遺伝的アルゴリズムによる量子回路生成

矢吹 太朗　　伊庭 斉志

東京大学大学院新領域創成科学研究科基盤情報学専攻
〒 113-8654 東京都文京区本郷 7-3-1
tel: 03-5841-6704
e-mail: yabuki@miv.t.u-tokyo.ac.jp

あらまし

1994 年に Shor が因数分解の量子アルゴリズムを提案して以来，量子計算は大きな注目を集めるようになった．しかしながら，我々がまだ量子計算に慣れていないためか，従来のコンピュータを凌ぐような量子アルゴリズムはその後あまり見つかっていない．また，状態の重ね合わせを長時間保つことができないなどの理由で，実験的には非常に小さい量子回路しか実現していない．そこで我々は遺伝的アルゴリズムを量子回路生成に応用することを提案する．問題に対する深い理解を必要とはしないこの方法で，これまで知られていたよりもシンプルな量子テレポテーションの回路を生成することに成功した．

キーワード

遺伝的アルゴリズム，量子テレポテーション，量子コンピュータ，量子計算，量子回路

Genetic Algorithms for Quantum Circuit Design

Taro Yabuki　　Hitoshi Iba

Department of Frontier Informatics, Graduate School of Frontier Sciences, The University of Tokyo
Hongo 7-3-1 Bunkyouku, Tokyo 113-8654
tel: 03-5841-6704
e-mail: yabuki@miv.t.u-tokyo.ac.jp

Abstract

After the Shor's discovery of the quantum algorithm to factorize a large number in 1994, the field of the quantum computation has attracted the attention of researchers. However, very few quantum algorithms that surpass the classical computer have been discovered since then. This is partly because we are not much familiar with the quantum computation. Besides, to keep a superposition is so difficult that only a very small quantum system is realized experimentally. Thus we propose to apply genetic algorithms to the quantum circuit design. We show by experiments that without deep knowledge of the problem we can evolve a circuit for the quantum teleportation simpler than ever known.

keywords

genetic algorithms, quantum teleportation, quantum computer, quantum computation, quantum circuit

1　はじめに

1.1　量子計算の歴史

量子コンピュータ (quantum computer, QC) の概念は 1980 年に Benioff によって生み出された．背景には Moore の法則で表されるようなチップの高密度化と，計算における情報処理量と消費エネルギーの研究があった．Feynman は量子力学の計算に QC が適していると考え，Deutsch は 1985 年に量子チューリングマシン (quantum Turing machine, QTM) を定式化したが [3]，実用的な問題で QC が従来のコンピュータ (classical computer, CC) を凌ぐようなものが見つからず，しばらく研究は停滞した．

1994 年に Shor が大きな数の因数分解を QC 上で非常に速く行うアルゴリズムを発表し [5]，この分野は一気に注目を集めるようになった．現在使われている公開鍵暗号は，大きな数の因数分解が難しいことが前提になっているからである．

以後，物理学と情報科学の境界領域で QC に関するさまざまな研究が行われている[1]．

1.2　なぜ遺伝的アルゴリズムなのか

CC よりも速そうな量子アルゴリズムは，Shor の後あまり発見されていない．これにはさまざま原因が考えられるが，QC が CC より優れていないというよりは，我々が量子計算にまだ慣れていないためだと思われる．

量子アルゴリズムを実行するための量子回路（ユニタリー変換と観測の組み合わせ）を設計する上での困難には，独立ではないが次のようなものがある．

- 与えられた問題を解くための量子回路をどのようにして作ったらよいのかわからない．
- どのようなユニタリー変換を施せばよいかわかっていても，その変換をより基本的なユニタリー変換を用いてどのように構成すればよいかわからない．
- 回路を構成できてもそれが効率のよいものかどうかの判断基準があまりない．
- 解空間の性質がよくわからないため，局所的な変化と大局的な変化のつながりがわからない．

[1] QC に関する入門的なレビューとしては [7] が，アーカイブとしては http://xxx.lanl.gov/archive/quant-ph があり，さまざまな情報は http://www.qubit.org/からたどれる．

