様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

# 科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月 ２３ 日現在

機関番号：１３６０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2022
課題番号：１９Ｋ１１８２１

研究課題名（和文）大規模高速な形式検証を実現するメタスケーラブル定理証明器と並列モデル検査器の融合

研究課題名（英文）Fusion of Meta-Scalable Theorem Prover and Parallel Model Checker to Realize Large-Scale Fast Formal Verification

研究代表者

和崎　克己（Wasaki, Katsumi）

信州大学・学術研究院工学系・教授

研究者番号：７０２７１４９２

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：検証対象とする回路の厳密プロパティ検査を目的とし、論理ゲート素子間の接続をメッセージパッシング型並列計算でモデル化する研究を実施した。定理証明は回路構造と接続の正当性に関するプロパティ検査を行った。スケーラブルでかつ繰り返し構造を有するPEの実例として、高速乗算回路の高基数コンプレッサモジュールについて実際に多ソート代数を理論的基盤とする定理証明を記述し、Mizarプルーフチェッカを用いた機械検証を行ったところ、回路合成の構造上の正しさならびに入出力関係の正しさなど所望のプロパティ検証に成功した。

研究成果の学術的意義や社会的意義
LOTOSコード生成器によって下位設計（ペトリネットモデル）が得られ、状態空間生成器を用いて初期状態から駆動するが、状態空間生成時の既生成マーキングを記憶するハッシュメモリの効率化を図るため、削除可能状態のオンライン判定アルゴリズムに関する検討を行った点に学術的意義がある。なおペトリネット検証系に関する基礎研究として、サブマーキング法を用いた状態空間の抽象化と準ホーム状態の存在検知、一般ペトリネットのSATソルバーを用いた構造解析による強L3活性構造の検知などに関する成果を得た点についても学術的意義がある。

研究成果の概要（英文）：For the purpose of rigorous property checking of circuits to be verified, a study was conducted to model the connections between logic gate elements using message-passing parallel computation. Theorem proving was done by property checking on the circuit structure and the validity of the connections. As an actual example of PE with scalable and repetitive structures, we actually wrote a theorem proof for a high radix compressor module of a high-speed multiplier circuit using multisort algebra as the theoretical basis, and performed machine verification using the Mizar proof checker. The desired properties, such as the correctness of the circuit synthesis structure and input-output relations, were successfully verified.

研究分野：数理情報学

キーワード：非同期並列システム　ハードウェアコンパイラ　定理証明器　モデル検査器　形式検証系　関数型言語系　状態空間生成　ペトリネット

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

高性能プロセッサの開発技術は進展を続けているが，一方厳密な信頼性の担保に関わる研究は未だ途上にある．プロセッサ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）の確立が喫緊の課題となっている．定理証明系を用いた非同期回路に対する正当性（プロパティ）検証も従来から行われてきたが，実サイズの並列演算器への適用例は殆ど無い．

回路モデルの実装向けデータを得るため，一般にハードウェアコンパイラを使用して上位設計データを作成し論理合成することで抽象度の低い設計とする．テスト手法やモデル検査器を使って，実サイズの並列演算器として接続し検証する際，単一の検証用プロセスを実行するのみでは，対象演算器の全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実行時間が非常に長くなり，検査工程として実用で無くなる問題が存在している．検証性能の飛躍的改善のため，定理証明系とモデル検査系をハイブリッド利用した，クラスタ基盤による検証システムの構築が課題の核心である（図 1）．

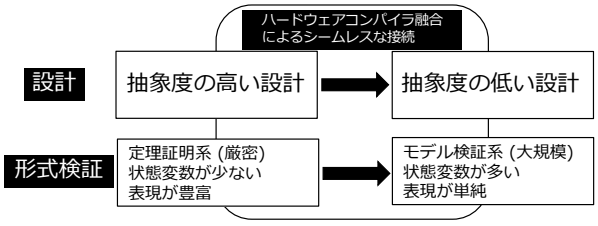


図１　定理証明器のプロパティ厳密証明と，モデル検査器による大規模な振る舞い解析をシームレスに接続．

２．研究の目的

目的 1）定理証明器のプロパティ厳密証明と，モデル検査器による大規模な振る舞い解析をシームレスに接続するために，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で融合する．

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自動生成する．プルーフチェッカが証明検査済みの数式定義・定理証明の成果を，後段で検査エンジニアが再利用可能な点が，本研究の特長となっている．

