様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　６月１４日現在

機関番号：１２６１２
研究種目：基盤研究(C)
研究期間：2010　～　2012
課題番号：２２５００００１１

研究課題名（和文）マルチコア並列処理を指向した準数値アルゴリズムと実装法の研究

研究課題名（英文）Research on multi-core oriented parallel algorithms and implementation techniques for seminumerical processing

研究代表者
村尾　裕一（MURAO　HIROKAZU）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：60174265

研究成果の概要（和文）：
GPU や汎用 CPU に普及しているマルチコアプロセッサを数式処理をはじめとした準数値アルゴリズムに活用する方法の研究を行った。具体的には、多倍長整数の RNS 表現、多項式と線形代数の基本演算、陰関数の正確描画、多項式の補間による決定を題材として、マルチコア並列処理に適した計算法の構築を実証的に行った。関連研究として、数式データの Web での活用技術の検討、パズルの最短経路解の GPU による探索の実験も行った。

研究成果の概要（英文）：
We investigated appropriate methods to apply multi-core parallelism with GPUs and general-purpose CPUs to computer algebraic or seminumerical algorithms. More concretely, we treated RNS representation of big-integers, basic arithmetics of polynomials and in linear algebra, exact method for plotting implicit functions, polynomial interpolation, and developed multi-core oriented parallel computing methods for these topics based on empirical studies. As related topics, we investigated Web technology for treating mathematical expressions interactively, and developed a GPU-accelerated optimal solver for Rubik cubes.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２０１０年度	1,000,000	300,000	1,300,000
２０１１年度	700,000	210,000	910,000
２０１２年度	600,000	180,000	780,000
年度			
年度			
総　計	2,300,000	690,000	2,990,000

研究分野：総合領域
科研費の分科・細目：情報学、情報学基礎
キーワード：情報数理

１．研究開始当初の背景

マルチコアのプロセッサは広く普及し、高い並列処理性能を有するに至ったグラフィックスプロセッサ（以下 GPU）の利用も含めた、一般の数値計算で活用するための研究は盛んに行われている。一方、数式処理や暗号

計算などで用いられる準数値処理に関しては、

- 複雑な数理的技法のソフトウェアも十分に実用化されているとはいえ、計算対象とその複雑さはいくらでも大規模になる可能性を秘めており、その度合は数値計算の場合よりも著しい
- 数式処理の分野での進展は、代数や理論的な研究が極端に進んでおり、数式処理システム等のソフトウェアの利用者は増加する一方で、コンピュータの利用技術は追い付いておらず、その乖離の度合は数値計算の場合よりも大きい

などを考慮すると、高性能な並列処理を効果的に適用できれば、大きな効果が期待され、新聞にも報じられたように計算科学における何らかのブレークスルーとなるだろう。このような期待は世界的なもので、国際的なワークショップも近年になり復活している。何らかの変革を実現するには、理論的には解明済みの算法を数学的に既知のこととせずに、適切な計算題材と算法を選び出すことと、そのための並列処理向きの計算技法を開拓することが必要である。実際、今日脚光を浴びているグレブナー基底も実用的な計算ができるようになるまでには、数値計算で培われた計算手法の導入など、20 年以上の時間を要している。本研究の目的は、このような認識のもとで、準数値処理におけるマルチコア並列処理に適した算法を検討し、適切な計算技法を開拓することである。特に GPU に関しては、CUDA, OpenCL などの汎用的なプログラミング環境も登場してきているが、記号処理や数式処理への利用可能性は全くの未知数である。本計画ではその有効利用を主要な研究テーマのひとつとする。同様の研究は米・仏やカナダのグループなど数例があるが、上述のとおり算法の数理的理解と計算技法に関する知識と洞察を必要とするため実践的な研究を行っている者は世界でも非常に限られている。そのため本計画の研究内容の大半は独自のものと言うことができる。

２．研究の目的

本研究の目的は、マルチコア CPU を数式処理などの準数値処理に活用するためにスレッド並列処理に適したアルゴリズムを開発し、ソフトウェアの適切な構成法と実装法を見出すことである。GPU を含めたマルチコア CPU の高い性能は数値処理において発揮されるが、数式処理等の記号処理において直接生かすことは難しい。本研究では、数式処理や暗号計算で用いられるある種の準数値アルゴリズムに対して数値処理を融合させた算法を構築し、その数値処理部分にマルチコア処理を適用してその性能を活用するという計算法を開拓する。具体的には、RNS で表現された多倍長整数の演算、多項式基本演算のためのライブラリ、陰関数描画、多項式補間による未知多項式の決定などを計算題材とし、これらを様々なマルチコアアーキテクチャに適合させる計算手法を開拓する。同時に、数式をより扱い易くするためのインタフェースについても検討する。

