様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年６月８日現在

機関番号：１５４０１
研究種目：基盤研究（C）
研究期間：２００９～２０１２
課題番号：21500016
研究課題名（和文）　FPGA の抽象モデル化とハードウェアアルゴリズムの評価の研究

研究課題名（英文）　Research on abstract models of FPGAs and evaluation of hardware algorithms
研究代表者
中野　浩嗣（NAKANO Koji）
広島大学・大学院工学研究院・教授
研究者番号：30281075

研究成果の概要（和文）：
FPGA を用いたさまざまな高速化を検討した結果，FDFM(Few DSP blocks and Few memory blocks)アプローチを考案した．最近の FPGA には，DSP ブロックとメモルブロックが大量に搭載されている．我々が提案する FDFM アプローチとは、少数の DSP ブロックとメモリブロックを用いて，複雑な計算をするコプロセッサを組み込むという考え方である．このアプローチにより，RSA 暗号処理や画像のパターマッチングなどが高速に行えることを実証した．

研究成果の概要（英文）：
We have investigated various approaches for accelerating computation using FPGAs and found a new approach that we call FDFM(Few DSP blocks and Few memory blocks) approach. Recent FPGAs have a number of embedded DSP blocks and memory blocks. The FDFM approach uses few DSP blocks and few memory blocks to install a co-processor to compute complicated computations. We have shown that RSA encryption, image pattern matching, etc. can be done very fast.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	８００，０００	２４０，０００	１，０４０，０００
２０１０年度	１，１００，０００	３３０，０００	１，４３０，０００
２０１１年度	７００，０００	２１０，０００	９１０，０００
２０１２年度	８００，０００	２４０，０００	１，０４０，０００
年度			
総　計	３，４００，０００	１，０２０，０００	４，４２０，０００

研究分野：情報工学
科研費の分科・細目：情報学・情報学基礎
キーワード：　FPGA，アルゴリズム，組込みハードウェア，ブロック RAM

１．研究開始当初の背景

プロセッサの動作周波数を向上させることによる高速化は限界にきており，プロセッサメーカは，１つの LSI チップに複数のプロセッサを搭載するマルチコア化の方向に進んでいる．　一方，アルゴリズムのハードウェア化による高速化は，通常の台数効果をはるかに凌駕することもある．実際，書き換え可能な FPGA にアルゴリズムを回路化してダウンロードすることにより，高速化を達成する研究が盛んに行われている．　FPGA(Field Programmable Gate Array とは，ユーザの設計した論理回路データをダウンロードすることにより，内部回路を定義・変更することができる集積回路である．FPGA には，LUT(ルックアップテーブル)，フリップフロ

ップ，ブロックメモリ，乗算器，などの組込み回路が大量（数千～数十万程度）に分散配置されており，それらの初期データとプログラマブル配線を設定することにより，任意の論理回路を埋め込むことができる．

しかし，さまざまに行われてきた FPGA を用いた計算の高速化の研究では，特定の FPGA へ実装した場合の使用回路量と計算時間でハードウェアアルゴリズムの評価を行なってきた．異なる FPGA に実装した場合，直接的な性能比較はできないので，既知の実装結果に対して，新たに考案したハードウェアアルゴリズムが真に優れているかどうかが明確でない．FPGA のデバイスファミリーやスピードグレードは膨大であり，供給停止が頻繁にあるので，同じ FPGA を手にいれるのは必ずしも可能でなく，直接比較は困難である．

２．研究の目的

本研究はこのような状況を鑑み FPGA のアーキテクチャをさまざまなレベルで抽象化した FPGA モデルを提案し，そのモデル上でさまざまな問題を解く効率よいハードウェアアルゴリズムを設計することである．設計したハードウェアアルゴリズムを FPGA に実装・性能評価を行い，提案した FPGA モデルの妥当性を検証する．この研究成果により，FPGA を利用して問題を高速に解きたいときに，FPGA モデルをターゲットにハードウェアアルゴリズムを最適化しておけば，実際に FPGA で効率よく動作する論理回路を得ることができ，DSP 以外の幅広い分野に FPGA を利用するのが容易となる．また，FPGA 向けのハードウェアアルゴリズムの性能を FPGA モデル上で理論的に評価できるので，FPGA 向けハードウェアアルゴリズムの客観的評価が行えるようになる．