このような困難があるのに対し，遺伝的アルゴリズム (genetic algorithm, GA)[10] はランダムな解の候補から始めることができて，その回路全体を見て評価することだけできれば実行できるため，この問題に向いていると思われる．例えば可変長の遺伝子を使って回路のサイズに淘汰圧をかければ，よりシンプルで物理的に実装しやすい回路を生成することも可能である．量子ビット (quantum bit, qubit) の重ね合わせを長時間保つことが現在の技術では難しいため，重ね合わせが壊れるまでに通過できるゲートの数は少ない．そのため，出力は同じでもよりシンプルな回路は望ましいのである．実際，それまで知られていた量子回路よりもシンプルなものを作ることに成功した例がある [8]．さらに，GA によって CC よりも効率のよい量子回路を作ることに成功した例もある [6].

我々は，量子計算の比較的単純で扱いやすいが興味深い例である量子テレポテーションの回路生成に GA を応用した．人間が作った正しい回路を与えて進化させた既存の研究と異なり，本質的な制限と望ましい出力を考慮するだけで正しい回路を獲得できること，それによってこれまで知られていたよりもシンプルな回路が得らることを本稿では示す.

2　量子計算

まず，量子計算の原理を説明する．以下の議論のビットまたは qubit は本来チューリングマシンまたは QTM のテープ上のものなのだが，レジスタやメモリと考えれば充分である．

2.1　Qubit

ビットが 0 であることを示すのに $|0\rangle$ という表記をする．また，5 つのビットが順に 0,1,0,1,1 の場合，$|1\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle$，$|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle$，$|11010\rangle$ など書く．これが 2 進数だと思って，それを 10 進数に変換し $|26)$ とも書く．ビット列は右から 0 番目，1 番目，$\cdots$ と数えることにする．

CC のビットは 0 または 1 のどちらか一方の値しかとることができないが，例えば電子のスピンが上向きか下向きかによって 0 と 1 を表すような qubit は，重ね合わせ $a|0\rangle + b|1\rangle$ を持つことができる．

0 番目の qubit が $|0\rangle+|1\rangle$，1 番目の qubit が $|0\rangle-|1\rangle$，であるような 2-qubits 系はテンソル積を用いて，

$$(|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) = |00\rangle + |01\rangle - |10\rangle - |11\rangle$$

のように表すことができる．系がこのような状態にあるときに 1 番目（左側）の qubit を観測すると，系は 1 番目の qubit が 0 の $|00\rangle + |01\rangle$ または 1 番目の qubit が 1 の $-|01\rangle - |11\rangle$ に等確率で遷移する．

係数を並べたベクトルで状態を記述すること，つまり状態 $\sum a_i|i)$ を $\boldsymbol{a} = (a_i)$ で表すこともある．例えば上の遷移は，$(1\ 1\ -1\ -1) \to (1\ 0\ 1\ 0)$ または $(0\ -1\ 0\ -1)$ のようにも表せる．

2.2 観測

状態 $a|0\rangle + b|1\rangle$ の係数 a, b は確率振幅と呼ばれる複素数である．この状態にある qubit を観測すると，確率 $|a|^2$ で $|0\rangle$ が確率 $|b|^2$ で $|1\rangle$ が観測される．確率を表すため，確率振幅は $|a|^2 + |b|^2 = 1$ と規格化されていなければならない．以下の議論では断らなくても確率振幅は規格化されているものとする，つまり規格化のための定数倍を省略している場合がある．

2.3 ユニタリー発展・量子論理ゲート

状態の時間発展には先にあげた観測と Schrödinger 方程式で記述されるユニタリー発展がある．量子計算においてこれは量子論理ゲートの組み合わせで表される．例えば，制御 NOT(controlled not, CNOT) ゲート CNOT_{01} は図 1 のように表される．以下ではゲートの添え字でそのゲートが作用する qubit を表すことにする．CNOT の場合，左側の添え字が target を，右側の添え字が controll を表すことにする．1 つ以上のゲートと観測の組み合わせを量子回路と呼び，図に書いた場合は左から右へ読む．

