



Title	形式的手法を用いたCPUの自動検証と通信プロトコル用回路の自動合成
Author(s)	北嶋, 暁
Citation	大阪大学, 1998, 博士論文
Version Type	
URL	https://hdl.handle.net/11094/40682
rights	
Note	著者からインターネット公開の許諾が得られていないため、論文の要旨のみを公開しています。全文のご利用をご希望の場合は、大阪大学の博士論文についてをご参照ください。

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

氏 名	きた 北 じま 嶋 あきら 暁
博士の専攻分野の名称	博 士 (工 学)
学 位 記 番 号	第 1 3 9 2 8 号
学 位 授 与 年 月 日	平成10年 3 月 25 日
学 位 授 与 の 要 件	学位規則第4条第1項該当 基礎工学研究科物理系専攻
学 位 論 文 名	形式的手法を用いた CPU の自動検証と通信プロトコル用回路の自動合成
論 文 審 査 委 員	(主査) 教 授 谷 口 健一 (副査) 教 授 橋 本 昭 洋 教 授 今 井 正 治

論 文 内 容 の 要 旨

本論文は、非パイプライン CPU の形式的設計検証の自動化と、通信プロトコルの形式仕様からの回路自動合成についてまとめたものである。近年ハードウェアの設計において、設計の正しさを論理的に証明する方法（形式的検証）や、形式仕様から回路を合成する方法が注目されている。しかし、証明作業に手間がかかるという問題点があり、また、相互に通信して協調動作する複数のモジュールで構成されるシステムを記述した形式仕様からの合成法はほとんど提案されていない。そこで、以下を行った。

第一に、非パイプライン CPU について、その設計検証が自動でかつ実用的な時間で行えることを調べた。従来、命令を逐次実行する非パイプライン CPU については証明が自動で行えることが分かっているが、命令プリフェッチのように命令の実行が重なるような効率化をした場合では、一般に帰納的な証明が単純には行えないために自動化が難しく、また、自動で証明できる場合でも、膨大な時間を要することもある。本論文では、CPU の基本的な命令セットを備えた教育用 8 ビット CPU KUE-CHIP 2 を例題として、設計およびその正しさの検証を行った。設計は各命令ごとの動作を記述した要求仕様（命令セットアーキテクチャ）から、RT（レジスタ転送）レベルまで行った。設計した CPU の制御は、命令のプリフェッチを含んでいる。証明は、段階的に行う方法および直接行う方法を採用し、いずれも自動で行った。証明が成功したときの CPU 時間は、段階的に証明を行った場合は、他の順序回路の証明にも使用できる汎用の証明支援系を用いて13時間程度要したが、直接証明した場合は、非パイプライン CPU だけを対象とした証明系を用いて2分程度であった。また、ALU などの各機能部品についても、ゲートレベルまで設計を行い、かつその正しさを自動で証明した。証明に用いた方法では証明に要する時間は命令の数に比例する程度しか増えないことなどより、他の同様の非パイプライン CPU の設計が正しいことの証明も同様に自動で行える。

第二に、形式的に記述された通信プロトコルの局の動作仕様から RT レベルの回路を自動的に合成する方法を考案した。考案した合成法では、まず形式的言語 LOTOS で記述された仕様を、EFSM（拡張有限状態機械）群と、その間の同期指定とに変換し、そこから各 EFSM 群の同期も含めた実行を制御する回路を合成する。ここで、同期指定とは、EFSM 群のどの部分集合において、どの条件が成り立つときにそれらの EFSM 群が同時にどの動作を行うかの指定の集合である。指定された同期の実行は、マルチランデブと呼ばれる。合成の結果得られる回路は、回路化した EFSM 群と、それらの間のデータパス、それらの EFSM 群に対しマルチランデブを行うことを指示する制御部からなる。各 EFSM は、それぞれの同期指定について、その EFSM ではその時点でそのマルチランデブの動作が実行

可能であるか否かを判定し、それぞれの結果を制御部に通知する。制御部は、どの EFSM 間のマルチランデブを実行すべきかを決め、各 EFSM にその実行を指示する。各 EFSM は、制御部からマルチランデブを行う指示があった場合はその指示どおりの動作を行い、指示がなかった場合は個々に動作する。ファイル転送プロトコルの一つに対して本手法を適用した結果、得た回路は、ゲート数・遅延時間とも実用上問題ない程度であった。

論文審査の結果の要旨

本論文では、非パイプライン CPU について設計が正しいことの証明を自動で行う方法を示し、また、通信プロトコルの形式仕様記述からの回路の合成法を提案している。

本論文の前半では、命令プリフェッチを含む非パイプライン CPU について、対象とするクラスを定め、そのクラスの CPU に対し、CPU の命令セットで定義された各命令の意味が設計したレジスタ転送レベルで正しく実装されていることの証明を自動で行う方法を与えている。証明の自動化が望まれている理由として、そのクラスを含め、前後の命令の実行が重なる場合には、一般には自動では証明できず、従来の定理証明系を用いた対話的な証明では証明に手間がかかるということが挙げられる。対象とするクラスでは、実現における実行制御において、1 命令の実行中に閉路を含まない点、および命令実行が重なるのは命令プリフェッチだけである点以外には制約を課していないため、そのクラスでも実用的な回路を設計することができる。本手法に基づいて作成した自動証明系を用いて、19種類の基本的な命令を備えた教育用 8 ビット CPU KUE-CHIP 2 の設計検証を行った。証明に成功したときの作業時間は約 2 分であり、実際上問題のない程度である。本手法は、命令語のビット長には依存せず、また、命令数が多い場合でも有効である。これは、命令ごとに場合分けを行うことと、対象とするクラスの CPU の場合は命令数にかかわらず 1 命令の実行に要するステップ数はほぼ同じと見なせることによる。このように、非パイプライン CPU の設計検証が、自動でかつ実用的にも問題ない時間で行えることを示し、実用面で意義のある成果を上げている。

通信プロトコルの形式仕様記述からの回路の合成法では、入力となる形式仕様において、従来の方法では扱っていなかった三つ以上の EFSM が同期してデータ交換などを行い協調動作するモデルを対象としており、適用できる範囲が広がっている。合成される回路において、同期が行えるかどうかの判定を複数の同期についてそれぞれ行う必要があるが、あらかじめ同期を分類し、判定に必要なモジュールの数が少なくなるよう工夫している。同期が行えるかどうかの判定と競合の回避の実現に必要なモジュール数の合計は、分類した同期の数に比例する程度であり、また、各 EFSM の状態数には依存しないので、EFSM 群の規模が大きくなっても妥当なゲート数の回路が得られると期待できる。提案した合成法は、通信プロトコル仕様をハードウェア回路として実現した場合の性能を素早く見積ることができる点や、回路を試作して実際に動作確認を行う用途に使用できる点からも、実用上有望であると言える。

以上のように、本論文は形式的手法を用いたハードウェアの設計技術の進展に貢献しており、博士（工学）の学位論文として価値あるものと認める。