Grover アルゴリズムの NMR 量子計算シミュレータ試作

An Experimental Simulator for NMR Quantum Computation of Grover's Algorithm

http://www.tani.cs.chs.nihon-u.ac.jp/g-2005/katsu/

谷 研究室　勝間田 智
Satoru KATSUMATA

概要

近年，量子コンピュータの実現に関する研究が盛んに行われており，中でも比較的容易に実現可能な NMR 量子コンピュータへの関心は高い．そこで，量子アルゴリズム初学者のために Grover のアルゴリズムを NMR 量子計算するシミュレータを作成した．

1　はじめに

1982 年に Feynman が量子力学的振る舞いを量子システムに利用することを提案した [1]．1985 年には Deutsch が量子チューリングマシン (QTM) を紹介し [2]，以後多くの研究者が QTM に基づく量子コンピュータを実行する方法について議論している．量子アルゴリズムでは，1994 年 Shor の因数分解アルゴリズム [3]，1996 年 Grover のファイル検索アルゴリズム [4] が提案され，これらを実現する計算機の登場が期待された．そして 1997 年，Bulk 量子チューリングマシン (BQTM) に基づく NMR(Nuclear Magnetic Resonance:核磁気共鳴) 量子コンピュータが紹介された [5].

1999 年 IBM では 3 キュービットの NMR 量子コンピュータを使い，Grover アルゴリズムの実行に成功した．現在 7 キュービットまで実現しており，15 について Shor アルゴリズムの実行に成功している．

量子アルゴリズムを直感的に理解するために，本研究では初学者向けのシミュレータ作成を目標とした．手軽に個人でアルゴリズムの振る舞いを調べることができるツールとして，既存の Grover アルゴリズムシミュレータに加え，Mathematica による Grover アルゴリズムの NMR 量子計算シミュレータを作成した．

2　準備

2.1　量子コンピュータの基礎数理

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$|0\rangle, |1\rangle$ は C^2 上のベクトルである．

$|x\rangle, \langle x|$ をそれぞれ**ケットベクトル** (列ベクトル)，**ブラベクトル** (行ベクトル) という．

C^2 上の作用素 A の共役転置行列 A^* を A の**共役作用素**という．作用素とは正方行列のことである．

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}$$

の共役作用素は

$$A^* = \begin{bmatrix} a^*_{00} & a^*_{10} \\ a^*_{01} & a^*_{11} \end{bmatrix}$$

である．

C^2 上の作用素 U が**ユニタリ**であるとは $UU^* = I$ が成り立つことをいう．I は C^2 上の単位行列である．

C^2 上の作用素 A が**エルミート**であるとは $A = A^*$ が成り立つことをいう．

C^2 上の n 個のベクトル

$|x_i\rangle = x_{i0}|0\rangle + x_{i1}|1\rangle,\ i = 1, ..., n$

について考える．

第 $i := 2^{n-1}i_1 + 2^{n-2}i_2 + \cdots + i_n (i_1, ..., i_n = 0, 1)$ 成分が $x_{1,i_1} \cdots x_{n,i_n}$ であるベクトルを $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ と表し，これを $|x_1\rangle, ..., |x_n\rangle$ の**テンソル積**という．

$|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ は $|x_1, ..., x_n\rangle$ ともかく．$|i_1\rangle \otimes \cdots \otimes |i_n\rangle$ は $|i\rangle_n$ または $|i\rangle$ ともかく．

規約

ある複素数 $x_{i_1,...,i_n}$ において

$$|x\rangle = \sum_{i_1,...,i_n=0}^{1} x_{i_1,...,i_n} |i_1, ..., i_n\rangle$$

$|x\rangle$ はシステムの状態を表す．

規約

上の $x_{i_1,...,i_n}$ は

$$\sum_{i_1,\ldots,i_n=0}^{1} |x_{i_1,\ldots,i_n}|^2 = 1$$

をみたす．$x_{i_1,\ldots,i_n}$ を $|i_1,\ldots,i_n\rangle$ の**確率振幅**と呼ぶ．

規約

「状態の線形結合は，一般に，また状態である．」

これを状態の**重ね合わせの原理**という．

規約

状態 $|x\rangle$ はユニタリ作用素 U により

$$|y\rangle = U|x\rangle$$

に推移する．

規約

いま，量子システムが状態 $|x\rangle$ にある．**観測量** A を観測すると，$k = 1,\ldots,m$ に対して，確率

$$P_k = |x_{k,1}|^2 + \cdots + |x_{k,r_k}|^2$$

で**観測値** a_k が得られ，観測直後に状態は

$$\frac{1}{\sqrt{\sum_{j=1}^{r_k} |x_{k,j}|^2}} \sum_{j=1}^{r_k} x_{k,j}|a_{k,j}\rangle$$

