科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月 １７ 日現在

機関番号：１３６０１
研究種目：基盤研究(C)
研究期間：2011～2013
課題番号：２３５００１７４

研究課題名（和文）グリッド環境の定理証明器とモデル検査器をハードウェアコンパイラ融合した形式検証系

研究課題名（英文）Formal Verification System by using Hardware Compiler Fusioning of Theorem Prover and Model Checker on the Grid Environment

研究代表者
和崎　克己（WASAKI, Katsumi）

信州大学・工学部・教授

研究者番号：７０２７１４９２

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：グリッドコンピューティング環境上へ実装した定理証明器と，様々なターゲット実装コードを出力可能なハードウェアコンパイラを融合し，上流から下流工程まで一貫した高機能な形式検証系を構築し，非同期並列回路システムの検証能力の飛躍的向上を図る．対象回路の構成情報は，関数型言語系の上で記述し，この言語系からのコンパイラ出力として，ターゲット実装コードと，プルーフチェッカへの証明式の列を同時に得る．対象回路は，非同期論理ゲート素子のモデルを二線式 4 値論理に基づいたメッセージパッシング型並列計算でモデル化し，回路接続の正当性証明はプルーフチェッカーを用いて検証する．

研究成果の概要（英文）：A theorem prover that implements to the grid computing environment fuses the output hardware compiler target implementation various code. To build a formal verification system which is consistent high to function downstream from the upstream, thereby dramatically improving the ability for verification of asynchronous parallel circuit system. The configuration informations of the target circuit has been described on the functional language system. As compiler output of the language system, we can get the target implementation code and the type of proof to proof checker. The target circuit has been modeled by message passing parallel computer based on the 4-valued logic two-wire model of asynchronous logic gate element. Finally, proof checker can verify its correctness proof by using of the circuit connection.

研究分野：数理情報工学

科研費の分科・細目：情報学・知能情報学

キーワード：探索・論理・推論アルゴリズム　プルーフチェッカ

１．研究開始当初の背景

申請者は,「ロジック」の問題に関して，演算回路を数学的定義に基づいて設計し，設計検証と動作の正しさをMizarプルーフチェッカを用いて証明する手法について検討を行ってきた．

また申請者は，ある関数型言語系を台言語として利用した，様々な対象コードを出力できる上位ハードウェアコンパイラ:Melasy+ を開発中であった（和崎 2008）．非同期並列システムの上位設計から，Verilog-HDL や VHDL などのハードウェア記述言語，ならびに NuSMV モデル検査向けの記述言語への自動変換が可能な段階まで開発が進んでいた．

対象回路の構成情報は，簡易な回路記述に文法を縮約した，一種の関数型プログラミング言語系の上で記述し，この言語系からのコンパイラ出力として，プルーフチェッカが処理できる形式の数式定義，定理証明列が自動的に得られるようにする．対象関数型言語系として，Objective Caml を使用する．

一方，定理証明器によって形式検証済みの回路モデルを，ハードウェアコンパイラが出力するモデル検査記述用の言語へ自動変換後，実サイズの並列演算器として接続し検証する際，1台の検証用プロセッサを利用するのみでは，計算モデルのふるまい状態空間が巨大となり，要求仕様を含む探査アルゴリズムのための計算時間が非常に長くなり，実用的で無くなる問題点が存在していた．このように，検証性能の飛躍的改善のため，多数の並列プロセッサを用いたグリッド環境を用いた検証システムの構築が急務であった．

２．研究の目的

(1) 具体的には，グリッドネットワーク管理ミドルウェアとして Globus-2 を使用し，クラスタ並列計算ライブラリとして MPICH-G2 を用いて，多数の計算ノードを同時に稼動させ，プルーフチェッカならびにモデル検査器の並列化を行う．検証対象は，パイプラインあるいはトーラス接続された超並列演算器（PE）である．この設計検証のために，グリッドネットワーク上で動作するプルーフチェッカを用いてプロパティ検証を実行する．上位の超並列接続のための制御器のモデルによって多数の PE をネットワーク・オートマタによって論理接続する．最終的に得られた実サイズ設計に対して，多数の PE 群の動作検証のため，ふるまい状態空間を最適分割することで，グリッドネットワーク上での高速検証が実際に可能であることを研究期間内に明らかにする．

