様式 C-19

科学研究費補助金研究成果報告書

平成２３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：2008～2010
課題番号：２０５００１３０
研究課題名（和文）　関数型言語系とグリッド環境上のプルーフチェッカを融合した超並列演算器の設計検証法
研究課題名（英文）　Design verification method of massively parallel arithmetic unit combined using a functional language and the Grid computing system
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

研究成果の概要（和文）：　プルーフチェッカ（Proof Checker）を，ネットワーク環境上へ実装し，並列システムの検証能力の向上を図る．対象回路の構成情報は，関数型言語系の上で記述し，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る．並列性実現のため「パイプライン機構」を説明する計算モデルとして，ペトリネット表現モデルを導入した．次に，関数型言語系上のハードウェアコンパイラを開発した．更に検証済み演算器の形式検証を実施した．

研究成果の概要（英文）：　The main outcome of this project is to improve the ability to verify that the parallel system. For instance, A proof checker (mathematical theorem prover) has been implemented on the network environment. The target information of circuit configurations describes using a functional language. The output code from the compiler uses to prove the sequence of proof expressions by proof checker. To achieve parallelism, this research project introduced a representation model by Petri net. The "pipeline" mechanism is used as a computational model to explain. Next, this project developed a meta hardware compiler based on a functional programming language. Finally, several formal verification tools have tested in the term of project.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,600,000 円	480,000 円	2,080,000 円
２００９年度	1,200,000 円	360,000 円	1,560,000 円
２０１０年度	700,000 円	210,000 円	910,000 円
年度			
年度			
総　計	3,500,000 円	1,050,000 円	4,550,000 円

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

「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（Proof Checker）を用いて証明する手法について検討を行ってきた．

構築した数学構造としては，回路内の全信号点を表す状態空間，入出力信号間の写像で定義される演算子，演算に必要な入力信号点を表す演算子から信号点への写像，及び演算結果を表す演算子から出力信号点への写像，といった４つの空間と写像の対として定義した，多ソート代数構造を用いた．この代数計

算モデルの正当性の証明をプルーフチェッカを用いて行う．

検証済みの計算モデルを VHDL（ハードウェア記述言語）などへ自動変換し，ゲートアレイ試作用デバイスを用いて並列演算器の実装を行い，動作検証を行った．しかしながら，超大規模集積回路（VLSI）へ実装したいパイプライン型超並列演算器などの検証時，1 台のプロセッサを利用するのみでは，論理検証とハードウェア変換のための計算時間が膨大で，この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環境の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としては Globus を使用し，並列コンピューティング環境としては MPICH-G2 を用いて多数のプロセッサを同時に稼動させ，プルーフチェッカの並列化を行う．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．PE の論理演算子，演算子とハードウェアゲートとの関係，ゲート論理演算器の計算を多ソート代数でモデル化する．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．これによって，多数の PE 群の動作検証のための問題サイズを分割することで，グリッドネットワーク上のプルーフチェッカによる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．業界標準の Verilog-HDL ハードウェア記述言語から，関数型言語系への自動変換は極めて容易である．

以上，(1)(2)の方策と融合により，形式検証系と回路設計との間の概念障壁（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．

(3) 国産高速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として誠にふさわしいと考えられる．

３．研究の方法

(1) 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，超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，プルーフチェッカへの証明式の列を得る．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．

(2) 研究方法の要旨：最初に「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する．他方，並列性実現のため「パイプライン機構」を説明する計算モデルとして，ペトリネット表現モデルを導入する．次に，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．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．次年度以降は，ハードウェアコンパイラの作成と並列化プルーフチェッカの性能評価を行う．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．性能評価のために，ゲートアレイ配置配線ソフトウェアを導入し，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．最後に，関数型言語系の上のハードウェアコンパイラを利用して，実際の回路規模を対象とした検証系の性能評価を実施する．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

(1) 平成 20 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る．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．以下に各ステップの詳細について述べる．

① 「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．

② 並列性実現のため「パイプライン機構」を説明する計算モデルとして，ペトリネット表現モデルを導入した．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．