目的 2）多数の演算素子（PE）群の動作検証のため，状態空間生成を最適分割することで，メニーコアプロセッサ上での高スケーラブルな検査性能を明らかにする．

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．既に定理証明器で各 PE 単位でのプロパティ検証は完了しているが，この PE を計算目的に応じて接続した構成に対し，モデル検査器は各 PE 単位での振る舞い解析結果（状態空間）を縮約・最適分割することで，対象演算器全体の動作を現実的な速度で検証可能にする．

以上，1) 2) の戦略と系の融合により，システムの上位設計と形式検証系との間の概念障壁，即ち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いて，検証作業の高速化と信頼性向上に寄与する極めて斬新な研究を構成している．

３．研究の方法

従来，定理証明とモデル検査の処理系は別であるため，プロパティ検証で記述した再帰的・繰り返し構造などのメタ情報を，検査・検証時のモデル記述や並列化分割のためのヒントとして利用できない状況にあった．このため，検査時の分割問題の最適化が困難で，並列アクセラレータ

が直接適用できない問題があった.

今回, 定理証明器とモデル検査を組み合わせたハイブリッド検証系を, メニーコアプロセッサ上で効率良く稼働させる新たな着想を得た. 具体的には, 定理証明のプロパティ検証情報とモデル検査時の空間最適分割問題を融合し, メニーコア・クラスタ基盤上へ実装する. システム統合のため, 状態空間の最適分割・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う (図 2)

非同期回路や並行システムに関する形式化記述として, Mizar Mathematical Library (MML) を利用する. MML はオートマトンやペトリネットといった数学モデルは既に定理証明済の状態で, 本研究の証明ライブラリとして即時活用できる状態にある.

続いて, 並列化検証システム全体の性能評価を行う. 言語系からのコンパイラ出力として, 検証済みライブラリと結合して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. 実システムレベルでの性能評価のために, intel Xeon Phi 並列アクセラレータと, FPGA/CPLD 統合設計開発ツールを使用し, 検証済み演算器の実ターゲット上での稼働実験・形式検証統合システムの飛躍的な高性能化を完成する.

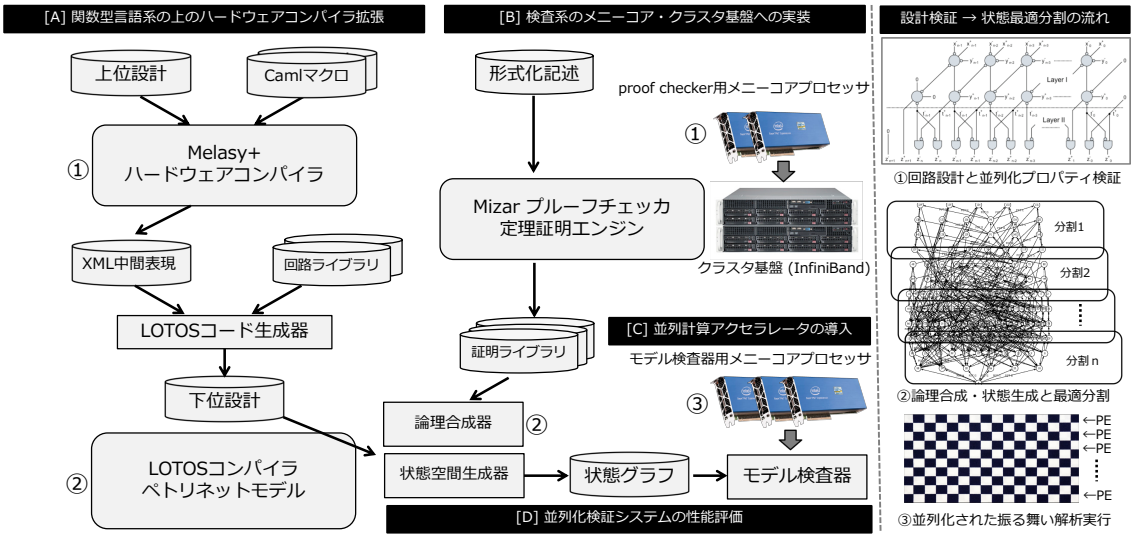


図 2　関数型言語系の上に実装した Melasy+ハードウェアコンパイラ, LOTOS コンパイラ, 定理証明系 (プルーフチェッカ), ならびにモデル検査系のハイブリッド融合構造図.

## 4. 研究成果

(1) 検証対象とする回路の厳密プロパティ検査を目的とし, 論理ゲート素子間の接続をメッセージパッシング型並列計算でモデル化する研究を実施した. 定理証明は回路構造と接続の正当性に関するプロパティ検査を行った. スケーラブルでかつ繰り返し構造を有する PE の実例として, 高速乗算回路の高基数コンプレッサモジュールについて実際に多ソート代数を理論的基盤とする定理証明を記述し, Mizar プルーフチェッカを用いた機械検証を行ったところ, 回路合成の構造上の正しさならびに入出力関係の正しさなど所望のプロパティ検証に成功した.

