

平成17年度科学研究費補助金（基盤研究（S））研究状況報告書

ふりがな(ローマ字)		SUGIHARA KOUKICHI					
①研究代表者氏名		杉原 厚吉		②所属研究機関・部局・職		東京大学・大学院情報理工学系研究科・教授	
③研究課題名	和文	超ロバスト計算パラダイムの構築					
	英文	Construction of Superrobust Computation Paradigm					
④研究経費		平成15年度	平成16年度	平成17年度	平成18年度	平成19年度	総合計
17年度以降は内約額 金額単位：千円		17,300	20,200	17,000	18,400	17,600	90,500
⑤研究組織（研究代表者及び研究分担者）							
氏名	所属研究機関・部局・職	現在の専門	役割分担（研究実施計画に対する分担事項）				
杉原 厚吉	東京大学・大学院情報理工学系研究科・教授	幾何数理工学	企画とまとめ、超ロバスト幾何計算				
小柳 義夫	東京大学・大学院情報理工学系研究科・教授	並列数値処理	超ロバスト並列計算				
山本 博資	東京大学・大学院新領域創成科学研究科・教授	情報理論	符号化を利用した超ロバスト計算				
室田 一雄	東京大学・大学院情報理工学系研究科・教授	数理工学	構造不変性に基づく超ロバスト計算				
竹村 彰通	東京大学・大学院情報理工学系研究科・教授	統計学	不確実性のモデル化に基づく超ロバスト計算				
萩谷 昌己	東京大学・大学院情報理工学系研究科・教授	計算機科学	超ロバスト分子計算				
今井 浩	東京大学・大学院情報理工学系研究科・教授	量子情報科学	超ロバスト量子計算				
松井 知己	東京大学・大学院情報理工学系研究科・助教授	大域的最適化	離散問題の連続緩和に基づく超ロバスト計算				
村重 淳	東京大学・大学院新領域創成科学研究科・助教授	数値解析	精度保証に基づく超ロバスト計算				
大石 泰章	東京大学・大学院情報理工学系研究科・講師	制御理論	離散と連続のシームレス結合に基づく超ロバスト制御				
駒木 文保	東京大学・大学院情報理工学系研究科・助教授	統計学	超ロバスト統計計算				
須田 礼仁	東京大学・大学院情報理工学系研究科・助教授	並列計算	超ロバストグリッド計算				
堀田 武彦	東京大学・大学院情報理工学系研究科・助教授	非線形解析	非線形超ロバスト計算				
岩田 覚	東京大学・大学院情報理工学系研究科・助教授	離散最適化	超ロバストネットワーク計算				
松尾 宇泰	東京大学・大学院情報理工学系研究科・講師	数値解析	物理法則不変性に基づく超ロバスト計算				
⑥当初の研究目的（交付申請書に記載した研究目的を簡潔に記入してください。）							
<p>計算は、数値誤差、データの不確実性、機器の故障、伝送誤りなど多くの外乱にさらされている。それらの外乱が発生しても安定に動作するロバストな計算技術の確立は安全な情報化社会を実現するための重要な課題である。本研究の目的は、従来から開発されつつある分野ごとの個別のロバスト計算技術を継続的に発展させるとともに、それらを横断的に整理し、分野の境界を超える共通で普遍的なロバスト計算原理を抽出することによって、ロバスト計算のためのアルゴリズム設計パラダイムを構築することである。研究課題につけた「超」は、この対象横断的な普遍的計算原理をめざすことを意味するものである。具体的には、本研究に参加する研究者が、物理シミュレーション、並列計算、制御、幾何計算、離散最適化、符号化計算などのそれぞれの研究分野で今まで個別に開発してきたロバスト計算のための技術を持ち寄り、その中から「対象構造の一貫性の保持」とでも言うべき共通の計算原理を抽出し体系化する。さらに、現在のデジタル計算機の限界を超える新しい計算原理として期待されている量子計算や分子計算の分野でのロバスト計算技術の知見も取り込むことによってこのパラダイムをより強力なものにする。</p>							

