5706

量子信号検出理論における誤り率計算アルゴリズムへ GPU を用いた性能改善の一検討

A study on performance improvement of error rate calculation algorithm using GPU in Quantum Detection Theory

07538　松田健
指導教員　清水哲也

1. はじめに

光通信量子暗号 Y-00 の性能を評価する方法として，盗聴者の誤り率を用いる方法がある．現在，Y-00 で使用されている信号数は数千信号である．数千信号の誤り率を計算するには CPU では問題がある．そこで，本研究では，この問題の解決策として GPU を用いるという方法でアプローチを行う．

2. 研究方法

計算アルゴリズムでは，前処理として信号を行列にし，その行列の平方根を求める．この部分について CUDA を用いて並列化することで改善されると考えられる．行列 A の平方根を求める式を以下に示す．固有値をλ，固有ベクトルをλとする．

$$A^{1/2} = QD^{1/2}Q^{\dagger}$$

$$D^{1/2} = \mathrm{diag}[\sqrt{\lambda_1}, \sqrt{\lambda_2}, \sqrt{\lambda_3}, \ldots, \sqrt{\lambda_n}]$$

$$Q = [\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n]$$

$Q^{\dagger}$は共役転置行列，diag は対角行列である．

今回扱う行列 A は大規模行列であるため固有方程式を用いた固有値及び固有ベクトルを求める方法は実用的ではない．そこで，大規模行列に対応したアルゴリズム[1]を用いて C 言語でプログラムを作成し，CPU で実行出来るようにする．これを GPU でも実行出来るように変換し，CPU と比較すると同時に固有値と固有ベクトルを求めるのに特化したライブラリとも比較する．上記の結果から今後の改善方法や並列化の有用性について検討する．

3. 結　果

C 言語で大規模な N×N 非対称正方行列に対応した全固有値を近似的に求めるプログラムを作成した．本研究で作成した固有値と固有ベクトルを求めるプログラムを以下の表1に示す．

表1　作成したプログラムの名称と詳細

プログラム名	詳細
CPU_EIG	CPU で固有値と固有ベクトルを近似的に求めるプログラム
CLPCK_EIG	CPU で線形演算ライブラリ CLAPACK を用いて固有値と固有ベクトルを近似的に求めるプログラム
CUDA_EIG	GPU で CUDA を用いて固有値と固有ベクトルを近似的に求めるプログラム
CULA_EIG	GPU で線形演算ライブラリ CULA を用いて固有値と固有ベクトルを近似的に求めるプログラム

固有値と固有ベクトルを求めるアルゴリズムは幾つか存在する[2]．CPU_EIG 並びに CUDA_EIG で使用したアルゴリズムと処理工程を図1に示す．

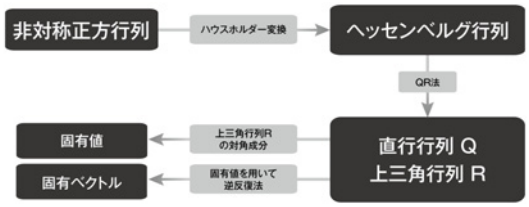

図1　固有値と固有ベクトル計算アルゴリズム

本研究で作成した各プログラムの扱える N の最大数と計算速度の結果を表2に示す．

表2　各プログラムの扱える N の最大数と計算速度

プログラム	リソース	N の最大数	計算速度 N=500
CPU_EIG	CPU	約 1000	151.700 sec
CLPCK_EIG	CPU	約 12500	0.890 sec
CUDA_EIG	GPU	約 730	8.921 sec
CULA_EIG	GPU	約 5560	0.717 sec

4. まとめ

今回のプログラム作成では大規模な非対称正方行列に対応した固有値と固有ベクトルを求めるアルゴリズムを調べ，CPU_EIG 並びに CUDA_EIG を作成した．

CPU_EIG と CUDA_EIG を比較すると，計算時間に CUDA による並列化の効果が見られる．また，線形演算ライブラリを用いた場合は，N が 1000 以下では CULA_EIG が比較的良い結果であったが，それ以上の N ではリソースの演算能力及び搭載しているメモリの関係上 CPU_EIG が良い結果となった．線形演算ライブラリを使わないプログラムでは誤差が目立ってしまったが，この原因は近似解を求めているからであり，今後はこの誤差をできる限り無くす必要がある．

5. 今後の発展

今回の結果より扱える N の最大数と誤差の問題が残ったため，アルゴリズムの再検討と並列化におけるブロックやスレッドを更に考慮したプログラムにするなどの方法で問題を解決する必要がある．

文　献

[1] 川上一郎, “数値計算の基礎”, pp. 123-140, Jan 23.2008
[2] 桂田祐史, “行列の固有値問題”, pp. 2-26, May 26.2006
[3] 大石進一, “数値計算講義ノート7固有値問題の解放(2)”, pp. 15-22, May 12.2003
[4] 山本有作, “マルチコアプロセッサ向けの固有値計算アルゴリズム”, pp. 1-24, Feb 8.2011