に推移する．

ここに A はエルミート作用素であり，r_k は A の異なる固有値 a_k の重複度である．

量子力学では，状態 $|0\rangle$ と状態 $|1\rangle$ が同時に存在しており，重ね合わせは $\alpha|0\rangle + \beta|1\rangle$ と表せる．この重ね合わせを観測すると $|0\rangle$ または $|1\rangle$ が観測される．$|0\rangle$ が観測される確率は $|\alpha|^2$，$|1\rangle$ が観測される確率は $|\beta|^2$ であり，$|\alpha|^2 + |\beta|^2 = 1$ が成り立つ．

古典コンピュータの基本情報量であるビットは 0 か 1 のどちらかの状態しかとらない．3 ビットの場合，すべての状態を表すのに $2^3 = 8$ 通りのパターンを考える必要がある．量子コンピュータでは 0 と 1 の重ね合わせの状態をとるので，3 ビット 8 通りの状態を一度に表すことができる．よって従来のビットと区別して基本情報量を**キュービット**と呼んでいる．つまり n キュービットの場合，2^n 通りの計算を一括して行える．よって 3 キュービットの場合，8 通りの計算を一括して処理できる．

20 ビットの場合，古典コンピュータでは解の候補をすべて調べるのに $2^{20} = 1,048,576$ 通り計算を行わなければならないが，量子コンピュータでは重ね合わせを利用して一回の処理で済む．

量子回路は量子論理ゲートから構成されており，1 キュービットのゲート (2×2 のユニタリ作用素) と 2 キュービットの **Toffoli ゲート** (**制御 NOT**:control NOT) を基本ゲートとしている (図 1, 図 2)．制御 NOT の入出力を表 1 に示す．図 1 の制御 NOT は XOR(exclusive-or:排他的論理和) を計算する量子コンピュータといえる．図 2 は $|y\rangle = U|x\rangle$ を意味している．

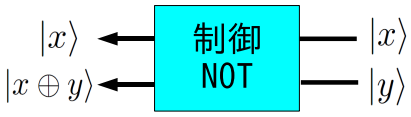

図 1：制御 NOT

入力		出力	
$\|x\rangle$	$\|y\rangle$	$\|x\rangle$	$\|x \oplus y\rangle$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

表 1：制御 NOT の入出力

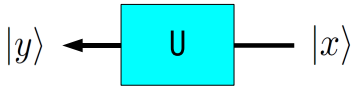

図 2：ユニタリ作用素

この基本ゲートで量子チューリングマシンのすべての動作を模倣することができるとされている．また，基本ゲートの数がほぼ計算時間に対応していると考えられるので，できるだけ少ない数の基本ゲートで量子コンピュータを構成することを考えていく．

2.2 NMR 量子計算

NMR と類似の観測を実行できる量子チューリングマシンを Bulk 量子チューリングマシン (BQTM) と呼び，以下のように定義する．

定義

Bulk 量子チューリングマシン M は，以下の条件をみたす 7 項組 $\langle Q, \Sigma, \Gamma, \delta, q_0, B, F\rangle$ である．

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. $\Sigma \subseteq \Gamma$ は**入力記号**の集合
5. $q_0 \in Q$ は**初期状態**
6. $F \subseteq Q$ は**受理状態**の集合
7. $\delta : Q \times \Gamma \times \Gamma \times Q \times \{L, R\} \to C$(複素数全体の集合) は M の**状態遷移関数**

