【 57 】

氏名	北道淳司（きたみちじゅんじ）
博士の専攻分野の名称	博士（工学）
学位記番号	第 14179 号
学位授与年月日	平成10年10月14日
学位授与の要件	学位規則第4条第2項該当
学位論文名	代数的手法を用いた同期式順序回路の段階的設計および形式的検証
論文審査委員	（主査）教授 谷口 健一 （副査）教授 今井 正治　教授 柏原 敏伸

論文内容の要旨

近年，ハードウエアの設計規模の増大に伴い設計の上流工程における設計法の確立が望まれている。また設計により得られた回路が要求される機能，いわゆる要求仕様を満たすことを形式的に保証するには，数学的枠組みに基づく検証手法が必要である。

本研究では，具体的に設計された回路が要求仕様を満たすことを形式的に証明することを目的とし，その証明を実際上可能とするために要求仕様から具体的な論理設計レベルの仕様まで段階的にかつ各段階では回路を局所的に具体化するという制約のもとで設計を行い，各段階における具体化の正しさを代数的手法を用いて証明するという方針を採用する。代数的言語は意味定義が厳密，簡明かつ記述者がデータタイプや関数等を自由に定義できる記述能力などの特徴をもち，プログラム設計の検証において代数的手法による検証の有用性の評価も行われており，本研究の対象とする回路設計及び形式的検証に有望であると思われる。

まず要求仕様レベルから論理設計レベルまでの設計レベルにおける回路モデルとして拡張有限状態機械モデルを採用し，それを代数的言語で記述する。このモデルのもとで，2つの回路とそれらの状態の対応のもとでの回路の等価性（設計の正しさ）を形式的に定義する。

各段階における局所的な具体化では，抽象的な一動作を実現する動作アルゴリズムの設計などが行われる。各段階において回路を局所的に具体化するという制約に基づいた設計による回路は，具体レベルで直接設計されたものに比べてデータ転送の並列度が低いなどの点で各資源の有効な利用を行えない可能性があるが，提案手法では冗長な動作や状態を取り除くとか2つのデータ転送を一つに取りまとめるなどの比較的単純な12種類の簡約化ルールを設計者が回路に適用するという方法を取り入れる。簡約化ルールはいくつかの回路設計を行った経験から定め，また各ルールの適用前後の回路の等価性はあらかじめ保証されているので設計者がそれらのルールを繰返し用いて結果的に複雑な簡約化作業を行っても作業前後の回路の等価性は保証される。設計例題として，クイックソート法及びマックスソート法によるソート回路，CPU及びGCD回路などを用い，いずれの場合も，直接具体レベルにおいて設計した回路と同じものを得た。

局所的な具体化では抽象的な一動作を実現する動作アルゴリズムの設計などが行われるが，このような設計の正しさの証明は動作アルゴリズムの途中状態において各部品間に成り立つべき関係を表した不変表明と呼ばれる補題を用いた構造的帰納法により行うことができる。不変表明を用いた構造的帰納法の手順の管理，代数的証明技法の一定手順による適用などの機能をもつ検証支援系により，設計例題の設計の正しさの検証を行った。CPU の検証は完全に自動的に，GCD 回路及びソート回路の検証は最初の数レベルは不変表明やユーザが定義した関数に関する補題の考案など試行錯誤を必要とするが，それ以外の作業は自動で行えた。

また，代数的証明技法の一つである整数上の加算，不等式等を含む論理式の真偽判定手続きの高速化のために，論理式を表すデータ構造のうち同じ部分データを共有して保持するというデータタイプを提案し，その上での高速な処理方法を用いた判定系を実現した。提案する判定系は現在のところ，データの共有という手法しか用いていないが，それ以外のいくつかの高速化手法を実現している従来手法との比較実験の結果，同程度の計算時間で論理式の真偽判定が行えることがわかった。

上述のように，局所的な設計という制約のもとで要求仕様から論理設計レベルまで設計支援系を用いて段階的設計を行い，検証支援系により設計の正しさを証明することができ，提案する代数的手法を用いた設計法，検証法及び新たに提案した判定系の有用性が確認された。

論文審査の結果の要旨

本論文は，同期式順序回路の設計に関して，回路の要求仕様を記述するレベルからバス構成などのアーキテクチャ，マイクロプログラムあるいは各部品の制御入力への論理式を具体的に指定するような論理設計レベルに至るまでの，代数的手法を用いた段階的設計法，形式的検証法及び検証に用いる高速な論理式の真偽判定の方法を提案している。具体的な実現仕様が要求仕様を満たすことの形式的検証を可能とするために，設計は段階的かつ局所的に行い，その各設計が正しいことを証明するという方法を取っている。また，回路記述法，設計の正しさの形式的定義，設計法及び検証法の枠組みとして，任意の設計レベルにおいて統一的な手法が適用できるようにしている。

提案された段階的設計法のための回路設計支援系を作成し，CPU，メモリ内のデータを整列させるソート IC などいくつかの例題回路の設計に適用している。局所的に個々の動作を具体化するという段階的設計によって得られる回路には非効率な部分が含まれることもある。そこで，引き続く動作を一つにまとめるとか制御のループ構造を変形するといった効率化のための回路簡約ルールを用意し，設計者が支援系を用いてそれらの簡約ルールを回路に随時適用することにしている。いずれの例題回路の設計においても，要求仕様からの完全な段階的設計と簡約ルールの適用によって，具体的な論理設計レベルで人手によって直接設計した効率的な回路と全く同じものが設計できることが確認されている。

さらに，各段階の設計の正しさを証明するための代数的手法を用いた形式的検証法を提案している。設計の正しさの検証は，検証者の考案した不変表明を用いた構造的帰納法，代数的定理証明機能である項書き換え，場合分け，整数上の論理式の恒真性判定等を一定手順で適用することによって行う。作成された検証支援系及び高速化された論理式の恒真性判定ルーチンを用いて，実用的な計算時間で検証が可能であることが例題回路に対する検証実験によって確かめられている。

以上のように，本論文において提案された手法および支援系により，従来行われていなかった要求仕様からの正しさを保証した回路設計が可能となる。例題回路の設計及び検証を行ってその有用性を実証しており，本研究は，上流工程における回路設計及び回路検証技術の進展に寄与している。よって，博士（工学）の学位論文として価値あるものと認める。