様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　　元 年　　６ 月 １１ 日現在

機関番号：１２１０２
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００１６８

研究課題名（和文）メニーコア超並列クラスタにおける有理数演算ライブラリに関する研究

研究課題名（英文）Research on Rational Number Arithmetic Library in Many-Core Massively Parallel Cluster

研究代表者
高橋　大介（TAKAHASHI, Daisuke）

筑波大学・計算科学研究センター・教授

研究者番号：００２９２７１４

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：多倍長整数演算の階層においてSIMD命令を用いたベクトル化を行った。具体的にはSIMD命令を用いて複数の被除数と除数に対する符号なし64ビット整数除算を高速化し性能評価を行った。この手法を用いて、数学定数の特定の桁を計算するBBP型公式の高速計算法を提案した。また、多倍長整数乗算において基数縮小表現を用いることでIntel AVX-512命令によるベクトル化を行った。そして、有理数算術演算プログラミング環境において有理数算術演算を高速化するためのモジュラー算術演算の実装を行った。

研究成果の学術的意義や社会的意義
多倍長演算ライブラリとしてGNU Multi-Precision Library（GMP）が知られているが、SIMD命令はほとんど用いられていない。本研究課題では多倍長乗算および複数の被除数と除数に対する符号なし64ビット整数除算をSIMD命令を用いて高速化することができた。多倍長演算は現在公開鍵暗号などで広く用いられており、本研究課題で提案した手法はこれらの高速化に貢献できると期待できる。

研究成果の概要（英文）：We performed vectorization using SIMD instructions in the hierarchy of multiple-precision integer arithmetic. Specifically, we evaluated the performance by speeding up unsigned 64-bit integer division for multiple dividend and divisor using SIMD instructions. Using this method, we proposed a fast calculation method of BBP type formula that calculates a specific digit of mathematical constants. In addition, vectorization with Intel AVX-512 instruction is performed by using reduced-radix representation in multiple-precision integer multiplication. We implemented modular arithmetic to speed up rational arithmetic in a rational arithmetic programming environment.

研究分野：高性能計算

キーワード：有理数算術演算　多倍長整数演算　モジュラー算術演算　SIMD化

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

数値計算の多くは浮動小数点演算によって行われることが多い。しかし、大規模な科学技術計算を行うにあたり、最近になって倍精度（64 ビット）浮動小数点演算では精度が不足するケースがあることが指摘されてきた。このような場合、より精度の高い 4 倍精度（128 ビット）浮動小数点演算や多倍長精度浮動小数点演算が用いられている。しかし、多倍長精度浮動小数点演算を用いたとしても数値を表す記憶領域は固定長であるため、計算誤差の介入は避けられない。

一方で有理数演算を用いることで計算誤差の介入を排除できるという利点があるが、記憶領域を多く使うこと、計算時間が膨大になるという欠点があり、これまで広く使われてこなかった。しかし、有理数演算をメニーコア超並列クラスタで行うことにより、扱える問題サイズの増大および計算時間の短縮を図ることが可能であると考えられる。さらに、多倍長精度乗算に高速フーリエ変換（Fast Fourier Transform、FFT）を用いて n 桁どうしの多倍長精度乗算を O(n log n log log n)の計算量で行うことで、有理数演算の計算時間を大幅に短縮することができる。

有理数演算を行うことができるライブラリとして，GMP（GNU Multiple-Precision Library）が知られている。しかし、GMP においては SIMD 命令を用いたベクトル化がほとんど行われていないという課題があった。これまでに研究代表者はメニーコアプロセッサである Intel Xeon Phi コプロセッサにおいて SIMD 命令およびスレッド並列を用いた多倍長精度浮動小数点演算の実現と評価を行い、桁数が大きな領域においては GMP に比べて高速に計算できることを示した。また、FFT を用いた多倍長精度乗算の計算時間の大部分は FFT の処理であるため、FFT を高速化することが重要になる。これまでに研究代表者は並列 FFT アルゴリズムの研究に従事してきており、並列化した FFT ライブラリ FFTE のソースコードを http://www.ffte.jp/で公開している。

２．研究の目的

本研究の目的は、有理数演算をメニーコア型超並列クラスタで行うことにより、扱える問題サイズの増大および計算時間の短縮を図ると共に、実現した有理数演算ライブラリの性能評価を行い、有理数演算の有効性を実証することである。