BQTM では観測の規約が以下のように変更される．BQTM のテープの区画 (セル) が重ね合わせ状態 $\alpha|0\rangle+\beta|1\rangle$ にあるとき，実数値 $\theta=|\beta|^2-|\alpha|^2$ が測定される．ここで，$|\alpha|^2+|\beta|^2=1$ なので，$-1\leq\theta\leq 1$ が成り立つ．実数 θ は，符号付きの小数点以下 k 桁の 2 進数として表される．ただし，k は定数とする．以下では，観測誤差 $\varepsilon=1/2^k$ と置く．このとき，重ね合わせ状態 $\alpha|0\rangle+\beta|1\rangle$ にある BQTM のセルを観測すると，以下の関係式をみたす実数値 θ が確率 1 で読み出せる．

$$|\beta|^2-|\alpha|^2-\varepsilon\leq\theta\leq|\beta|^2-|\alpha|^2+\varepsilon$$

BQTM の場合には部分的観測は行えない．つまり，BQTM の複数のセルを観測するときに行えることは，各セルにおいて実数値 θ を独立に得ていくことだけである．また，観測を行っても，しばらくの間，重ね合わせ状態は破壊されずに残るものとする．すなわち，重ね合わせ状態が収縮する前に，重ね合わせ状態にあるセルを定数回観測できるものと仮定する．

3 ファイル検索問題

3.1 Grover のアルゴリズム

ファイル検索問題の定義

ソートされていない $N=2^n$ 個のデータファイルの中から，指定された一つのファイルを見つけ出す問題を考える．一般に古典コンピュータで解くとすれば $O(N)$ だけの探索の手間がかかるが，量子コンピュータを用いると $O(\sqrt{N})$ の手間で済む．

Grover のアルゴリズムの定義

$N=2^n$:ソートされていないファイル数

$0\sim N-1$ までのアドレスが付けられている

非負整数集合 $\{0,1,...,N-1\}$ から集合 $\{0,1\}$ への関数

$$f(x):=\begin{cases}1,\ \text{if } x=z\\ 0,\ \text{if } x\neq z\end{cases}$$

z:目的ファイルのアドレス

x:与えられるアドレス

f:オラクル (oracle) 関数

Grover のアルゴリズムとは，オラクル関数 f が与えられたとき，

入力: x

出力: $f(z)=1$ をみたす z

となる．

Grover のアルゴリズムの概要

ファイル検索問題を解く量子コンピュータを作るために，オラクル関数 f を用いてユニタリ作用素 U_f を作り，それを一様な確率振幅をもつ状態 $|\varphi_0\rangle:=(|0\rangle+\cdots+|N-1\rangle)/\sqrt{N}$ に k 回施し，その結果，状態が

$$U_f^k|\varphi_0\rangle=|z\rangle$$

に推移するようにする．

手順

ユニタリ作用素 U_f を作るために，まず，オラクル関数 f から定まる選択的回転 R_f

$$\forall x,y=0,...,N-1,$$
$$R_f(x,y):=e^{i\pi f(x)}\delta_{xy}=(-1)^{f(x)}\delta_{xy}$$

を用意する．いま，z を用いて R_f を表すと

$$R_f=I-2|z\rangle\langle z|$$

とも書ける．I は N 次の単位行列である．

状態

$$|\varphi\rangle=\sum_{x=0}^{N-1}w_x|x\rangle$$

に R_f を施すと，システムの状態は

$$R_f|\varphi\rangle=w_0|0\rangle+\cdots+(-1)w_z|z\rangle+\cdots+w_{N-1}|N-1\rangle$$

に推移する．ただし，$|w_0|^2+\cdots+|w_{N-1}|^2=1$ である．

次にウォルシュ-アダマール変換

$$\forall x,y=0,1,...,N-1,$$
$$W(x,y):=\frac{1}{\sqrt{N}}(-1)^{x_0y_0+\cdots+x_{n-1}y_{n-1}}$$

と選択的回転変換

$$\forall x,y=0,1,...,N-1,$$
$$R(x,y):=e^{i\pi(1-\delta_{x0})}\delta_{xy}=(-1)^{1-\delta_{x0}}\delta_{xy}$$

