2008－AL－116 (8)
2008／1／23

ノイズ環境化におけるGroverのアルゴリズムのシミュレーション

大久保 誠也† 西野 哲朗*
† 電気通信大学大学院 電気通信学研究科 情報通信工学専攻
* 電気通信大学 電気通信学部 情報通信工学科

あらまし: 本論では，Groverの量子探索アルゴリズムの並列シミュレーションについて取り扱う．Groverのアルゴリズムは代表的な量子探索アルゴリズムである．一方，量子計算においては，ノイズの解析が大変重要である．そこで，Groverのアルゴリズムのシミュレーション・プログラムを作成し，2種類のノイズが混入した場合のGroverのアルゴリズムのシミュレーションを行った．さらに，OpenMPを用いた並列処理を行い，シミュレーションを高速化した．

Parallel Simulation of Grover's Algorithm in a Noisy Environment

Seiya Okubo† Tetsuro Nishino*
†The Graduate School of Electro-Communications,The University of Electro-Communications
*Department of Information and Communication Engineering, The University of Electro-Communications

Abstract: In this paper, we deal with a parallel simulation of Grover's quantum search algorithm. Grover's algorithm is a famous quantum search algortihm. On the other hand, noise analysis is important in quantum computation. Thus, we implemented a simulation program for Grover's algorithm, and we simulated Grover's search algorithm when two types of noises are simultaneously included. Moreover, we performed parallel processing and improved the execution time of the simulation by using OpenMP.

1 はじめに

計算という概念を形式的に定義するために，1936年にA.Turingは**Turing機械**(Turing Machine, 以下**TM**と略す)というモデルを提案した．TMは計算の本質を抽象化しており，現在の計算機の標準的なモデルとなっている．

1985年に，D.Deutschは量子計算機のモデル化を行った[4] [3]．Deutschは量子力学に基づいた新しい計算モデルとして，量子Turing機械を提案した．1994年にP.W.Shorは，整数の因数分解を多項式時間内に高い成功確率で行う量子アルゴリズムを示した[7]．また，1996年にはL.K.Groverが，データベース検索に関する効率的量子アルゴリズムを提案した[5]．このように，量子Turing機械は通常のTuring機械と比べて高速に計算を行うことができる可能性がある．

Groverのアルゴリズムについては様々な研究が行われており，アルゴリズム実行中にノイズが混入した場合の理論的研究もなされている[6][2]．論文[6]においては，任意の初期状態から動作させるGroverのアルゴリズムに関する解析が行われており，それに関連して，Groverのアルゴリズムが初期状態のノイズに耐性を持つことが指摘されている．一方，論文[2]においては，量子計算の汎用シミュレーターを開発し，それを用いた計算機実験の一部として，ユニタリ変換適用時にノイズが混入した場合に対するGroverのアルゴリズムのシミュレーションが行われている．しかしながら，これらの研究は，ノイズの影響に特に着目しているものではない．

そこで，本論では，より現実に近いシミュレーションを行うために，その双方のノイズが同時に生じた場合のシミュレーションを行った．また，その際，OpenMPを用いて効率的な並列処理を行ったので，そのパフォーマンスについても報告する．

2 量子計算

量子 Turing 機械 (Quantum Turing Machine, 以下 **QTM** と略す) は，通常の Turing 機械に量子並列化機能を付加したものである．量子 Turing 機械では，テープ上の 1 つの区画に 0 と 1 の任意の重ね合わせを保持することが可能である．

定義 1 [8] 量子 Turing 機械 M とは以下を満たす 7 項組 $\langle Q, \Sigma, \Gamma, \delta, q_o, B, F\rangle$ である．ただし，

1. Q は**状態**の有限集合，
2. Γ は**テープ記号**の有限集合，
3. $B \in \Gamma$ は**空白記号**，
4. $\Sigma \subseteq \Gamma - \{B\}$ は**入力アルファベット**，
5. q_0 は**初期状態**，
6. $F \subseteq Q$ は**最終状態**の有限集合，
7. $\delta : Q \times \Gamma \times \Gamma \times Q \times \{L, R\} \to \mathbf{C}$($\mathbf{C}$ は複素数全体) は，M が次に行なうべき 1 ステップの動作を指定する**状態遷移関数**とする．

$\delta(p, a, b, q, d) = c$ は M が状態 p で記号 a を読んでいるとき，状態 q に移り，記号 b を書き込み，ヘッドが方向 d に 1 区画移動するという事象の確率振幅を表している．ここで，このように遷移する確率は確率振幅の絶対値の 2 乗 $|c|^2$ となる．

また，QTM においては，この状態遷移関数から誘導される状態遷移行列 M_δ がユニタリ行列でなければならない．ここで，ユニタリ行列とは，以下の式を満たす行列として定義される．

$$MM^\dagger = M^\dagger M = I$$

ただし，$M^\dagger$ は M の転置共役行列であり，I は，単位行列である [8].