(2) 他方,（今回採用する Mizar プルーフチェッカのような）数学証明の形式検証系においては，検証対象の回路の構造や各機能モジュール間の接続といった構成情報を，形式検証系が理解できるような数学構造ならびに各定理から導かれる結論の継承関係へ正しく変換する必要性がある．一般に，このような数式証明系の記述は，回路設計を実際に行っているエンジニアには大変難しく，設計現場への検証系の導入は困難さが伴う．また，数学構造を理解しなければ回路検証ができないという，ジレンマを抱えてしまうことにもつながりかねない．

このため，対象回路の構成情報は，簡易な回路記述に文法を縮約した，一種の関数型プログラミング言語系の上で記述し，この言語系からのコンパイラ出力として，プルーフチェッカが処理できる形式の数式定義，定理証明列を得るものとする．

以上，(1) (2) の方策と融合により，回路上位設計と形式検証系との間の概念障壁（セマンティックギャップ）を埋めることに成功し，大規模かつ並列度の高いプロセッサ向け回路設計時における検証作業の高速化と信頼性向上に寄与するものである．

(3) グリッドネットワークと並列化アプリケーション構築は，未だ黎明期にある．形式検証系と回路設計との融合，特に関数言語系の上のコンパイラ出力を利用して双方を結合する方策については，他に例が無い．

高性能・高信頼性の国産プロセッサ開発技術の確立が切望されている状況に鑑み，その設計検証技術の向上は工学的・学術的に大きなインパクトを持つ．特に，シミュレーション手法による不完全な品質検査に代わる，信頼性の高い演算器実装に関する数理的手法（形式検証手法）の確立が，当該分野におけるこの研究計画の特色と独創性を有する点である．

更に，高速ネットワーク接続環境の地球的規模の広がりに伴い，計算機資源の有効利用として注目されるグリッドコンピューティング環境を，この数理的手法と融合させることにより，線形的な性能向上という結果が期待される．我が国が，数理情報学と通信ネットワーク学との横断的学際領域の創出に寄与できる点において，この研究計画は意義深いと考えている．

更に，形式検証系と回路設計技術者との間を，業界標準言語から関数型言語系への自動変換，ならびにその上で稼働するコンパイラ出力を利用して，形式検証系へ入力するといった理論と技術の融合は，この学際領域において大変稀有な研究課題であるとともに，その研究成果により，形式検証学者と回路設計技術者との間のセマンティックギャップを埋めることであり，その点において当該分野の新しい研究課題として誠にふさわしいと考えられる．

３．研究の方法

(1) 関数型言語系の上にハードウェアコンパイラを開発する．対象回路の構成情報は，簡易な回路記述に文法を縮約した，一種の関数型プログラミング言語系の上で記述し，この

言語系からのコンパイラ出力として，モデル検査器ならびにプルーフチェッカが処理できる形式の数式定義，定理証明列が自動的に得られるようにする．対象関数型言語系として，Objective Caml を使用する．Verilog-HDL や VHDL などのハードウェア記述言語から，関数型言語系への自動変換を行う援用プログラムも並行して作成する．

(2) モデル検査器とプルーフチェッカを，グリッドコンピューティング環境上へ実装する．ミドルウェアとして Globus-2，並列化ライブラリとして MPICH-G2 を使用する．高速なノード間接続のために，光高速ネットワークバス（InfiniBand・新規購入）を導入し，現有設備のスレーブノード ×30 台を計算クラスタとして構成する．システム統合のため，証明の分割・合成を行うためのシステム構築ならびに並列化ライブラリを利用したプログラム開発を行う．

(3) 並列化検証システムの性能評価を行う．検証対象は，パイプラインあるいはトーラス接続された超並列演算器（PE）とする．計算を多ソート代数でモデル化し，超並列接続のための制御器のモデルによって多数の PE をネットワーク・オートマタによって論理接続する．

(4) クラスタ計算機上の並列化検証システムの速度性能向上のため，CUDA-GPU 並列アクセラレータ（新規購入）を導入し，検証済み演算器のシミュレーション・形式検証統合システムを完成する．この時，各演算用のクラスライブラリを作成し，回路情報と計算モデルとのマッチングを行うための方策を検討する．

(5)作成した，関数型言語系の上のハードウェアコンパイラと，グリッド環境上の高性能並列検証システムとを結合利用し，実際の回路規模の LSI 設計データ等を対象とし，FPGA/CPLD 統合設計開発ツールを導入し，検証系全体のユーザビリティ評価を実施する．以上と並行して，形式検証系に関する海外共同研究者（Canada, France）との合同調査研究を遂行する．

