様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ６ 月　 ８ 日現在

機関番号：１５４０１
研究種目：挑戦的萌芽研究
研究期間：2013～2015
課題番号：２５５４００２４

研究課題名（和文）ＦＰＧＡを用いた汎用計算技術ＧＰＦＰＧＡを実現するための開発環境の構築

研究課題名（英文）Development tools and environment for General-Purpose computing on FPGA (GPFPGA)

研究代表者
中野　浩嗣（Nakano, Koji）

広島大学・工学（系）研究科（研究院）・教授

研究者番号：３０２８１０７５

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：本研究の目的はGPFPGAの手法を開発し，FPGAによる汎用計算の可能性を明らかにすることである．そのため，FDFMアプローチを考案した．　これは少ない個数のDSPブロックとメモリブロックで専用プロセッサを構成するものである．このアプローチにより，次の処理をFPGAにより高速化した．（１）リアルタイム直線検出（２）画像中の円検出（３）RSA公開鍵のブレイク（４）LZW法を用いたデータの圧縮（５）上位ｋ番目の選択（６）多倍長演算．
実験結果より，ソフトウェアのよる計算処理より１００倍程度の高速化が可能な場合もあった．このことより，FDFMアプローチが汎用計算に対して効果的であることが示せた．

研究成果の概要（英文）：The main purpose of this work is to develop a GPFPGA(General Purpose computing using Field Programmable Gate Arrays) method and to show capability of general purpose computing using FPGAs. For this purpose, we have developed FDFM approach (Few DSP slices Few Memory block approach), which implement a special-purpose processor using few DSP slices and Few Memory blocks in an FPGA. By this approach, we have accelerated the computation as follows: (1) real-time line detection in an image using Hough transform, (2) circle detection in an image, (3) breaking RSA keys in a network, (4) LZW-compression/decompression (4) Top-k selection, (6) multiple-precision arithmetic.
Experimental results show that our FPGA implementation may be 100 times faster than conventional CPU implementation. This fact implies that FDFM approach is very efficient for general-purpose computing.

研究分野：情報工学

キーワード：FGPA　ハードウェアアルゴリズム　開発環境

１．研究開始当初の背景

FPGA(Field Programmable Gate Array)は，ユーザーが書き換え可能なFPGAである．FPGAは，CLB(Configurable Logic Block)，DSP slice及びBlock RAMから構成される．CLBは組み合わせ回路や順序回路を埋め込むことができる．DSP sliceは乗算器，加算器やレジスタなどを持っている．Block RAMは小容量のデュアルポートメモリである．基本的にFPGAは信号処理の高速化をターゲットに設計されており，DSP sliceやBlock RAMをいかに効果的に用いるかという点が，FPGAを用いた高速計算の鍵である．しかし，FPGAを効果的に利用するのは容易でなく，信号処理以外の汎用の計算を行うのは極めて困難である．

２．研究の目的

本研究では，FPGAを用いた汎用計算(GPFPGA, General Purpose Computing on FPGA)の考え方を導入し，そのための設計手法や開発環境を構築することにある．その結果，一般的な計算処理をFPGAで容易に行うことができるようになる．

３．研究の方法

FPGAのDSP sliceやBlock RAMを効果的に用いるためのツールを開発する．それを用いて，具体的な一般の計算処理に適用し，GPFPGAの考え方によるFPGA利用が効率よく実現可能であることを示す．

４．研究成果

FPGAを用いた汎用計算(GPFPGA，General Purpose Computing on FPGA)を実現する方法として，FDFMアプローチ(Few DSP slices and Few Memory blocks)を考案した．最新のFPGAは，DSP sliceとMemory block (Block RAM)を大量に，多いものでは２０００個以上もっている．DSP Sliceは，信号処理で用いる演算を行うための組み込みハードウェアである．乗算器，加算器，ビット毎の論理演算，パイプラインレジスタ，セレクタなどを内蔵している．これらの接続や設定を変更することにより，信号処理で用いられる畳み込み演算が高速に行える．また，Block RAMは小容量（１８ｋビット）のメモリであり，独立制御可能な２つのポートをもち，高速アクセスが可能である．FPGA設計ではこれら２種類の組み込みハードウェアをいかに巧妙に用いるかという点が重要である．