③ 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 1）．

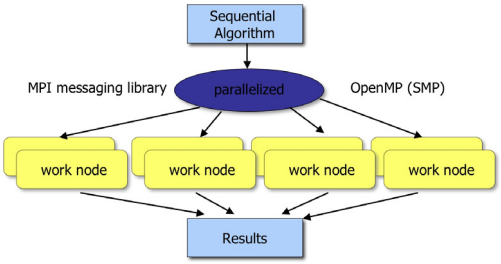

図 1: 逐次実行する自動推論プログラムをグリッドコンピューティング環境上へ実装

(2) 平成 21 年度においては，ハードウェアコンパイラの作成と並列化プルーフチェッカの性能評価を行った．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した．性能評価のために，ゲートアレイ配置配線ソフトウェアを使用し，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拡充した．以下に各ステップの詳細について述べる．

① 関数型言語系上のハードウェアコンパイラ開発：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 2）．

② 並列化プルーフチェッカの性能評価：検証対象は，パイプラインあるいはトーラス接続された並列演算器（PE）とした．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こととした．

③ 形式検証系に関する海外共同研究者（Canada，France）との合同調査研究の継続：実施体制としては，・申請者：並列化システム構築とコンパイラ開発，・Canada 研究者：ネットワーク・オートマタによる問題分割の理論検討，・France 研究者：検証対象（超並列演算器）の仕様作成と関数型言語系の保守，という構成をとった．

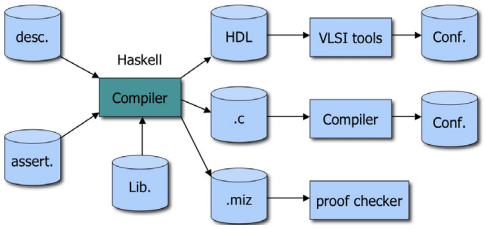

図 2: Haskell 関数型言語系の上に実装したハードウェアコンパイラと HDL・プルーフチェッカ用証明列の自動生成の流れ

(3) 平成 22 年度においては，プルーフチェッカ統合を行ったハードウェアコンパイラの拡張と実稼働試験ならびに関連ケーススタディ評価を行った．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，この言語系からの中間出力を経由して，VHDL ハードウェア記述言語が自動的に得られるようにした．統合設計検証環境の評価のために，ゲートアレイ配置配線ソフトウェアを使用し，検証済み演算器のシミュレーション・形式検証を行った．検証ケーススタディとして高機能分散バスアービタ，マルウェア静的分類アルゴリズム，無線通信システム応用等を行った．以下に各ステップの詳細について述べる．

① プルーフチェッカ統合を行ったハードウェアコンパイラの拡張：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した．中間出力を経由して，VHDL ハードウェア記述言語コードが自動的に得られるように変換を行う援用プログラムを並行して作成した．

② 検証済み演算器のシミュレーション・形式検証：検証対象は，パイプラインあるいはシストリック・トーラス接続された並列演算モデル(PE)とした．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こととした．これにより，分散バスアービタなどの検証に成功した．

③ 形式検証系に関する海外共同研究者との合同調査研究の継続：実施体制としては，・申請者：並列化システム構築とコンパイラ開発，・Canada 研究者：ネットワーク・オートマタによる問題分割の理論検討，・France 研究者：検証対象（超並列演算器）の仕様作成と関数型言語系の保守，という構成をとった．

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 5 件）

[1] Hiroyuki MATSUURA, Masahiro NAKANO, Katsumi WASAKI：Quantum Circuits, Lots, Interference and Basis of Neuro-Computations ； ICIC Express Letters, ICIC International, 3, (1), 7-14, 2009. （査読有）

[2] Naoki IWASAKI, Katsumi WASAKI：A Meta Hardware Description Language Melasy for Model-Checking Systems ； Proceedings of the 5th International Conference on Information Technology：New Generations (ITNG2008), 273-278, 2008.（査読有）

[3] Katsumi WASAKI：Correctness of the Stability of the 4-2 Compressor Cell for Partial Product Reduction in Parallel Multiplier Circuits ； Mechanized Mathematics and Its Applications, 7, (2), 17-25, 2008.（査読有）

[4] Katsumi WASAKI：Stability of the 4-2 Binary Addition Circuit Cells. Part I ； Formalized Mathematics, 16, (4), 377-387, 2008.（査読有）

[5] Katsumi WASAKI：Stability of n-Bit Generalized Full Adder Circuits (GFAs). Part II；Formalized Mathematics, 16, (1), 73-80, 2008.（査読有）

