

Title	振舞い近似手法を用いた状態チャートに対する不変性の検証
Author(s)	立石, 孝彰
Citation	
Issue Date	2003-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/939
Rights	
Description	Supervisor:片山 卓也, 情報科学研究科, 博士

振舞い近似手法を用いた 状態チャートに対する不変性の検証

立石 孝彰

北陸先端科学技術大学院大学 情報科学研究科

2003年1月9日

論文の内容の要旨

開発対象システムや分散オブジェクトなどの振舞いをモデル化するために状態チャートと呼ばれる状態遷移システムいることが多い。互いにイベントを用いて協調動作を行う複数の状態チャートにおいては、検証対象となる状態チャートの振舞いは、他の状態チャートの振舞いに依存する。このような依存関係のある状態チャートの検証を行う場合、互いの相互作用を考慮して検証を行わなければならない。このための一般的な手法は、すべての状態チャートを合成して、一つの大きな状態チャートを構成することであるが、しばしば状態爆発という問題が起こる。

ところが、他の状態チャートから送信されるイベントが、どのように検証対象の状態チャートに作用するかを考慮することによって、対象状態チャートを合成後の振舞いに近似することができる。このような近似を用いた手法は、繰返し適用することができ、検証に必要なだけ状態チャートの振舞いを詳細にすることができる。

状態チャートのような状態遷移システムでは、活性と安全性の2つの性質の検証に分類できる。本研究では、安全性の検証を行うことが目的であり、属性値に対する不変性を検証するための手法を提案した。そして、近似された状態チャートで検証できる性質は、合成された状態チャートでも検証できることを証明した。このような振舞い近似手法を、様々な通信方法に適用できるように汎用性を持たせて定義した。

この不変性の検証のために、状態チャートを TSE(遷移列式, Transition Sequence Expression) と呼ぶ正規表現に類似した式を用いて表すことにする。状態チャートから TSE を求める方法は、有限オートマトンを正規表現に変換する方法と同じであり、自動的に遷移列式を求めることができる。単一状態チャートに対する検証では、TSE の前後に表明を付け、表明が正しいことを証明する。このような遷移列式を A-TSE(表明付き TSE) と呼ぶ。この証明には演繹的体系を用いて行うため、無限の属性値を持ち得る属性の検証を行うことができた。このために、Hoare 論理に類似した演繹的体系を提案し、その体系が、表明付き遷移列式の意味に対して健全かつ完全であることを証明した。

本研究では、近似手法を不変性検証のために用いるが、このような手法は状態チャートに対するテストとっても有効な手法である。

キーワード: 状態チャート, 状態爆発, 分散オブジェクト, 検証, 不変性