４．研究成果

定理証明器(プルーフチェッカ，Proof Checker)と，様々なターゲット実装コードを出力可能なハードウェアコンパイラを融合し，上流から下流工程まで一貫した高機能な形式検証系を構築し，非同期並列回路システムの検証能力の飛躍的向上を図った．対象回路の構成情報は，関数型言語系の上で記述し，この言語系からのコンパイラ出力として，ターゲット実装コードと，プルーフチェッカへの証明式の列を同時に得た．

(1) 平成 23 年度においては，検証対象として，パイプラインあるいはトーラス接続された超並列演算器(PE)を取り扱った．この設計検証のために，プルーフチェッカを用いてプロパティ検証を実行した．上位の超並列接続のための制御器のモデルによって多数の PE をネットワーク・オートマタによって論理接続した．対象回路の構成情報は，簡易な回路記述に文法を縮約した，一種の関数型プログラミング言語系の上で記述し，この言語系からのコンパイラ出力として，プルーフチェッカが処理できる形式の数式定義，定理証明列を得るものとした．

上記のため，関数型言語系の上にハードウェアコンパイラを開発した．対象回路の構成情報は，簡易な回路記述に文法を縮約した，一種の関数型プログラミング言語系の上で記述し，この言語系からのコンパイラ出力として，NuSMV, SPIN モデル検査器ならびにプルーフチェッカが処理できる形式の数式定義，定理証明列が自動的に得られるようにした．対象関数型言語系として，Objective Caml を使用した．Verilog-HDL や VHDL などのハードウェア記述言語から，関数型言語系への自動変換を行う援用プログラムも並行して作成した（図１）．

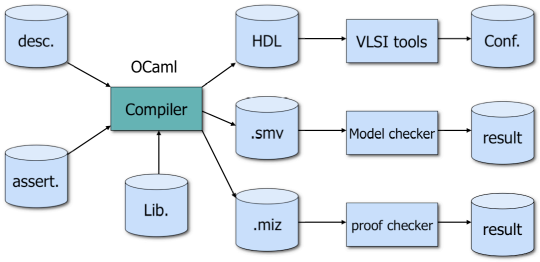

図 1: Object Caml 関数型言語系の上に実装したハードウェアコンパイラと HDL・プルーフチェッカ用証明列の自動生成の流れ

(2) 平成 24 年度においては，プルーフチェッカ（Proof Checker）を，グリッドコンピューティング環境上へ実装し，並列システムの検証能力の向上を図った．対象回路の構成情報は，関数型言語系の上で記述し，この言語系からのコンパイラ出力として，プルーフチェッカへの証明式の列を得た．対象回路は，論理演算器の計算を多ソート代数でモデル化し，証明はプルーフチェッカを用いて検証する．論理演算子，演算子とハードウェアゲートとの関係，ゲート同士の信号線による接続等の定義・定理を基に，回路を結合・合成し，演算回路が正しく動作することを検証する．形式検証系として Mizar 証明検査システムを用いる．

まず「多ソート代数モデル」による並列演算器の計算モデルを作成した．高速演算性を実現するための加算キャリー先見回路やモニタ回路，ならびに RSD 数系を利用した Carry-save generic Adder が必要だが，これらの演算素子を，自然数 N のオーダで帰納的な計算モデルとして構成し，プルーフチェッカによる数学的帰納法で証明可能とした．

次に，並列性実現のため「パイプライン機

構」を説明するモデルとして，ペトリネットツール（HiPS）を導入した．ペトリネットによって分割・合成されたネットワーク・オートマタによりノードあたり証明問題サイズの縮小を図った．

更に，プルーフチェッカを，グリッドコンピューティング環境上へ実装する準備を行った．システム統合のため，証明の分割・合成を行うためのシステム構築ならびに並列化ライブラリを利用したプログラムの検討を行った（図 2）．

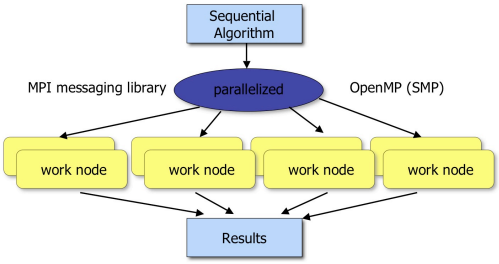

図 2: 逐次実行する自動推論プログラムをグリッドコンピューティング環境上へ実装

(3) 平成 25 年度においては，並列構成時に必要な高位設計記述のため，COINS コンパイラ基盤を用いて，水平・垂直分散モジュールのインターフェース定義から中間系への自動変換を行う援用プログラムも並行して作成した．

