トップエスイー修了制作

モデル検査の業務適用について

富士通株式会社　田嶋裕司　tajima.yuji@jp.fujitsu.com

開発における問題点

モデル検査技術を業務に適用できるか？

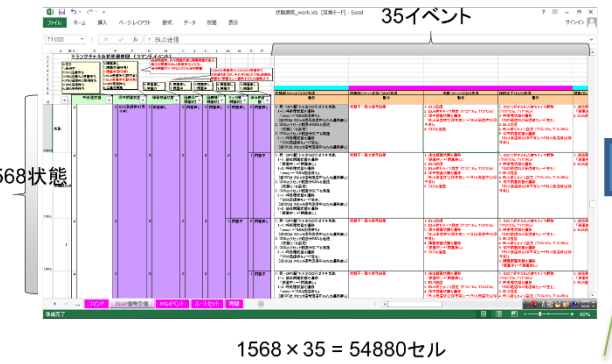
社内でモデル検査活用に向けて推進は行っているが、小さな規模のモデルに対しては、実績はあるものの、大規模なモデルに対しては、状態爆発発生や、うまく抽象化が出来ない等、なかなか成果が出ていない。

手法・ツールの適用による解決

実際の業務に使用している交換機ソフトウェアの回線管理状態（1568状態×35イベント）を対象にしてモデル検査を試行する。
ZIPC（状態遷移表作成ツール）での状態遷移表をPromela言語に変換するツール（社内開発）を使用して、SPINでモデル検査を行う方針とする。

適用方法

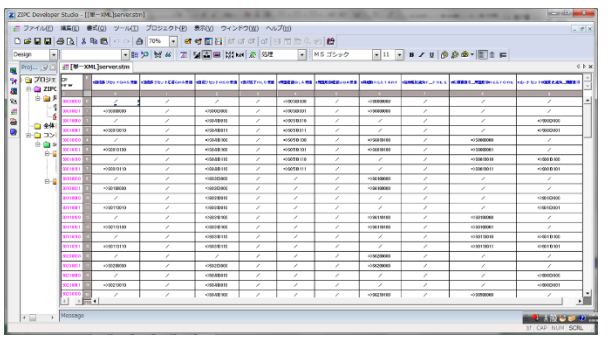
エクセルの状態遷移表



1568×35 = 54880セル

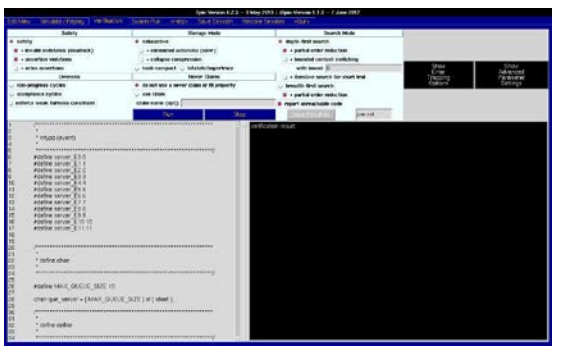
状態遷移表のアクションセル記載（自然言語）から、状態遷移に関連する部分を抜き出し、各セルに遷移先状態を7桁の表記で表現する。

ZIPCの状態遷移表



ZIPCでの状態遷移表記述から、Promela変換を行い、SPINでのモデル検査を実施する。

SPINでのモデル検査



モデル作成について

・STEP1
イベントとしては一部を対象として。状態については、全てを対象にしてZIPCを作成した。
1568×5=7840セル（状態遷移セル率=29%）
⇒ Promelaの変換ツールがメモリ不足により変換失敗

・STEP2
抽象化が必要なので、状態のうち、論理的に取り得ない状態を精査。回復系イベントを優先するよう精査を行った。
263×12=3156セル（状態遷移セル率=43%）
⇒ Promelaの変換ツールは成功したが、SPINでの検証において状態爆発

・STEP3
状態遷移の処理を再確認したところ、2つのイベントは状態を行き来するだけなので、精査対象にする事にした。それを行うことにより、ZIPCの静的ドキュメントチェックツールにて、遷移することのない状態についても削除を実施。
状態数112×イベント10=1120セル（状態遷移セル率=42%）
⇒ SPINでのデッドロックの検証が可能になった

モデル検査について

モデル検査として、イベント精査の関係上、回復系イベントが対象になっているので、各状態から回線の空きand閉塞無し状態に遷移できるかの到達可能性としての検証を行った。
⇒6個の反例が見つかったが、解析の結果、回復系イベントでは無いと判断して、イベント精査してしまったものが必要という事が分かった。⇒今回対象としたシステムはモデル検査を適用するには規模が大きすぎた。

まとめ

モデル検査適用にあたり、どの程度の規模の状態遷移表に対して、モデル検査が適用できるのかの一つの指針を得ることができた。

状態数	イベント数	セル数	状態遷移セル率	Promela変換ツール適用可否	SPIN適用可否
1568	5	7840	29%	否	ー
263	12	3156	43%	可	否
112	10	1120	42%	可	可

今後は、今回得られた指針を参考にして、社内のプロジェクトにおいて適用可否を判断して、モデル検査適用を進めて行きたい。