の行列の積として表される変換

$$D:=WRW$$

を考える．ここに，$x=x_0+2x_1+\cdots+2^{n-1}x_n$，$y=y_0+2y_1+\cdots+2^{n-1}y_n$ である．

変換 $D=WRW$ は

$$D=-I+2|\varphi_0\rangle\langle\varphi_0|$$

と表される．ただし，$|\varphi_0\rangle:=(1/\sqrt{N})\sum_{x=0}^{N-1}|x\rangle$ である．また，これを状態

$$|\varphi\rangle=\sum_{x=0}^{N-1}w_x|x\rangle$$

に施すと，状態は

$$D|\varphi\rangle=\sum_{x=0}^{N-1}(\bar{w}-(w_x-\bar{w}))|x\rangle$$

に推移する．ここに

$$\bar{w}:=\frac{1}{N}\sum_{x=0}^{N-1}w_x$$

である．

この変換 D を**平均に関する反転変換**と呼ぶ.
$D_{ij} = -\delta_{ij} + \frac{2}{N}$($\delta_{ij}$:Kronecker's Delta) である.

ここで選択的回転 R_f と平均に関する反転 D の合成
$$U_f := DR_f = (-I + 2|\varphi_0\rangle\langle\varphi_0|)(I - 2|z\rangle\langle z|)$$
を考え，これを状態
$$|\varphi\rangle = \sum_{x=0}^{N-1} w_x|x\rangle$$
に施すと，状態は
$$U_f|\varphi\rangle = \sum_{x=0,x\neq z}^{N-1} (2\bar{w} - w_x)|x\rangle + (2\bar{w} + w_z)|z\rangle$$
に推移する．ここに，$\sum_{x=0}^{N-1} |w_x|^2 = 1$ であり，また
$$\bar{w} = \frac{1}{N}\left(\sum_{x=0,x\neq z}^{N-1} w_x - w_z\right)$$
である。

U_f を k 回施したときの状態を求める.
U_f を
$$|\varphi_0\rangle := \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$
に k 回施したときの状態を
$$U_f^k|\varphi_0\rangle = a_k|z\rangle + \sum_{x\neq z} b_k|x\rangle$$
と書くことにすると
$$a_0 = b_0 = \frac{1}{\sqrt{N}}$$
$k = 1, 2, 3, ...$ に対して
$$a_k = \frac{N-2}{N}a_{k-1} + \frac{2(N-1)}{N}b_{k-1},$$
$$b_k = -\frac{2}{N}a_{k-1} + \frac{N-2}{N}b_{k-1}$$
が成り立つ.

$k = 1, 2, 3, ...$ に対して
$$a_k = \sin((2k+1)\theta),\ b_k = \frac{1}{\sqrt{N-1}}\cos((2k+1)\theta)$$
が成り立つ．ここに
$$\sin\theta = \sqrt{\frac{1}{N}},\ \cos\theta = \sqrt{1 - \frac{1}{N}}$$
である.

以上より，状態 $|\varphi_0\rangle$ に U_f を k 回施した結果，状態は
$$U_f^k|\varphi_0\rangle$$
$$= \sin((2k+1)\theta)|z\rangle + \sum_{x\neq z}\frac{1}{\sqrt{N-1}}\cos((2k+1)\theta)|x\rangle$$
に推移することがわかった．このとき $0, 1, ..., N-1$ を固有値にもつエルミート作用素で表される観測量を観測すると，探しているファイルのアドレス z が得られる確率は
$$P_c = \sin^2((2k+1)\theta)$$
で与えられる.

ファイルの総数 N は十分大きいとする．また
$$m := \left\lfloor\frac{\pi}{4\theta}\right\rfloor$$
とおく．このとき，U_f を $|\varphi_0\rangle$ に m 回施して観測すると，検索に成功する確率 P_c は
$$P_c \geq 1 - \frac{1}{N}$$
で抑えられ，このとき
$$m = O(\sqrt{N})$$
が成り立つ.