⑦これまでの研究経過（研究の進捗状況について、必要に応じて図表等を用いながら、具体的に記入してください。）

本研究では、従来から開発されつつある分野ごとの個別のロバスト計算技術を横断的に整理し、分野の境界を超える共通で普遍的なロバスト計算の方法を抽出することによって、ロバスト計算のためのアルゴリズム設計原理、すなわち超ロバスト計算パラダイムの構築を目指している。初年度には、この目的のために、超ロバスト計算原理の初期仮説として、「計算対象がもつべき何らかの不変構造の保持を、計算の過程で積極的に保証する機構を組み込むことによって、ロバストな計算アルゴリズムを作ることができる」という命題を設定した。そして研究参加者それぞれが開発しつつある個別のロバスト計算技術に、この仮説が当てはまるか否かを検討した。その結果、この初期仮説が多く分野に当てはまる見通しが立ったため、第2年度もこの仮説が適用できる事例を継続して蓄積した。これをまとめたのが、表1である。

表1. 不変構造に着目したロバスト計算技術の開発成果

外乱の種類	計算分野	不変構造	ロバスト計算技術		
数値誤差	数値解法	区間代数構造	精度保証計算	(小柳, 村重)	
		物理シミュレーション	エネルギー保存則	収束保証計算	(松尾)
	幾何計算	運動量保存則			
		位相不変量	位相優先法, 記号摂動法	(杉原)	
力学的系	力学系		デジタル位相優先法	(杉原)	
		散逸性	運動形態解析	(堀田)	
	物理的雑音	機械制御	エネルギー非増加性	連続と離散のシームレス統合	(大石)
情報通信	非同期計算	同期系列	誤り訂正, 秘密分散	(山本)	
		計算の非依存性	データマッピング	(小柳, 須田)	
組合せ爆発	最適化	離散凸性	離散凸解析の体系	(室田)	
		双対性	劣モジュラ関数最小化	(岩田)	
		符号不変性	構造的行列理論	(室田, 岩田)	
確率的ゆらぎ	小数データ検定	マルコフ性	完全サンプリング法	(松井)	
	量子計算	量子状態	デコーヒーレンス解析	(今井)	
	分子計算	DNA ゲート	ハイブリット結合	(萩谷)	
	統計計算	情報幾何空間	ベイズ推測・ベイズ予測	(竹村, 駒木)	

表1の成果のうち、いくつかの代表例について説明すると次のとおりである。幾何計算の分野では、計算対象の背景にある位相構造の一貫性の保持が計算のロバスト化に役立つことを以前から指摘してきたが、新たに対象のデジタル近似から得られるデジタルトポロジーの構造を利用する方法を開発した。数値計算・物理シミュレーションの分野では、エネルギー保存則、運動量保存則など背景となる物理現象が満たす法則を、微分方程式を差分方程式で近似する際に失われないように配慮することによって、計算が発散しないことを保証できるようになった。並列計算の分野では、データおよび計算の依存関係を表すグラフ構造の性質を利用して、ロバストで均等な負荷分散を実現する方法を構成し、分子動力学の並列計算に適用してその有効性を確認した。統計計算の分野では、統計モデル多様体の座標変換に対する不変量に着目して性能のよいベイズ予測・ベイズ推測の方法を開発した。情報通信の分野では、FV 符号語に生じた誤りビットの伝播を防止することのできる同期系列の効率のよい導出法を構成した。最適化の分野では、離散凸関数が満たす性質として、離散ヘッセ行列と局所2次展開を定義し、それによってある種の離散凸関数を特徴づけることができた。小数データ検定の分野では、背景となるマルコフ過程を抽出し、その定常分布に厳密に従うサンプルを生成する完全サンプリング法を構成した。

⑧特記事項 (これまでの研究において得られた、独創性・新規性を格段に発展させる結果あるいは可能性、新たな知見、学問的・学術的なインパクト等特記すべき事項があれば記入してください。)