関数型言語系の上のハードウェアコンパイラの機能拡張については，具体的には Objective Caml 関数型言語系を台言語として，その上の Syntax sugar として再帰的データ構造を用いた sub-circuit 定義向けの回路記述モジュールを構築し，対象並列回路をスケーラブルな形で記述可能にすることに成功した．

実際の回路規模を対象とした各種検証系向けコード生成器の性能評価実施については，回路記述モジュールが生成する回路情報の内部表現（中間系）に基づき，Verilog-HDL や VHDL といった下位ハードウェア記述言語向けのコード生成器を開発した．

定理証明器ならびにモデル検査器の，グリッドコンピューティング環境上への実装については，定理証明器（プルーフチェッカ）と NuSMV, SPIN モデル検査器に対して，並列コア搭載高性能プロセッサ上での稼働性能評価ならびにネットワーク接続された PC クラスタ機（現有設備）を用いた性能評価を継続的に行った．

最後に，システム統合のため，状態空間の分割・合成を行うためのアルゴリズム開発と並列化ライブラリを利用したプログラム開発を行った．具体的には，COINS コンパイラ基盤を用いて，CUDA アーキテクチャ向け水平・垂直分散モジュールのインターフェース定義から HID 中間系への自動変換を行う援用プログラム（Melasy2）も並行して作成した．

５．主な発表論文等

（研究代表者，研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 8 件）

[1] Sho NISHIDA, Katsumi WASAKI : Structural Analysis and Retargetable Netlist Generation using an Upstream Hardware Compiler : Melasy+ ; International Journal of Advanced Computer Science, 3(1), 26-32, 2013.（査読有）

[2] Naoki MIYAMOTO, Katsumi WASAKI : An Integrated Design and Verification Environment Handling the Transformation from Upstream Design to the Model Checking Process ; International Journal of Advancements in Computing Technology, 4(14), 372-380, 2012.（査読有）

[3] Hiroshi YAMAZAKI, Czeslaw BYLINSKI, Katsumi WASAKI : Morphology for Image Processing, Part I ; Formalized Mathematics, 20(1), 61-63, 2012.（査読有）

[4] Sho NISHIDA, Katsumi WASAKI : Retargetable Netlists Generation and Structural Synthesis based on A Meta Hardware Description Language : Melasy+ ; Proceedings of the 9th International Conference on Information Technology : New Generations (ITNG2012), 827-830, 2012.（査読有）

[5] Kazuto IDE, Katsumi WASAKI : Improved Analysis Algorithms of Free-Choice Nets for Behavioral Properties ; Advances in Information Technology and Applied Computing, (1), 195-200, 2012.（査読有）

[6] Bishnu Prasad GAUTAM, Katsumi WASAKI : SOA-based Campus Administration Management System using Multi-layered Architecture : Campus-SIA ; DPSWS2012, 219-226, 2012.（査読有）

[7] Yutaka YAMADA, Katsumi WASAKI : Automatic Generation of SPIN Model Checking Code from UML Activity Diagrams ; International Journal of Advancements in Computing Technology, Vol.3, No.8, pp.189-197, 2011.（査読有）

[8] Yutaka YAMADA, Katsumi WASAKI : Automatic Generation of SPIN Model Checking Code from UML Activity

Diagram and Its Application to Web Application Design；Proceedings of the 7th International Conference on Digital Content, Multimedia Technology and its Applications (IDCTA2011), 139-144, 2011.（査読有）

〔学会発表〕（計 15 件）

[1] 大羽陽介, 和崎克己：LOTOS を用いたシストリックアレイ並列計算モデルの動的再構成法；平成 25 年度電子情報通信学会信越支部大会講演論文集, (1B-4), 9, 2013 年 10 月 5 日, 長岡技術科学大学

[2] 井出和人, 和崎克己：活性安全自由選択ネットの被覆マークグラフへの分割および活性化マーキング導出法；平成 25 年度電子情報通信学会信越支部大会講演論文集, (1C-5), 14, 2013 年 10 月 5 日, 長岡技術科学大学