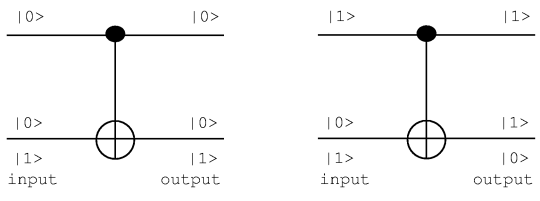

図 1: controlled-NOT gate

状態をベクトルで記述すると，ゲートは行列で記述できる．この行列はユニタリー行列でなければならない．このことはベクトルのノルムが確率の和を表し，確率の和は変化しないことから理解できる．上にあげた CNOT_{01} の行列表示は，

$$\mathrm{CNOT}_{01} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

量子チューリングマシンと量子回路は同等であること [9]，任意のユニタリー変換が 2-qubit の CNOT と 1-qubit のユニタリー変換[2]の組み合わせで作れること [4] が証明されている．

2.4 Entangled state

QC の複数の qubits は，それぞれ独立ではなく絡み合った状態，entangled state になることができる．例えば target が $|0\rangle + |1\rangle$，controll が $|1\rangle$ の 2-qubit 系 $(|0\rangle + |1\rangle)|1\rangle = |0\rangle|1\rangle + |1\rangle|1\rangle$ に CNOT_{10} を作用させると，EPR-pair と呼ばれる entangled state$|0\rangle|1\rangle + |1\rangle|0\rangle$ になるが，これはテンソル積では表せない．ここで 0 番目の qubit（左側）を観測して $|0\rangle$ が得られたとすると，その瞬間に 1 番目の qubit（右側）は $|1\rangle$ になる[3]．

3 量子テレポテーション

Alice が離れた場所にいる Bob に $|f\rangle = a|0\rangle + b|1\rangle$ という 1-qubit の情報を伝えることを考える．Alice が a, b を知っていれば，それを古典的な方法で伝えればよい．そうでない場合，Alice が $|f\rangle$ を観測すれば，状態は変わってしまうし，状態をコピーして観測することもできないため[4]，Alice が $|f\rangle$ のすべてを知ることはできないから，その qubit を直接持っていく以外に情報を伝える方法はないように見える．Bennett らによる量子テレポテーションはこれを可能にする [1].

---

[2]任意の 1-qubit のユニタリー変換は少数のユニタリー変換の組み合わせで作ることができる．

[3]この性質は非相対論的に見え，Einstein-Podolsky-Rosen(EPR) のパラドックスを生んだが，実験的に確かめられている．

[4]$|a\rangle$ と $|b\rangle$ が独立なベクトルとして，

$$C|a\rangle|0\rangle = |a\rangle|a\rangle,\ C|b\rangle|0\rangle = |b\rangle|b\rangle$$

となるようなコピー回路 C があったとする．このとき，

$$\begin{aligned} C(\alpha|a\rangle| + \beta|b\rangle)0\rangle &= \alpha|a\rangle|a\rangle + \beta|b\rangle|b\rangle \\ &\neq (\alpha|a\rangle| + \beta|b\rangle)(\alpha|a\rangle| + \beta|b\rangle) \end{aligned}$$

なのではじめの仮定に矛盾する．よって状態をコピーする回路はない (no cloning theorem.)

3.1 アイディア

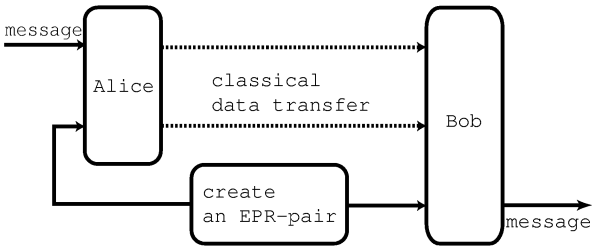

図 2: Idea of quantum teleportation.