(2) LOTOS コード生成器によって下位設計 (ペトリネットモデル) が得られ, 状態空間生成器を用いて初期状態から駆動するが, 状態空間生成時の既生成マーキングを記憶するハッシュメモリの効率化を図るため, 削除可能状態のオンライン判定アルゴリズムに関する検討を行った. なおペトリネット検証系に関する基礎研究として, サブマーキング法を用いた状態空間の抽象化と準ホーム状態の存在検知, 一般ペトリネットの SAT ソルバーを用いた構造解析による強 L3 活性構造の検知などに関する成果を得た.

(3) 上位設計としての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関数型プログラミング言語系の上で記述するが, LOTOS コード生成器は既にフランス INRIA/VASY から CADP ツールの提供とライセンスを受けており, モデル検査が実際に実行できるまでの環境の構築は終わっており, この課題に関する研究は順著に進捗している. CADP ツール側では特にイタレーション・モデルの記述に適した LOTOS-NT(LNT)拡張言語へのサポートは可能な状態であるので, 今後は, 成果物である DILL ライブラリの LNT 化など, 今後の進捗が待たれている.

５．主な発表論文等

〔雑誌論文〕　計3件（うち査読付論文　3件／うち国際共著　0件／うちオープンアクセス　1件）

| | |
|---|---|
| １．著者名<br>Kohei FUJIMORI, Katsumi WASAKI | ４．巻<br>1346 |
| ２．論文標題<br>A Method for Improving Memory Efficiency of the Reachability Graph Generation Process in General Petri Nets | ５．発行年<br>2021年 |
| ３．雑誌名<br>Advances in Intelligent Systems and Computing, Springer | ６．最初と最後の頁<br>255-263 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/978-3-030-70416-2_33 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Katsumi WASAKI | ４．巻<br>1346 |
| ２．論文標題<br>Hardware Logic Library and High-level Logic Synthesizer Combining LOTOS and A Functional Programming Language | ５．発行年<br>2021年 |
| ３．雑誌名<br>Advances in Intelligent Systems and Computing, Springer | ６．最初と最後の頁<br>313-321 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.1007/978-3-030-70416-2_40 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスではない、又はオープンアクセスが困難 | 国際共著<br>－ |

| | |
|---|---|
| １．著者名<br>Katsumi Wasaki | ４．巻<br>28(1) |
| ２．論文標題<br>Stability of the 7-3 Compressor Circuit for Wallace Tree. Part I | ５．発行年<br>2020年 |
| ３．雑誌名<br>Formalized Mathematics | ６．最初と最後の頁<br>65-77 |
| 掲載論文のDOI（デジタルオブジェクト識別子）<br>10.2478/forma-2020-0005 | 査読の有無<br>有 |
| オープンアクセス<br>オープンアクセスとしている（また、その予定である） | 国際共著<br>－ |

〔学会発表〕　計20件（うち招待講演　0件／うち国際学会　8件）

| |
|---|
| １．発表者名<br>Daichi YAMAMICHI, Seigo SHIGENAKA, Kazuhisa NAKASHO, Katsumi WASAKI |
| ２．発表標題<br>A Web Platform for Hosting the Mizar Mathematical Library |
| ３．学会等名<br>14th Conference on Intelligent Computer Mathematics (CICM 2021), Fifth Workshop on Formal Mathematics for Mathematicians (FMM2021)（国際学会） |
| ４．発表年<br>2021年 |

１．発表者名
Hideharu Furushima, Kazuhisa Nakasho and Katsumi Wasaki

２．発表標題
Mizar数学ライブラリの定理検索を行うWebアプリケーション

３．学会等名
第24回プログラミングおよびプログラミング言語ワークショップ（PPL 2022）

４．発表年
2022年

１．発表者名
三浦朋己，和﨑克己

２．発表標題
サブマーキング法を用いたペトリネット状態空間の抽象化と準ホーム状態

３．学会等名
第20回情報科学技術フォーラム（FIT2021）

４．発表年
2021年

１．発表者名
芳澤祐大，和﨑克己

２．発表標題
一般ペトリネットのSATソルバーを用いた構造解析による強L3活性構造の検知

３．学会等名
第20回情報科学技術フォーラム（FIT2021）

４．発表年
2021年

１．発表者名
三浦朋己，和﨑克己

２．発表標題
ペトリネット構造解析によるホーム状態存在性の判定

３．学会等名
情報処理学会 第84回全国大会

４．発表年
2022年

１．発表者名
芳澤祐大，和崎克己

２．発表標題
一般ペトリネットの構造的性質を用いた強L3/L2活性構造の検知

３．学会等名
情報処理学会 第84回全国大会

４．発表年
2022年

１．発表者名
Yojiro HARIE, Katsumi WASAKI

２．発表標題
An Approach for Flow Net Subgraph to Modelling and Analysis of Flexible Manufacturing Systems