3 Grover のアルゴリズム

Grover のアルゴリズムが対象とする **探索問題**とは，次のような問題である．

入力 ：整数 $N = 2^n$.
問題 ：N 個の状態 $x_1, x_2, \cdots, x_N$ に対し，関数 $f : \{0,1\}^n \to \{0,1\}$ を計算する量子オラクルが与えられたときに，$f(x) = 1$ を満たす状態 x_v を発見せよ．

ここで，各状態 $x_i (1 \le i \le N)$ は n ビットの 2 進列でラベル付けされ，条件を満たさない状態 x に対しては，$f(x) = 0$ が成り立つものとする．また，任意の状態 x に対し $f(x) = 0$ か否かは単位時間で判定できるものとする．

探索問題を解くには，古典的アルゴリズムでは平均 $0.5N$ 回オラクルにアクセスする必要があるが，Grover の量子アルゴリズムでは，$O(\sqrt{N})$ 回のオラクルへのアクセスで十分である．

論文 [5] で，以下のアルゴリズムが示されている．

1. 量子メモリ・レジスタを，各状態が同じ振幅を持つ重ね合わせ
$\left(\frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \frac{1}{\sqrt{N}}, \cdots, \frac{1}{\sqrt{N}}\right)$
になるように初期化する（このように各状態に対する振幅を並べてベクトル表現にしたものを，状態ベクトルと呼ぶ）．
2. 以下のユニタリ変換を $O(\sqrt{N})$ 回繰り返す．
   (a) 量子メモリ・レジスタが状態 x にあるとする．
   - $f(x) = 1$ の場合は **位相反転** を適用する．
   - $f(x) = 0$ の場合は何も行わない．

   (b) 以下のような行列 D により定義される**拡散変換** D を適用する．
$$D_{ij} = \frac{2}{N} \text{ if } i \neq j \text{ and } D_{ii} = -1 + \frac{2}{N}$$
3. 最終的に得られた状態を測定する．すると，少なくとも，0.5 以上の確率で状態 S_v が得られる．

上のステップ 2 の部分が Grover のアルゴリズムの核心であり，これによって，所望の状態の振幅を $O\left(\frac{1}{\sqrt{N}}\right)$ ずつ増やすことができる．したがって，ステップ 2 を $O\left(\sqrt{N}\right)$ 回繰り返すことにより，所望の状態を得る確率を 1 に近づけることができる．

拡散変換 D は平均についての反転演算として解釈できる．すなわち，上のアルゴリズムで行なっていることは，

a) 所望の状態の振幅の符号を反転させることによって平均値から遠ざけ，

b) 平均値を中心として折り返すことにより，所望の状態の振幅をより大きく，その他の状態の振幅をより小さくする

ことと説明できる．

4 作成したシミュレータ

量子状態は非常にノイズに弱いため，量子アルゴリズムを実行する際には，この影響を考える必要がある．本研究では Grover のアルゴリズムを実行する際，アルゴリズムの各ステップにおいて次のようなノイズが発生する可能性を考え，シミュレーションを行った．

- ステップ 1 における初期状態作成時に，振幅が一様な状態を作ることができない場合．
- ステップ 2 ユニタリ変換を適用する際，理想的な適用ができず，誤差が生じた場合．
- デコヒーレンスによる，量子状態の崩壊．

本研究で作成したシミュレータの処理の流れは，以下の通りである．

1. すべての状態の振幅を $\frac{1}{\sqrt{2^n}}|x\rangle$ にする．
2. 初期化時のノイズとして，乱数値を，すべての振幅に加算する．
3. 正規化を行い，状態ベクトルの長さを 1 にする．
4. 以下の変換を繰り返す．
   (a) $f(x)=1$ となる x の振幅の符合を反転する．
   (b) 拡散変換 D の対角成分を状態ベクトルに適用する．
   (c) 拡散変換 D の非対角成分を状態ベクトルに適用する．
   (d) ユニタリ変換適用時とデコヒーレンスによるノイズとして，乱数値を，すべての振幅に加算する．
   (e) 正規化を行い，状態ベクトルの長さを 1 にする．