これまでの研究成果を十分に活用し、以下の点について明らかにする。(1) 多倍長整数演算および有理数演算の階層において SIMD 命令を用いたベクトル化を行う。(2) 線形計算の階層において MPI と OpenMP によるハイブリッド並列化を行うことで、扱える問題サイズの増大および計算時間の短縮を図る。(3) メニーコア超並列クラスタにおいて実現した有理数演算ライブラリの性能評価を行い、有理数演算の有効性を実証する。

３．研究の方法

研究計画の進め方は以下の通りである。(1) 多倍長整数演算と有理数演算の階層において SIMD 命令を用いたベクトル化を行う、(2) 線形計算の階層において MPI 並列化および MPI と OpenMP によるハイブリッド並列化を行う、(3) メニーコア超並列クラスタにおいて有理数演算ライブラリの性能評価を行う。

多倍長整数演算と有理数演算の階層において SIMD 命令を用いたベクトル化を行う。桁数が約 1 万桁を超える多倍長整数どうしの乗算において、FFT を用いることで計算時間を短縮することが有効である。そこで FFT において SIMD 命令を用いたベクトル化を行う。その際にはキャッシュブロッキングなどの高速化手法も適用する。また、FFT のデータ点数が n=2^p・3^q・5^r のような場合にも対応できるようにする。多倍長整数の加減算や乗算においてベクトル化を阻害する要因はキャリーやボローの伝搬の処理である。これらの処理をベクトル化するために、桁上げ先見（carry look-ahead）方式や桁上げ飛び越し（carry skip）方式を用いることができる。また有理数演算において、分数の通分や約分を行うためには最大公約数（GCD）の計算を高速に行う必要がある。そこで、GCD を高速に計算するアルゴリズムとして知られている再帰 2 進 GCD アルゴリズムについても SIMD 命令を用いたベクトル化を行う。

平成 29 年度は、線形計算の階層において MPI 並列化および MPI と OpenMP によるハイブリッド並列化を行う。ハイブリッド並列化を行うにあたっては、各 MPI プロセス内における並列度をメニーコアプロセッサのコア数よりも多くする必要がある。また、計算と通信のオーバーラップを行うことで、実行時間を短縮するなどの工夫も行う。

平成 30 年度は、有理数演算ライブラリを用いたベンチマークプログラムの作成およびメニーコア超並列クラスタにおける性能評価を行う。

４．研究成果

(1) SIMD 命令を用いた複数の整数除算の高速化

整数除算は多くのアプリケーションで広く用いられている演算の一つである。一般的に除算は加減乗算に比べて遅いことが知られている。多くのプロセッサでは整数加減乗算の SIMD 命令がサポートされているが、整数除算の SIMD 命令をサポートしているプロセッサはほとんど存在しないのが現状である。また、逆数を用いて整数除算を求めるアルゴリズムが提案されているが、

いずれも SIMD 命令を用いたベクトル化は考慮されていない。そこで、SIMD 命令を用いて複数の被除数と除数に対する符号なし 64 ビット整数除算を高速化し性能評価を行った。提案手法では、IEEE 754 規格に準拠した浮動小数点演算を用いて符号なし 64 ビット整数除算を行う。Newton-Raphson 法を用いると共に、単精度および倍精度浮動小数点演算を用いて SIMD 化を行うことで Intel 64 命令セットの符号なし 64 ビット整数除算命令や Intel SVML（Short Vector Mathematical Library）に含まれている符号なし 64 ビット整数除算の組み込み関数に比べて高速に整数除算が行えることを示した。さらに、SIMD 命令である Intel AVX-512 命令を用いて複数の 128 ビットの被除数と 64 ビットの除数に対する符号なし整数除算を高速化した。被除数が 128 ビットで除数および商が 64 ビットの符号なし整数除算は、96 ビットの被除数と 64 ビットの除数に対する符号なし整数除算を 2 回行うことで計算することができる。96 ビットの被除数と 64 ビットの除数に対する符号なし整数除算を行う際には、上位 64 ビットの被除数と上位 32 ビットの除数に対する符号なし整数除算で商を近似する。最終的には剰余が除数の値より小さくなるように商の近似値を補正することにより正確な商が得られる。Intel Xeon Phi 7250 プロセッサにおける性能評価の結果、提案手法が Intel 64 命令セットの符号なし整数除算命令に比べて約 2.3 倍高速に整数除算を実行できることを示した。

