形式的技法を用いた仕様検証

情報処理システムの新しい検証方法

情報処理技術がめざましい発展を遂げている一方で、情報処理システムの誤動作が社会に及ぼす影響は、「バグ」という言葉で広く知られている。バグはシステムの設計･製作段階で混入する。バグを発見するためには通常、仕様書の査読、製作完了後のテスト等が行われるが、多くのバグは査読ではなく、テストによって発見されている。従って従来からの方法では2つの大きな問題がある。それは経験や知識にないバグは発見しづらいことと、製作完了後に見つかるバグは膨大な改修作業を要するので開発コストを上げてしまうことである。我々はこの問題を解決するため、システム製作前の仕様書作成段階で、経験や知識に依存しない形式的技法を用いてシステム検証を行った。形式的技法は、状態遷移系として記述したシステムが論理式で表現された要求仕様(検査項目)を満たすか否かを数学的に証明するものである。形式的技法には2つの方法がある。論理的な推論を積み重ねて証明する定理証明法と、今回我々が行ったモデル検査法である。モデル検査では、モデルと呼ばれる有限個の状態を持つ仮想システムが、検査項目を満たすか否かを機械的･網羅的に検査する。これを計算機上で自動的に行うのがモデル検査ツールである。しらみつぶしに検査するため、検査項目を満たさない状態、すなわちバグが1つでも存在すると必ず発見できる。

企業で設計中の計算機組み込み系システムの仕様書を題材としてモデル検査を行った。モデル検査ツールはSMV(Symbolic Model Verifier)を用いた。まず、入手した査読済みの仕様書に従ってモデルを構築した。システムに要求される動作仕様を検査項目とし、計算木論理CTL(Computation Tree Logic)の論理式で表現し、作成したモデルと併せてSMVに入力し検査を行った。検査の結果、仕様書作成時及び査読時には発見できなかったバグを6件発見した。実システム製作前にバグを発見できたため、改修作業は仕様書の改訂だけで済み、開発工程でのコストを削減することができた。また通常のテストでは想定していなかった状況で発生するバグも発見できたので、モデル検査のメリットである“網羅的な検査”の有効性を確認でき、システムの品質向上に貢献できた。

我々は本事例を通して、実際の製品開発過程で形式的技法を用いることが有効であることを確認し、新しい仕様検証の手法確立に向けての一歩を踏み出せた。近い将来この手法を情報処理システムの標準的な検証手法として開発工程に組み込むことを考えている。

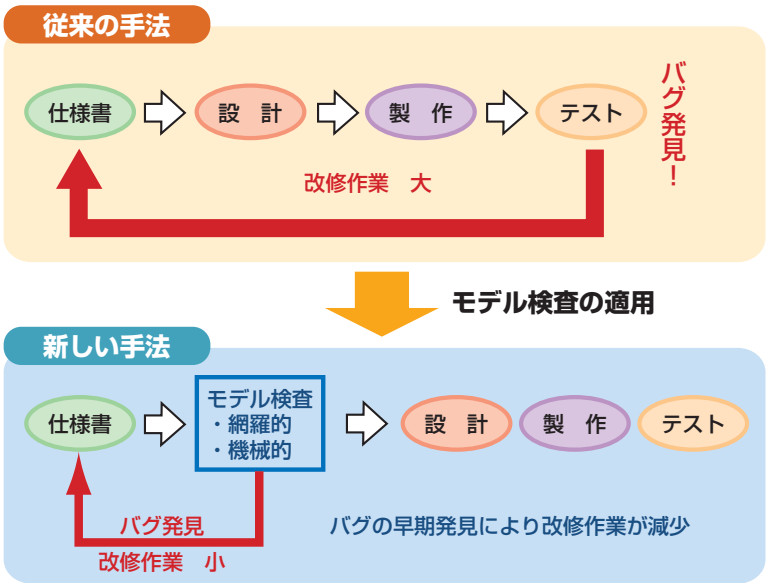

図 従来の手法と新しい手法の比較

はやみずこうじ
早水公二
kouji-hayamizu@aist.go.jp
システム検証研究ラボ

関連情報

- 共同研究者：高橋孝一, 渡邊宏, 水口大知（システム検証研究ラボ）.
- システム設計検証技術研究会　http://unit.aist.go.jp/informatics/consortium/
- 形式的技法　http://www.afm.sbu.ac.uk.