プログラムのステップ 1〜3 までがアルゴリズムのステップ 1 に，プログラムのステップ 4 がアルゴリズムのステップ 2 に相当する．

ノイズをのせる際には，各量子状態の振幅の実数成分と虚数成分に対して，一様ランダムに $-\alpha$以上α 以下の値を加算している．ここで，α はノイズの影響の強さを決めるパラメータである．しかし，次のステップで正規化を行っているため，パラメータ α の値だけではノイズの強さを評価できないことに注意する必要がある．今後，ステップ 3 におけるノイズのパラメータを α_1，ステップ 4d におけるノイズのパラメータを α_2 と表記する．

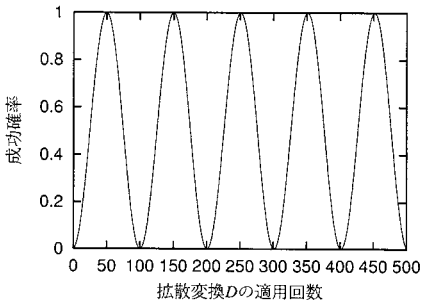

図 1: ノイズが無い場合における成功確率

また，拡散変換 D 適用時，拡散変換 D の各成分は 1 回ずつしか状態ベクトルに適用されず，かつ，状態ベクトルの各成分に適用される拡散変換 D の成分は対角成分が 1 回と，非対角成分が 2^n-1 回であり一定である．そこで，プログラムにおいては，ユニタリ変換実行時とデコヒーレンスによるノイズは，アルゴリズムのステップ 4d においてまとめて付加している．

ステップ 4 において拡散変換を対角成分と非対角成分に分けて計算しているが，これは OpenMP による分散計算を行うための配慮である．

5 実験結果

$n=12$ であり $f(x)=1$ となるような x は一つしか無い場合における計算機シミュレーションを行った．

図 3 と図 4 は，ノイズが無い環境下におけるシミュレーション結果である．図 1 に，$f(x)=1$ となるような x を観測する確率と拡散変換 D の適用回数の関係のグラフを示す．横軸が拡散変換 D の適用回数，縦軸が $f(x)=1$ となるような x を観測する確率である．また，図 2 に，プログラムのステップ 4d 終了時における，各量子状態の観測確率を示す．横軸が各状態，縦軸が各量子状態の観測確率である．拡散変換を t 回適用した時点における Grover のアルゴリズムの成功確率は $\sin((2t+1)\theta)$ であることが知られているが，その通りになっていることがわかる．

図 3 と図 4 に，$\alpha_1=0.01, \alpha_2=0$ とした場合の実験結果を示す．ここで，図 3 は，10 回実験を行った結果の平均値を示している．しかしながら，個々の結果も大

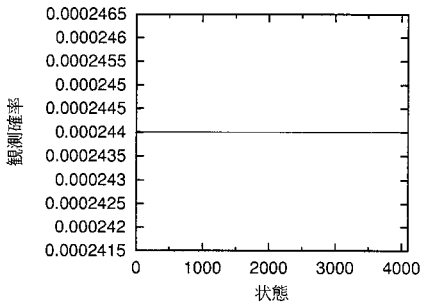

図 2: ノイズが無い場合における量子状態の初期状態

きく変わらない結果を得ることができた．この図から，成功確率の最大値がノイズが無いときと比べ低下していることがわかる．しかしながら，拡散変換 D の適用回数が増えても，成功確率の極大値は変わらない．また，図4は，平均ではなく，ある特定の実験の結果を示している．この図から，ノイズが混入することで成功確率の最大値が低下するが，位相は変化しないことがわかる．さらに，拡散変換を t 回適用した時点における，ノイズがない場合の量子状態を $v(t)$，ノイズがある場合の量子状態を $y(t)$ としたとき，$|v(t)-y(t)|$ 値の変化を図5に示す．横軸はステップ，縦軸は $|v(t)-y(t)|$ である（常に一定値であることがわかる）．これは，論文 [1] に示されているように量子計算におけるエラーは各ステップで生じる状態ベクトルのずれの和として累積することと，Grover のアルゴリズムが本質的には回転変換の繰り返しであるためと考えられる．