(1) 新位相優先法の開発

幾何計算の分野においては、数値誤差と退化に対してロバストなアルゴリズムを設計するために、私たちが従来から開発してきた位相優先法を、図形のデジタル近似構造と組み合わせることによって、その汎用性と使いやすさを格段に高めた。位相優先法とは、計算対象となる幾何構造の背景にある位相的性質の一貫性を数値計算結果より優先させることによって、計算のロバスト性を確保するアルゴリズム設計法である。この方法は、浮動小数点表示がいらぬなど多くの利点をもつものの、対象の位相的性質を抽出するために、問題ごとに対象の洞察が必要であり、初心者には利用しにくいものであった。本研究では、位相抽出作業を、対象のデジタル近似を利用した位相抽出に置き換えることによって、この問題点を克服し、位相優先法を初心者にも使いやすい設計原理へと進化させた。これにより、従来は難しかった高次元一般化ボロノイ図などの曲線・曲面を多く含む幾何構造も扱えるようになり、3次元球ボロノイ図などのアルゴリズムの実装に成功した。これらの成果について第10回計算と組合せ国際会議(COCOON2004)において、研究代表者 杉原厚吉が招待講演を行った。またこの成果は、ロバスト幾何計算が必要とする実務家からも注目され、メッシュ生成の分野で世界最大である Meshing Roundtable 国際会議でも本年9月に杉原が招待講演をする予定である。さらにこの手法は、東京大学より「勢力圏計算法およびそのプログラム」と題する特許としても申請した。

(2) 離散凸解析の体系化

離散世界における最適化を横断的に眺めることのできる理論作りをめざして、離散凸性に着目したアルゴリズムの体系化を行っている。その中で効率のよい最適化アルゴリズムの背景にマトロイド性や劣モジュラ性などの共通の構造が潜むことを明らかにした。特に、連続世界から離散世界へ移るとき、値の離散性だけでなく方向の離散性も重要であるという認識と、それから生まれる2種類の離散凸性を基礎として、離散凸関数のクラスの階層を構築するとともに、連続世界で重要な共役性と双対性が離散の世界でもいろいろな形で成立することを明らかにしてきた。また、これらの理論構造に立脚して、ネットワークの最小費用流問題を劣モジュラ流問題へ一般化し、それを解くアルゴリズムも構成した。さらに、最近では数理経済学などへの応用も展開している。これらの一連の成果に対して、研究分担者 室田一雄は、2005年2月に井上学術賞を受賞している。また、このような枠組に基づいて、劣モジュラ関数の最小化問題に対して、長い間未解決であった強多項式アルゴリズムを構成することもできた。この成果に対して、研究分担者 岩田寛は2004年8月に Fulkerson 賞を受賞している。また、室田、岩田が指導した大学院学生 平井広志、針谷尚幸、松岡祐治がそれぞれ別の論文で日本オペレーションズ・リサーチ学会学生論文賞を受賞している。

(3) マルコフチェーンの完全サンプリング

2組の要因の有意差を小数データからロバストに検定するための一手段である2元分割表の完全なサンプリング法を構成することができた。これは、与えられた2元分割表データに対して、同じ行和と列和をもつすべてのデータからサンプルを偏りなく得るための手法である。本手法では、そのようなサンプルが現れるマルコフ過程を構成し、定常状態に達したところでサンプリングを行う。一般に、このようなマルコフ過程が定常状態に達するまでのステップ数は膨大であるが、時間を逆方向に動かしながら過程を追跡するというアイデアによって、短時間に定常状態サンプリングを可能にした。この成果に対して、研究分担者 松井知己の指導する大学院生 来嶋秀治は、2005年2月に NZIMA Conference and ACCMC Student Award を受賞している。

