

アルゴリズム活動グループ

小柳義夫¹, 須田礼二¹, 西田晃¹, 武市正人², 胡振江², 笥一彦²
山本博資², 小川朋宏², 杉原厚吉², 西田徹志²

情報理工学系研究科 コンピュータ科学専攻¹, 数理情報学専攻²

1 はじめに

コンピュータおよびネットワークの高速化・大容量化や、携帯電話を始めとしたユビキタスなネットワーク環境の充実により、ビジネス・行政・研究開発などの大規模なシステムから家電製品などの身近な機器まで、我々の社会は、ますますコンピュータやネットワークに大きく依存するようになって来ている。そのため、ひとたびそれらに障害が生じると社会全体に大きな損害をもたらすことになる。それらの障害は、ハード的なもの以外に、使われているソフトウェアやアルゴリズムの脆弱さに起因する場合が多い。例えば、デジタル計算機における有限精度計算による誤差、ネットワーク環境における負荷変動、通信路の雑音、モデルと実際の対象との不整合など、さまざまな要因がアルゴリズムの動作を不安定にする可能性がある。

アルゴリズム活動グループでは、対象として「計算機、ソフトウェア、通信、応用」の各分野におけるアルゴリズムを取り上げ、上記のような不安定要因を詳しく調べると共に、それらの不安定要因が存在しても、ロバストに安全に動作するアルゴリズムの開発を目指している。

具体的には、高速な並列計算機をロバストに実現するための「超ロバスト並列計算」、ロバストなソフトウェアを構成するための「ロバストソフトウェア構成法」、ロバストに安全で高品質高効率な通信や記録システムを実現するための「符号化におけるロバスト計算」、ロバストな幾何計算を目指す「超ロバスト幾何計算」の4つのテーマをサブプロジェクトとして研究を行っている。次節

で、各サブプロジェクトの本年度の研究成果と活動内容の概要を紹介する。

2 本年度の成果の概要

2.1 超ロバスト並列計算

研究者：小柳義夫, 須田礼仁, 西田晃

(情報理工学系研究科 コンピュータ科学専攻)

目的：グリッドのようにネットワークや計算機の構成・性能が動的に変動する並列計算機において、資源の故障や追加、負荷の変動などの外乱に対してロバストに適応し、計算能力を効率よく引き出す手法を開発する。数値アルゴリズムと並列化手法の両面から性能のロバストネスを導く。

成果：さまざまなグリッド等の汎用の並列計算環境で性能を最大限引き出すためには、効率的な通信の実装が必要であり、さまざまな環境に応じた集団通信のスケジュールを得る手法が必要である。そのために、ネットワークをトポロジー的には木構造で取り扱い、ハブ・通信遅延・バンド幅などを含めて、通信のモデル化を行った。また、集団通信の中で代表的である Broadcast のスケジューリングの最適解を求めるために、木の同型判定と下限計算による効率的な枝刈りを行う分枝限定法を用いたアルゴリズムを提案・実装し、その有効性を明らかにした。

また、さまざまな並列環境に高度に適応した数値ライブラリーを用意することにより、ロバストな並列処理を容易に利用できるよう

にする ERXPP (Easy and Robust Extension of Parallel Performance) の概念を提案し、その有用性の実証のために、惑星大気の流体シミュレーションによる予備評価を行った。さらに、そのときに必要となる、データの再分散問題を MMDL (multi-master divisible load) として拡張モデル化し、MMDL のデータ再分散に対するスケジューリングアルゴリズムを提案し、その有効性を明らかにした。

2.2 ロバストソフトウェア構成法

研究者：武市正人，胡振江，笈一彦
(情報理工学系研究科 数理情報学専攻)

目的：モデル検査等の形式的手法に基づいて、ロバストなソフトウェアを構成する方法を確立し、融合プロジェクトを通じて、その手法の有効性を実証する。

成果：モデル検査技術を利用したプログラム解析の自動生成を課題として、時相論理式で記述されたプログラムの性質の解析処理を自動化するツールの開発とその実用性の検証を行った。具体的には、実用言語 Java と相互に変換可能な中間言語である Jimple のプログラムが、時相論理 CTL-FV による性質記述を満たしているかどうかをモデル検査技術により検証できるツールを開発した。

