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 24 年　5 月　12 日現在

機関番号：１５４０１
研究種目：若手研究(B)
研究期間：2008　～ 2011
課題番号：20700030
研究課題名（和文）　部分計算による FPGA を用いた計算高速化理論の確立

研究課題名（英文）　A study on establishment of a theory for accelerating computation based on partial-computation using FPGAs
研究代表者
伊藤　靖朗　(YASUAKI ITO)
広島大学・大学院工学研究院・助教
研究者番号：４０３９７９６４

研究成果の概要（和文）：
本研究では､部分計算によるＦＰＧＡを用いた計算高速化理論の確立を目指す.部分計算とは,問題のパラメータの一部を固定することで問題を解く時間を大幅に短縮する手法のことである。この部分計算の性質を満たす問題に対して書き換え可能な LSI である FPGA（Field Programmable Gate Array）を用い，高速計算化を様々な問題、画像の２値処理、２値画像のラベリング処理、コラッツ予想の検証、RSA 暗号計算に対して高速化を実現した。

研究成果の概要（英文）：
In this study, we have tried to establish a theory of accelerating computation using FPGA based on the notion of partial computation. Partial computation is a computing technique to reduce computing time by fixing a part of parameters of a problem. For various problems that have a property of the partial computation, such as image halftoning, image component labeling, verification of Collatz conjecture, and RSA encryption, we achieved accelerating solutions using FPGAs (Field Programmable Gate Arrays) that are programmable VLSIs.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	800,000	240,000	1,040,000
2009 年度	800,000	240,000	1,040,000
2010 年度	800,000	240,000	1,040,000
2011 年度	800,000	240,000	1,040,000
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：計算機工学
科研費の分科・細目：情報学・ソフトウェア
キーワード：FPGA, ハード・ソフト協調設計

１．研究開始当初の背景

デバイス技術の進歩により、高速なプロセッサ・CPU が開発され、様々な計算処理が短時間で行えるようになってきた。しかし、プロセッサの動作周波数の増加も鈍化しており、半導体技術の改良によるプロセッサの高速化に限界が見えてきている。一方、計算の高速化のためには、アルゴリズムを ASIC 上にハードウェア化した専用 LSI を用いる方法が有力であり、実際、隠面消去やフーリエ変換などの計算では単一プロセッサの能力をはるかに凌駕する性能を発揮している。
しかし、これは多数のユーザが要求する特殊な機能の実現であったからこそ実現したこ

とであり大量生産による低価格化が重要な鍵である。今までは普遍的な処理をハードウェア化することが常識であった。

２．研究の目的
既存の普遍的な処理をハードウェア化するという常識を打破することによってハードウェアアルゴリズムの適用範囲を拡大すると同時に、従来とは全く異なる形態で利用することにより、真に処理の高速化を図ることが本研究の目的である。

３．研究の方法
本研究では、部分計算によるＦＰＧＡを用いた計算高速化理論の確立を目指す。部分計算とは、ある性質 P を満たす問題を解決するために、FPGA を用いた部分計算ツールの開発を行う。ここである性質 P とは、以下の２つの条件からなる。その問題を解決するのに、1. 関数 f(x,y)の計算を頻繁に繰り返す必要がある。2. 関数 f(x,y)の第一引数 x は固定した値であり、第二引数 y はさまざまな値をとる。この場合、第一引数 x を中にとりこんだ関数 f'(y)(=f(x,y))が高速に計算できれば、問題を解く時間を大幅に短縮することができる。この部分計算の性質を満たす問題に対して書き換え可能な LSI である FPGA (Field Programmable Gate Array) を用い、高速計算化理論の確立を目指す。

４．研究成果
部分計算の性質を満たす問題に対して FPGA を用いた高速解法を以下の問題に適用し、高速化を実現した。

(1) 画像の２値処理
画像の２値処理では、局所全解探索手法を用いた新しい FM スクリーニング手法と、その FPGA を用いた計算高速化手法を提案した。２値画像の生成には、局所全解探索を用い、この処理で必要なガウスフィルタの計算を部分計算の性質を用いることにより高速化を図った。実験の結果、高品質で鮮明な２値画像を生成することを示し、FPGA を用いてその計算を実行するハードウェアを実装し、高速化を実現した。

