早稲田大学大学院理工学研究科

博 士 論 文 概 要

論 文 題 目

多数桁計算における高速アルゴリズムの研究

Studies on Fast Algorithms for High-precision Computation

申 請 者

氏 名		
	後	保範
	Yasunori	Ushiro

専攻・研究指導 (課程内のみ)

2004 年 11 月

本研究の目的は、多数桁で構成される計算システムの基となる高速アルゴリズムを確立し、その有効性を評価することである。多数桁計算システムで最も重要かつ基本となる計算アルゴリズムは、多数桁の乗算に関するものである。その理由は、n桁の加減算の計算量は$O(n)$であるのに対して、筆算方式（筆算と同じ計算方式のこと）による乗算の計算量は$O(n^2)$になり、計算量のオーダーが異なるためである。次に重要な計算アルゴリズムの一つは、多数桁関数の計算である。三角関数や指数関数等の数学関数はTaylor展開で無限級数に展開でき、n桁の関数値の計算量は必要な項数までの和を計算すると$O(n^2)$以上となるためである。関数計算と同様に多数桁計算で重要なアルゴリズムとして、4倍精度以上の多倍長精度の値を要素に持つ行列計算がある。その理由は、多数桁高速乗算方式が筆算方式より高速にできるのは、数百桁と長い桁数が必要のためである。これらに対応するため、多数桁高速アルゴリズムとして高速剰余変換の定義と多数桁乗算への応用、分割有理数化法による級数の多数桁計算、及び多倍長精度の高速行列乗算を考案している。また、これらの数値実験結果として、多数桁の分割乗算及び2002年11月24日に達成した円周率の世界記録計算が述べられている。

本論文は7章から構成される。第一章「はじめに」では研究の目的と概要が述べられている。

第二章「高速剰余変換による多数桁乗算」では、高速剰余変換の定義と多数桁乗算への応用が述べられている。多数桁計算の計算量を削減するためのアルゴリズムは種々考案されており、桁数nが大きい場合は高速フーリエ変換(FFT)が一番高速で、乗算の計算量は$O(n(\log n)(\log \log n))$となる。しかし、FFTは本来、信号処理や偏微分方程式を数値的に解くために考案された計算法であり、多数桁乗算を目的としたものではない。そのため、FFTを使用した多数桁乗算は計算過程が直感的に把握しにくく、多数桁乗算の応用への見通しが悪いと見ることもできる。また、FFTだけを使用した多数桁乗算は、途中変換でメモリを多く使用する欠点がある。使用メモリ量を削減する方法として、Karatsuba法と合わせて使用する方法があるが、メモリ量を削減するためKaratsuba法の適用回数を増やすと、計算量が増加するジレンマがある。本研究では、FFTに剰余理論を取り込んだ高速剰余変換（Fast Modulo Transformation、FMT）を定義し、多数桁乗算への応用として複素FMTの直接利用、巡回乗算、2段階FMT及び分割乗算が考案されている。複素FMTの直接利用により、FFTによる多数桁乗算に実FFTを利用していたのを、半分の要素の複素FMTで計算可能にした。実FFTは、入力が実数の複素FFTの結果が共役複素数になるのを利用した計算で、複素FFTの結果から変換すると最初と最後の要素を特別扱いする必要があり、分散メモリでの並列化等が複雑で性能劣化の元になっていた。巡回乗算はFFTによる正巡回と負巡回乗算が知られていたが、FMTでは±1だけでなく自然数αに対して$\pm\alpha$で巡回する多数桁乗算も可能となる。2段階FMTによる乗算とは、1要素に多数桁を持つ2N要素の乗算を

$P=\omega^N+1$を法とする整数FMTで行い、そこで発生する要素ごとの負巡回乗算にもFMTを使用する方法である。基底ωは2以上の任意の整数を選ぶことができる。多数桁の乗算において、FFTとFMTでは導出法は異なるが計算式は同一で、FFTに整数上の変換も含めればFMTに対する理論はFFTにそのまま適用できる。