３．研究の方法

研究の具体的な題材と内容について説明する。先ず、数値処理の得意なプロセッサ群を活用するために、数値処理を主要な計算とすることは必須である。数値・数式を融合させたり、大規模な並列・分散処理を行うにはいくつかの手法が考えられるが、本研究では、大規模化する可能性のある代数的算法の中から基本的な準数値算法を抽出し、計算対象の式を代数的な意味構造に依らないデータ構造で表現して数値処理的高速化技法を適用することにする。数式処理に数値処理を導入する計算手法は、限定子除去(QE) の柱形代数分解(CAD) 法の高速算法等の最新鋭の計算手法とも一致する。これらの高位かつ複雑な数理的算法（の基本部分）にまで、計算機科学及びソフトウェアの技術を適用し高性能なハードウェアを活用できるようにすることは本研究の究極の目標である。具体的には次の題材を対象として研究を進める。

- 任意多倍長整数と RNS 表現 : 数式処理では数として任意精度の多倍長整数を扱うが、複数の法の元での剰余の列として表現すれば容易に並列化される。計算精度の問題は、用いる法の数すなわち並列度に置き換えられる。同様の数理的手法が RNS と呼ばれてハードウェア分野で広く研究され活用されていることに気づいた。それら手法及び Montgomery 乗算等の暗号計算で培われた算法を、並列処理に適した形にしてソフトウェアにも導入する。その際、メモリ管理に関する工夫とメモリ階層を意識した計算手法も検討する。
- 多項式基本演算および基本線形演算ライブラリの整備と拡張 : 従来から開発してきた数式処理向けの基本演算ライブラリを拡張し、キャッシュ・メモリの構成・スレッドの利用法を考慮した CUDA や Cell 等への適合、16bit 整数版の開発を行う。更に、次項の描画のための区間数と上記の RNS への拡張を行う。
- 陰関数を含めた関数の描画 : 孤立点を持つような陰関数をも正確に描画するために、独自の描画法の改良を進めている。その方法は、描画空間の全てのセルに対し描画すべきか否かの評価と描画対象セル群の探索からなり、その計算量は一般には膨大だが、適切な近似や実装法により実用に耐えるところまで改良が進んでいる。ここで

数式処理は必須であり、更なる正確さや性能の改良を追求するには数式のままでの変換と式の大量の評価・数値化の高速処理が必要なため、数値処理だけではなし得ず、かつ高性能な数値演算プロセッサを活用するという格好の題材となる。ここでは、前項の区間数の利用を主に検討し算法と実装の研究を行う。また、描画情報の適切な表現法と再描画のための算法や計算手法を検討する。

- 多項式の補間法による式の構成：式の数値化を伴う計算として多項式補間がある。ある未知の多項式について、その評価値を大量に求めその数値列から多項式を特定する方法で、評価の部分には高い並列性があり、実際、代表者らによる従来の結果が示すように、並列処理は究めて有効である。多変数の場合、古典的な算法は計算量の増加が並列度では追い付かず使いものにならなくなる可能性があるが、数式処理で培われた疎な多項式に対する算法を用いてこの問題を解決する。その算法の改良と、数値処理部と数式処理部の間でのデータの交換方法の実装が主な研究課題となる。
- 構造を持つデータ（数式）に対するデータ交換法と通信技術の確立：上述の計算では、大量の数値処理と汎用の数式計算を分離し適切なプロセッサに役割分担させるという手法をとるため、プロセッサ間での数式と数値の円滑な送受信の方法が必要となる。データ交換の方法には W3C が規定する MathML や OpenMath の方式と既存ソフトウェアを参考にする。これを発展させ、WEB 環境下での数式計算のデバッグ環境の可能性についても検討する。