(2)２値画像のラベリング処理
２値画像の連結成分のラベリングとは、２値画像の連結成分に対してユニークな ID を割り当てる処理のことで、オブジェクト認識の前段階で用いられる。この処理では、k-concave な２値画像に対して、FPGA の内部メモリのみを用いて少ないレイテンシで連結成分のラベリングを実行するハードウェアアルゴリズムを提案した。

(3)コラッツ予想の検証
コラッツ予想とは、任意の 0 でない自然数 n に対して、n が偶数の場合 n を 2 で割る 、n が奇数の場合 n に 3 をかけて 1 を足すという操作を繰り返すと、有限回で 1 に到達するという予想で、数学の未解決問題の一つである。ここでは、実際に上記操作を計算することで、この予想を検証するシステムを作成した。具体的には、FPGA の内部メモリや信号処理計算用の DSP ブロックを用い、複数回の操作を 1 回の処理で行うことで高速化を実現した。

(4)RSA 暗号計算
書き換え可能な回路を補助するための大容量の組込み RAM と高速信号処理用の DSP を効果的に利用することにより、RSA 暗号の計算に必要なモンゴメリ乗算を実装した。また、計算量が多い RSA 復号計算に重点を置き、中国人剰余定理と上記回路を組み合わせることでさらなる高速化を実現した。

以上の結果より、本研究テーマである部**部分計算による FPGA を用いた計算高速化手法は様々な問題に対して有効であることがわかった。本手法はこれら以外にも十分適応可能であると考えられ、今後も様々な問題に対して計算高速化を実現していきたいと考えている**.

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 5 件）
1. 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, 2012, 査読有, http://www.ijnc.org/index.php/ijnc/article/view/35

2. Song Bo, 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 Journal of Networking and Computing, Vol. 1, No. 2, pp. 277-289, 2011,査読有, http://www.ijnc.org/index.php/ijnc/article/view/29

3. 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, 2011, 査読有, http://www.ijnc.org/index.php/ijnc/article/view/13

4.Yasuaki Ito, Koji Nakano, Low-Latency Connected Component Labeling Using an FPGA, International Journal on Foundations of Computer Science, Vol. 21, No.3, pp.405-426, 2010, 査読有, http://dx.doi.org/10.1142/S0129054110007337

5.Yasuaki Ito, Koji Nakano, A New FM Screening Method to Generate Cluster-Dot Binary Images Using the Local Exhaustive Search with FPGA Acceleration, International Journal on Foundations of Computer Science, Vol. 19, No. 6, pp. 1373-1386, 2008, 査読有, http://dx.doi.org/10.1142/S0129054108006339

〔学会発表〕(計６件)

1. Bo Song, Yasuaki Ito, and Koji Nakano, CRT-based Decryption using DSP blocks on the Xilinx Virtex-6 FPGA, Proc. of Workshop on Advances in Parallel and Distributed Computational Models, pp. 527-536, May 16th, 2011, Anchorage, U.S.A, 査読有.

2. 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, Proc. of International Conference on Networking and Computing, pp. 140-147, November 18th, 2010, Hiroshima, 査読有.

3. Yasuaki Ito, Koji Nakano, Efficient Exhaustive Verification of the Collatz Conjecture using DSP48E blocks of Xilinx Virtex-5 FPGAs, Proc. of Workshop on Advances in Parallel and Distributed Computational Models (CD-ROM of International Parallel and Distributed Processing Symposium), April 19th, 2010, Atlanta, U.S.A, 査読有.

4. Yasuaki Ito and Koji Nakano, A Hardware-Software Cooperative Approach for the Exhaustive Verification of the Collatz Conjecture, Proc. of International Symposium on Parallel and Distributed Processing with Applications, pp. 63-70, August 10th, 2009, Chengdu, China, 査読有.

5. Yasuaki Ito, Koji Nakano, Optimized Component Labeling Algorithm for using in Medium Sized FPGAs, in Proc. of International Conference on Parallel and Distributed Computing, Applications and Technologies, pp. 171-176, December 3rd, 2008, Dunedin, New Zealand, 査読有.

6. Yasuaki Ito, Koji Nakano, Component Labeling for k-Concave Binary Images Using an FPGA, Proc. of Workshop on Advances in Parallel and Distributed Computational Models(CD-ROM of International Parallel and Distributed Processing Symposium), April 14th, 2008, Miami, U.S.A, 査読有.

〔その他〕

６．研究組織

(1)研究代表者

伊藤　靖朗　(YASUAKI ITO)

広島大学・大学院工学研究院・助教

研究者番号：４０３９７９６４