量子テレポテーションのアイディアは図 2 のとおりである．テレポテーションの手順は，

1. EPR-pair を作り，一方を Alice にもう一方を Bob のところに飛ばす.
2. Alice は自分の持っていた qubit と飛んできた EPR-pair のかたわれとを絡み合わせる．これによってすべての qubits が絡み合うことになる.
3. Alice は自分のところにある 2 つの qubits を観測する．その影響は Bob のところにある qubit にも及ぶ.
4. 観測結果を Alice から伝えられると，Bob は qubit にある適当な操作をすることで情報を復元できる.

詳細は次のとおりである．EPR-pair($|00\rangle + |11\rangle$) を生成し，その一方を Alice にに，もう一方が Bob に届ける．はじめ Alice が持っていた qubit を一番左に書くことにすると状態は，

$$(a|0\rangle + b|1\rangle) \otimes (|00\rangle + |11\rangle)$$
$$= a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle$$

になる．Alice が CNOT_{21} と H_1 を行った後で[5]，左の 2 つの qubits を読むと状態は $|00\rangle(a|0\rangle + b|1\rangle)$, $|01\rangle(a|1\rangle + b|0\rangle)$, $|10\rangle(a|0\rangle - b|1\rangle)$, $|11\rangle(a|1\rangle - b|0\rangle)$ のいずれかになる．例えばもし Alice が 11 を観測しそのことを Bob に伝えれば，Bob は自分のところにある qubit が $(a|1\rangle - b|0\rangle)$ であることがわかり，$\frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ によって Alice が持っていた状態 $|f\rangle = a|0\rangle + b|1\rangle$ を復元できる．Alice が他の値を観測した場合も同様である．Alice が持っていた状態は壊れ，まったく同じものを Bob が持つことになるからこれはテレポテーションであるが，Alice が読んだ値を Bob に伝えるのは古典的方法（光速以下）であるから，このテレポテーションで情報が伝わるのも光速以下である.

[5] $\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$.

3.2 回路の詳細

上で示したアイディアを実現するために Brassard が提案した回路が図 3 である [2]．図中の L は $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$，R は $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$，S は $\begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$，T は $\begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}$，M は観測のことである．この回路には観測も含めて 11 個のゲートがあることに注意して欲しい．量子テレポテーションが 8 個のゲートで実現できることを 6 節で示す.

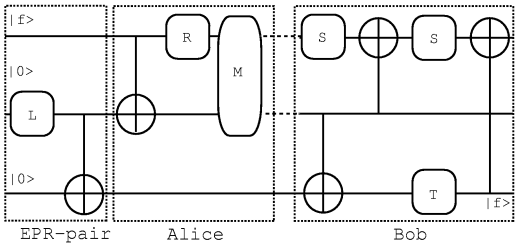

図 3: Brassard's circuit[2].

4 既存の研究

図 3 の回路は次の 3 つの部分に分けられる（1 と 3 はユニタリー変換である.）

1. $\mathrm{L}_1, \mathrm{CNOT}_{01}, \mathrm{CNOT}_{21}, \mathrm{R}_2$
2. 観測
3. $\mathrm{S}_2, \mathrm{CNOT}_{01}, \mathrm{CNOT}_{12}, \mathrm{S}_2, \mathrm{T}_0, \mathrm{CNOT}_{20}$

Williams らはこれらのユニタリー変換を，GA を使ってより基本的なユニタリー変換から合成した [8]．例えば初めのユニタリー変換 U の行列は次のとおりである（これは図 3 に示した回路の個々のゲートに対応するユニタリー変換の合成によって簡単に確かめられる.）

$$U = \frac{1}{2}\begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ -1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 0 & -1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & -1 & 1 & 0 & -1 & 0 \\ -1 & 0 & -1 & 0 & 0 & 1 & 0 & -1 \end{pmatrix}.$$