３．研究の方法

提案した複数の FPGA モデル上に，さまざまなハードウェアアルゴリズムを設計する．これらのハードウェアアルゴリズムを FPGA に実装し，ハードウェア量と計算時間の評価を行う．FPGA モデル上でのハードウェア量・計算時間の評価と FPGA に実装した場合の実験によるハードウェア量・計算時間の適合度を調べる．結果によっては，より実際の FPGA 反映するように，FPGA モデル自体を修正して，その上でハードウェアアルゴリズムを再設計・評価する．そして，同様に，FPGA モデルと実際の FPGA でのハードウェア量・計算時間の一致度を検証する．

実際の FPGA のアーキテクチャの詳細をモデルに多く取り入れるほど性能評価が正確になるが，FPGA モデルは複雑になり，ハードウェアアルゴリズムの設計と評価が困難になる．アーキテクチャの本質的でない部分を省略したなるべく単純なモデルにすれば，設計と評価が容易になるが，理論的性能評価が実験的評価と一致しなくなる．さまざまなハードウェアアルゴリズムの理論的な評価と実装による評価を比較し，FPGA モデルの複雑さと理論的・実験的評価の一致度のトレードオフのバランスがよい FPGA モデルを最終的に提案する．そしてそのような FPGA モデル状でハードウェアアルゴリズムを評価・最適化し，実際の FPGA に回路化することにより，モデルの正当性を検証する．さらには，実用的な処理を題材に，FPGA を用いた究極の高速化を目指す．

４．研究成果

さまざまな FPGA モデルを検討した結果，１つの有望な方法として，FDFM(Few DSP blocks and Few memory blocks)アプローチを考案した．最近の FPGA には，DSB ブロックとメモルブロックが大量に搭載されている．我々が提案する FDFM アプローチとは、少数の DSP ブロックとブロック RAM を用いて，複雑な計算をするコプロセッサを組み込むという考え方である．この方法により複雑な計算が少ないリソースで行うことができ、また高スループットが必要な場合はこのコプロセッサを大量に並べるということも可能であり，フレキシブルな設計が可能となる．さらに，FPGA に高速パターンマッチングアルゴリズムや多倍長演算対応 CPU を実装し，性能評価を行った．特に，多倍長演算対応 CPU を用いて，RSA 暗号化のための多倍長演算アルゴリズムを実装した．RSA 暗号化をハードウェア実装するのは複雑であり，設計が困難であった．多倍長演算 CPU はこれをソフトウェア的に容易に実装でき，かつハードウェア実装と同等の性能が実現できる．

また，付随する研究の成果として，メモリブロックを容易に用いる方法についても検討した．現在の FPGA では，同期読み出し可能なメモリブロックのみサポートされている．非同期読み出しが可能であれば，設計が容易であるが，デバイスの高速化のためにサポートされていない．そこで，非同期読み出しのメモリブロックを想定して設計しておけば，自動的に同期読み出しに変換できることを示した．これにより，ハードウェアアルゴリズム設計者は，設計が容易な非同期読み出しのメモリブロックを仮定して容易に差設計作業が行えるようになる．

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 Yuki Ago, Yasuaki Ito, Koji Nakano, An FPGA implementation for neural networks with the FDFM processor core approach, International Journal of Parallel, Emergent and Distributed Systems, to appear.,2013. 査読有

② Yasuaki Ito, Koji Nakano and Song Bo, The Parallel FDFM Processor Core Approach for CRT-based RSA Decryption, International Journal of Networking and Computing, Vol. 2, No. 1, pp. 79–96, January 2012. http://www.ijnc.org/ 査読有

③ Md. Nazrul Islam Mondal, Koji Nakano and Yasuaki Ito, An Algorithm to Obtain Circuits with Synchronous RAMs, Journal of Communication and Computer, Volume 9, Number 5, pp. 547-559, May 2012. http://www.davidpublishing.com/ 査読有