(4) ボロノイ図とその応用国際会議シリーズの立ち上げ

ロバスト計算が充実しつつある幾何計算の分野で代表的なボロノイ図をテーマに取り上げて、その各種の応用を論じる国際会議を2004年9月に本基盤研究と東京大学 COE 情報科学技術戦略コアプログラムとの共催で開催した。ボロノイ図は、自然現象、社会現象などの多様な場面で現れる基本幾何データ構造であるが、近年の超ロバスト計算技術の発展により、その実用場面への応用が可能となりつつある。この機会をとらえて、化学、材料科学、都市工学、画像処理、グラフィックスなど広範な応用分野の研究者が学際的に交流することを目的としたものである。海外から十数名の参加者を得て24件の発表を行った。この会議は、当初は単発の会議として企画したが、海外からの強い要請により、各国の持ち回りで毎年開催することが決まった。第2回目は2005年10月にソウルで開かれ、2006年はヨーロッパまたは北米での開催が予定されている。このように新しい国際会議のシリーズを日本から立ち上げることができ、この分野への大きな国際貢献となった。

⑨研究成果の発表状況 (この研究費による成果の発表に限り、学術誌等に発表した論文(掲載が確定しているものを含む。)の全著者名、論文名、学協会誌名、巻(号)、最初と最後のページ、発表年(西暦)、及び国際会議、学会等における発表状況について記入してください。なお、代表的な論文3件に○を、また研究代表者に下線を付してください。)

- L. Ros, K. Sugihara and R. Thomas: Shape representation using trihedral mesh projections. *Visual Computer*, vol. 19, no. 2-3, 2003, pp. 139-150.
- K. Murotani and K. Sugihara: Globally smooth interpolation using Gregory patches over irregular meshes. *International Journal on Shape Modeling*, vol. 9, no. 1, 2003, pp. 21-39.
- K. Sugihara: Hyperpolygons generated by the invertible Minkowski sum of polygons. *Pattern Recognition Letters*, vol. 25, 2004, pp. 551-560.
- K. Sugihara, M. Sawai, H. Sano, D.-S. Kim and D. Kim: Disk packing for the estimation of the size of a wire bundle. *Japan Journal of Industrial and Applied Mathematics*, vol. 21, no. 3, 2004, pp. 259-278.
- 神田毅, 杉原厚吉, 森本康彦: 幾何アルゴリズム加速のための混合演算に関する研究. *日本応用数理学会論文誌*, vol. 14, no. 2, 2004, pp. 117-150.
- 室谷浩平, 杉原厚吉: 大域的滑らかさを優先した標高データからの地形復元法の提案. *GIS-理論と応用*, vol. 12, no. 1, 2004, pp. 1-13.
- A. Nukada, A. Nishida and Y. Oyanagi: Parallel implementation of FFT algorithm on distributed shared memory architecture and its optimization. *IPS Transactions on Advanced Computing Systems*, vol. 44(SIG 6 (ACS 1)), 2003, pp. 1-8.
- A. Fujii, A. Nishida and Y. Oyanagi: Parallel AMG algorithm by domain decomposition. *IPSJ Transactions on Advanced Computing Systems*, vol. 44 (SIG 6 (ACS 1)), 2003, pp. 9-17.
- 蓬来祐一郎, 西田晃, 小柳義夫: 木構造型ネットワークにおける最適ブロードキャストスケジューリング. *情報処理学会論文誌「コンピューティングシステム」*, vol. 45, no. SIG3, 2004, pp. 100-108.
- M. Iwamoto and H. Yamamoto: A construction method of visual secret sharing schemes for plural secret images. *IEICE Trans. on Fundamentals*, vol. E86.A, no. 10, 2003, pp. 2577-2588.
- Y. Matsunaga and H. Yamamoto: A coding theorem for lossy data compression by LDPC codes. *IEEE Trans. on Inform. Theory*, vol. 49, no. 9, 2003, pp. 2225-2229.
- J. Geelen, S. Iwata and K. Murota: The linear delta-matroid parity problem. *J. Combinatorial Theory*, vol. B88, 2003, pp. 377-398.
- S. Moriguchi and K. Murota: Capacity scaling algorithm for scalable M-convex submodular flow problems, *Optimization Methods and Software*, vol. 18, no. 2, 2003, pp. 207-218.
- K. Murota: Note on multimodularity and L-convexity. *Mathematics of Operations Research*, 2005, 掲載予定.
- H. Hirai and K. Murota: M-convex functions and tree metrics. *Japan Journal of Industrial and Applied Mathematics*, vol. 21, no. 3, 2004, pp. 391-403.
- K. Murota and A. Shioura: Fundamental properties of M-convex and L-convex functions in continuous variables. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, no. 5, 2004, pp. 1042-1052.
- 力徳正輝, 平井広志, 室田一雄: 2段階アルゴリズムによるSVMの解法. *日本応用数理学会論文誌*, vol. 14, no. 4, 2004, pp. 221-234.
- S. Moriguchi and K. Murota: Discrete Hessian matrix for L-convex Functions. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2005, 掲載予定.
- K. Murota and A. Shioura: Conjugacy relationship between M-convex and L-convex functions in continuous variables. *Mathematical Programming*, vol. 101, no. 3, 2004, pp. 415-433.
- K. Murota and A. Tamura: Proximity theorems of discrete convex functions. *Mathematical Programming*, vol. A99, no. 3, 2004, pp. 539-562.
- K. Murota, H. Saito and R. Weismantel: Optimality criteria for a class of nonlinear integer programs. *Operations Research Letters*, vol. 32, no. 5, 2004, pp. 468-472.
- K. Murota and A. Shioura: Quadratic M-convex and L-convex functions. *Advances in Applied Mathematics*, vol. 33, no. 2, 2004, pp. 31-41.