基本的なユニタリー変換（{CNOT, L, R} を採用，これは universal set ではない）の並びを遺伝子とし，それらの合成でできるユニタリー変換を S とする．U と S がどのぐらい似ているかを表す関数 f を，

$$f(S,U) \equiv \sum_{i=1}^{2^N}\sum_{j=1}^{2^N} |U_{ij} - S_{ij}|$$

のように定義し，この関数によって淘汰圧をかけ（値が小さいほうが適合度が大きい）進化させた．

1 のユニタリー変換に対しては従来と同じものしか発見できなかったが，3 のユニタリー変換は 4 つのゲートで実現できるということを発見した．

しかしながら彼らの方法には次の点で不満がある．まず目標のユニタリー変換を与えていることである．全体の動作に要求されるのは，入力 $(p|0\rangle + q|1\rangle) \otimes |0\rangle \otimes |0\rangle$ に対し，出力が $(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle) \otimes (p|0\rangle + q|1\rangle)$ だということだけであって，これだけでは全体のユニタリー変換を書き下すことはできない．つまり目標のユニタリー変換を与えるには他にかなりのヒューリスティクスが必要である．また，目標のユニタリー変換を与えてしまったために，後で示すようなよりシンプルな回路を発見できなくなってしまっている．

さらに，このような個体の作り方では前半のユニタリー変換を，

$$\mathrm{L}_1, \mathrm{CNOT}_{12}, \mathrm{CNOT}_{02}, \mathrm{CNOT}_{01}, \mathrm{R}_2$$

のように合成してしまうことがありうるが，これは 5.1 で述べるこの問題への制約 2,3 に反する．2 番目の qubit を操作してから，つまり Alice の操作が始まってからは 0 番目の qubit を操作することはできないのである．その時 0 番目の qubit は Bob のところにあるからである[6]．

Williams らの生成した回路を図 4 に示す．Brassard によるゲートを 11 個必要とする回路（図 3）に比べて，かなり簡単なものができている．

5 提案する手法

5.1 必要とした知識

我々の提案する手法では，人間が作った正しい回路をあらかじめ与える必要はなく，以下のような制限を課すだけで回路を生成する．

[6]実は 4 つ以下のゲートでこのユニタリー変換を合成する方法は図 3 に示したものしかないため，(回路のサイズにも淘汰圧をかけて）実験すれば正しい解が得られる可能性が大きい．

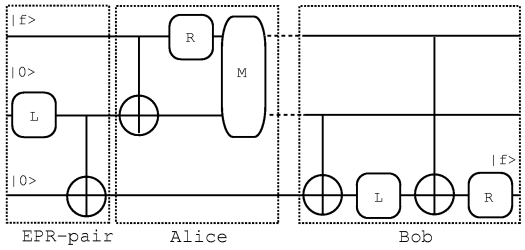

図 4: Williams's circuit[8].

- 量子テレポテーションの回路の性質（Williams らはこの 2 と 3 を考慮しなかった.）
  1. 3-qubit のシステムである．
  2. EPR-pair 生成部では 0 番目と 1 番目の qubit しか操作できない[7]．
  3. Alice は 1 番目と 2 番目の qubit しか操作できない[8]．
- 探索空間を狭めるための仮定（1 番目は当然の，2 番目は Williams らにならった仮定である.）
  1. 観測は 1 回のみ，1 番目と 2 番目の qubit を測定する．
  2. 使用するゲートは {CNOT, L, R} である．

5.2 遺伝子

遺伝子は例えば次のような $\{0,1,2,3\}$ のいずれかの文字から成る 1 次元の固定長の配列である．

EPR-pair				Alice の操作			Bob の操作			
112	231	001	**3**31	132	012	221	**3**02	001	100	002	201

遺伝子は 3 文字をひとまとまりとするコドン単位で解釈される．初めの文字がゲートの種類を，後の 2 文字がその作用する qubit を表す．ただし初めの文字が 3 のコドンで，最初のものは EPR-pair 生成部と Alice の操作の区切りを，2 番目のものは Alice の操作と Bob の操作の区切りつまり観測を表す．各コドンが実際にどのような操作を表すかは，これらで区切られる 3 つの領域で若干異なる．

上の遺伝子は次のように解釈される．4 番目のコドンの 1 文字目は 3 であるから，このコドンは EPR-pair 生成部と Alice の操作とを分ける．3 ではじまる次のコドンは 8 番目のものである．これは観測を表し，この後はボブの操作になる．

[7]2 番目の qubit は Alice のところにあるため．
[8]0 番目の qubit は Bob のところにあるため．

EPR-pair 生成部は表 1 のとおりに解釈される[9]. 112 は L_1，231 は無意味，001 は $CNOT_{01}$ を表す. Alice の操作の部分は表 2 によって解釈され，無意味，$CNOT_{12}$，R_2 を表している．Bob の操作についても同様である．できあがるのは図 4 に示した回路である.