第三章「分割有理数化法による級数の多数桁計算」では、無限級数関数の多数桁関数値の高速計算方法が述べられている。多数桁関数で表されるπ(円周率)やe(自然対数の底)等の数学定数は無限有理級数で入力値がO(1)桁の有理数である。一方、多数桁関数の計算をシステム的に閉じるには、入力値が結果と同一精度の桁数の必要がある。そこで、入力値の桁数がO(1)桁と短い有理数の場合に有効な計算法と、入力値が結果と同一の桁数の場合に有効な計算法が考案されている。第1の方法は、有理級数の和の計算にトーナメント方式を適用し2項ずつ通分して有理数化し、多数桁除算で目的の桁数の実数にする方法である。第2の方法は多数桁精度の入力値Vに分母の桁数β、2β、4β、…、2^pβ桁ずつの有理数に分解し、分割ごとに関数値を計算し、それらに加法定理を使用してVでの関数値を計算する方法である。二つの計算方法を合わせて分割有理数化法(Divide and Rationalize Method、DRM法)と名付ける。無限級数で展開される関数の通常の計算方法では、精度的に必要な項数で打ち切りそれらの和を計算する。そのため、n桁乗算の計算量をM(n)とするとき、入力の桁数がO(1)桁の有理数の場合はn桁精度の関数値計算に$O(n^2)$の計算量が、入力値がn桁精度の場合にはO(M(n)n)の計算量が必要である。これに対して、n桁精度の関数値の計算にDRM法を適用すると、入力値がO(1)桁の有理数の場合は計算量を$O(M(n)(\log n)^2)$に、入力値がn桁精度で加法定理が適用できる場合は、計算量を$O(M(n)(\log n)^3)$に削減できる。本方法は各種関数値の計算で有名なBrentのアルゴリズムより適用範囲が広く、連分数の計算や基底変換にも利用可能で、これまで知られているアルゴリズムより単純で分かり易いという特長を持つ。

第四章「多倍長精度の高速行列乗算」では、多倍長精度の値を要素にもつ行列乗算の高速化法と数値実験結果が述べられている。現在の計算機は、10進16桁程度の倍精度浮動小数点演算はハードウエアで高速に行える。また、4倍精度演算もFORTRANやC言語で可能なものが多いが、ソフトウエア実行であるため計算速度は倍精度演算に比較して1桁程度遅くなる。ここでは、4倍精度以上の多数桁の数値を係数とする連立一次方程式の解の計算における高速化を目的に、その基本となる行列乗算の高速化アルゴリズムを考案した。多数桁の乗算には入力値を一定の桁数に分割し筆算方式で計算する方法以外に、中国剰余定理(百五減算)及びFFTを使用する方式がある。しかし、多数桁乗算でこれらの方法が筆算方式より高速になるのは数百桁と計算桁数が長い時である。一方、多数桁の値を係数とするn次元の行列乗算にこれらの方式を適用する場合は、それらの線形性が利用可能である。この点に着目すると、n次元の行列乗算に利用する、中国剰余定理及

びFFTの適用回数を$O(n^3)$から$O(n^2)$に削減して、多数桁の乗算が可能になる。この原理を利用して、多倍長精度の値を係数にもつn次元の行列乗算に、$O(n^2)$回の中国剰余定理又はFFTを適用する高速計算アルゴリズムが考案されている。計算桁数が比較的短いときに中国剰余定理が有利で、計算桁数が長くなるとFFTが有利となる。行列乗算において、中国剰余定理は4倍精度から筆算方式より高速になる。ここでは理論と数値実験結果が共に示されている。