証明
m は $\pi/4\theta - 1 < m \leq \pi/4\theta$ を満たす．したがって
$$\tilde{m} := \frac{\pi}{4\theta} - \frac{1}{2},\ (2\tilde{m}+1)\theta = \frac{\pi}{2}$$
とおくと
$$-\frac{1}{2} = \frac{\pi}{4\theta} - 1 - \left(\frac{\pi}{4\theta} - \frac{1}{2}\right)$$
$$< m - \tilde{m}$$
$$\leq \frac{\pi}{4\theta} - \left(\frac{\pi}{4\theta} - \frac{1}{2}\right) = \frac{1}{2}$$
すなわち，$|m - \tilde{m}| \leq 1/2$ が成り立つ．したがって，
$$|(2m+1)\theta - (2\tilde{m}+1)\theta| = 2\theta|m - \tilde{m}| \leq 2\theta\frac{1}{2} = \theta$$
が得られ，
$$\left|(2m+1)\theta - \frac{\pi}{2}\right| \leq \theta$$
が成り立つ．したがって
$$-\sin\theta = \cos\left(\frac{\pi}{2} + \theta\right)$$
$$\leq \cos((2m+1)\theta)$$
$$\leq \cos\left(\frac{\pi}{2} - \theta\right) = \sin\theta$$
すなわち
$$\cos^2((2m+1)\theta) \leq \sin^2\theta = \frac{1}{N}$$
を得る．したがって，検索に成功する確率は
$$P_c = 1 - \cos^2((2m+1)\theta) \geq 1 - \frac{1}{N}$$
と評価される．また $\theta \geq \sin\theta = \sqrt{1/N}$ より，
$$m = \left\lfloor\frac{\pi}{4\theta}\right\rfloor \leq \frac{\pi}{4\theta} \leq \frac{\pi}{4}\sqrt{N}$$
が得られる.

確率ができるだけ大きくなるような k を選ぶことが望ましかったが，以上の議論より，$k = \frac{\pi}{4}\sqrt{N}$ とすれば良いことがわかった.

3.2 Grover のアルゴリズムの一般化

複数個のファイルを指定したときのファイル検索問題について考える.
集合 $A \subseteq \{0, 1, ..., N-1\}$

$$f(x) := \begin{cases} 1, \text{ if } x \in A \\ 0, \text{ if } x \notin A \end{cases}$$

$f(x) = 1$ となる x を探す．f はオラクル関数である．

選択的回転変換

$$R_f = I - 2\sum_{z\in A} |z\rangle\langle z|$$

を状態 $|\varphi\rangle$ に施すと，

$$R_f|\varphi\rangle = \sum_{x\notin A} w_x|x\rangle - \sum_{x\in A} w_x|x\rangle$$

に推移する．

選択的回転変換 R_f と平均値に関する反転 D の合成

$$U_f := DR_f = (-I + 2|\varphi_0\rangle\langle\varphi_0|)\left(I - 2\sum_{z\in A}|z\rangle\langle z|\right)$$

を状態 $|\varphi\rangle$ に施すと，

$$U_f|\varphi\rangle = \sum_{x\notin A}(2\bar{w} - w_x)|x\rangle + \sum_{x\in A}(2\bar{w} + w_x)|x\rangle$$

に推移する．

状態 $|\varphi_0\rangle$ に U_f を k 回施した結果，状態は

$$U_f^k|\varphi_0\rangle = \sum_{x\in A}\frac{1}{\sqrt{|A|}}\sin((2k+1)\theta)|x\rangle + \sum_{x\notin A}\frac{1}{\sqrt{N-|A|}}\cos((2k+1)\theta)|x\rangle$$

に推移する．このとき $0, 1, \cdots, N-1$ を固有値にもつエルミート作用素で表される観測量を観測すると，探しているファイルのアドレスが得られる確率は

$$P_c = \sum_{x\in A}\left(\frac{1}{\sqrt{|A|}}\sin((2k+1)\theta)\right)^2 = \sin^2((2k+1)\theta)$$

指定されたファイルのアドレス集合 A の要素数 $|A|$ はファイル総数 N に比べて十分小さいとする．また

$$m := \left\lfloor \frac{\pi}{4\theta} \right\rfloor$$

とおく．このとき，U_f を $|\varphi_0\rangle$ に m 回施して観測すると，検索に成功する確率 P_c は

$$P_c \geq 1 - \frac{|A|}{N}$$

で抑えられ，このとき

$$m = O\left(\sqrt{\tfrac{N}{|A|}}\right)$$

が成り立つ．

証明

m は $\pi/4\theta - 1 < m \leq \pi/4\theta$ を満たす．したがって

$$\tilde{m} := \frac{\pi}{4\theta} - \frac{1}{2},\ (2\tilde{m}+1)\theta = \frac{\pi}{2}$$

