アルゴリズム活動グループ

山本博資

新領域創成科学研究科複雑理工学専攻

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，家電製品などの身近な電子機器から，ビジネス・行政・研究開発などの大規模なシステムまで，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，ハードウエアに起因するもの以外に，使われているソフトウエ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，コンピュータ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「コンピュータ, ソフトウエア, 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柔軟に対応し，かつ目的をロバストに達成でき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」，ロバストな文章処理技術の方法論を構築するための「ロバスト構造化文書処理技術」，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：ネットワークや計算機の構成・性能が不均質であったり，動的に変動したりするような並列計算環境において，ネットワーク・計算機の故障や負荷の変動などの外乱にロバストに対応し，計算機能力を効率よく引き出す手法の開発を目指す．

成果：非一様な計算機で構成された並列計算機 (ヘテロクラスタ）のための LU 分解の実装と，Multi-Master Divisible Load モデルに基づく効率的な再配分スケジューリングの手法の開発を行った．

LU 分解は，連立一次方程式の解法において重要であるばかりでなく，LU 分解に含まれる部分演算の多くが他の行列演算に含まれていたり類似したりしているため，科学技術計算の高性能計算において重要な問題である．行列の長方形領域を列ベース分割する場合の最適通信スケジューリングを提案しているが，それを利用した列ベース分割に基づく並列 LU 分解を実装した．また，その性能を 1 次元分割や 2 次元格子分割と比較し，その得失を明らかにした．

データ再分散は並列計算の基本問題の一つであるが，Multi-Master Divisible Load モデ

ルを用いて，再分散のための通信とその後の計算を同時にスケジューリングし，漸近最適なスケジューリングを極めて高速に求めるアルゴリズムを導いてきている．本年度は，そのアルゴリズムにおいて，プロローグ部分にも計算を導入して定常ラウンドと同等に扱い，余った計算をエピローグ部分に回す改良を行った．さらにラウンドサイズをできるだけ大きく取ることによりラウンド数を削減した．その結果，理論的下限に非常に近い値を実現できるようになった．

2.2 ロバスト構造化文書処理技術

研究者：武市正人，胡振江，松崎公紀
（情報理工学系研究科 数理情報学専攻）

目的：XML (eXtensible Markup Language) などの構造化文書のなかにプログラムの記述を許す PSD (Programable Structured Document) の手法を提案し，関数プログラミングやプログラム変換手法などを適用することにより，ロバストでかつ効率的な構造化文書処理の実現を目指す．

成果：仕様記述に適した双方向に変換可能なプログラム言語 X を設計した．言語 X は，文書から表示への変換を記述するための言語であり，言語 X で書かれた全ての変換に対して，その逆変換である表示から文書への変換の自動導出が可能である．この言語 X を用いることにより，XML の文書から生成されるエディタ上の表示情報を編集したとき，その変更を元の文書に正しく反映させることができる．

コンピュータのファイルは，別名（ファイルのショートカットやシンボリックリンクなど）を用いることにより利便性を増しているが，一方で複数の名前が非対称な関係で用いられるためユーザに混乱を生じさせている．そのような問題を解決するために，双方向変換の技術を用いて，ファイルの参照すべてを対称かつ統一的に抽象化して取り扱うことができるファイルマネージャ「梅林 (Bi-Link)」を実現した．梅林では，ファイル参照を双方向変換により複数のファイル参照に変換する方法を用いている．その結果，複数のファイル参照は互いに同期され，1 つに加えられた変更は別の同期されたファイル参照に反映される特徴を持つ．

さらに，対話的学習教材の作成支援環境として，利用者が与えた入力に基づいて内容が動的に変化する文章である iDocument およびその作成ツール iDocument Builder を開発した．また，iDocument の応用として，チュートリアル (iTutotial) や教科書 (iTextBook)，試験 (iExam) などを対話的や動的に行えるシステムも開発した．

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 +，藤田八郎 +
(+ 情報理工学系研究科 数理情報学専攻)
(* 新領域創成科学研究科 複雑理工学専攻)

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」な通信および記録を実現するための符号化技術の開発を目指す．

成果：定常性やエルゴード性を一切仮定しない一般情報源に対して，データ圧縮符号として重要な FV (Fixed-Variable length) 符号の漸近性能を明らかにした．また，高性能なユニバーサル符号の一部としてよく利用されているが，特性解析が困難であった MTF (Move-to-Front) 法の性能を理論的に詳細に解析し，MTF 法で圧縮限界であるエントロピーレートを達成できる情報源のクラスを明らかにした．

誤り訂正に関しては，量子連接符号の構成法を提案した．さらに，情報セキュリティ問題に関しては，一般アクセス構造に対する強い秘密分散法の構成方法，量子秘密分散法の理論解析と構成法，木構造を用いるグループ鍵管理システムの漸近特性，相関情報源を伴う

シャノン暗号システム，盗聴者に対して安全なネットワーク符号化法などに対して符号化定理を証明した．特にシャノン暗号システムに関しては，従来安全性指標としてよく用いられている曖昧さ（暗号文を知ったときの平文に対する条件付きエントロピー）ではなく，暗号文を知ったときに平文を推測するために必要な推測回数の期待値や平文の推測確率を安全性指標として用いる場合に対して，符号化定理を証明している．