(2) 数学定数の特定の桁を計算する BBP 型公式の高速計算法

π のような数学定数の n 桁目の数字だけを計算することは、最初の n 桁をすべて計算するよりも簡単ではないと広く信じられていた。ところが、1995 年に発見された BBP（Bailey-Borwein-Plouffe）型公式により、いくつかの超越数の n 桁目の数字だけをさまざまな基数で計算できることが示された。BBP 型公式は多倍長精度演算が不要であり、容易に実装できる。またメモリをほとんど必要としない特徴がある。BBP 型公式における主要な計算である、べき剰余の計算は Montgomery 乗算を用いることで時間の掛かる除算を実質的に行うことなく、乗算、加減算およびシフト演算のみで計算することができる。また、192 ビットの被除数を 64 ビットの除数で割る整数除算において、剰余の値が事前に分かっていれば、この除算は exact division アルゴリズムを用いることで高速に行うことができる。さらに、複数のべき剰余と複数の整数除算に対して SIMD 化および並列化を行うことができることを示した。

(3) Intel AVX-512 命令を用いた整数乗算

整数乗算は多くのアプリケーションで用いられている演算の一つである。多倍長演算ライブラリとして GMP が知られているが、SIMD 命令はほとんど用いられていない。そこで、SIMD 命令である Intel AVX-512 命令を用いて多倍長整数乗算を高速化した。多倍長整数の加減算や乗算においてベクトル化を阻害する要因はキャリーやボローの伝搬の処理である。これらの処理をベクトル化するために、Reduced-radix 表現を用いることでキャリーの伝搬処理の回数を削減すると共に、ベクトル化を行うことができた。Intel Xeon Phi 7250 プロセッサにおける性能評価の結果、提案手法が GMP に比べて最大で約 2.5 倍高速に整数乗算を実行できることを示した。

(4) モジュラー算術演算

本研究課題で開発した有理数演算プログラミング環境では、分母・分子を可変長の多桁数で保持する有理数を、C++の演算子多重定義を用いて実装することで、四則演算を+、-、*、/の記号で書くことができる。これにより、有理算術演算による数値計算を、浮動小数点演算のようにプログラミングできるが、計算の高速化が課題となっていた。有理数算術演算プログラミング環境において有理算術演算を高速化するためのモジュラー算術演算（modular arithmetic）を可能とするための bigint クラスと modular クラスを作成した。

５．主な発表論文等

〔雑誌論文〕（計 2 件）

① Daisuke Takahashi, On the computation and verification of π using BBP-type formulas, The Ramanujan Journal, (in press).（査読有）
② Daisuke Takahashi, Computation of the 100 quadrillionth hexadecimal digit of π on a cluster of Intel Xeon Phi processors, Parallel Computing, Vol. 75, pp. 1-10 (2018).（査読有）

〔学会発表〕（計 4 件）

① 高橋大介, Intel AVX-512 命令を用いた複数の整数除算の高速化, 日本応用数理学会 2018 年度年会, 2018 年 9 月 4 日, 名古屋大学東山キャンパス（愛知県名古屋市）.
② Takuya Edamatsu and Daisuke Takahashi, Acceleration of Large Integer Multiplication with Intel AVX-512 Instructions, Proc. 20th IEEE International Conference on High Performance Computing and Communications (HPCC-2018), pp. 211-218 (2018).
③ 高橋大介, 数学定数の特定の桁を計算する BBP 型公式の高速計算法, 日本応用数理学会 2017 年度年会, 2017 年 9 月 7 日, 武蔵野大学有明キャンパス（東京都江東区）.
④ 高橋大介, SIMD 命令を用いた整数除算の高速化, 日本応用数理学会 2016 年度年会, 2016

年 9 月 12 日，北九州国際会議場（福岡県北九州市）.

６．研究組織
(1)研究協力者
研究協力者氏名：寒川　光
ローマ字氏名：SAMUKAWA HIKARU

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。