

論文要旨

論文題目 Studies on Asynchronous System Specification for Formal Verification
和文題目 形式的検証における非同期システムの動作記述に関する研究

本論文は、モデル検査手法の動作仕様記述における時相論理式を、帰納的に導出する手法を提案する。本提案法では、信号遷移グラフ (STG) によりシステムをモデル化し、さらにその発火規則を用い、関係状態図 (Relational State Graph) に変換する。その後、時相論理における分岐時相論理の一つである CTL (Computation Tree Logic) で扱いやすいように、関係状態図を分岐表現 (branch expression) に変換する。その分岐表現から時相論理式を導出する。従来は、時相論理を熟知したシステム設計者が、手作業で動作仕様を記述する必要があったが、本提案法を用いることで、設計者は効率よく動作仕様記述を導出できることがわかっている。

本研究の成果を要約すると以下の通りである。

1. モデル検査手法の動作仕様記述における時相論理式を、帰納的に導出する手法を提案し、その導出手順を示している。

システムを形式的に検証する手法は、重要な役割を果たすようになってきている。これまで形式的検証手法が研究されてきたが、その動作仕様記述に関しては、システム設計者にとって容易に理解することが難しい現状にある。本研究では、システム設計者の能力に依存していた時相論理式の記述とは異なり、システムを検証するために必要な信号遷移イベントのみを抽出し、不必要なイベントを省いている。それらのイベントを抽出するために、strong/weak temporal order relation を定義した。これらの定義を適用し、帰納的に時相論理式を記述することができる。

2. 提案する手法を適用し、制御モジュールの動作記述例を示し、検証に必要な信号遷移のみを考慮した時相論理式の記述が行えることを示している。

システム全体のなかで、その振る舞いが複雑になる傾向にあるのは制御回路である。本研究では、非同期システムでの平行な動作を仲裁するための制御回路とアービタモジュール、パイプラインモジュール、そして DME モジュールに関しての時相論理式の記述例を示し、本手法を用いる有効性を示している。

3. ベンチマーク回路を用い、本手法と従来手法の検証結果を比較し、その有効性を示している。

小規模な回路を検証結果では、本手法と従来手法では顕著な結果にはならないが、パ

イプラインの段数, DME モジュールの接続数を増やしていくと, 検証に要する時間, メモリ容量の効率化が図れることを示している. 特に, パイプラインの段数を 19 段に増やした場合, 従来手法では検証不能に陥るが, 本手法では可能である. また, DME モジュールでは, 接続数を 6 とした場合, 従来手法で検証不能となる. 本手法を用いることで, これまで検証不可能であった回路の動作記述を行い, その検証を行うことが可能となる.

氏 名 山 田 親 稔

(様式第5-2号)

2005年8月1日

琉球大学大学院
理工学研究科長 殿

論文審査委員

主査 氏名 仲尾 善勝

副査 氏名 長田 康敬

副査 氏名 アシリア モハammad' レ

副査 氏名 和田 知久



学位(博士)論文審査及び最終試験の終了報告書

学位(博士)の申請に対し、学位論文の審査及び最終試験を終了したので、下記の通り報告します。

記

| | | | |
|---|--|--------|-------------|
| 申請者 | 専攻名：総合知能工学専攻 氏名：山田 親稔 学籍番号：[REDACTED] | | |
| 指導教員 | 仲尾 善勝 | | |
| 成績評価 | 学位論文 | 合格 不合格 | 最終試験 合格 不合格 |
| 論文題目 | Studies on asynchronous system specification for formal verification | | |
| 審査要旨 (2000字以内) | | | |
| <p>本論文は、モデル検査手法の動作仕様記述における時相論理式を帰納的に導出する手法を提案している。本提案法では、信号遷移グラフ(STG)によりシステムをモデル化し、さらにその発火規則を用い、関係状態図(Relational State Graph)に変換する。その後、時相論理における分岐時相論理の一つであるCTL(Computation Tree Logic)で扱いやすいように、関係状態図を分岐表現(Branch Expression)に変換する。その分岐表現から時相論理式を導出する。従来は、時相論理を熟知したシステム設計者が、手作業で動作仕様を記述する必要があったが、本提案法を用いることで、設計</p> | | | |

(次頁へ続く)

者は効率よく動作仕様記述を導出できるようになった。

本研究の成果を要約すると以下の通りである。

1. モデル検査手法の動作仕様記述における時相論理式を、帰納的に導出する手法を提案し、その導出手順を示している。

システムを形式的に検証する手法は、重要な役割を果たすようになってきている。これまで形式的検証手法が研究されてきたが、その動作仕様記述に関しては、システム設計者にとって容易に理解することが難しい現状にある。本研究では、システム設計者の能力に依存していた時相論理式の記述とは異なり、システムを検証するために必要な信号遷移イベントのみを抽出し、不必要なイベントを省いている。それらのイベントを抽出するために、“strong/weak temporal order relation”を定義した。これらの定義を適用し、帰納的に時相論理式を記述することが可能になった。

2. 提案する手法を適用し、制御モジュールの動作記述例を示し、検証に必要な信号遷移のみを考慮した時相論理式の記述が行えることを示している。

システム全体のなかで、その振る舞いが複雑になる傾向にあるのは制御回路である。本研究では、非同期システムでの並行な動作を仲裁するための制御回路とアービタモジュール、パイプラインモジュール、そして DME モジュールに関しての時相論理式の記述例を示し、本手法を用いた場合の有効性を示している。

3. ベンチマーク回路を用い、本手法と従来手法の検証結果を比較し、その有効性を示している。

小規模な回路の検証結果では、本手法と従来手法では顕著な相違は現れないが、パイプラインの段数、DME モジュールの接続数を増やしていくと、検証に要する時間、メモリ容量の効率化が図れることを示している。特に、パイプラインの段数を 19 段に増やした場合、従来手法では検証不能に陥るが、本手法では可能になった。また、DME モジュールでは、接続数を 6 とした場合、従来手法で検証不能となる。本手法を用いることで、これまで検証不可能であった回路の動作記述を行い、その検証を行うことが可能となった。

以上のように、本研究は、工学的に価値のある新しい成果を得ているため、提出された学位論文は博士の学位論文に値するものとして学位論文の審査を合格とする。また、論文発表会における発表ならびに質疑応答の結果、申請者は専門分野および関連分野の十分な知識ならびに本学大学院博士後期課程修了者として十分な研究能力を有していることが確認できたので最終試験も合格とする。