様式 C-19

科学研究費補助金研究成果報告書

平成２２年　３月２６日現在

研究種目：基盤研究(C)
研究期間：2007～2009
課題番号：19500042
研究課題名（和文）　ハードウェア特殊化技術の展開と応用

研究課題名（英文）　Advances and Applications of Hardware Specialization Techniques

研究代表者
市川　周一（ICHIKAWA SHUICHI）
豊橋技術科学大学・工学部・准教授
研究者番号：70262855

研究成果の概要（和文）：

論理回路の入力の一部が事前に判明すれば，論理を簡単化して回路規模を削減し，動作速度を改善することができる（ハードウェア特殊化）．得られた回路は入力データに依存するため，特殊化の実現には再構成可能論理デバイス（FPGA 等）が最適である．本研究では，(1) 制御プログラムを論理回路に変換して小型高速な制御回路を生成，(2) 個体ごとに異なる命令セットをプロセッサに与えてセキュリティを高める，(3) 応用とデータに合わせて並列計算機の構成を最適化する，等の研究を行った．

研究成果の概要（英文）：

If the input of logic circuit is partially or wholly predetermined, the circuit can be optimized to reduce the logic scale and to improve the maximum operational frequency. This technique is called “hardware specialization”. Since the derived circuit depends on the predetermined input data, it is reasonable to adopt reconfigurable logic devices (e.g., FPGA) to implement specialized circuit. In this project, the following three cases were examined as practical examples of hardware specialization techniques: (1) conversion of control software into logic circuit for small and highly responsive control systems, (2) diversification of processor for secure applications by giving different instruction sets for each instance, and (3) optimization of computer cluster configurations for a specific set of application and data size.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,600,000	480,000	2,080,000
2008 年度	1,000,000	300,000	1,300,000
2009 年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：　計算機工学，情報科学
科研費の分科・細目：　情報学，計算機システム・ネットワーク
キーワード：　計算機システム，小型化，高速化，Field Programmable Gate Array (FPGA)，部分評価，多様化，セキュリティ，組込みシステム

１．研究開始当初の背景

一般に，ソフトウェアの入力の一部分が実行前に確定している場合，可能な部分を実行前に評価することにより，不要なコードを除去して実行速度を改善することができる．例えばif文の判定条件を事前に決定できれば，実行時に if 文で条件分岐する必要はなく，不要な実行部(then か else のどちらか)を除去できる．このような技術を特殊化(specialization) あるいは部分評価(partial evaluation) とよぶ．

特殊化技術は，もともとソフトウェアの小型化・高速化のために検討されてきたが，ハードウェアにも適用可能である．ハードウェアを特殊化することにより，論理規模削減や性能向上が期待できる．しかし一方，得られる回路は入力に依存しており汎用性を失っているため，大量生産や再利用に適さない．そのため，1990 年代に FPGA 技術が発達するまで，ハードウェア特殊化が実用的な意義をもつことはなかった．

FPGA (Field Programmable Gate Array) は，構成データを書き換えることにより，論理機能を何度でも変更可能なLSI である．1990 年代後半に急速な進歩をとげ，現在では組込みシステムの SoC (system on chip)から専用回路による高性能計算まで，幅広い応用分野で用いられている．しかし多くの場合 FPGA は「ASIC の安価な代替品」として扱われており，実行時に論理を変更できるという本質的な長所が生かされていない．FPGA の長所を積極的に生かすことができれば，従来型計算機システムでは実現不可能な新たな計算パラダイムが実現できる可能性がある．本研究で扱うハードウェア特殊化も，FPGA なしでは実現できない計算パラダイムのひとつである．特殊化により，従来システムでは不可能な高性能，低コスト，低消費電力，知的財産保護などが実現できる可能性がある．

２．研究の目的

本研究の目的は，これまで進めてきたハードウェア特殊化の研究を更に発展させ，新たな適用分野を探求すると共に，実用化のための基盤整備を行うことである．

研究テーマとしては以下の２つを想定しているが，これ以外の新しい分野への応用も積極的に検討してゆく．

(1) 制御回路の特殊化

① 制御プログラム（命令列）を論理回路に変換し，小型・高速・高秘匿性回路を実現する．

② このテーマは従来も研究してきたが，技術的制約が多かった．そのため本研究で，より実用的技術を開発評価することを目的とする．

(2) プロセッサアーキテクチャの特殊化

① プロセッサの多様性を増してセキュアな情報基盤を実現すること．

② 特殊化技術により，ユーザの利便性を損なうことなくプロセッサに多様性を持たせることができる．これにより知的所有権保護やセキュリティ向上を図ることができる．

３．研究の方法

(1) 制御回路の特殊化

産業用機械などのシーケンス制御には，Programmable Logic Controller (PLC) が多く用いられているが，大規模な制御では処理速度不足が問題になる場合がある．Field Programmable Gate Array (FPGA) は，論理構成を何度でも変更可能なLSI である．PLC で実現していた制御論理を，FPGA を用いてハードワイヤード化すれば，柔軟性を保ったまま処理速度を改善することが可能になる．