$\alpha_1 = 0.02 \sim 0.8$ に対する計算機実験の結果を，図6 ～ 図17に示す．これらの結果から，ノイズの影響が大きくなるほど成功確率が徐々に低下していくことがわかる．また，位相はノイズの影響に無関係であること，$|v(t)-y(t)|$ の値は拡散変換 D の適用回数に関わらず一定値を保つこともわかる．

$\alpha_1 = 0.01$ から $\alpha_1 = 0.02$ への成功確率の低下幅は大きいが，α_1 の値が大きくなるほど低下幅は小さくなっていく．同様に，$|v(t)-y(t)|$ の値も，$\alpha_1 = 0.01$ から $\alpha_1 = 0.02$ への低下幅は大きいが，α_1 の値が大きくなるほど低下幅は小さくなっていく．したがって，成功確率の最大値は初期状態生成時の $|v(t)-y(t)|$ の値と強い関係があることがわかる．

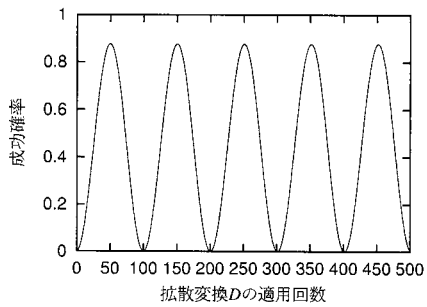

図 3: $\alpha_1 = 0.01, \alpha_2 = 0$ の場合における成功確率

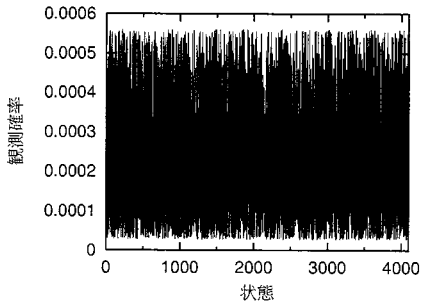

図 4: $\alpha_1 = 0.01, \alpha_2 = 0$ の場合における初期状態

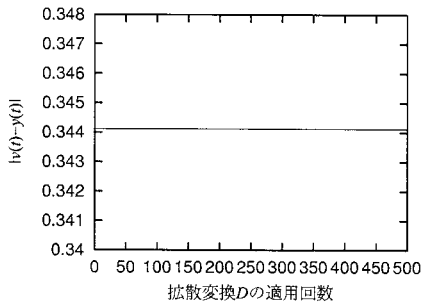

図 5: $\alpha_1 = 0.01, \alpha_2 = 0$ の場合の $|v(t)-y(t)|$ の値

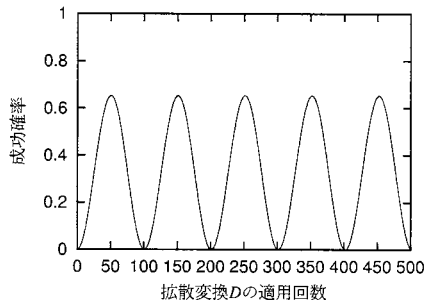

図 6: $\alpha_1 = 0.02, \alpha_2 = 0$ の場合における成功確率

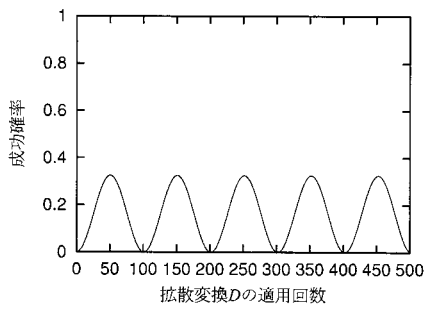

図 9: $\alpha_1 = 0.04, \alpha_2 = 0$ の場合における成功確率

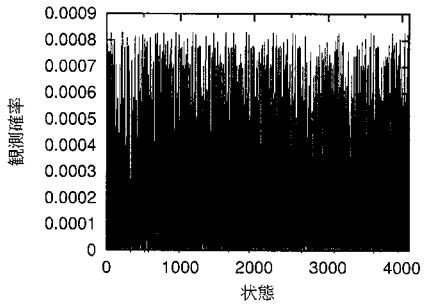