４．研究成果

実証的な研究を進めるためには、先ず対象とする計算機環境をある程度絞る必要がある。汎用 CPU でのマルチスレッド処理の応用については、従来から実証実験を進めてきており、マルチコア CPU の一般化・普及に伴いその利用技術（OpenMP, コンパイラによる SIMD 命令のサポート等）が強化されているとは言え、準数値処理での利用技術に大きな影響を及ぼすような変革は研究期間中にはもたらされていない。注目すべきは 128 ビット SIMD の SSE から拡張された AVX 命令で、その後整数にも対応する AVX2 へと進展しているが、製品が流通し始めたのは本計画終了後であり、この一般的な用途での利用と利用法の検討は今後の課題である。性能向上を目指すには数値計算で培われた技術を用いればよいことは従来の実験から既知である。更に、その方面においては、本研究の目的の一部ともしている線形代数の計算において、性能を極め記録を達成するための方法の開拓と最大規模の計算が木村欣司（京都大学）により独自の手法を用いて実施されている。これらのことから、本計画では汎用のマルチコア CPU は比較の基準としての利用にとどめ、GPU の応用を主たる焦点として研究開発を進めることとした。一方 GPU については、本計画を立案する時点では、GPGPU の研究では NVIDIA 社の CUDA の利用が主流で、かつ、性能を引き出すにはハードウェア資源を意識したプログラミングが必要で、本計画では、計算規模に見合った資源の適切な利用法に関する知見を得ることも目標のひとつとした。その後の GPU の新機種ではキャッシュを豊富に搭載するようになり、その結果、そのような知見の獲得はほぼ不要となった。その一方、ATI/AMD 社も GPGPU の開発環境 Stream の提供を開始したり、タブレットなどで用いられる SoC もマルチコアするばかりか GPU の搭載も予定され、更に、汎用 CPU も含めたこれらのマルチコアプロセッサ向けのプログラミング API として OpenCL が定義され実用的にもなってきた。このような状況において、本計画の研究内容を将来にわたり有用なものとするために、多様な開発環境や API の調査が必要となり、想定外に多大な時間を要することとなった。まとめると、あくまでもその時点での状況だが、整数計算に基づく暗号計算でも ATI 社の GPU が優れる（場合がある）こと、OpenCL は十分に利用価値があり高まっていくであろうこと、NVIDIA 社の GPU でも OpenCL は十分に利用可能で実行性能は CUDA による場合よりは現時点では劣るとは言え数倍程度に収まること、NVIDIA 社のタブレット向けのチップがかなりの高性能化することと次々世代では CUDA が利用可能となること、などが知見として得られた。結果として、NVIDIA 社一社に限っても様々な開発形態がありうるように、可能性は多様すぎるため、本計画では、これらの進展を観察しつつも、研究開発は取り敢えず CUDA に絞って進めることとした。

(1) 任意多倍長整数と RNS 表現：
多倍長整数を扱うアルゴリズムに中国剰余定理を適用してアルゴリズム全体を並列化する手法は、有効な方法としてよく知られているが、GPU での SIMT 処理を用いる場合にはその粒度をどの程度まで小さくできるかを検討すること（或いは、回路設計で培われた RNS 技術の GPU 向けのソフトウェア実装）が本課題の目的である。これまでに、ひとつの数値処理当たりある程度の演算量が必要となる例として、Montgomery 乗算による大量の冪乗剰余計算を試しているが、数体系の変換がオーバーヘッドとなり有効ではなかった。本計画では、両端の値を有理数とした区間数を考え、更にそこ

で扱う整数値をRNSで表現し算術計算を行うこととし、そのような数を大量に扱う場合にSIMTによる並列処理を行う。そのような計算の例として後述の陰関数描画があり、実証済みの研究結果は発表を行い、また、別の計算手法についてはどのような計算部品に分解すべきかを検討し論文としてまとめた（未発表）。関連する話題では、RNS表現された一連の多倍長整数の符号判定にSIMTによる並列処理がある。我々は多倍長数相当の表現に変換を行う旧来の方法では用いる数式の子細な変更が演算量ひいては計算時間に大きく影響することを経験し報告しているが、回路設計の分野で開発されている浮動小数を用いる方法との比較も必要であろう。現実には、必要となる小数の精度と、GPU実機（低価格な一般的な機種）での精度と性能の問題があるため、理論的究明にとどまった。

