氏名	竹中（たけなか） 崇（たかし）
博士の専攻分野の名称	博士（工学）
学位記番号	第 15520 号
学位授与年月日	平成12年3月24日
学位授与の要件	学位規則第4条第1項該当 基礎工学研究科情報数理系専攻
学位論文名	拡張有限状態機械群およびout-of-order型パイプラインCPUの形式的設計検証
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　教授 東野 輝夫

論文内容の要旨

本論文は、筆者が大阪大学大学院基礎工学研究科に在学中に行なった計算機科学の研究のうち、同期式順序回路の形式的検証に関する研究をまとめたものである。

本論文では、第一に、抽象度が高く一つの拡張有限状態機械で表される要求仕様から、より抽象度が低くレジスタを共有する拡張有限状態機械群で表される実現仕様を設計したときの、その設計の正しさの検証法を考案した。本手法による設計では、まず要求仕様の各一遷移を実現するようなより具体的な遷移の系列を考案する。そして、これらの遷移を制御する複数有限制御部群を設計する。検証では、要求仕様、実現仕様、及び、要求仕様の各遷移の具体化である「遷移の対応」を与え、要求仕様の遷移 t それぞれについて遷移 t が実行される状況からこれに対応する遷移系列の通りにのみ遷移が順に実行され、その実行終了後に遷移 t に続いて実行されうる遷移に対応する遷移系列が実行でき、最終的に要求仕様の制御部の各状態が実現仕様での状態の組み合わせに一意に対応することと、要求仕様の遷移それぞれの動作内容が対応する遷移系列によって達成されることを確認する。例題回路としてPCIバスを介してCPUとメモリを接続するPCIバスインターフェイス回路を実際に設計し、その設計の正しさを検証した。この回路規模は制御部数9、遷移数96であった。検証が成功した時のCPU時間は約20分であった。

第二に、out-of-order型パイプラインCPUに対して、一遷移で一命令を実行する命令セットアーキテクチャレベルの要求仕様から、一遷移で一つのパイプラインステージを実行するレベルの実現仕様を設計したときの、その設計の正しさの検証法を考案した。本手法では、out-of-order型パイプラインCPUの要求仕様と実現仕様のあるクラスを制約条件 C によって定め、このクラスのCPUに対し設計した実現仕様が要求仕様を満たすことの十分条件 V を与えた。定めたクラスのCPUは、n 段パイプラインの、あるステージ以降のステージからなる部分パイプラインでのみvisibleレジスタの読み書きやALU演算など命令本来の実行処理を行う。そして、out-of-order型であっても、この部分パイプラインでは命令実行順の入れ換えは起きず、この部分パイプラインの実行を先に開始した命令が後続して実行される命令に影響されない。十分条件 V は、命令がこの部分パイプラインを実行し始めるときの条件と、部分パイプラインおける一命令の実行処理の正しさに関する条件等からなる。検証実験では、命令のスケジューリングのためのバッファを持ち6段パイプラインからなるCPUの設計の正しさの検証を行った。検証に必要となったCPU時間は約8時間であった。

論文審査の結果の要旨

本論文では、拡張有限状態機械群およびout-of-order型パイプラインCPUのそれぞれについて、その設計の正しさの形式的検証法を提案している。

拡張有限状態機械群に対して提案した手法では、「遷移の対応」の通りに実現回路群が状態遷移していくことと、このときに要求仕様の動作内容が達成されることという実現の正しさの十分条件を調べるという方法を採用し、さらに実現回路群がこれらの条件を満たすことの確認において要求仕様の制御部の各状態が実現回路群での状態の組み合わせに一意に対応するように制限して、検証に要する計算時間を抑えることに成功している。その十分条件は、本論文で提案している設計スタイルに従って設計するとき、正しい設計なら通常満たすことが予想されるので、実用的見地からきつすぎるということはない。また、PCIバスインターフェイス回路の検証実験によって、拡張有限状態機械群の典型的な例題回路を実用的と思われる手間と計算時間で検証できることを示している。提案手法によって、検証時に一般に生じる状態の組み合わせ爆発を回避でき、実用上有望であるといえる。

out-of-order型パイプラインCPUに対しては、対象とするクラスを定め、そのクラスのCPUに対し実現仕様が要求仕様を正しく実現することの十分条件Vを与えている。従来、out-of-order型CPUの検証では、後続する命令の影響を切り離した帰納的な証明ができるように、また、証明支援系を用いて実用的な時間で行えるようにその設計例に応じて証明の方針を考案していたが、それは一般には困難である。本論文の提案手法では、n段パイプラインのあるステージ以降の部分パイプラインでは先に開始した命令が後続して実行される命令に影響されない等の制約が成立するようなパイプライン実行方式のクラスを対象とし、実現の正しさの検証を、その部分パイプラインを実行し始めるときの条件とその部分パイプラインでの命令の実行処理に関する条件等の確認にうまく分離している。特に後半の条件の確認は後続する命令の影響を切り離した一命令ごとの帰納的な議論で行うことができる。また、十分条件VはそのクラスのCPUに汎用的に適用することが可能であり、検証者は設計例に応じて証明の方針を考案する必要がない。例題CPUの検証実験では、そのクラスのCPUを実際に設計し、今まで行われていなかった規模のCPUの検証が実用時間で行えることを示している。提案手法によって、一定の証明方針に沿って実用時間で検証を行え、実用面で意義があるといえる。

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検証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。