④ Md. Nazrul Islam Mondal, Koji Nakano, Yasuaki Ito, A Rewriting Approach to Replace Asynchronous ROMs with Synchronous Ones for the Circuits with Cycles, International Journal of Networking and Computing, Vol. 2, No. 2, pp. 269-290, July 2012. http://www.ijnc.org/ 査読有

⑤ Yasuaki Ito, Koji Nakano, Efficient Exhaustive Verification of the Collatz Conjecture using DSP blocks of Xilinx FPGAs International Journal of Networking and Computing, Vol. 1, No.1, pp. 49–62, Jan 2011. http://www.ijnc.org 査読有

⑥ Song Bo, Kensuke Kawakami, Koji Nakano, Yasuaki Ito An RSA Encryption Hardware Algorithm using a Single DSP Block and a Single Block RAM on the FPGA International Journal of Networking and Computing, Vol. 1, No.2, pp. 277–289, July, 2011. http://www.ijnc.org/、査読有

⑦ Md. Nazrul Islam Mondal, Koji Nakano, Yasuaki Ito, A Graph Rewriting Approach for Converting Asynchronous ROMs into Synchronous Ones, IEICE TRANSACTIONS on Information and Systems Vol.E94-D No.12 pp.2378-2388, Dec 2011. http://dx.doi.org/10.1587/transinf.E94.D.2378 査読有

⑧ Yasuaki Ito and Koji Nakano, Low-latency Connected Component Labeling Using an FPGA, International Journal on Foundations of Computer Science, Vol.21, No. 3. pp. 405-425, June 2010. doi: 10.1142/S0129054110007337 査読有

〔学会発表〕（計８件）

① Md. Nazrul Islam Mondal, Koji Nakano, and Yasuaki Ito, An Algorithm to Remove Asynchronous ROMs in Circuits with Cycles, International Conference on Networking and Computing, 大阪、日本、２０１１年１１月３０日

② Yuki Ago, Atsuo Inoue, Koji Nakano, and Yasuaki Ito, The Parallel FDFM Processor Core Approach for Neural Networks, International Conference on Networking and Computing, 大阪、日本、２０１１年１１月３０日

③ Bo Song, Yasuaki Ito, and Koji Nakano, CRT-based Decryption using DSP blocks on the Xilinx Virtex-6 FPGA, Workshop on Advances in Parallel and Distributed Computational Models,アンカレッジ、米国、２０１１年５月１６日

④ Ian McLoughlin and Koji Nakano, A Perspective on the Experiential Learning of Computer Architecture, IEEE/ACM Int'l Conference on Cyber, Physical and Social Computing (CPSCom), 杭州、中国、２０１０年１２月１８日

⑤ Bo Song, Kensuke Kawakami, Koji Nakano, and Yasuaki Ito, An RSA Encryption Hardware Algorithm Using a Single DSP Block and a Single Block RAM on the FPGA, International Conference on Networking and Computing, 広島、日本、２０１０年１１月１７日.

⑥ Md. Nazrul Islam Mondal, Koji Nakano, and Yasuaki Ito, A Rewriting Algorithm to Generate AROM-free Fully Synchronous Circuits, International Conference on Networking and Computing, 広島、日本、２０１０年１１月１７日.

⑦ Yasuaki Ito, Koji Nakano, Efficient Exhaustive Verification of the Collatz Conjecture using DSP48E blocks of Xilinx Virtex-5 FPGAs, アトランタ、米国、２０１０年４月１９日

⑧ Yasuaki Ito, Koji Nakano, A Hardware-Software Cooperative Approach for the Exhaustive Verification of the Collatz Cojecture, International Symposium on Parallel and Distributed Processing with Applications, 成都、中国、２００９年８月９日

〔その他〕
ホームページ等
http://www.cs.hiroshima-u.ac.jp/

６．研究組織
(1)研究代表者
中野　浩嗣　(NAKANO KOJI)
広島大学・大学院工学研究院・教授
研究者番号：30281075
(2)研究分担者
伊藤　靖朗（ITO YASUAKI）
広島大学・大学院工学研究院・助教
研究者番号：40397964
(3)連携研究者
（　　）
研究者番号：