とおくと

$$\cos^2((2m+1)\theta) \leq \sin^2\theta = \frac{|A|}{N}$$

が成り立つ．したがって，検索に成功する確率は

$$P_c = 1 - \cos^2((2m+1)\theta) \geq 1 - \frac{|A|}{N}$$

と評価される．また $\theta \geq \sin\theta = \sqrt{|A|/N}$ より，

$$m = \left\lfloor \frac{\pi}{4\theta} \right\rfloor \leq \frac{\pi}{4\theta} \leq \frac{\pi}{4}\sqrt{\frac{N}{|A|}}$$

が得られる．

確率ができるだけ大きくなるような k を選ぶことが望ましかったが，以上の議論より，$k = \frac{\pi}{4}\sqrt{\frac{N}{|A|}}$ とすれば良いことがわかった．

3.3 NMR 計算機上での Grover のアルゴリズム

初期状態を考える．$|0\rangle$ と $|1\rangle$ の個数は等しいため観測値 $\theta = |\beta|^2 - |\alpha|^2 = 0$ となる．

振幅増幅を行った結果，以下の状態の重ね合わせが得られたとする．

- 所望の解の振幅が $\sqrt{a}$ である状態，たとえば，$|1\rangle$ であったとする．
- 振幅が $\sqrt{\frac{1-a}{N-1}}$ である $|0\rangle$ が $N/2$ 個.
- 所望の状態以外で，振幅が $\sqrt{\frac{1-a}{N-1}}$ である $|1\rangle$ が $N/2-1$ 個.

このとき，観測値 $\theta = a + \frac{1-a}{N-1} \times (N/2-1) - \frac{1-a}{N-1} \times (N/2) = \frac{aN-1}{N-1}$ となる．θ が閾値を越えていれば観測できるので，$a \geq \frac{\varepsilon N - \varepsilon + 1}{N}$ を満たさなければならない．したがって，必要な振幅は $\sqrt{\frac{\varepsilon N-\varepsilon+1}{N}}$ となる．Grover のアルゴリズムでは，j 回のオラクルコールを行った時点での所望の解の振幅は $a = \sin((2j+1)\phi)$ である．ただし，$\phi = 1/\sqrt{N}$ である．したがって，$\varepsilon \ll 1$ の時，$\frac{1}{2}\sqrt{\varepsilon N}$ 回のオラクルコールを行った時点で必要な振幅を満たす．

4 シミュレーション

Grover アルゴリズムにおける各状態の確率振幅の変化を Mathematica を使用して棒グラフに表した．5 キュービット (32 個の状態の重ね合わせ)，目的ファイルのアドレスを 14 としたときのグラフを以下に示す．つまり初期状態

$$|\varphi_0\rangle = x_0|00000\rangle + x_1|00001\rangle + \cdots + x_{14}|01110\rangle + \cdots + x_{31}|11111\rangle,$$
$$x_i = \frac{1}{4\sqrt{2}},\ i = 0, ..., 31$$