1文字目	2文字目 0	2文字目 1	2文字目 2	2文字目 3	
0	$CNOT_{01}$	$CNOT_{10}$			0
	$CNOT_{01}$	$CNOT_{10}$			1
	$CNOT_{01}$	$CNOT_{10}$			2
					3
1	L_0	L_1			0
	L_0	L_1			1
	L_0	L_1			2
					3
2	R_0	R_1			0
	R_0	R_1			1
	R_0	R_1			2
					3
3	separator				*

表 1: EPR-pair 生成部

1文字目	2文字目 0	2文字目 1	2文字目 2	2文字目 3	
0		$CNOT_{12}$	$CNOT_{21}$		0
		$CNOT_{12}$	$CNOT_{21}$		1
		$CNOT_{12}$	$CNOT_{21}$		2
					3
1		L_1	L_2		0
		L_1	L_2		1
		L_1	L_2		2
					3
2		R_1	R_2		0
		R_1	R_2		1
		R_1	R_2		2
					3
3	measurement				*

表 2: Alice の操作

5.3 適合度の計算

個体の評価は次のように行う.

[9]表の空欄はその配列が何も意味を持たないことを表す.

1文字目	2文字目 0	2文字目 1	2文字目 2	2文字目 3	
0		$CNOT_{10}$	$CNOT_{20}$		0
	$CNOT_{01}$		$CNOT_{21}$		1
	$CNOT_{02}$	$CNOT_{12}$			2
					3
1	L_0	L_1	L_2		0
	L_0	L_1	L_2		1
	L_0	L_1	L_2		2
					3
2	R_0	R_1	R_2		0
	R_0	R_1	R_2		1
	R_0	R_1	R_2		2
					3
3					*

表 3: Bob の操作

1. 乱数 $\alpha, \beta, \gamma \in [0, 2\pi]$ を作る.

2. 3 種類の初期状態 $(p\ q) = (e^{i\beta}\cos\alpha\ e^{i\gamma}\sin\alpha)$, $(e^{i\gamma}\cos\beta\ e^{i\alpha}\sin\beta)$ $(e^{i\alpha}\cos\gamma\ e^{i\beta}\sin\gamma)$ を用意する[10].

3. $(p|0\rangle + q|1\rangle) \otimes |0\rangle \otimes |0\rangle = (p\ 0\ 0\ 0\ q\ 0\ 0\ 0)$ に先に示した方法で解釈したとおりのゲートを順に施す.

4. 望ましい最終状態に近い最終状態を与える回路を作った個体の適合度を大きくする.

5. 50 世代ごとに初めの乱数を変える.

途中で観測をした場合には，その後の分岐をすべて調べる．つまり，観測の前の段階で (a_i) で表される状態だった場合，観測後は $(a_0\ a_1\ 0\ 0\ 0\ 0\ 0\ 0)$, $(0\ 0\ a_2\ a_3\ 0\ 0\ 0\ 0)$, $(0\ 0\ 0\ 0\ a_4\ a_5\ 0\ 0)$, $(0\ 0\ 0\ 0\ 0\ 0\ a_6\ a_7)$ のいずれかになるが，これらをすべて追跡するのである.

望ましい最終状態は $(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle) \otimes (p|0\rangle + q|1\rangle) = (ap\ aq\ bp\ bq\ cp\ cq\ dp\ dp)$ である[11]．各個体が作る回路を通った最終状態は 12 個（初期状態が 3 通りあり，観測によってそれぞれ 4 通りに分岐するため）あるがそれらを $\boldsymbol{a}_j = (a_{j,i})$ と書くことにする．最終状態と望ましい最終状態の

[10]3 種類用意するのは，後で定義する $error_j$ の値が乱数そのものにはあまりよらないようにするためである.

[11]2 つずつ順に取ればすべて $p : q$ の比になっている.

