

不均一計算環境のための負荷分散法 / 特殊化技術のセキュリティ分野への 応用

市川 周一 (第7工学系, 情報環境コア)

1 はじめに

筆者の元々の専門分野は、並列計算機アーキテクチャやマイクロプロセッサ設計である。しかし本学に赴任後はテーマをやや応用側にシフトし、以下のようなテーマを扱ってきた。

- 並列処理応用の静的負荷分散
- 再構成可能論理による専用計算回路
- 専用回路技術の組込み・制御システムへの応用
- 情報セキュリティ, コンピュータセキュリティ

上のリストからはテーマ間の関係が判りにくいですが、簡単にいえば高速処理が大きな研究目標である。例えば、応用プログラムを高速化するために複数の計算機を使うことが有効であれば、ソフトウェアによる並列化技術で高性能化する。ハードウェア化によって大きな性能向上が見込めるならば、専用計算回路を設計して高速化を図る。最後の項目“セキュリティ”だけは他のテーマと少々趣が異なるが、これは純粋に好奇心から研究を始めたものである。

さて、メディア科学リサーチセンター・情報環境コアでは、情報ネットワークや情報システム環境の研究を行なっている。コアの研究キーワードに“分散並列計算”や“情報セキュリティ”が含まれていることから、筆者の専門分野と情報環境コアの関連については自明であろう。以下、本稿では、過去2年ほどの研究結果のなかから、情報環境コアの研究活動に関連するテーマを紹介する。

2 Optimizing Process Allocation of Parallel Programs for Heterogeneous Clusters [1]

本研究に関する英文論文 [1] のアブストラクトを以下に引用する。

The performance of a conventional parallel application is often degraded by load-imbalance on heterogeneous clusters. Though it is simple to invoke multiple processes on fast PEs to alleviate load-imbalance, the optimal process allocation is not

obvious. Kishimoto and Ichikawa presented performance models for HPL (High Performance Linpack), with which the sub-optimal configurations of heterogeneous clusters were actually estimated. Their results on HPL are encouraging, whereas their approach is not yet verified with other applications. This study presents some enhancements of Kishimoto's scheme, which are evaluated with four typical scientific applications: CFD (computational fluid dynamics), FEM (finite element method), HPL (linear algebraic system), and FFT (fast Fourier transform). According to our experiments, our new models (NP-T models) are superior to Kishimoto's models, particularly when non-negative least squares (NNLS) method is used for parameter extraction. The average errors of the derived models were 0.2% for CFD benchmark, 2% for FEM benchmark, 1% for HPL, and 28% for FFT benchmark. This study also emphasizes the importance of predictability in clusters, listing practical examples derived from our work.

本研究では、プログラムの実行時間予測モデルを構築することにより不均一クラスタ上でのプロセス配置を最適化する手法を提案し、4つの典型的科学技術応用について定量的評価結果を示している。本手法は岸本・市川 [2] の手法を拡張・改良したものである。また本研究の一部は、高橋・市川 [3] および河合・市川 [4] として発表されたものである。

3 マルチコア PC クラスタの最適構成予測手法の検討 [5]

PC クラスタは、使用するノード数やプロセス数など、クラスタの構成により性能が変わる。可能なクラスタ構成の中から最適な構成を予測するため、河合・市川 [4] は実測値から実行時間予測モデルを構築し、4つの科学技術応用について(準)最適な構成が予測できる事を示した。

近年プロセッサのマルチコア化が進んでいるが、マルチコア PC クラスタは不均一な並列環境であり、最適構成の予測は簡単でない。本研究では、河合らの手法をマルチコア PC クラスタに適用する方法について検討し、多くの場合について相対誤差 20%以下の

準最適構成を予測できることを示した。

本研究は未だ予備的な段階にあるが、今後、より大規模で正確な測定を行い、手法を改良・検証してゆく予定である。

4 Diversification of Processors Based on Redundancy in Instruction Set [6]

本研究に関する英文論文 [6] のアブストラクトを以下に引用する。

By diversifying processor architecture, computer software is expected to be more resistant to plagiarism, analysis, and attacks. This study presents a new method to diversify instruction set architecture (ISA) by utilizing the redundancy in the instruction set. Our method is particularly suited for embedded systems implemented with FPGA technology, and realizes a genuine instruction set randomization, which has not been provided by the preceding studies. The evaluation results on four typical ISAs indicate that our scheme can provide a far larger degree of freedom than the preceding studies. Diversified processors based on MIPS architecture were actually implemented and evaluated with Xilinx Spartan-3 FPGA. The increase of logic scale was modest: 5.1% in Specialized design and 3.6% in RAM-mapped design. The performance overhead was also modest: 3.4% in Specialized design and 11.6% in RAM-mapped design. From these results, our scheme is regarded as a practical and promising way to secure FPGA-based embedded systems.

本研究では、プロセッサにインジェクション攻撃などに対する耐性を与えるために、命令セットが内包する自由度を利用して命令セットアーキテクチャを多様化する手法を提案し、その実装方法と定量的評価結果を示したものである。本研究は、市川・澤田・畑の研究 [7][8] を基にして、さらに改良と検討を加えた結果である。

5 おわりに

不均一クラスタのための負荷分散法 [1] [5] に関しては、今後、さらに改良を加えて、実用的なシステムを構築してゆきたいと考えている。具体的には、予測精度の向上と、不均一ネットワークのモデル化、既存モデルとの融合などのテーマが考えられる。

セキュリティ技術に関しても、これまでの本研究室での蓄積を生かし、FPGA 等を用いた特殊化技術を軸として、ハードウェア側の立場から研究を進めてゆく予定である。

発表論文

- [1] Shuichi Ichikawa, Sho Takahashi, Yuu Kawai: “Optimizing Process Allocation of Parallel Programs for Heterogeneous Clusters,” *Concurrency and Computation: Practice and Experience*, (accepted).
- [2] Yoshinori Kishimoto, Shuichi Ichikawa: “Optimizing the Configuration of a Heterogeneous Cluster with Multiprocessing and Execution-Time Estimation,” *Parallel Computing*, Vol. 31, No. 7, pp. 691–710 (2005).
- [3] 高橋翔, 市川周一: “不均一クラスタの最適構成予測モデルの各応用への適用と評価,” *情報処理学会研究報告 2006-HPC-105*, pp. 97–102 (2006).
- [4] 河合裕, 市川周一: “実行時間予測モデルの構築法の改善,” *情報処理学会研究報告 2007-HPC-109*, pp. 79–84 (2007).
- [5] 市川周一, 高木翔一郎: “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).
- [6] 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).
- [7] 市川周一, 澤田豊志, 畑尚志: “命令セットの冗長性とプロセッサの多様化,” *2007 年 暗号と情報セキュリティシンポジウム (SCIS2007)*, 2E2-4 (2007).
- [8] 澤田豊志, 市川周一, 畑尚志: “命令セットに含まれる自由度の評価とその応用,” *電子情報通信学会 2007 年総合大会*, D-6-2 (2007).