である．ただし N=32 より振幅増幅回数 k=4 となる．

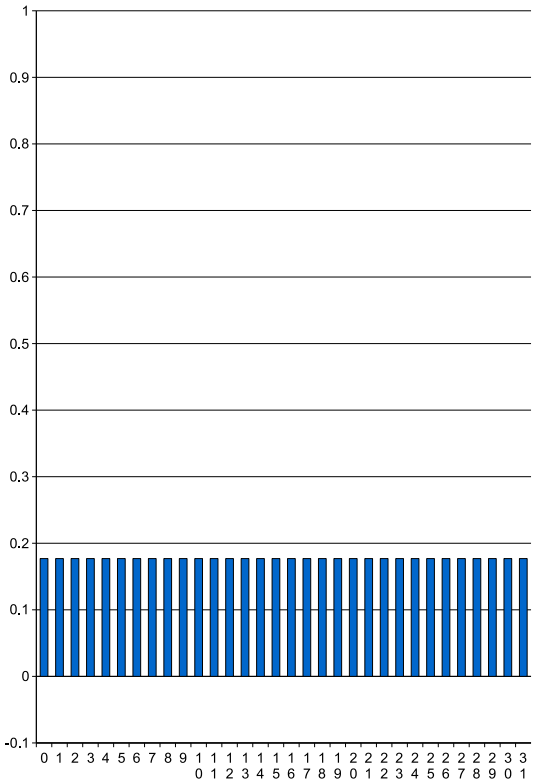

図 3：初期の確率振幅

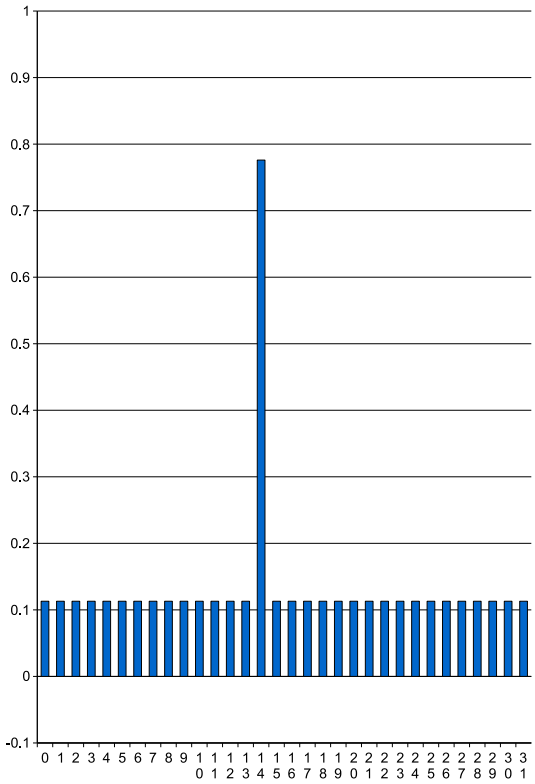

図 5：2 回の振幅増幅後

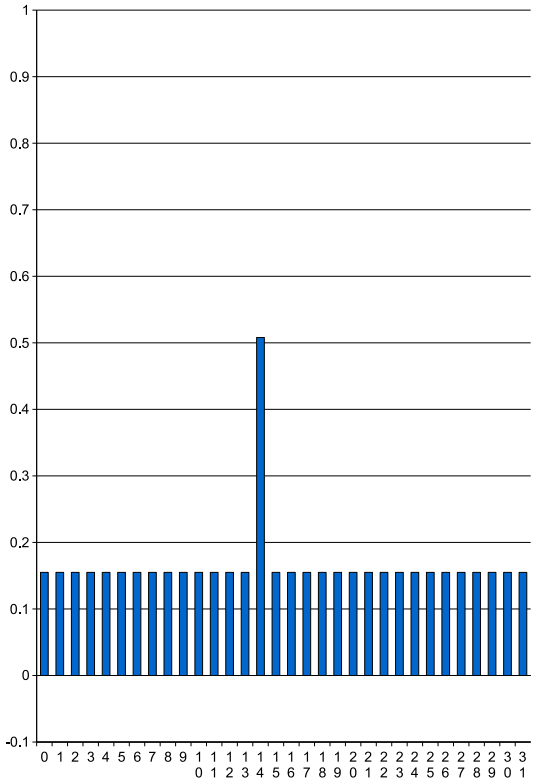

図 4：1 回の振幅増幅後

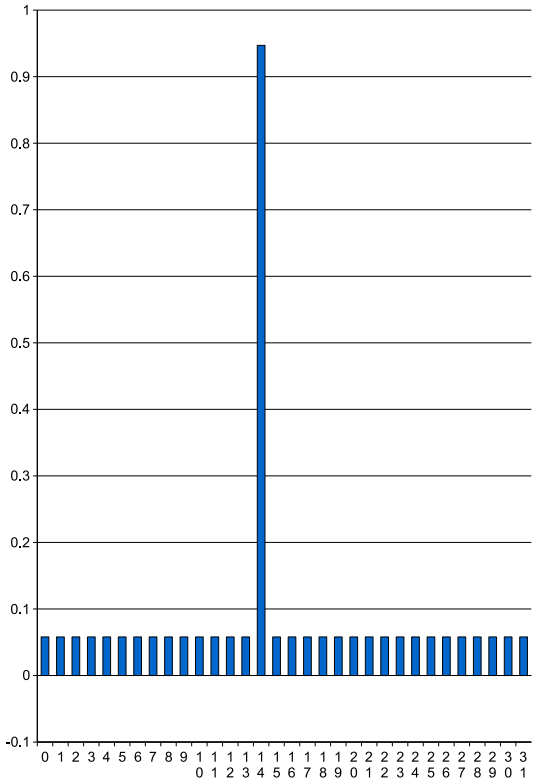

図 6：3 回の振幅増幅後

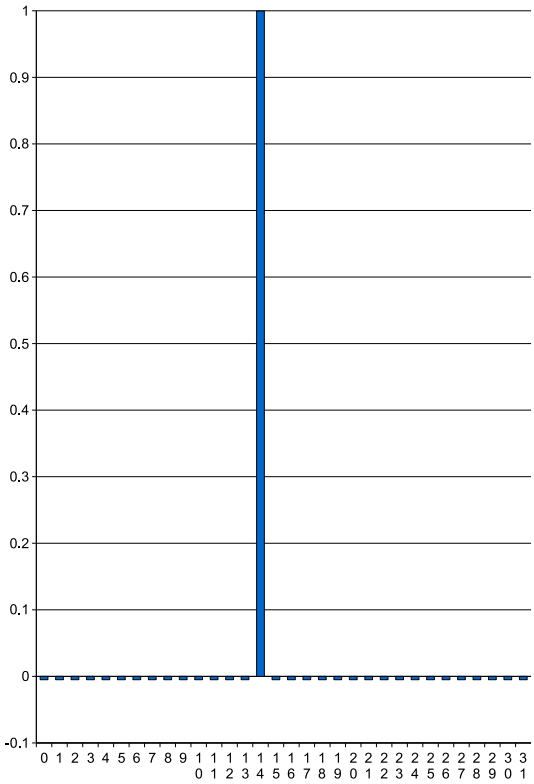

図 7：4 回の振幅増幅後

これより量子計算では，14 番目の状態が確率 $\frac{536431921}{536870912} = 0.999$ で観測される．しかし実際はこのような確率振幅はわからず，出力は 14 というファイルのアドレスのみである．

NMR 量子計算では観測規約の変更により $\varepsilon = \frac{1}{32}$ とすると，必要な確率振幅 $r = \frac{3\sqrt{7}}{32} = 0.24804$ となる．振幅増幅 $k = \lceil \frac{1}{2} \rceil = 1$ 回を終えた時点で，$\theta = 0.26633$ が観測され，$x_{14} = \frac{23}{32\sqrt{2}} = 0.50823$ を得る．$x_{14} \geq r$ を満たすので，14 が目的ファイルのアドレスであることがわかる．

5 今後の課題

- 観測誤差 ε を考慮した NMR 量子計算シミュレータの作成
- Shor の因数分解アルゴリズムのシミュレータ作成
- 対称暗号系秘密鍵を解読する NMR 量子アルゴリズムの追実験

参考文献

[1] R.Feynman, "Simulating Physics with Computers", *International Journal of Theoretical Physics*, Vol. 21, pp.467-488 (1982).