2.4 超ロバスト幾何計算

研究者：

杉原厚吉，西田徹志，谷口隆晴，松浦史郎（情報理工学系研究科 数理情報学専攻）

目的：形と動きに関する幾何学的な情報を処理するアルゴリズムでは，数値誤差により位相構造の判定を誤ることにより，実際の世界ではあり得ない状況が生じてアルゴリズムが破綻する可能性がある．このように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指す．

成果：円に対するユークリッド距離ボロノイ図の構成アルゴリズムを，下記のようにさまざまな手法により作成した．(1) 円の中心点のボロノイ図から出発して接続関係を変更していくことにより構成するアルゴリズム．(2) 厳密計算法の考え方を直接適用して構成するアルゴリズム．(3) ディジタル位相優先法による構成アルゴリズム．また，(3) に関しては，円のパッキング問題に適用することにより，その有効性を確認した．さらに，3 次元の球ボロノイ図についても，3 次元ディジタル画像近似を利用することで，安定に計算できる見通しを得た．

流れの中の最短到達時間問題は，流れを伴う領域内の始点の集合から終点の集合まで動くのにかかる最短時間を求める問題である．最短時間で進むためには，等距離曲線の法線方向へ進める必要があるが，法線を決定するときにその近傍の粒子に依存する方式では破綻を起こす．これに対して，近傍に依存することなく法線方向を決定し，破綻が生じない安全な数値計算法を考案した．

さらに，波動シミュレーションにおける境界条件の取り扱いに関して，十分滑らかな解に対する無反射境界条件の有効性の検証と，不適切な問題に対する数値解の特徴づけに関して研究を行った．

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．

(A) 国際ワークショップ：

The Fourth Workshop on Programmable Structured Documents

日時： 2005 年 12 月 7 日〜9 日
会場： 東京大学山上会館
招聘者 4 名，参加者数約 30 名

(B) セミナー：

【超ロバスト幾何計算セミナー】

- “On-line Character Animation,” S. Y. Shin (2005/5/12)
- “EA とその関連研究,” 杉山学 (2005/10/28)
- “点対応を用いた複数の 2 次元画像からの 3 次元復元 —因子分解法の数理—,” 藤木淳 (2005/11/30)
- “Voronoi diagram of spheres and its applications,” D. Kim (2005/12/1)
- “Point-Based Methods in Shape Modeling and Physical Simulation,” L. J. Guibas (2006/2/10)

【ロバスト符号化セミナー】

- “Relationship among Complexities of Individual Sequences over Countable Alphabet,” 葛岡成晃 (2005/7/16)
- “暗号技術における擬似乱数生成,” 藤岡淳 (2005/7/16)
- “Redundancy of Symbol Decomposition Algorithms for Memoryless Source,” 川端勉 (20058/19)
- “無ひずみデータ埋め込みのためのユニバーサル法,” 横尾英俊 (2005/10/1)
- “Unconditionally Secure Steganography,” 四方順司 (2005/10/1)
- “Web ページのアクセス数計数に対する暗号学的アプローチ,” 尾形わかは (2005/10/1)
- “On Gaussian Approximation, Asymptotically Optimal Linear and Nonlinear Detectors in CDMA and Multiuser Detection,” M.Burnashev (2005/11/17)
- “文脈自由文法を用いた効率的な圧縮アルゴリズム,” 坂本比呂志 (2005/12/12)
- “CFTP を用いた Perfect Sampling,” 松井知己 (200512/12)
- “情報統計力学の方法,” 田中利幸 (2006/3/7)

【アルゴリズムセミナー】

- “Stiff systems of ODEs and sparse matrix techniques,” S. Skelboe (2005/11/21)

これらの研究集会には,「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 2005-06) Masaki MORIGUCHI and Kokichi SUGIHARA, “Isotropic and Feature-Preserving Mesh Simplification Based on Constrained Centroidal Voronoi Diagrams,” February 2005.
2. (SRCTR 2005-09) Kento EMOTO, Zhenjiang HU, Kazuhiko KAKEHI, and Masato TAKEICHI, “A Compositional Framework for Developing Parallel Programs on Two-Dimensional Arrays,” April 2005.
3. (SRCTR 2005-11) Akimasa MORIHATA, Kazuhiko KAKEHI, Zhenjiang HU, and Masato TAKEICHI, “Reversing Iterations: IO Swapping Leads You There And Back Again,” May 2005.
4. (SRCTR 2005-30) Kiminori MATSUZAKI, Zhenjiang HU, and Masato TAKEICHI, “Design and Implementation of General Tree Skeletons,” October 2005.
5. (SRCTR 2005-38) Kokichi SUGIHARA, “Sliver-free Perturbation for the Delaunay Tetrahedrization,” December 2005.
6. (SRCTR 2006-01) Hiroshi KAWAHARADA and Kokichi SUGIHARA, “C^k-continuity of Stationary Subdivision Schemes,” January 2006.

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」が開講されているが，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.

胡振江（5 月 25 日），杉原厚吉・川原田寛 (RA)（10 月 5 日），杉原厚吉・森口昌樹 (RA)（12 月 21 日）