PLC プログラムの記述には，ラダー図が広く利用される．ラダー図表現における処理の最小単位を段と呼び，段は条件部と処理部から構成される(図1)．処理部には，出力命令(a)やデータ処理命令など(b) が設定可能である．PLC プログラムは複数の段から構成され，それらが上から下へ繰り返し処理されることでシーケンス制御を実現している．

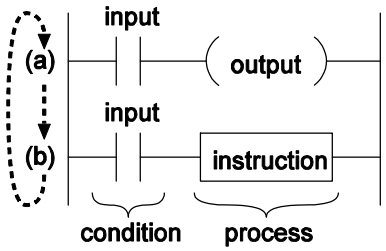

図1 ラダー図の例

PLC の動作を論理回路で忠実に再現するには，ラダーの1段に1状態を割り当てて，ラダー図を逐次処理すればよい．この回路をSD (Sequential Design) と呼ぶ．SD を高速化するには，PLC プログラムの各段の依存関係を適切に維持しながら，並列実行可能な制御回

路を並列に動作させればよい．依存関係の例を図2 に示す．

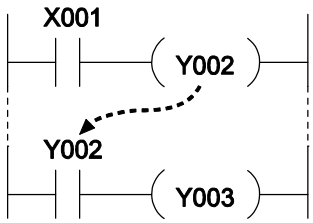

図2 データ依存の例

ある段の出力Y002 を下の段で利用する場合，下の段はY002 の値が定まるまで実行できない(データ依存関係)．そこで依存関係に従って各段のレベル付け行い，各レベルを1状態として順序回路を生成すると，回路を高速化できる(LD: Levelized Design)．

さらにLDの各段を全て組合せ回路化することにより，ラダー図を１巡１サイクルで処理することが可能になる．この設計をFlat Design (FD)と呼ぶ．

制御プログラムからこれらの論理設計を自動生成するコンバータを開発し，幾つかの実用的制御プログラムを用いて評価した．さらにFPGAボード上に実装して，実際の制御機器で動作することを確認した．

(2) プロセッサアーキテクチャの特殊化

Forrest らは，多様性によりシステムの信頼性を高めることを提案した．システムが均一であるとソフトウェアのポータビリティは向上するが，同時に悪意の複製や解析も容易になる．多くのウイルスはスタックオーバーフロー等を利用してバイナリコードのインジェクションを行なうが，これはプロセッサアーキテクチャを仮定した攻撃である．個々のシステムで命令セットが異なっていれば，単にソフトウェアを複製しても動作しないばかりでなく，命令セット全体の知識なしでリバースエンジニアリングをすることも難しくなる．また，バイナリコードのインジェクションを受けても，感染を免れることができる．

このように多様化には多くの利点があるが，実際にはPC やサーバの世界では，プロセッサアーキテクチャの寡占化が進みつつある．第一の原因はソフトウェア資産を保護し活用するためである．第二の原因はLSI技術の本質で，同一チップの大量生産を行うため必然的にアーキテクチャの寡占化が促進される構造になっている．

近年，組込み応用などシステム集積用途に，FPGA (Field Programmable Gate Array) が広く用いられている．FPGAは再構成可能な汎用論理LSI であり，最先端プロセスを使用して，1 chip に大規模論理(100 万ゲート以上)・大容量メモリ(1M バイト以上)・高速演算器などを搭載可能である．FPGAを用いれば，プロセッサの単品生産も可能なので，システムの多様性を生み出すことは容易である．一方，プロセッサの多様化には様々な方法があり，FPGA上で実用的な多様性が妥当なコストで実現できるか自明ではない．

そこで本研究では，実現可能な自由度の大小を幾つかのアーキテクチャについて評価し，既存手法と定量的に比較する．さらにFPGA 上で実装評価して，実装コストと性能について定量的に議論する．

４．研究成果

(1) 制御回路の特殊化

三菱電機製 PLC 製品(FX-2N)の命令セットを解析し，SD/LD/FD などの論理設計を出力するコンバータを開発した．Altera Stratix II FPGA をターゲットデバイスとして評価した場合，或る実用的制御プログラムで，PLC ソフトウェアに対して184倍(SD)～8050倍(FD)の高速化が得られることが分かった．(詳細な評価結果は雑誌論文[1]参照のこと)

