発表概要

多値モデル検査を利用したモデル化の誤りの発見

辰巳淳朗[†] 亀山幸義[††]

本研究は，モデル検査のためのモデル化の誤りを発見することを目標とし，そのための第 1 段階として，モデルに含まれる冗長性を発見する手法を提案する．標準的なモデル検査法では，検査対象のシステムと仕様をそれぞれ有限オートマトンと時相論理式で表現（モデル化）し，それらを入力として検査を行う．検査結果が偽である場合は反例が出力されるため，それに基づいて誤りの原因を特定することができる．一方，検証結果が真である場合，真であるという以外の情報は得られない．設計の初期段階ではモデル化に誤りを含むことが多く，モデル化の誤り等により，偶然，検査結果が真となる場合があることを考えると，この場合により多くの情報を引き出すことが必要かつ有益である．そこで本研究では，モデル化における誤りや設計上のヒントを得るため，多値モデル検査を利用した極小モデル発見技法を提案する．ここで極小モデルとは，与えられた仕様を満たすモデルのうち冗長性が極小であるモデルを指す．極小モデルにより，モデル化のうち不要な部分や誤りのある部分を特定することができる．本研究では，モデルの冗長性発見のための基本技法を提案するとともに，効率化についての考察を行う．特に，状態数爆発問題に対処するための基本技法である抽象化と冗長性発見手法の組合せが可能なことを示すため，シミュレーション定理の厳密な証明を行う．さらに本研究では，上記の手法がモデル抽象化技法と組み合わせて適用可能であることを鉄道の信号システム（連動図表）を具体的な事例として示す．

Towards Modeling-error Detection Using Multi-valued Model Checking

Yoshiaki Tatsumi[†] and Yukiyoshi Kameyama[††]

We address the problem of locating errors in the modeling phase for model checking. As the first step toward the problem, we propose a technique to detect redundancy in a given model. A model checker checks if, given a Kripke structure and a temporal logic formula, the structure satisfies the formula. In order to supply these inputs to a model checker, we need to do modeling, that is, to represent a system and a specification by a Kripke structure and a formula. Since this phase is usually done by hand, it is error-prone. In this presentation, we propose a method to find, starting from a possibly wrong model and a specification formula, a minimal model (with respect to the degree of redundancy). In order to efficiently compute the minimal model, we use multi-valued (lattice-valued) model checking techniques. One of our main results is a rigid proof of the simulation theorem extended to a multi-valued case. Finally we apply our technique to a railway signaling system and show that our technique can be combined with abstraction which is necessary to reduce the size of models.

（平成 18 年 1 月 16 日発表）

† 筑波大学大学院理工学研究科
Master's Program in Science and Engineering, University of Tsukuba
†† 筑波大学システム情報工学科コンピュータサイエンス専攻
Department of Computer Science, Graduate School of Systems and Information Engineering, University of Tsukuba