FDFMアプローチでは少数のDSP sliceと少数のBlock RAMを組み合わせて，特定用途のプロセッサを構成する．最小構成は，１つのDSP Sliceと１つのBlock RAMである．最新のFPGAでは，２０００個以上のDSP SliceとBlock RAMを持つので，２０００個以上の特定用途のプロセッサを構成することもでき，並列処理による最大限のスループットを得ることもできる．

この FDFM アプローチにより，次の６つの成果を得た．

（１）ハフ変換による画像のリアルタイム直線検出（引用文献①）

画像の輝度勾配情報を利用したハフ変換により検出精度のよい直線成分抽出ハードウェアをFPGAに実装した．回路は２６０MHzで動作し，スループットは，ほぼ１ピクセル／クロックサイクルである．よって，一秒間に約２６０万ピクセルの直線成分検出が行える．

（２）画像中の円検出（引用文献②）

２値画像中の円を検出するハードウェアを設計し，FPGAに実装した．４００×４００の画像に対する円検出は，９７０４３４クロックサイクルで行える．動作周波数は１８１MHzなので，約５msで円検出を完了させることができる．この処理時間は，CPUによるソフトウェア処理の場合に比べて，約１８９倍高速である．

（３）RSA暗号化キーの分解（引用文献③）

２つのRSA暗号化において，暗号化キーが素数を共有するとき，最大公約数を求めることにより，復号化キーを簡単に求めることができる．つまり，暗号文の解読が簡単に行えるようになる．このような欠陥のある暗号化キーを大量のキーの集合から求めるハードウェアを設計し，FPGAに実装した．設計したハードウェアはあらゆる暗号化キーの組み合わせに対して，ユークリッド互除法により最大公約数を求める．DSP ブロックを効果的に利用することにより，これまでに知られている最高速のGPUを用いた計算処理にくらべて約６倍の高速化を達成した．また，CPUによる逐次処理に比べて約５００倍高速である．

（４）可逆圧縮LZW法による展開の処理の高速化（引用文献④）

オリジナルのデータが復元可能な可逆圧縮法であるLZW手法の展開ハードウェアを設計した．設計した回路は１３個のBlock RAMを用いており，LZW 展開を高速に行うことができる．このLZW展開プロセッサは，CPUによるLZW展開に比べて約２．１６倍高速である．また，１５０個のLZW展開プロセッサを並べて同時に動作させた場合，約２６４倍高速である．

（５）マージソート回路による上位ｋ番目の選択回路（引用文献⑤）

Block RAMをバッファに用いたマージソートによりソーティングを行う回路を設計した．この回路はこれまでの入力の上位ｋ番目を出力し続ける回路である．メモリの割当を工夫し，使用量を約半分に削減することができた．

（６）多倍長演算プロセッサ（引用文献⑥）

多倍長演算を行うハードウェアアルゴリズムの設計は困難である．そこで，多倍長演算を機械語命令としてもつプロセッサを FDFMアプローチにより設計した．このプロセッサではソフトウェア的に多倍長演算を行うこ

とができ，開発が用意になる．このプロセッサは１個の DSP slice と２個の Block RAM を用い，約３１０MHｚで動作する．応用として RSA 暗号化をソフトウェア的に実装した．その結果，２０４８ビットの暗号化処理が約６００msで行うことができた．また，３０６個のプロセッサを並べることも可能であることを示した．

＜引用文献＞

① Xin Zhou, Yasuaki Ito, Koji Nakano, An Efficient Implementation of the Gradient-based Hough Transform using DSP slices and block RAMs on the FPGA, Proc. of International Parallel and Distributed Processing Symposium Workshops, pp. 762-770, May 2014

② Xin Zhou, Yasuaki Ito, Koji Nakano, An Efficient Implementation of the One-Dimensional Hough Transform Algorithm for Circle Detection on the FPGA, Proc. of International Symposium on Computing and Networking, pp.447-452, Dec, 2014.