図 7: $\alpha_1 = 0.02, \alpha_2 = 0$ の場合における初期状態

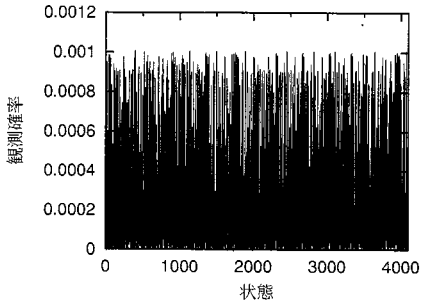

図 10: $\alpha_1 = 0.04, \alpha_2 = 0$ の場合における初期状態

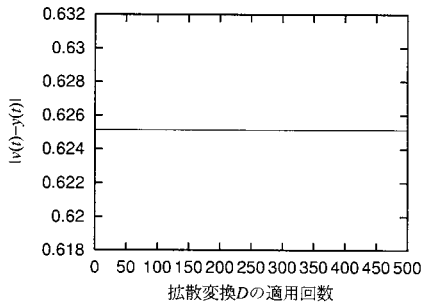

図 8: $\alpha_1 = 0.02, \alpha_2 = 0$ の場合の $|v(t) - y(t)|$ の値

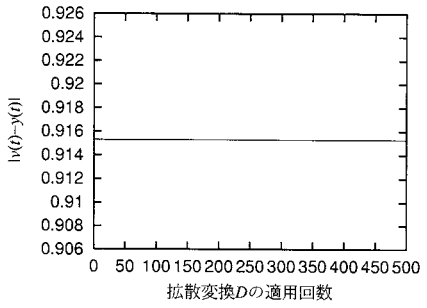

図 11: $\alpha_1 = 0.04, \alpha_2 = 0$ の場合の $|v(t) - y(t)|$ の値

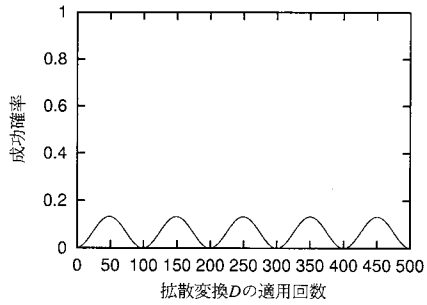

図 12: $\alpha_1 = 0.06, \alpha_2 = 0$ の場合における成功確率

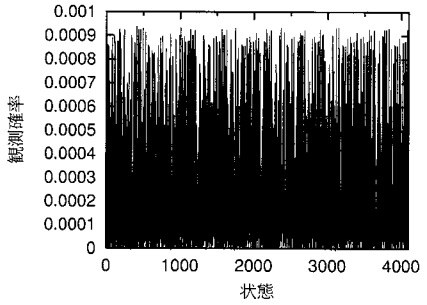

図 13: $\alpha_1 = 0.06, \alpha_2 = 0$ の場合における初期状態

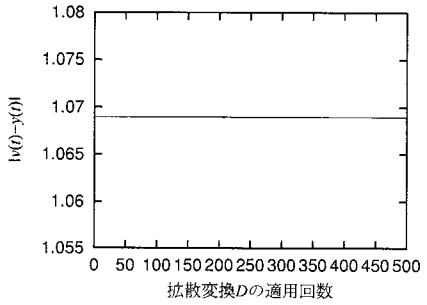

図 14: $\alpha_1 = 0.06, \alpha_2 = 0$ の場合の $|v(t) - y(t)|$ の値

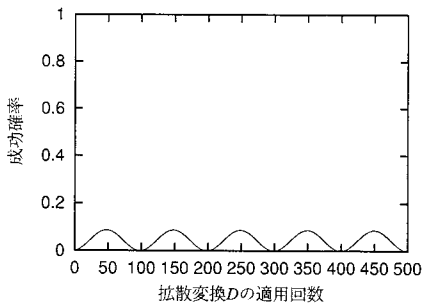

図 15: $\alpha_1 = 0.08, \alpha_2 = 0$ の場合における成功確率

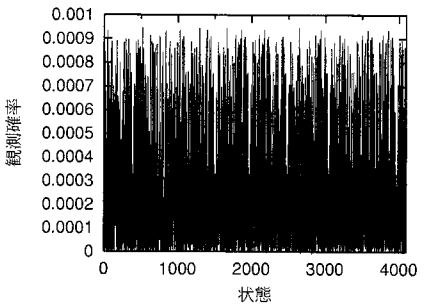

図 16: $\alpha_1 = 0.08, \alpha_2 = 0$ の場合における初期状態

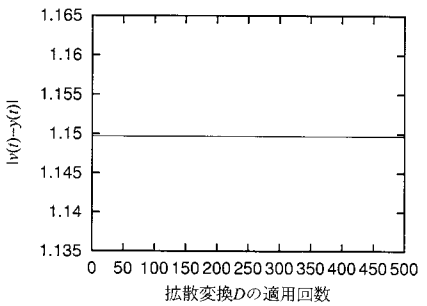

図 17: $\alpha_1 = 0.08, \alpha_2 = 0$ の場合の $|v(t) - y(t)|$ の値