第五章「多数桁の分割乗算」では、第二章の適用例としてファイルI/Oを使用した多数桁分割乗算方式と数値実験結果が述べられている。本研究で考案した高速アルゴリズムが、理論通りの高速性を示すか評価するため、それらを重点的に適用した数値実験を行った。FMTの適用例として、DiskファイルI/Oを利用した多数桁の分割乗算方式が示されている。本研究で提案された分割乗算法は、拡張FMTの適用によりFMTを分割しても分割しない時と同じ計算量にする方法と、ダイレクトI/Oにより必要なデータを非連続に入出力して、総I/O量を分割数に依存させなくする方法で構成される。分割乗算法については、複素FMTを使用する方法と2段階FMTを使用する方法の、それぞれの具体的アルゴリズムと数値実験結果が示されている。ファイルI/Oを使用した多数桁の分割乗算は、使用計算機のメモリ容量を越えた桁数の乗算をする場合に必要となる。FFTを使用した多数桁乗算をm分割すると、計算量は分割しないときのm倍になると言われていた。また、ファイルI/Oを利用しFFTによる多数桁乗算をm分割すると、ファイルI/Oの総量も分割しないときのm倍になると言われていた。これに対して、FMTによるm分割乗算のアルゴリズムを使用することにより、n桁計算の計算量は$O(n(\log n)(\log\log n))$でファイルI/Oの総量は$O(n)$となり、共に分割しない時と同じで、n桁計算に必要なメモリ量は分割しない時の約1/mに減少する。

第六章「1.2兆桁π計算の世界記録」では、第三章の適用例として10進1兆2411億桁の円周率世界記録達成について述べられている。また、DRM法の適用例として、2002年11月24日に達成した10進表現で1兆2411億桁、16進表現で1兆307億桁の円周率の世界記録達成について記述されている。本計算は、DRM法の有効性を実際の大規模な計算で確認するために実施されたもので、１プロセッサーによるπ計算の基本プログラムは申請者が一人で作成した。本記録は、同一メモリ容量(1Tバイト)の計算機を使用して、前回の記録約2061億桁を6倍更新した。そのため、πの計算公式を算術幾何平均法(AGM法、ガウス・ルジャンドル公式)からArctan公式に変更し、DRM法と2段階FFT(2段階FMT)による多数桁乗算を適用し、約8万行の計算プログラムで実施された。この計算では、DRM法の基底変換の適用性を評価することも目的とし、従来とは異なり16進数のπを計算し、10進数に変換する方式を採用した。円周率の世界記録樹立計算では、誤演算防止対策等の多数の工夫点に付いても記述されている。