③ Xin Zhou, Koji Nakano, and Yasuaki Ito, Parallel FDFM Approach for Computing GCDs Using the FPGA, Proc. of International Conference on Parallel Processing and Applied Mathematics (PPAM 2015, LNCS 9573), pp. 238-247, 2015.

④ Xin Zhou, Yasuaki Ito, and Koji Nakano, An Efficient Implementation of LZW Decompression in the FPGA, to appear in Proc. Of International Parallel and Distributed Processing Symposium Workshops, 2016

⑤ Naoyuki Matsumoto, Koji Nakano, Yasuaki Ito, Optimal Parallel Hardware K-Sorter and Top K-Sorter, with FPGA implementations, Proc. of International Symposium on Parallel and Distributed Computing, pp. 138-147, June 2015.

⑥ Tatsuya Kawamoto, Yasuaki Ito, Koji Nakano, A flexible-length-arithmetic processor based on FDFM approach in FPGAs, Proc. of International Symposium on Computing and Networking, pp. 364-370, December 2015.

５．主な発表論文等

〔雑誌論文〕（計４件）

①Tatsuya Kawamoto, Xin Zhou, Yasuaki Ito, Koji Nakano, An FPGA implementation for a flexible-length-arithmetic processor employing the FDFM processor core approach, IEICE Transactions on Information and Systems, 査読有, December 2016 （採録決定）.

②Xin Zhou, Koji Nakano, Yasuaki Ito , Efficient Implementation of FDFM Approach for Euclidean Algorithms on the FPGA, International Journal of Networking and Computing, 査読有, July 2016(採録決定).

③ Xin Zhou, Norihiro Tomagou, Yasuaki Ito, Koji Nakano, Implementations of the Hough Transform on the Embedded Multicore Processors, International Journal of Networking and Computing, 査読有, Vol. 4, No. 1, pp. 174-188, January 2014. http://ijnc.org/index.php/ijnc/article/view/79

④ 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, 査読有, Vol. 28, No. 4, pp. 308-320, 2013. DOI: 10.1080/17445760.2012.684686

〔学会発表〕（計６件）

① Xin Zhou, Yasuaki Ito, Koji Nakano, An Efficient Implementation of LZW Decompression in the FPGA, International Parallel and Distributed Processing Symposium, シカゴ（米国), ２０１６年５月２３日.

② Xin Zhou, Koji Nakano, Yasuaki Ito, Parallel FDFM Approach for Computing GCDs Using the FPGA, International Conference on Parallel Processing and Applied Mathematics, クラクフ（ポーランド), 2016年９月７日.

③ Tatsuya Kawamoto, Yasuaki Ito, Koji Nakano, A flexible-length-arithmetic processor based on FDFM approach in FPGAs, International Symposium on Computing and Networking, 札幌産業振興会館（札幌), 2015年12月10日.

④ Naoyuki Matsumoto, Koji Nakano, Yasuaki Ito, Optimal Parallel Hardware K-Sorter and Top K-Sorter, with FPGA implementations, International Symposium on Parallel and Distributed Computing, リマソール（キプロス）2015年６月30日

⑤ Xin Zhou, Yasuaki Ito, Koji Nakano, An Efficient Implementation of the One-Dimensional Hough Transform Algorithm for Circle Detection on the FPGA, International Symposium on Computing and

Networking，グランシップ（静岡），2014 年 12 月９日

⑥ Xin Zhou, Yasuaki Ito, Koji Nakano, An Efficient Implementation of the Gradient-based Hough Transform using DSP slices and block RAMs on the FPGA, International Parallel and Distributed Processing Symposium Workshops，フェニックス（米国），2014 年 5 月 19 日

６．研究組織
(1)研究代表者
中野 浩嗣（Koji Nakano）
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 （Yasuaki Ito）
広島大学・大学院工学研究院・准教授
研究者番号： 40397964