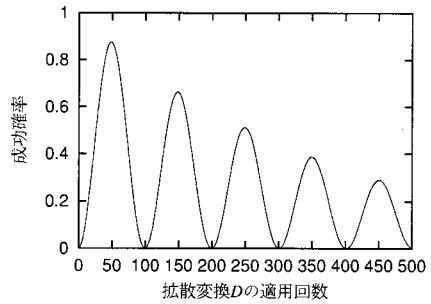

図 18: $\alpha_1 = 0, \alpha_2 = 0.001$ の場合における成功確率

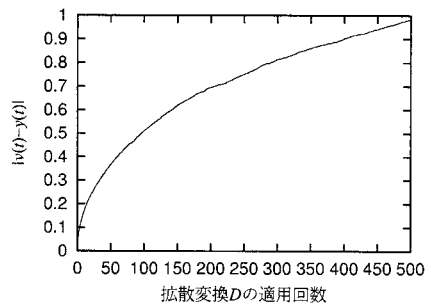

図 19: $\alpha_1 = 0.01$, $\alpha_2 = 0.001$ の場合の $|v(t) - y(t)|$ の値

$\alpha_1 = 0, \alpha_2 = 0.001$ の場合の実験結果を，図 18~19 に示す．拡散変換 D の適用回数が増加するにしたがって，成功確率の極大値が徐々に低下していくことがわかる．その低下幅は，最初は大きく，徐々に減少していく．また，$|v(t) - y(t)|$ の値も徐々に大きくなっていくことがわかる．

$\alpha_1 = 0.01, \alpha_2 = 0.001$ の場合の実験結果を，図 21 に示す．$\alpha_1 = 0, \alpha_2 = 0.001$ の場合と比べ，初期状態にノイズが混入している分，成功確率が低下していることが分かる．

最後に，OpenMP を用いた分散計算について述べる．OpenMP は主に共有メモリ型並列計算機で用いられる，並列計算環境を利用するために標準化された規格である．利用者はディレクティブをプログラムに埋め込むことにより，容易に並列計算を利用することができるが，その並列化の効率はコンパイラに依存する．本研究では，シミュレーションのほぼすべてのステップにおいて，この OpenMP を用いて並列化を行った．実行環境は UltraSparc IV 1.5GHz，コンパイラは Sun Studio 11 である．使用した CPU コア数と実行時間の関係を，表 1 と図 22 に示す．OpenMP による簡単な並列化であるが，CPU コア数が少ないときは，OpenMP だけで，十分な並列化が行えていることがわかる．CPU コア数が 10 以上になると実行時間に差は見られなくなるが，より大規模な実験（つまり，n の値が大きいとき）においては，効率的に動くと予想される．