第七章「おわりに」ではまとめと今後の方針が述べられている。

研 究 業 績

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
論文　(1)	○ 後 保範：高速剰余変換による多数桁乗算，情報処理学会論文誌，Vol.44 No.12，pp.3131-3138(2003).
(2)	○ 後 保範，金田康正，高橋大介：級数に基づく多数桁計算の演算量削減を実現する分割有理数化法，情報処理学会論文誌，Vol.41 No.6，pp.1811-1819 (2000).
(3)	小国 力,○後 保範,長堀文子：スーパーコンピュータにおけるリストベクトルの利用技術,情報処理学会論文誌，Vol.27 No.1，pp.11-19 (1986).
(4)	小国 力,○後 保範,西方政春,長堀文子：直接解法による連立一次方程式のコンピュータ解法の特性解析，情報処理学会論文誌，Vol.25 No.5，pp.804-812(1984).
総説　(1)	○ 後 保範：多倍長精度の値を係数とする行列の高速乗算方式，京大数理研講究録 [偏微分方程式の数値解法とその周辺II] 1198，pp. 170-178 (2001).
(2)	○後 保範，金田康正，高橋大介：無限級数に基づく多数桁計算の演算量削減を実現する分割有理数化法，京大数理研講究録 [数値計算における前処理の研究] 1084，pp.60-71 (1999).
(3)	田村良明，吉野さやか，○後 保範，金田康正：円周率－高速計算法と数値の統計性，情報処理学会第25回プログラミング・シンポジウム報告集，pp.1-15(1984).
(4)	Y.Kanada, Y.Tamura, S.Yoshino, ○Y.Ushiro：Calculation of π to 10,013,395 Decimal Placed Based on the Gauss-Legendre Algorithm and Gauss Arctangent Relation, Computer Center University of Tokyo Technical Report, pp.1-13 (1983).
講演　(1)	○後 保範：円周率世界記録と多数桁乗算方式，早稲田大学理工学部，戸田セミナー (2004/7/17)
(2)	○後 保範：高速剰余変換(FMT)の応用，第32回数値解析シンポジウム (NAS2003) (2003/5/21-23)
(3)	○後 保範：円周率世界記録6倍更新の工夫，早稲田大学 7Fセミナー (2003/5/16)
(4)	○後 保範：FFTと百五減算による多数桁乗算，第31回数値解析シンポジウム(NAS2002) (2002/6/12-14)
(5)	○後 保範：反復解法への多倍長精度高速計算の適用，第30回数値解析シンポジウム(NAS2001) (2001/5/23-25)
(6)	○後 保範：多倍長精度の値を係数とする行列の高速乗算方式，京大数理解析研究所 [偏微分方程式の数値解法とその周辺 II] (2000/11/20-22)
(7)	○後 保範：多倍長精度の行列乗算方式，第29回数値解析シンポジウム(NAS200) (2000/6/7-9)
(8)	○後 保範：逆数型無限級数のn桁計算の演算量を削減する前処理方式，京大数理解析研究所 [数値計算における前処理の研究] (1998/11/9)
(9)	○後 保範，長堀文子：ベクトル計算機による整数上のFFT計算，情報処理学会全国大会 No.27 (1983/10)

研 究 業 績

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
その他 (論文)(1)	Ogita,T., Oishi,S., Ushiro,Y.：Computation of Sharp Rigorous Component wise Error Bounds for the Approximate Solutions of Systems of Linear Equations, Reliable Computing Vol.9, pp.229-239 (2003).
(2)	Ogita,T., Oishi,S., Ushiro,Y.：Fast inclusion and residual iteration for solutions of matrix equations, Computing [Supplement 16, Inclusion Methods for Nonlinear Problems], pp.171-184 (2002).
(3)	Ogita,T., Oishi,S., Ushiro,Y.：Fast verification of solutions for sparse monotone matrix equations, Computing [Supplement 15, Topics in Numerical Analysis], pp.175-187 (2001).
(総説)(1)	後 保範：行列乗算におけるストラッセンの方法の拡張，京大数理研講究録 [数値計算アルゴリズムの研究] 1040, pp.61-99 (1998).
(2)	後 保範：有限要素法の連立一次方程式ベクトル並列向き反復解法，京大数理研講究録 [数値解析とそのアルゴリズム] 791, pp.49-62 (1992).
(3)	後 保範：対称用改定CR法の収束性，京大数理研講究録 [数値解析と計算科学]746, pp.37-46 (1991).
(4)	後 保範：ナビェストーク方程式への連立ILUCGS法適用効果，京大数理研講究録 [数値解析と科学計算] 717, pp.104-117 (1990).
(5)	後 保範：偏微分方程式向き数値シミュレーション言語DEQSOL，第3回ベクトル計算機応用シンポジウム論文集，pp.115-123 (1987).
(6)	後 保範，今野千里，他3：DEQSOLとスーパーコンピュータ向け応用ソフト，日立評論[スーパーコンピュータに関する論文集]，Vol.69 No.12, pp.35-42 (1987).
(7)	後 保範，栂野佳子：スーパーコンピュータS-810による拡散方程式の数値計算，京大数理研講究録 [スーパーコンピュータのための数値計算アルゴリズムの研究] 613, pp.12-27 (1987).
(8)	後 保範：大型疎行列に対するPCG,PCR法，コンピュートロール，No.12, pp.16-22 (1985).
(9)	後 保範：移流拡散方程式に対するベクトル向きPCG法，京大数理研講究録 [大型の線形計算に関する研究] 548, pp.147-168 (1985).
(10)	後 保範：ベクトル計算機向きICCG法，京大数理研講究録 [並列数値計算アルゴリズムとその周辺] 514, pp.110-134 (1984).
(11)	後 保範，西方正春，長堀文子：スーパーコンピュータ“HITAC S-810”による行列計算，日立評論[最近のコンピュータ技術とスーパーコンピュータに関する論文集]，Vol.65 No.8, pp.29-34 (1983).
(12)	後 保範：ベクトル計算向き不完全三角分解，京大数理研講究録「数値計算アルゴリズムの研究」453, pp.102-126 (1982).
(13)	後 保範，小高俊彦：ベクトル計算機による大規模計算，情報処理学会 数値解析研究会資料 2 , pp.1-10 (1982).
(14)	その他 10 件