[3] 太田淳也, 和崎克己：ペトリネット援用ツールにおける状態空間生成アルゴリズムの並列化と実装；平成 25 年度電子情報通信学会信越支部大会講演論文集, (2A-4), 22, 2013 年 10 月 5 日, 長岡技術科学大学

[4] 太田淳也, 和崎克己:ペトリネット援用ツールを用いたモデル設計とポスト検証ツール向け状態空間生成アルゴリズム；FIT2013（第 12 回情報科学技術フォーラム）講演論文集, (A-015), 171-174, 2013 年 9 月 5 日, 鳥取大学

[5] 井出和人, 和崎克己:活性安全自由選択ネットの被覆マークグラフへの分割アルゴリズムと実装；FIT2013（第 12 回情報科学技術フォーラム）講演論文集, (A-016), 175-178, 2013 年 9 月 5 日, 鳥取大学

[6] 小林一平, 和崎克己：並行ループを有するワークフローネットに対する活性化マーキング法の提案；平成 24 年度電子情報通信学会信越支部大会講演論文集, (1D-4), 19, 2012 年 10 月 13 日, 新潟大学

[7] 太田淳也, 和崎克己：階層化ペトリネットツールによるモデル設計と状態空間生成及び検査ツール連携；平成 24 年度電子情報通信学会信越支部大会講演論文集, (2D-3), 37, 2012 年 10 月 13 日, 新潟大学

[8] 西田　翔, 和崎克己：COINS コンパイラ基盤を用いた並列処理記述言語 Melasy2 のフロントエンド設計；平成 24 年度電子情報通信学会信越支部大会講演論文集, (2D-5), 39, 2012 年 10 月 13 日, 新潟大学

[9] 井出和人, 和崎克己：自由選択ネットの活性・安全性判定解析アルゴリズム改善と援用ツールへの実装；FIT2012（第 11 回情報科学技術フォーラム）, (RA-003), 17-21, 2012 年 9 月 5 日, 法政大学（査読有）

[10] 西田　翔, 魚住有記歌, 和崎克己：上位ハードウェア設計言語 Melasy+ による NuSMV コード生成と設計検証；FIT2012（第 11 回情報科学技術フォーラム）, (C-026), 319-322, 2012 年 9 月 5 日, 法政大学

[11] 西田　翔, 和崎克己：上位ハードウェア設計言語 Melasy+ が生成する中間表現を用いた様々な構造解析とコード生成；平成 23 年度電子情報通信学会 信州大学 Student Branch 論文発表会 講演論文集, 1, 2011 年 12 月 20 日, 信州大学

[12] 宮本直樹, 和崎克己：上流設計からモデル検査プロセスまでの一貫設計検証環境；電子情報通信学会 2011 年度ソフトウェアインタプライズモデリング研究会ワークショップ, 信学技報（SWIM2011-19）, 111(308), 7-12, 2011 年 11 月 18 日, 東海大学.(査読有)

[13] 西田　翔, 和崎克己：上位ハードウェア記述言語 Melasy+ から生成されたネットリストに対する階層的構造解析；平成 23 年度電子情報通信学会信越支部大会講演論文集, (2D-5), 39, 2011 年 10 月 8 日, 新潟工科大学

[14] 西田　翔, 和崎克己：上位ハードウェア記述言語 Melasy+ が生成した中間表現に対するネットリスト生成と静的解析；平成 23 年度電気関係学会東海支部連合大会講演論文集, (I1-1), 1page(CD-ROM), 2011 年 9 月 26 日, 三重大学

[15] 宮本直樹, 和崎克己：UML シーケンス図の構造記述から線形時相論理式への自動変換手法；FIT2011（第 10 回情報科学技術フォーラム）講演論文集, (B-028), 311-314, 2011 年 9 月 9 日, 函館大学

〔その他〕
ホームページ・作成したツール公開

[1] 信州大学研究者総覧（業績データ）
http://soar-rd.shinshu-u.ac.jp/profile/ja.gCnejaTN.html#books_articles_etc

[2] Mizar Proof Checking System
http://markun.cs.shinshu-u.ac.jp/mirror/mizar/

[3] Formalized Mathematics（論文誌）
http://versita.metapress.com/content/121073/

[4] HiPS：Hierarchical Petri net Simulator
http://hips-tools.sourceforge.net/wiki/

６．研究組織

(1)研究代表者

和﨑　克己（WASAKI, Katsumi）
信州大学・工学部・教授
研究者番号：70271492

(2)研究分担者　　なし

(3)連携研究者　　なし