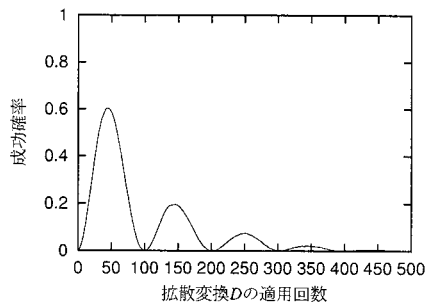

図 20: $\alpha_1 = 0, \alpha_2 = 0.002$ の場合における成功確率

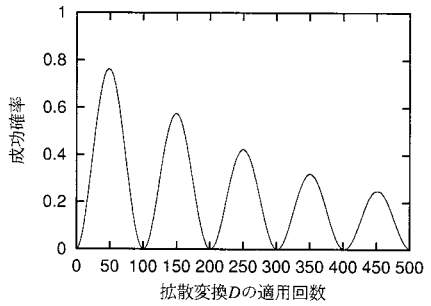

図 21: $\alpha_1 = 0.01, \alpha_2 = 0.001$ の場合における成功確率

6 おわりに

本研究では，Grover の量子探索アルゴリズムのシミュレータを作成し，ノイズが混入した場合を想定した計算機実験を行った．また，その際，OpenMP を用

CPU コア数	実行時間（秒）
1	76.80
2	38.53
4	19.67
8	10.37
12	7.90

表 1: 500 ステップを計算するのに必要な時間

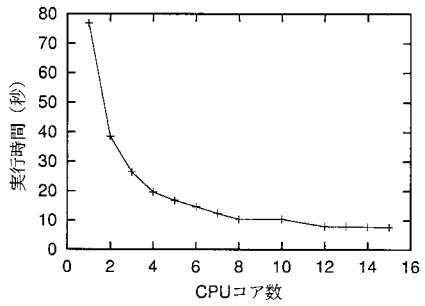

図 22: 500 ステップを計算するのに必要な時間

いた並列計算を行った．

初期状態にノイズが一様に混入した場合，成功確率の最大値は低下するが，位相は変化しないことがわかった．また，成功確率の極大値は拡散変換 D の適用回数に関わらず一定であることもわかった．

論文 [2] においては，$f(x)=1$ となるような x が r 個存在する探索問題に対し，拡散変換を t 回繰り返したときの Grover のアルゴリズムの成功確率 P(t) は

$$P(t) = P_{av} - \Delta P \cos 2[\omega t + \mathrm{Re}(\phi)]$$

であることが示されている．ここで，

$$\begin{aligned} P_{av} &= 1-(N-r)\sigma_l^2 - \frac{1}{2}\left[(N-r)\left|\bar{l}(0)\right|^2 \right. \\ &\quad \left. +r\left|\bar{k}(0)\right|^2\right] \\ \Delta P &= \frac{1}{2}\left|(N-r)\bar{l}(0)^2 + r\bar{k}(0)^2\right|. \\ \sigma_l^2(t) &= \frac{1}{N-r}\sum_{i=r+1}^{N}|l_i(t)-\bar{l}(t)|^2 \\ \tan\phi &= \sqrt{r/(N-r)}\bar{k}(0)/\bar{l}(0) \end{aligned}$$

である．また，$l_i(t)$ は拡散変換 D を t 回繰り返した時の $f(x)=1$ となる状態 i の振幅を，$\bar{l}(t)$ は $l_i(t)$ の平均値を，$k_i(t)$ は拡散変換 D を t 回繰り返した時の $f(x)=0$ となる状態 i の振幅を，$\bar{k}(t)$ は $k_i(t)$ の平均値をそれぞれ表している．本シミュレータから得られた一連の結果も，この理論的結果と一致している．

今後の課題としては，より妥当なノイズの混入方法を検討し，物理的に判明した各種パラメータを入力すると実験を忠実に再現するようなシミュレータの開発があげられる．

参考文献

[1] Bernstein, E. and Vazirani, U.: Quantum complexity theory, *SIAM J. Comput.*, Vol. 26, No. 5, pp. 1411–1473 (1997).

[2] Biham, E., Biham, O., Biron, D., Grassl, M. and Lidar, D.: Grover's Quantum Search Algorithm for an Arbitrary Initial Amplitude Distribution, quant-ph/*9807027* (1998).

[3] Deutsch, D.: Quantum Computational Networks, *Proc. R. Soc. Lond.*, Vol. A 400, pp. 97–117 (1985).

[4] Dutsch, D.: Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer, *Proc. R. Soc. Lond.*, Vol. A400, pp. 97–117 (1985).

[5] Grover, L.: Quantum Mechanics Helps in Searching for a Needle in a Haystack, *Physical Review Letters*, Vol. 79, No. 2, pp. 325–328 (1997).

[6] Niwa, J., Matsumoto, K. and Imai, H.: General-purpose parallel simulator for quantum computing, *Physical Review A 66* (2002).

[7] Shor, P.: Algorithms for Quantum Computation : Discrete Log and Factoring, *in Proceedings of the 35th Anniual IEEE Symposium on Foundations of Computer Science* (1994).

[8] 西野哲朗: 量子コンピュータの理論, 培風館 (2002).