トップエスイー修了制作

確率CSPモデル検査支援ツール

株式会社クレスコ　　大新 智行　　t-oojin@cresco.co.jp

開発における問題点

確率CSPに基づくモデル検査器PATは，個々に指定したイベント遷移確率から，モデル全体に関する確率を自動的に算出できるため，作成したモデルの妥当性・正当性を評価するのに有用である．しかし，ソフトウェア開発者の多くはモデル検査に馴染みが薄く，また馴染みがあっても確率CSP モデル作成には工数が掛かる．

手法・ツールの適用による解決

ソフトウェア開発者が通常の設計で使用する状態遷移図を使用し，確率CSPモデルへ自動変換するプロセスを提案し，その変換プロセスの一部を自動化した．これによりソフトウェア開発者は確率CSPモデルを自動作成可能であり，モデル検査器PATを使用することにより作成したモデルの妥当性・正当性を評価可能となる．

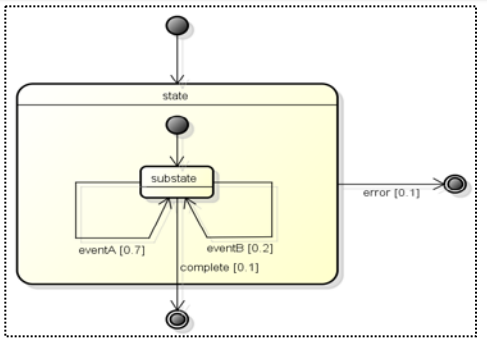
状態遷移図 → 確率CSPモデル 変換プロセスの提案

遷移確率付与

Step4

Feedback

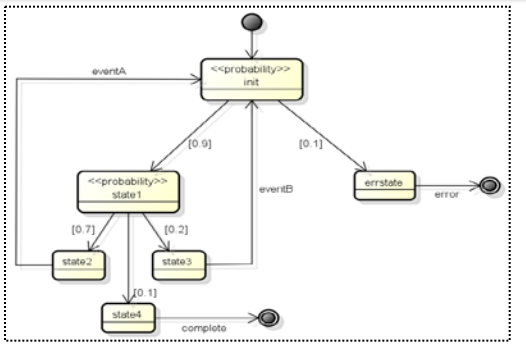
確率付状態遷移図
(Composite Stateを含む)



Step1

自動変換

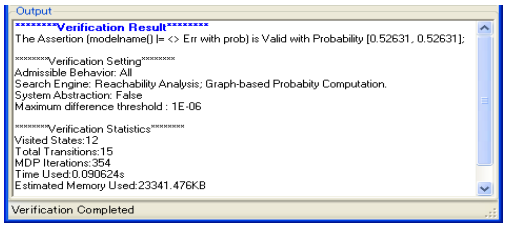
確率付状態遷移図
(Composite Stateを含まない)



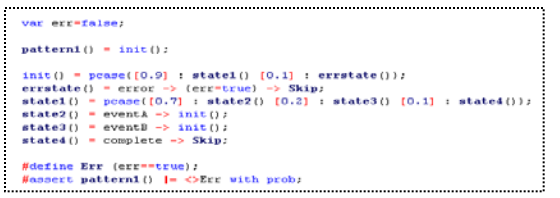
自動変換 Step2

Step3

PAT



確率算出結果

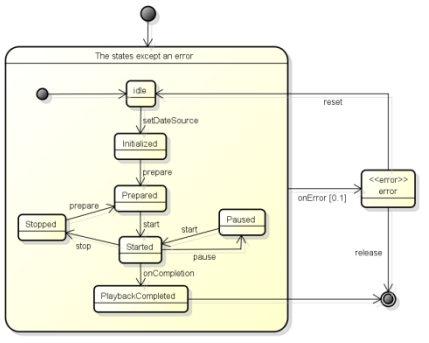


確率CSPモデル

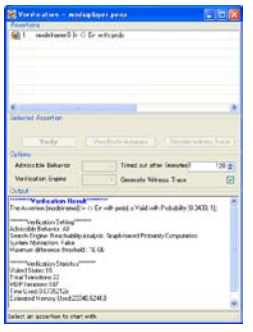
ソフトウェア開発者は設計で作成する状態遷移図に遷移確率を付与するだけでモデルに関わる確率を容易に算出でき，設計モデルへフィードバックすることが可能である．修了制作では，Step1とStep2の変換ルールの策定とStep2の自動変換ツールの試作を行った（Step1の自動変換ツールは未実装）．

適用事例

各状態でエラーが発生する確率からモデル全体でエラーが発生し終了状態になる確率を提案した変換プロセスにより算出した．



Android MediaPlayer（簡略版）



今後の課題

- 策定したStep1の変換ルールに従った自動変換ツールの作成
- 提案した変換プロセスへの時間の概念の導入(モデル検査器PATは時間と確率を同時に扱えるため、単位時間当たりのエラー発生確率等が算出できる)
- 並行システムへの変換プロセス適用