ずれを，

$$error_j \equiv \frac{1}{n} \sum_{i=0,2,4,6} \left| \frac{a_{j,i}}{a_{j,i+1}} - \frac{p}{q} \right|$$

で表す．ただし n は $(0,0)$ でない $(a_{j,i}, a_{j,i+1})$（i は偶数）の数で，和はそれらについてのみ取る．最終状態が $\mathbf{0}$ の場合は $error_j = 100$ とする．望ましい最終状態になっていれば $error_j = 0$ である．

個体の適合度 f は，$f = 1/(1 + 10 \sum error_j)$ で与える．ただしこの f が 1，つまり正しい回路が得られている場合は f に (1/ゲートの数) を加え，回路の大きさでも淘汰圧をかける．

5.4 GA のパラメータ

まずすべての個体をランダムに初期化した．適合度 f に対して，

$$f' = f - (\bar{f} - 2\sigma)$$

というシグマ・スケーリングをし，ルーレット方式で親となる個体を選択した．交叉率 0.7 の二点交叉，(1/遺伝子長) の確率で文字を書き換えるような突然変異を用い，世代ごとに 5,000 個体すべてを入れ替えながら 1,000 世代まで計算した．さまざまな遺伝子長に対し乱数の種を変えながら 10 回ずつ計算した．

6 結果

GA によって得られた回路で最も簡単なものを図 5 に示した．Williams らが生成した回路はゲートが 9 個必要なのに対し，この回路は 8 個のゲートで構成されている．実際，観測ゲートが $|00\rangle$ を観測した場合，最終状態は $(|00\rangle - |10\rangle)(p|0\rangle + q|1\rangle)$，$|01\rangle$ なら $(|11\rangle - |01\rangle)(p|0\rangle + q|1\rangle)$，$|10\rangle$ なら $(|00\rangle + |10\rangle)(p|0\rangle + q|1\rangle)$，$|11\rangle$ なら $(|01\rangle + |11\rangle)(p|0\rangle + q|1\rangle)$ となることは簡単に確かめられて，確かに 2 番目の qubit の状態が 0 番目の qubit に移されていることがわかる．

遺伝子長に対して，生成された回路中のゲート数をプロットしたのが図 6 である[12]．短い遺伝子を使うと，できあがる回路は小さくなっている．しかしながら，遺伝子長に対して，成功確率つまり 1,000 世代までに適合度が 1 になる確率を示した図 7 を見るとわかるように，短い遺伝子を使うと成功確率は下がる．

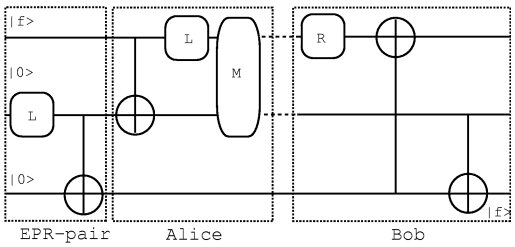

図 5: Circuit for teleportation(this work)

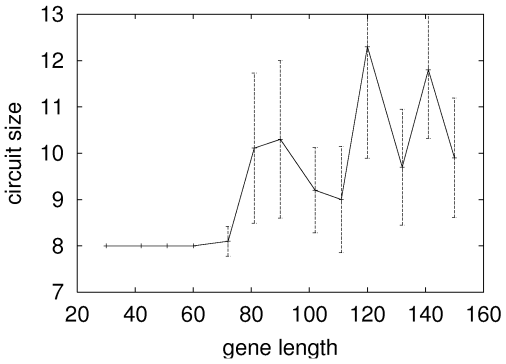

図 6: Number of gates in evolved circuit.

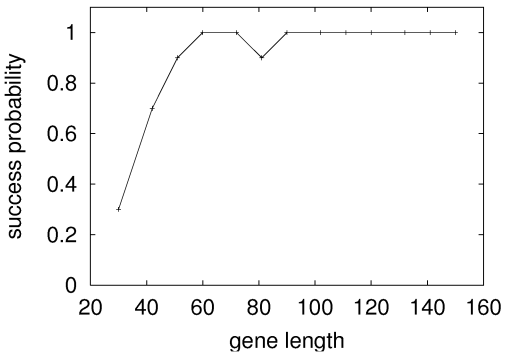

図 7: Probability of success.