さらに八洲熱学(株)と共同開発した整列巻取機 SPM05-02 (図 4) について，PLC 制御部を FPGA 制御ボード (図 3) に交換し，FPGA 制御部が正常に動作することを確認した．

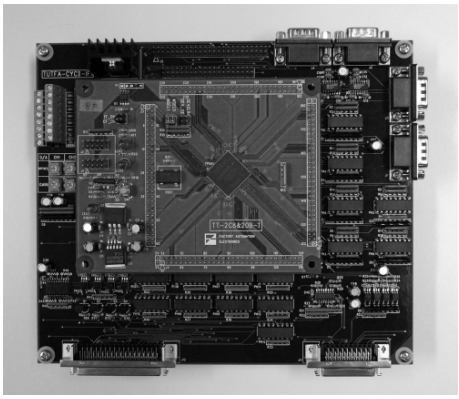

図３： FPGA 制御ボード

図４： 整列巻取機 SPM05-02

(2) プロセッサアーキテクチャの特殊化

本研究では，命令形式を変更せずに符号化の方法だけを変更することを検討した．例えば，加算命令の命令コード(opcode) が 1 で，減算命令の命令コードが 2 であるプロセッサ A を考える．ここで加算命令と減算命令の命令コードを入れ替えたプロセッサ B を考えたとしても，プロセッサ A と B の命令セットアーキテクチャには何ら本質的な相違は発生しない．単に命令列の表現(符号化)方法が異なるだけで，命令列の長さ，データ表現，メモリアクセス方法，条件分岐の方法，例外処理方法など，全てが同じである．プロセッサ A と B の相違を，マシンパーソナリティと名付けた．別な言い方をすれば，A と B は同じ命令セットアーキテクチャから特殊化されて生成されたものであるともいえる．

上記の手法の自由度を，幾つかの典型的命令セットで検討したところ，非常に多くの多様性が生成可能であることが分かった (表 1)．

表 1: Redundancy in four instruction sets.

	Number of instruction	Redundancy	Information [bit]
MIPS	170	2.34e+166	553
SH-3	188	1.63e+90	300
8080	111	2.34e+136	453
Java VM	201	1.59e+377	1253

更に MIPS 命令セットを例として上記の手法を実装評価した．実装対象としてはオープンソースの MIPS プロセッサ Plasma (図 5) を利用し，ターゲットデバイスとして Xilinx Spartan3 FPGA を採用した．

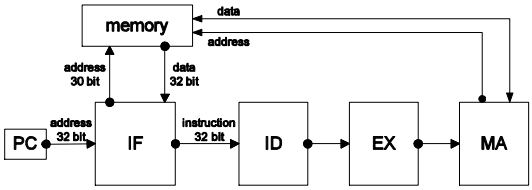

図 5： Plasma ブロック図

命令セットの多様化を実現するため，命令フェッチ(IF)部とデコード(ID)部の間に RAM による変換ブロックを追加した (図 6)．これによる論理規模の増大は 3.5%，性能低下は 11.6%にとどまることが分かった．得られるセキュリティの向上を考えれば，妥当なコストであると考えられる．評価結果の詳細は雑誌論文[3]を参照されたい．

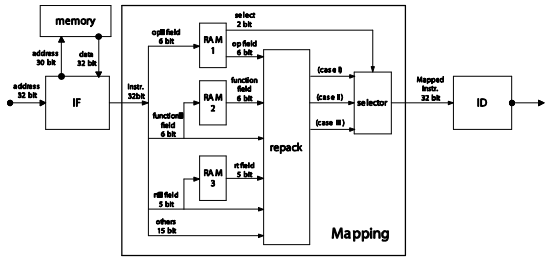

図 6： RAM によるマッピング

(3) 応用プログラムとデータ量に応じた並列計算機の構成最適化

近年，マイクロプロセッサのコスト低下とマルチコア化により，PC クラスタを始めとした並列計算環境において利用可能なプロセッサ数は飛躍的に増大している．

一方，応用プログラムの性質は多種多様であり，プロセッサ数を必要以上に増やすと通信量の増大により性能低下を招くことがある．最適なプロセッサ数は，応用プログラムの性質とデータ量の双方に依存するため，決して自明ではない．

更にマルチコア化によるメモリ階層の増大，通信方法と通信時間の不均一化など，システムの複雑さは増大している．そのため今日では，最適なプロセッサ数を知るだけでは十分でなく，最適なプロセス配置が分からない限り実行時間を最小化することはできない．