[2] D.Deutsch, "Quantum Computational Networks", *Proc. R. Soc. Lond.*, A400, pp.97-117 (1985).

[3] P.W.Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring", *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, 1994.

[4] Lov.K.Grover. A fast quantum mechanical algorithm for database seach. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pp.212-219, 1996.

[5] N.A.Gershenfeld and I. Chuang: "Bulk Spin-Resonance Quantum Computation", Science, Vol.275, pp.350-356, 1997.

[6] Kazuo OHTA, Tetsuo NISHINO, Seiya OKUBO and Noboru KUNIHIRO,"A Quantum Algorithm using NMR Computers to Break Secret-key Cryptosystems," New Generation computing, Vol.21, No.4, 2003.

[7] 上坂吉則,"量子コンピュータの基礎数理,"コロナ社, 2001.

[8] 西野哲朗,"量子コンピュータの理論,"培風館, 2002.

[9] 大田和夫, 西野哲朗, 國廣昇,"量子アルゴリズムに対する公開鍵暗号及び共通鍵暗号に対する安全性評価."
http://research.nii.ac.jp/kaken-johogaku/reports/H15_A04/A04-02.pdf.

[10] 細谷暁夫,"量子コンピュータの基礎,"サイエンス社, 1999.

[11] 榊原進,"はやわかり Mathematica 第 2 版,"共立出版, 2001.

[12] ジョージ・ジョンソン (著), 水谷淳 (訳),"量子コンピュータとは何か,"早川書房, 2004