図 8 は遺伝子長に対して，適合度が初めて 1 を超えた世代の平均をプロットしたものだが，遺伝子長 120（ゲートは最大で 40 個）で最小になっている．遺伝子を長くしたほうが適合度計算に時間がかかるが，たとえその効果を最大に見積もって，この世代数を遺伝子長倍したとしてもやはり遺伝子長 120 の場合がもっとも速く成功する．しかし図 6 を見るとわかるように，遺伝子長 120 ではあまりシンプルな回路は得られていない．

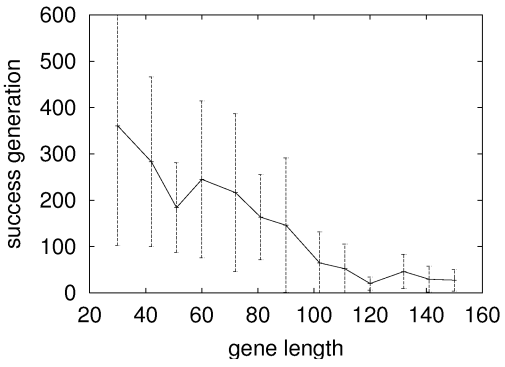

図 8: The generation of success.

遺伝子長 60（ゲートは最大で 20 個）の場合は常にゲート数 8 の回路が生成された．この回路は平均 350 世代（標準偏差 280）で発見できているが，それまでに試す回路は $5,000$(個体) $\times 350$(世代) $\sim 1.7 \times 10^6$ 通りである．一方，ゲートの種類は全部で 14 種類あるため[13]，回路のすべての可能性は $20^{14} \sim 10^{18}$ 通りである[14]．

7 おわりに

我々は GA を使って量子回路を生成する方法を考案し，量子テレポテーションに応用した．従来の研究では人間が作った正しい回路が与えられて，回路の性質は考慮されなかったのに対し，我々は本質的な制限と若干の仮定のみのもとで進化論的計算を行った．その結果正しい回路を獲得できたこと，さらにそれがこれまで知られていたよりもシンプルな回路であったことを示した．

[12]エラー・バーは標準偏差である．

[13]CNOT が 6 通り，L, R がそれぞれ 3 通り，そして観測と区切りである．

[14]ただし解がどれぐらい密度で分布しているかわからないため，これらの数値を直接比べることはできない．

参考文献

[1] C. H. Bennett, et al. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, Vol. 70, p. 1895, 1993.

[2] G. Brassard. Teleportation as a quantum computation. In *Proceedings of the Fourth Workshop on Physics and Computation*, p. 44. New England Complex Systems Institute, 1996. quant-ph/9605035.

[3] D. Deutsch. Quantum theory, the church-turing principle and the univarsal quantum computer. In *Proceeding Royal Society London*, Vol. A400, p. 97, 1985.

[4] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. *Proc. Roy. Soc. London*, Vol. A474, p. 969, 1995. quant-ph/9505018.

[5] P. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the 35th IEEE Symposium on Fundation of Computer Science*, p. 124, 1994.

[6] L. Spector, et al. Finding a better-than-classical quantum and/or algorithm using genetic programming. In *Proceedings of the 1999 Congress on Evolutionary Computation.* IEEE Press, 1999.

[7] A. Steane. Quantum computing. *Reports on Progress in Physics*, Vol. 61, p. 117, 1998. quant-ph/9708022.

[8] C. P. Williams and A. G. Gray. Automated design of quantum circuits. In *QCQC'98 LNCS 1509*, p. 113. Springer-Verlag, 1999.

[9] A. Yao. Quantum circuit complexity. In *Proceedings of the 34th IEEE Symposium on Fundation of Computer Science*, p. 352. IEEE Computer Society Press, 1993.

[10] 伊庭斉志. 遺伝的アルゴリズムの基礎. オーム社, 1994.