- T. Suzuki, S. Aoki and K. Murota: Use of primal-dual technique in the network algorithm for two-way contingency tables. *Japan Journal of Industrial and Applied Mathematics*, vol. 22, no. 1, 2005, pp. 133–146.
- 力徳正輝, 平井広志, 室田一雄: 2段階アルゴリズムによるSVMの解法. *日本応用数理学会論文誌*, vol. 14, no. 4, 2004, pp. 221–234.
- S. Aoki and A. Takemura: Minimal basis for a connected Markov chain over $3 \times 3 \times K$ contingency tables with fixed two-dimensional marginals. *Australian & New Zealand Journal of Statistics*, vol. 45, no. 2, 2003, pp. 229–249.
- A. Takemura and S. Kuriki: Tail probability via the tube formula when the critical radius is zero. *Bernoulli*, vol. 9, no. 3, 2003, pp. 535–558.
- S. Kuriki and A. Takemura: Tail probabilities of the limiting null distributions of the Anderson–Stephens statistics. *Journal of Multivariate Analysis*, vol. 89, 2004, pp. 261–291.
- H. Kamiya and A. Takemura: Characterization of rankings generated by linear discriminant analysis. *Journal of Multivariate Analysis*, vol. 92, 2004, pp. 343–358.
- A. Takemura and S. Aoki: Some characterizations of minimal Markov basis for sampling from discrete conditional distributions. *Annals of Institute of Statistical Mathematics*, vol. 56, no. 1, 2004, pp. 1–17.
- S. Aoki and A. Takemura: Markov chain Monte Carlo exact tests for incomplete two-way contingency tables. *Journal of Statistical Computation and Simulation*, to appear.
- M. Hagiya, R. Takemura, K. Takahashi and T. Saito: Verification of authentication protocols based on the binding relation. *Computer Software*, vol. 20, 2003, pp. 17–29.
- J. A. Rose, A. Takano, M. Hagiya and A. Suyama: A DNA computing-based genetic program for in vitro protein evolution via constrained pseudomodule shuffling. *Journal of Genetic Programming and Evolvable Machines*, vol. 4, 2003, pp. 139–152.
- W.-Y. Hwang, K. Matsumoto, H. Imai, J. Kim and H.-W. Lee: Shor-Preiskill-type security proof for concatenated Bennett-Brassard 1984 quantum-key-distribution protocol. *Phys. Rev. A*, vol. 67:024302, 2003.
- H. Fan, H. Imai, K. Matsumoto and X.-B. Wang: Phase-covariant quantum cloning of qubits. *Phys. Rev. A*, vol. 67:022317, 2003.
- Y. Asano, T. Ito, H. Imai, M. Toyoda, M. Kitsuregawa: Compact encoding of the web graph exploiting various power distributions. *IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E87-A, no. 5, 2004, pp. 1183–1184.
- M. Hayashi, H. Imai, K. Matsumoto, M. B. Ruskai, T. Shimono: Qubit channels which require four inputs to achieve capacity: Implications for additivity conjectures. *Contingency Tables, Quantum Information and Computation*, vol. 5, no. 1, 2005, pp. 13–31.
- Y. Asano, H. Imai, M. Toyoda and M. Kitsuregawa: Finding neighbor communities in the web using an inter-site graph. *IEICE Transaction on Information and Systems*, vol. E87-D, no. 9, 2004, pp. 2163–2170.
- S. Matuura and T. Matsui: New approximation algorithms for MAX 2SAT and MAX DICUT. *Journal of Operations Research Society of Japan*, vol. 46, 2003, pp. 178–188.
- T. Matsui, Y. Matsui and Y. Ono: Random generation of $2 \times 2 \times \dots \times 2 \times J$ contingency tables. *Theoretical Computer Science*, vol. 326, 2004, pp. 117–135.
- Y. Miyamoto and T. Matsui: Linear time approximation algorithm for multicoloring lattice graphs with diagonals. *Journal of Operations Research Society of Japan*, vol. 47, no. 2, 2004, pp. 123–128.
- R. Miyashiro and T. Matsui: A polynomial time algorithm to find an equitable home-away assignment. *Operations Research Letters*, vol. 33, 2005, pp. 235–241.
- S. Kijima and T. Matsui: Approximate counting scheme for $m \times n$ contingency tables. *IEICE Transactions on Information and Systems*, vol. E87-D, 2004, pp. 308–314.
- G. Tanaka, S. Murashige and K. Aihara: Bifurcation structures of period-adding phenomena in an ocean internal wave model. *International Journal of Bifurcation and Chaos*, vol. 13, 2003, pp. 3409–3424.

