考文献(1)からダウンロードすると2週間程度の評価期間が与えられ，その間に評価・検討を行う必要がある（**図1**）．

1. UPPAALとは

● 時間仕様を扱えるモデル検査ツール

ウパールと呼ぶこのツールは，時間仕様を扱えるモデル検査ツールである．つまり，SPINやNuSMV，LTSAのようにモデルを作って，検査式で検査する使い方をする．モデルの全ての状態を網羅的に検査するので結果に対する信頼性が高いのが特徴である．スウェーデンUppsala（ウプサラ）大とデンマークAalborg（オルボー）大が共同で開発したのでUPPAALと呼ぶ．UPPAALのモデルはプロセスを単位として構築する．モデル要素になるプロセスを時間オートマタで記述するので時間仕様を扱える．

時間オートマトンは，クロック変数x，yを使って時間制約を「$x<3$」とか「$x-y<10$」などの式で表してステート・マシンの振る舞いに制約を加えたものである．制約としては，各状態の滞在時間，各遷移のガード条件がある．また，勝手にインクリメントしていくクロック変数のリセットを行うことができる．UPPAALで使用できるロケーションに対する時間制約表現は**図2**のようになっている．クロック変数に対して「$x+y$」とか「$2*x$」，「$x>3$」などは使えない．NuSMVであれば使用できる．

UPPAALはほかのモデル検査ツールと同じようにシステムの振る舞いを複数の並列に動くプロセスによって表現する．UPPAALでは各プロセスをGUIによって定義でき

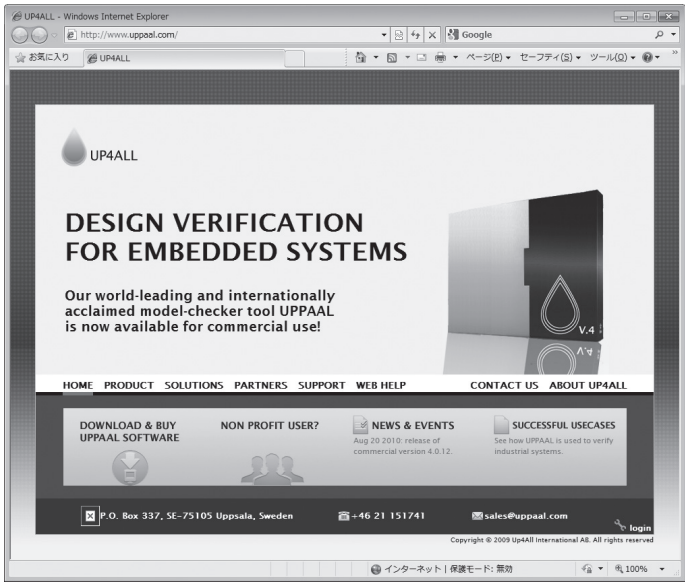

図1　UPPAALポータル（http://www.uppaal.com/）

x, yをクロック変数として，時間制約Γは以下の形式を使用できる

$$\Gamma ::= x \prec c \mid x-y \prec c \mid \neg\Gamma \mid (\Gamma \wedge \Gamma)$$

Where　$c \in N, \prec \in \{<, \leq\}$

cは整数
大小関係$\prec$は$<$か$\leq$のどちらか

図2　UPPAALにおけるロケーション時間制約表現

KEYWORD——形式手法，UPPAAL，NuSMV，時間仕様，検証