３．学会等名
31st International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2020)（国際学会）

４．発表年
2020年

１．発表者名
Yojiro HARIE, Katsumi WASAKI

２．発表標題
Analysis of the Structural Liveness and Boundedness in Weighted Free-Choice Net based on Circuit Flow Values

３．学会等名
2020 Computing Conference (CC2020)（国際学会）

４．発表年
2020年

１．発表者名
南　史弥，和崎克己

２．発表標題
特徴的構造を持つペトリネットにおける極小サイフォン検出アルゴリズムの動的選択

３．学会等名
FIT2020（第19回情報科学技術フォーラム）

４．発表年
2020年

１．発表者名
渡貫正也，和﨑克己

２．発表標題
可達判定条件が既知であるサブクラス定義に反する閉路検知機能を有するペトリネット解析ツールの開発

３．学会等名
FIT2020（第19回情報科学技術フォーラム）

４．発表年
2020年

１．発表者名
Yojiro Harie, Katsumi Wasaki

２．発表標題
An Approach for Flow Net Subgraph to Modelling and Analysis of Flexible Manufacturing Systems

３．学会等名
The 31st International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2020)（国際学会）

４．発表年
2020年

１．発表者名
張江洋次朗，和﨑克己

２．発表標題
フローネット変換を用いたペトリネットの構造的活性・有界性解析手法

３．学会等名
電子情報通信学会 第32回 回路とシステムワークショップ（KWS32）

４．発表年
2019年

１．発表者名
Yuta YOSHIZAWA, Katsumi WASAKI

２．発表標題
Detection of Strictly L3-Live Structures by Structural Analysis of General Petri Net Using SAT-Solver

３．学会等名
19th International Conference on Information Technology-New Generations (ITNG 2022)（国際学会）

４．発表年
2022年

１．発表者名
Tomoki MIURA, Katsumi WASAKI

２．発表標題
Space Abstraction and Quasi-Home States of Petri Nets Using the Submarking Method

３．学会等名
19th International Conference on Information Technology-New Generations (ITNG 2022)（国際学会）

４．発表年
2022年

１．発表者名
Hideharu FURUSHIMA, Daichi YAMAMICHI, Seigo SHIGENAKA, Kazuhisa NAKASHO, Katsumi WASAKI

２．発表標題
An Integrated Web Platform for the Mizar Mathematical Library

３．学会等名
15th Conference on Intelligent Computer Mathematics (CICM 2022)（国際学会）

４．発表年
2022年

１．発表者名
Yuya CHIBA, Katsumi WASAKI

２．発表標題
Description and Verification of Systolic Array Parallel Computation Model in Synchronous Circuit using LOTOS

３．学会等名
20th International Conference on Information Technology-New Generations (ITNG 2023)（国際学会）

４．発表年
2023年

１．発表者名
千葉悠矢，和崎克己

２．発表標題
グローバルクロック同期型シストリックアレイ並列計算モデルのLOTOS記述と振る舞い検証

３．学会等名
第21回情報科学技術フォーラム（FIT2022）

４．発表年
2022年

１．発表者名
三浦朋己，和﨑克己

２．発表標題
ペトリネット構造解析とオカレンスネットを用いたホーム状態の判定

３．学会等名
第21回情報科学技術フォーラム（FIT2022）

４．発表年
2022年

１．発表者名
芳澤祐大，和﨑克己

２．発表標題
一般ペトリネットにおける構造的性質を用いた強L2活性構造の存在性判定

３．学会等名
第21回情報科学技術フォーラム（FIT2022）

４．発表年
2022年

１．発表者名
千葉悠矢，和﨑克己

２．発表標題
グローバルクロック同期型シストリックアレイ並列モデルに対するモデル検査器を用いた多様な振る舞い解析

３．学会等名
情報処理学会 第85回全国大会

４．発表年
2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

| | 氏名<br>（ローマ字氏名）<br>（研究者番号） | 所属研究機関・部局・職<br>（機関番号） | 備考 |
|---|---|---|---|

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

| 共同研究相手国 | 相手方研究機関 | | | |
|---|---|---|---|---|
| ポーランド | University of Bialystok | | | |