研　究　業　績

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
(講演)(1)	後 保範：丸め誤差を対称に保った角柱周りの流れ解析，第33回数値解析シンポジウム (NAS2004) (2004/5/19-21)
(2)	後 保範：ストラッセン法の拡張方式におけるSR2201への適用効果，東京大学地震研究所共同研究集会「大規模計算と並列計算機」(1998/7/6-7)
(3)	後 保範：行列計算におけるストラッセンの方法の拡張，京大数理解析研究所「数値 計算アルゴリズムの研究」(1997/11/26-28)
(4)	Ushiro,Y.：Performance for Matrix Computation and its application, Cambridge University (Symposium on high performance computing for the tera-scale information age) (1996/7/8)
(5)	後 保範：有限要素法の連立一次方程式ベクトル並列向き反復解法，京大数理解析研究所「数値計算アルゴリズムの研究」(1991/11)
(6)	後 保範：ナビェストーク方程式への連立ILUCGS法適用効果，京大数理解析研究所「数値解析と科学計算」(1989/11/29-31)
(7)	後 保範：移流拡散方程式に対するベクトル向きPCG法，京大数理解析研究所「大型の線形計算に関するアルゴリズムの研究」(1984/9/6-8)
(8)	後 保範：スーパーコンピュータHITACH-S-810による拡散方程式の数値計算，電子通信学会全国大会 (1984/9)
(9)	後 保範：ベクトル計算機向き ICCG 法，京大数理解析研究所「並列数値計算アルゴリズムとその周辺」(1983/11/24-26)
(10)	後 保範：CG法と同時逆反復法の組み合わせによる固有値計算，京大数理解析研究所「数値計算のアルゴリズムの研究」(1982/11/18-20)
(11)	後 保範：不完全三角分解と共役傾斜法による大次元行列の固有値計算，情報処理学会全国大会 No.22 (1981/4)
(12)	その他 19 件
(特許)	
(米国)(1)	Ushiro,Y.：Method of and apparatus for preconditioning of a coefficient matrix of simultaneous linear equations. Patent(NO. 5,604,911), February 18, 1997
(2)	Ushiro,Y., Nagashima,S., Kawabe,S.：Processor for carrying out vector operation wherein the same vector element is used repeatedly in succession. Patent(NO. 4,621,324), November 4, 1986
(日本)(1)	江澤良孝，マーチン・フィールド，後 保範：連立一次方程式に関する計算装置， 特開 2002-149630，平成 14(2002)年 5 月 24 日
(2)	後 保範：連立一次方程式に関する計算装置， 特開平 06-168262，平成 6 年(1994)6 月 14 日
(3)	田中慎一，後 保範：連立一次方程式の並列計算装置， 特開平 06-028387，平成 6 年(1994)2 月 4 日
(4)	後 保範：連立一次方程式に関する計算装置， 特開平 05－081310，平成 5 年(1993)4 月 2 日