(2) 多項式基本演算および基本線形演算ライブラリの整備と拡張：
本題材については、計算手法はほぼ固まってきており、高速化にはキャッシュの活用法等の数値処理を対象とした高性能計算の分野で培われた技術を活用すればよいことは既知のとおりである。新規性を主張するには、木村欣司（京都大）が行っている、問題毎にギリギリまで検討を行った計算法と実装技術を（多大な労力をかけて）独自に開発する（賞賛に値する）必要があると考え、我々は普通のプログラミングでもGPUは十分に活用可能であることを示すにとどめた。計算例として、Wiedemannアルゴリズムによる、多数の有限体上の行列の逆行列の計算を扱い、計算精度の変更によるメモリ所要量と計算時間の変化の計測を行った。併せて、疎な行列についても、既知の方法での表現とメモリアクセスパターンによる計算時間の比較を行った。この結果については、国際会議でも発表を行っている。

(3) 陰関数を含めた関数の描画：
実装技術に関する研究については(1)で述べた。本項目の主な研究対象は、３次元の陰関数を（孤立特異点も含め）正確に描画するアルゴリズムの開拓と効率の良い具体的な計算法の実現であり、元々の開発者の齋藤友克（㈱アルファオメガ）らと連携研究者の主導で研究が進められた。数学的興味で扱う数式や（高次の）陰関数を扱う場合、浮動小数では精度が不足したり、孤立した特異点を見落とす可能性があるといった問題が発生する。これらへの適切な対処法を理論的に検討してきた結果、実用上はほぼ十分と思われる方法を考案してはいるが、完全と言えるアルゴリズムを発案するまでには至らなかった。一方で、正確な描画法を確立済みの２次元に投影して描画する方法の検討も行った。その場合、２次元の正確描画の処理速度が問題となるので、２次元描画の高速化も（上記の方法に従って）進めた。これらの研究の進展状況について、逐次、研究会等で発表を行った。

(4) 多項式の補間法による式の構成：
ここで用いる補間法は、代表者が過去に開発した、疎な多項式を決定するためのアルゴリズムである。このアルゴリズムは、過去に分散メモリの並列処理計算機でも実証したとおり、一部で高い並列処理効率（スーパーリニア）を示すが，一方で組合せ爆発の問題も存在している。この後半の問題は、GPUでの整数の計算精度不足にも起因するが、精度により問題規模がどのように変化するかと、多数のコアの利用によりどの程度緩和されうるのかの検討を実証的に進めた。多くのデータはプロセッサ間で共有が望まれる一方、ベクトル処理には向かないタスク並列型の処理にGPUの多数のコアを生かすことができるかが鍵となるが、適切な評価関数を設定するなどの工夫をすることにより、コア数に対して十分な性能の向上を得ることができた。また一方で、この問題は一定手数内の解の探索に等しいが、類似の問題となるRubik cubeの最短解の探索について、GPUによる効率化の実証実験を行い、同様の高速化が得られた。この手法と結果については、GPU関連の最大の国際会議で発表を行った。

(5) 構造を持つデータ（数式）に対するデータ交換法と通信技術の確立：
本計画では、実用的な数式の通信方式の開発も進め、その最も極端な場合としてタブレットPCでの活用法についても検討を行った。最新のWeb技術と連携させることにより、省略表記なども含めた数式の対話的な表示方法の提案を行った。

その他、上に挙げた題材以外にも、暗号計算やファイル圧縮・文字列探索などへのGPU並列処理技術の応用について、これまで進めてきた研究のまとめも行っている。

本計画の期間中に発生した想定外の事態と冒頭に述べた計算環境の変遷により、当初計画していた最低限のラインに到達できていない題材がいくつかある。本計画で得られた成果と知見をもとに、未達成の部分については研究を継続していくと共に、すべての面において発展を目指していく所存である。

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８件）

① 近藤祐史，兵頭礼子，村尾裕一，齋藤友克．3 変数陰関数描画について．数式処理，第 4 回基礎理論・システム合同分科会（2012 年 1 月 21～22 日．仙台青葉カルチャーセンター）報告．査読無．2013 年．53-54.

② 近藤祐史，兵頭礼子，村尾裕一，齋藤友克．有理区間数と GPU 並列による陰関数描画について．京都大学数理解析研究所講究録，No.1815．査読無．2012．163-167.

③ 近藤祐史，兵頭礼子，村尾裕一，齋藤友克．3 変数の陰関数描画について．数式処理．大会報告，査読無．第 18 巻，2 号．2012．68-71.