最適でないプロセス数・プロセス配置で並列応用を実行すれば，高価で貴重な並列計算資源(スーパーコンピュータなど)が無駄に費消されることになる．並列度が大きくなるほど損害も大きくなり，社会全体での総損害額は計り知れない．

本研究では，応用プログラムとデータサイズに応じて並列計算環境のハードウェア構成を最適化することにより，実行時間を最小化するとともに計算資源の効率的利用を可能にした．

本テーマは当初の研究目的には含まれない派生テーマであるため，紙数の都合で詳細は省略する．詳細は雑誌論文[2]などを参照されたい．

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３件）（すべて査読有）

[1] Shuichi Ichikawa, Masanori Akinaka, Hisashi Hata, Ryo Ikeda, Hiroshi Yamamoto: "An FPGA implementation of hard-wired sequence control system

based on PLC software," IEEJ Transactions on Electrical and Electronic Engineering, (to appear).

[2] Shuichi Ichikawa, Sho Takahashi, Yuu Kawai: "Optimizing Process Allocation of Parallel Programs for Heterogeneous Clusters," Concurrency and Computation: Practice and Experience, Vol. 21, No, 4, pp. 475--507 (2009).

[3] Shuichi Ichikawa, Takashi Sawada, Hisashi Hata: "Diversification of Processors Based on Redundancy in Instruction Set," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E91-A, No.1, pp. 211--220 (2008). 査読有

〔学会発表〕(計 12 件)

[1] 手塚康瑛, 市川周一, 野田善之: "振動抑制を考慮した追従システムの FPGA による実装," 電子情報通信学会技術研究報告 RECONF (to appear), (2010).

[2] 手塚康瑛, 市川周一, 野田善之: "ディジタルフィルタのハードウェア特殊化と制振制御への応用," 電子情報通信学会技術研究報告 RECONF2009-67, pp.83--88 (2010).

[3] 手塚康瑛, 市川周一, 野田善之, 森田定幸: "制御モデルからの専用回路生成と FPGA への実装," 平成 21 年度電気関係学会東海支部連合大会, O-423 (2009).

[4] Shuichi Ichikawa, Shoichiro Takagi: "Estimating the Optimal Configuration of a Multi-Core Cluster: A Preliminary Study," Proceedings of the International Conference on Complex, Intelligent and Software Intensive Systems (CISIS 2009), pp. 1245--1251 (2009).

[5] 松岡俊佑, 市川周一: "鍵埋め込み型 AES 暗号化回路の FPGA による実装と評価," 電子情報通信学会 2009 年ソサイエティ大会, A-3-13 (2009).

[6] 吉田幸太郎, 市川周一: "マルチコア PC クラスタのためのプロセス配置法の検討," 電子情報通信学会東海支部・平成 20 年度卒業研究発表会 (2009).

[7] Shuichi Ichikawa, Masayoshi Asakura, Yusuke Sakumoto: "Estimating the Optimal Configuration of a Heterogeneous Cluster: the Case of NAS Parallel Benchmarks," Proceedings of 8th International Conference on Applications and Principles of Information Science (APIS 2009), pp.241--244 (2009).

[8] 畑尚志, 市川周一: "メタスタビリティを利用した真性乱数生成回路の FPGA による実装," 情報処理学会研究報告, vol. 2009, no. 7, pp. 25--30 (2009). (情報処理学会コンピュータサイエンス領域奨励賞, 第 138 回 SLDM 研究会優秀学生発表賞)

[9] 市川周一, 畑尚志: "RS ラッチのメタスタビリティを利用した真性乱数生成回路," 2009 年 暗号と情報セキュリティシンポジウム (SCIS2009), 2F1-5 (2009).

[10] Shuichi Ichikawa, Yuu Kawai: "Constructing Execution-Time Estimation Models from Diverse Processing Elements of Heterogeneous Clusters," Proceedings of IEEE TENCON 2008, pp. 1--6 (2008).

[11] 市川周一, 高木翔一朗: "マルチコア PC クラスタの最適構成予測手法の検討," 電子情報通信学会 2008 年総合大会, D-6-4 (2008).

[12] 手塚康瑛, 市川周一: "組込みシステムのための実時間性能計測手法の開発," 電子情報通信学会 2008 年総合大会, D-6-5 (2008).

〔その他〕
ホームページ等

http://meta.tutkie.tut.ac.jp/~ichikawa/

６．研究組織

(1)研究代表者

市川　周一 (ICHIKAWA SHUICHI)
豊橋技術科学大学・工学部・准教授
研究者番号：70262855

(2)研究分担者

なし

(3)連携研究者

なし