

Title	項書換えを用いた安全性検証の組織化
Author(s)	清野, 貴博
Citation	
Issue Date	2003-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/938
Rights	
Description	Supervisor:二木 厚吉, 情報科学研究科, 博士

項書換えを用いた安全性検証の組織化

清野 貴博

北陸先端科学技術大学院大学

2003 年 1 月 9 日

論文の内容の要旨

ソフトウェア工学において、状態機械は重要な計算モデルの一つである。高信頼システムの設計では、作成するシステムを状態機械でモデル化し、それが望ましい性質を持つことを科学的に検証することが、信頼性確保に有用であるとされている。状態機械は、大きく有限状態機械と無限状態機械に分けられる。帰納的に定義される状態機械のモデルは、無限状態を持つ機械をモデル化でき、状態遷移の回数に関する帰納法によって、その性質を検証できる利点を持つ。反面、検証の完全な自動化が困難であり、検証が成功するかどうかは、検証者の知識や経験に依存するという欠点を持つ。

無限状態機械が持つ性質を帰納法によって半自動的に検証するツールは、数多く提案されている。代数仕様言語 CafeOBJ とその処理系は、それらの一つである。CafeOBJ 処理系は、CafeOBJ で記述された状態機械の仕様を項書換え系と見なして、簡約による等式推論を行い、様々な性質を検証できる。CafeOBJ 処理系を用いた検証では、簡約以外の作業は検証者が行わなければならない。その主たる作業は適切な場合分けをすることである。しかし、実際の検証においては、膨大な場合分けを要することが多く、こうした作業を手で処理することは現実的ではない。このため、場合分けを処理系により支援することが、有効であると考えられる。

本論文では、CafeOBJ 処理系によって場合分けを支援する手法を提案する。本論文で取り扱う“場合”とは、状態空間を分割して作った状態の集合である。最初に、基礎となる手法として、場合を項の組み合わせで表現する手法を提案する。これによって、次の二つの手法を現在の CafeOBJ 処理系で実現できる。一つ目は、検証に用いる場合分けをマトリクス状に整理する手法である。これは場合分けの網羅性を向上させる。このマトリクスは、状態機械の仕様に由来する軸と、表明に由来する軸から成り、後者をパラメタとしている。このため、表明ごとにマトリクスを再利用できる。二つ目は、検証を進める上で有効な場合分けや補題を発見するための手法である。前述のマトリクスだけでうまく検証できないときに、機械的に場合を生成し検証を試みることで、検証を進める手掛かりとなる場合分けの候補を発見できる。検証者は、見つかった場合分けを、前述のマトリクスに追加することで、検証を進めることができる。

なお、これらの手法を、実際に使用されているいくつかの鉄道信号システムの安全性検証に適用し、本手法の有効性を確かめた。

キーワード： 代数仕様, 状態機械, 安全性, 場合分け, 項書換え