④ 兵頭礼子，近藤祐史，村尾裕一，齋藤友克．Risa/Asir の行列演算と改良について．京都大学数理解析研究所，講究録 No.1785．査読無．2012．162-166．http://hdl.handle.net/2433/172729.

⑤ 村尾裕一，近藤祐史，兵頭礼子，齋藤友克．数式を省略して表示する方法の提案と検討．京都大学数理解析研究所講究録，No.1780．査読無．2012．232-242．http://hdl.handle.net/2433/171815.

⑥ 近藤祐史，兵頭礼子，村尾裕一，齋藤友克．GPU 並列処理による陰関数描画について．数式処理．第 3 回システム分科会研究会（2011 年 1 月 22 日．福岡大学）報告．査読無．第 18 巻，1 号．2011．35-39.

⑦ 村尾裕一，鈴木省吾，近藤祐史，齋藤友克．有理区間数と GPU 並列処理について．数式処理．大会報告．査読無．第 17 巻，2 号．2011．28-31.

⑧ Y.Nakano, H.Murao and D.Morimitsu. Design and Implementation of a WEB-browser Tool BrEdiMa for Mathematical Expressions. Communications of JSSAC. 査読有．Vol.1, No.1. 2012. pp.75-91. http://www.jssac.org/Editor/CJssac/V01/V01_105.pdf.

〔学会発表〕（計１１件）

① H.Hayakawa and H.Murao. Optimal Rubik’s Cube Solver on GPU. GTC2013(GPU Technology Conference 2013). 2013 年 3 月 18～21 日．San Jose McEnery Convention Center. CA, USA.

② 早川広記，村尾裕一．Rubik cube の最少手数解の探索の GPU を用いた高速化．Risa/Asir Conference 2013. 2013 年 3 月 16～18 日．神戸大学.

③ 村尾裕一．分割統治法による整数 GCD の高速アルゴリズムの実現に向けて．Risa/Asir Conference 2013. 2013 年 3 月 16～18 日．神戸大学.

④ 近藤祐史，兵頭礼子，村尾裕一，齋藤友克．3 変数の陰関数描画について．研究集会「数式処理―その研究と目指すもの―」．2012 年 12 月 25～27 日．京都大学数理解析研究所．（講究録用原稿準備中）.

⑤ H.Murao and H.Hagiwara. Exact Linear-system Solving via GPU-Accelerated Iterative Method over Finite-fields. PMAA2012: 7th International Workshop on Parallel Matrix Algorithms and Applications. 2012 年 6 月 28～30 日．Birkbeck University of London. UK.

⑥ 萩原尚，宮下宏樹，村尾裕一．数式処理への GPU の応用と有効性．Risa/Asir Conference 2012. 2012 年 3 月 20～22 日．神戸大学.

⑦ 萩原尚，村尾裕一．GPU を用いた有限体上の線形方程式の解法の高速化．HPCS2012:2012 年ハイパフォーマンスコンピューティングと計算科学シンポジウム．2012 年 1 月 24～26 日．名古屋大学．ポスターP3-2.

⑧ 宮下宏樹，村尾裕一．GPU を用いた疎な多項式補間の高速処理法．HPCS2012：2012 年ハイパフォーマンスコンピューティングと計算科学シンポジウム．2012 年 1 月 24～26 日．名古屋大学．ポスターP3-3.

⑨ 村尾裕一 ほか．GPU の準数値演算と文字列処理への応用．2010 年度特異値・固有値合同ワークショップ．2010 年 11 月 27 日．筑波大学.

⑩ 村尾裕一，宮下宏樹，萩原尚．準数値処理の GPU 並列処理の試行実験．Risa/Asir Conference 2011. 2011 年 3 月 23 日．神戸大学.

⑪ 兵頭礼子，近藤祐史，村尾裕一，齋藤友克．多変数代数方程式の零点位置の判定アルゴリズム．日本数式処理学会，第 3 回理論分科会研究会．2011 年 2 月 17 日．新潟大学.

６．研究組織
(1)研究代表者
村尾　裕一（MURAO HIROKAZU）
電気通信大学・大学院情報理工学研究科・准教授
研究者番号：60174265

(3)連携研究者
近藤　祐史（KONDOH YUJI）
香川高等専門学校・電子情報通信工学系情報工学科・准教授
研究者番号：20259948