さらに、Java プログラムに対して、最適化の仕様を宣言的に記述する手法を拡張し、それをもとにして最適化プログラムを実現する方法について研究を行った。この宣言的な手法により、記述された最適化仕様の正当性の検証が比較的容易に行えるようになった。また、CTL-FV のようなプログラム解析仕様を表すための時相論理として NCTL-FV を提案し、それに基づく最適化のための解析ツールを実現し、その有効性を明らかにした。

2.3 符号化におけるロバスト計算

研究者：山本博資，小川朋宏
(情報理工学系研究科 数理情報学専攻)

目的：データの特性や通信路の状態，不正者からの攻撃方法，あるいは計算機の計算精度などによらず，ロバストに「安全，高品質，高効率」な符号化技術の開発を目的とする。

成果：情報源の特性によらず高性能な圧縮が行えるユニバーサルデータ圧縮符号として，MPM (Multi-level Pattern Matching) 符号を取り上げ，それと同等の圧縮性能を持ち，かつ逐次的に圧縮可能な「逐次 MPM 符号」を提案し，その性能評価を行った。

破壊や漏洩の脅威にロバストな耐性を持つ秘密分散法に関しては，一般アクセス構造，複数の秘密画像を持つ視覚復号型秘密分散法，量子秘密分散法などに関して，効率のよい構成法を提案すると共に，その安全性を理論的に証明した。また，秘密鍵のような秘密情報 S が一部漏洩して安全でなくなったとき，その S と公開通信路上での情報交換により，新たに完全に安全な秘密情報を生成する「プライバシー増幅法」の効率よい実現法を提案し，その有用性を明らかにした。

さらに，量子仮説検定や，低密度パリティ検査符号 (LDPC 符号) の有歪み圧縮などへ応用に関しても成果を得ている。

2.4 超ロバスト幾何計算

研究者：杉原厚吉，西田徹志
(情報理工学系研究科 数理情報学専攻)

目的：幾何計算は一般に誤差に脆弱であるが，誤差が生じる計算環境でも安定して動作する幾何アルゴリズムの構築とその汎用的方法論としてのロバスト幾何計算技法の確立を目的とする。

成果：流れの中のボロノイ図の計算法として，高速前進法や粒子追跡法をロバストとなるように改良した新しい方式を提案し，その有用性を示した。

3次元立体に関しては，三角形メッシュで表された立体情報に対して，細分割を利用した形状データ圧縮法を構成した，また，凸とは

限らない一般曲面をロバストに多角形近似する，双対構造を利用した新しい形状表現法および細分割法を構成した．さらに，特異値スペクトル解析 (SSA) アルゴリズムを利用したロバストな3次元メッシュ電子透かし法を提案し，その有効性を評価した．

その他に，波の挙動をシミュレートするための無反射境界設定法の開発も行っている．

3 その他の活動

3.1 研究集会等

本年度，アルゴリズム活動グループの研究活動に関連して開催した研究集会等を下記に報告する．

1. ロバスト符号化セミナー：
一般化事後確率の計算と Kullback 情報量，松島敏恭 (早稲田大学 理工学部 工業経営学科)
日時：2003年 3月 31日 (月) 15時～17時
会場：東京大学工学部 6号館 セミナー室 A
2. ロバスト幾何計算セミナー：
Applications of Ellipsoids in Geometric Modeling and Processing, Prof. Myung-Soo Kim (Seoul National University)
日時：2003年 7月 18日 (金) 13時～14時
会場：東京大学理学部化学旧館 136号室
3. 超ロバストセミナー：
Caterpillar の列挙とこれからの研究，菊池 洋右 氏 (本プロジェクト PD 研究員)
日時：2003年 7月 31日 (木) 16時～17時
会場：東京大学理学部化学旧館 136号室
4. ロバスト符号化 映画上映会：
Claude Shannon に関する記念映画
日時：2003年 9月 29日 (月) 13時～14時
会場：東京大学工学部 6号館 63講義室

5. 特別セミナー：

How to Learn Japanese with Fun,
Prof. Dr. Emmerich Simoncsics (ウィーン工科大学)

日時：2003年 10月 7日 (火) 15時～16時 30分

会場：東京大学工学部 6号館 セミナー室 A

6. ロバストソフトウェア構成法セミナー：

A Development Calculus for Specifications, Prof. Wei Li (Beijing Univ. Aeronautics and Astronautics, 学長)

日時：2003年 10月 14日 (火) 15時～17時

会場：東京大学工学部 6号館 大会議室

7. ロバスト幾何計算セミナー：

Theory of Guaranteed Accuracy Computation, Professor Chee Yap (New York University),