- Y. Oishi and H. Kimura: Computational complexity of randomized algorithms for solving parameter-dependent linear matrix inequalities. *Automatica*, vol. 39, no. 12, 2003, pp. 2149–2156.
- F. Tanaka and F. Komaki: The sectional curvature of AR model manifolds. *Tensor*, 2003.
- F. Komaki: Simultaneous prediction of independent Poisson observables. *the Annals of Statistics*, vol. 32, no. 4, 2004, pp. 1744–1769.
- T. Fushiki, F. Komaki and K. Aihara: On parametric bootstrapping and Bayesian prediction. *Scandinavian Journal of Statistics*, vol. 31, no. 3, 2004, pp. 403–416.
- R. Suda: Stability analysis of the fast Legendre transform algorithm based on the fast multipole method. *Proceedings of the Estonian Academy of Sciences, Physics, Mathematics*, vol. 53, no. 2, 2004, pp. 107–115.
- R. Suda and S. Kuriyama: Another preprocessing algorithm for generalized one-dimensional fast multipole method. *Journal of Computational Physics*, no. 195, 2004, pp. 790–803.
- M. A. Sanjuan, T. Horita and K. Aihara: Opening a closed Hamiltonian map. *Chaos*, vol. 13, no. 1, 2003, pp. 17–24.
- S. Iwata and N. Zuiki: A network flow approach to cost allocation in rooted trees. *Networks*, vol. 44, no.4, 2004, pp. 297–301.

このほかに International computing and Combinatorics Conference (COCOON), Computational International Conference on Computational Science and Application (ICCSA), International Meeting on High Performance Computing for Computational Science (VECPAR), International Symposium on High Performance Computational Science and Engineering (HPCSE), IEEE International Symposium on Information Theory, ACM-SIAM Symposium on Discrete Algorithms (SODA), International IPCO Conference, World Congress of the Bernoulli Society for Mathematical Statistics and Probability, International Meeting on DNA Based Computers などの国際会議において英語による 34 件の発表を行った。

また、電子情報通信学会、情報処理学会、日本応用数理学会、日本流体力学会、情報理論とその応用シンポジウム、オペレーションズリサーチ学会などにおいて、35 件の発表を行った。