〔学会発表〕（計 13 件）

[1] Kousuke SHIROTORI, Katsumi WASAKI：Automatic Code Generation and Integrated Testing for Model Checking and Hardware Implementation using A Meta Description Language：Melasy+, 平成 22 年度 IEEE 信越支部セッション講演論文集, (11B-4), 206, 2010 年 10 月 2 日，長岡技術科学大学

[2] Pratima K. SHAH, Katsumi WASAKI：Upper Scalable Modeling of The Stream Processing Architecture by using A Specification Language：LOTOS；平成 22 年度 IEEE 信越支部セッション講演論文集, (11B-2), 204, 2010 年 10 月 2 日，長岡技術科学大学

[3] 白鳥航亮，和﨑克己 ： 上位ハードウェア

設計言語 Melasy+ による VHDL コード生成と動作検証；FIT2010（第 9 回情報科学技術フォーラム） 講演論文集, 1, (C-002), 371-374, 2010 年 9 月 8 日, 九州大学 伊都キャンパス

[4] 花里貴裕, 白鳥航亮, 和﨑克己 ： 上位言語 Melasy+ による自己テスト機能付バスアービタの設計と NuSMV を用いた検証 ； 情報処理学会第 72 回全国大会講演論文集, 1, (1M-4), 151-152, 2010 年 3 月 10 日, 東京大学 本郷キャンパス

[5] 白鳥航亮, 和﨑克己 ： 上位ハードウェア記述言語 Melasy+ に対する仕様パターン埋め込みと展開 ； 情報処理学会第 72 回全国大会講演論文集, 1, (1M-3), 149-150, 2010 年 3 月 10 日, 東京大学 本郷キャンパス

[6] 松山千尋, 和﨑克己 ： 時間ペトリネットを用いた非同期論理ゲートのモデルと階層化回路合成 ； 平成 21 年度電子情報通信学会信越支部大会講演論文集, (2D-3), 38, 2009 年 10 月 3 日, 信州大学 長野(工学)キャンパス

[7] 桑島芳朗, 和﨑克己 ：HDCaml ハードウェア上位記述に対する LOTOS コード生成系について ； 平成 21 年度電子情報通信学会信越支部大会講演論文集, (2B-4), 29, 2009 年 10 月 3 日, 信州大学 長野(工学)キャンパス

[8] 白鳥航亮, 和﨑克己 ： 上位記述言語 Melasy+ を用いたセル型 FIFO メモリの自己回復性の検証 ； 平成 21 年度電子情報通信学会信越支部大会講演論文集, (2B-3), 28, 2009 年 10 月 3 日, 信州大学 長野(工学)キャンパス

[9] 松山千尋, 和﨑克己 ：Time-Petri Net を用いた非同期回路のモデル化と階層化設計 ； FIT2009（第 8 回情報科学技術フォーラム） 講演論文集, 1, (C-038) , 523-526, 2009 年 9 月 4 日,東北工業大学 八木山キャンパス

[10] 白鳥航亮, 和﨑克己 ： 上位ハードウェア設計言語 Melasy+ による自己回復機能付き FIFO メモリの記述と検証 ；FIT2009（第 8 回情報科学技術フォーラム）講演論文集, 1, (C-011) , 451-454, 2009 年 9 月 3 日,東北工業大学 八木山キャンパス

[11] 伊藤比佐志, 和﨑克己 ： 整数有限列上の加算・乗算アルゴリズムの正当性証明に関する検討 ； 日本 Mizar 学会 2009 年春期総会予稿集 （ Proceedings of the Technical Symposium and General Assembly of Mizar JAPAN）, 4, (1), 6pages, 2009 年 6 月 19 日, 信州大学 長野(工学)キャンパス総合研究棟

[12] 野村達雄, 岩﨑直木, 和﨑克己 ： モデル検査に対応する上位ハードウェア記述言語 Melasy の VHDL コード生成 ； 情報処理学会第 71 回全国大会講演論文集, 1, (2L-2), 171-172, 2009 年 3 月 11 日, 立命館大学びわこ・くさつキャンパス

[13] 岩﨑直木, 野村達雄, 和﨑克己: モデル検査に対応する上位ハードウェア記述言語 Melasy と XML 中間表現 ； 情報処理学会第 71 回全国大会講演論文集, 1, (2L-1), 169-170, 2009 年 3 月 11 日, 立命館大学びわこ・くさつキャンパス

〔その他〕
ホームページ等
[1] 信州大学研究者総覧
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/

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