Voronoi diagram for spheres and its applications, Professor Deok-Soo Kim (Hanyang University)

日時：2004年 2月 6日 (金) 15時～17時

会場：東京大学工学部 6号館 セミナー室 A

これらのセミナーには，「アルゴリズム活動グループ」だけでなく，「超ロバスト計算プロジェクト」の他のグループや，本 COE の他のプロジェクトである「実世界情報システムプロジェクト」「大域ディペンダブル情報基盤プロジェクト」等からも多くの参加者を得て，グループ間およびプロジェクト間の研究交流としても役立っている．

3.2 テクニカルレポート

本年度，アルゴリズム活動グループの研究活動に関連して，下記のテクニカルレポートを発表した．なお，これらのテクニカルレポートだけでなく，学術論文誌，国際シンポジウム，学会等の大会や研究会などにおいても，成果を多数発表している．それらは，各サブプロジェクトの報告で紹介されている．

1. (SRCTR 2003-01) Shuji KIJIMA and Tomomi MATSUI, "Approximate Counting Scheme for $m \times n$ Contingency Tables," January 2003.
2. (SRCTR 2003-06) Mitsugu IWAMOTO and Hirosuke YAMAMOTO, "A construction method of visual secret sharing schemes for plural secret images," January 2003.
3. (SRCTR 2003-07) Mizuhito OGAWA and Zhenjiang HU and Isao SASANO and Masato TAKEICHI, "Catamorphic Approach to Program Analysis," January 2003.
4. (SRCTR 2003-08) Kohei MUROTANI and Kokichi SUGIHARA, "Watermarking 3D Polygonal Meshes Using the Singular Spectrum Analysis," January 2003.
5. (SRCTR 2003-09) Hiroshi KAWAHARADA and Kokichi SUGIHARA, "Compression of Arbitrary Mesh Data Using Subdivision Surfaces," February 2003.
6. (SRCTR 2003-19) Ken'ichiro TANAKA, Masaaki SUGIHARA, and Kazuo MUROTA, "Numerical Indefinite Integration by Double Exponential Sinc Method," May 2003.
7. (SRCTR 2003-21) Kiminori MATSUZAKI, Zhenjiang HU, and Masato TAKEICHI, "Parallelization with Tree Skeletons," May 2003.
8. (SRCTR 2003-33) K. Sugihara, M. Sawai, H. Sano, D.-S. Kim, and D. Kim, "Disk Packing for the Estimation of the Size of a Wire Bundle," September 2003.
9. (SRCTR 2003-40) Tetsushi NISHIDA and Kokichi SUGIHARA, "Boat-Sail Voronoi Diagram and Its Computation Based on a Cone-Approximation Scheme," November 2003.
10. (SRCTR 2003-44) Tetsushi NISHIDA and Kokichi SUGIHARA, "Stable Marker-Particle Method for the Voronoi Diagram in a Flow," December 2003.
11. (SRCTR 2003-45) Tetsushi NISHIDA and Kokichi SUGIHARA, "FEM-like Fast Marching Method for the Computation of the Boat-Sail Distance and the Associated Voronoi Diagram," December 2003.
12. (SRCTR 2004-02) Hisamoto HIYOSHI and Kokichi SUGIHARA, "Improving the Global Continuity of the Natural Neighbor Interpolation," January 2004.

3.3 超ロバスト計算原理講究

大学院情報理工学系研究科では、大学院学生への講義として「超ロバスト計算原理講究」が開講されたが、そのうち、アルゴリズム活動グループでは下記の者が講義を担当した。

杉原厚吉 (4月9日), 西田晃 (4月23日), 小川明宏 (6月18日) 杉原厚吉・宮代隆平 (RA) (7月2日), 杉原厚吉・岩本貢 (RA) (7月16日), 杉原厚吉・蓬莱祐一郎 (RA) (12月3日)

3.4 超ロバスト計算原理ミュージアム

超ロバスト計算原理プロジェクトでは、他分野の情報技術との積極的な融合を促進するために、超ロバスト計算原理ミュージアムを開設している。そこでは、分野外の人にも分かりやすい展示パネルを用意して、本プロジェクトで開発する計算原理を紹介しているが、本グループのサブプロジェクトもパネル展示を行っている。また、「符号におけるロバスト計算」サブプロジェクトでは、超ロバスト計算原理プロジェクトのシンボルマークを秘密画像としたカラー画像の視覚復号型秘密分散法のデモを作成し、展示している。