

平成 22 年度 情報工学コース卒業研究報告要旨

結縁 研究室	氏 名	伏 見 政 晃
卒業研究題目	大規模モデル検査を提供する Web サービスによる対話的ソフトウェア検証	
<p>ソフトウェアを作成した時、それが仕様を満たした正しい動作をするかどうかを検証する必要がある。システムがとりうる全ての状態において、その仕様を満たすかどうかを計算機で網羅的に検証する方法としてモデル検査が挙げられる。モデル検査ではシステムがとりうる全ての状態に対して検証を行うため、検証時に状態数が膨大になり、計算機のメモリの上限に達してしまうという状態爆発が発生する。</p> <p>この問題に対処するためにはシステムの抽象化を行う必要がある。しかし元のシステムの必要な性質を保ったまま抽象化を行うのは一般的に難しい作業である。これに対して、現在モデル検査ツール NuSMV による大規模モデル検査を提供する Web サービスが利用可能である。Web サービスによるモデル検査ではバッチ方式で検証が行われる。このため、途中で中断したり、システムの状態を確認することができないため、大規模なモデル検査を実行させた場合には、ターンアラウンド時間が大きくなる。記述したモデルの正しさが保証されていない場合、検証にかかる時間が増大する問題がある。</p> <p>本研究では、ソフトウェアモデル検査において、そのシステムの間状態を確認しながら検証を進める「対話的ソフトウェア検証」の手法を示す。Web サービスによる NuSMV モデル検査において対話的な検証を行う方法として、次の 2 つを提案する。1 つ目はシステムの間状態において反例が現れるような検査式を用いる方法、2 つ目はシステムとは独立のカウント変数を用意し、その値に応じて反例が現れるような検査式を用いるという方法である。</p> <p>Web サービスでのモデル検査における対話的検証の例として、MIPS のアセンブリ言語で記述されたバブルソートプログラムをモデル化し、検証を行った。その結果、より早い段階で現れる中間状態に対する反例を出した時は、それよりも後の中間状態に対する反例を出したときに比べ、検査に要した状態数が少なくなる傾向があった。このような結果から、Web サービスによってモデル検査を行っていく手法として、対話的検証が一つの方法であることを示せた。</p>		