

## 量子計算と線形 2 端子回路網

東京理科大学理工学部情報科学科 上坂吉則 (Yoshinori Uesaka)

Quantum Computation and Linear Circuits with Two Terminals

Yoshinori Uesaka (uesaka@is.noda.sut.ac.jp) Science University of Tokyo

**Abstract** : One of most important features in quantum computation might be said to be the linearity of state transitions. On the other hand we may easily find several classical resources causing linear state transitions. Thus it is natural to ask to what extent quantum computation can be simulated by such classical resources. The present paper tries to discuss the simulation ability by using passive linear circuits as a computation resource.

1. はじめに 量子計算で主役を演じていることの一つは状態の線形的推移にあるといっている。一方、状態を線形的に推移させるシステムは古典物理系にも多く見られる。この小論では古典線形系の一つである線形 2 端子回路網によって、量子計算とどの程度まで相似な計算ができるかを検討する。

量子計算の様子を単純に言い切ってしまうばつぎのようになるであろう。まず、量子システムの状態が線形空間のベクトルで表され、その状態推移がユニタリ作用素（行列）で引き起こされることに着目する。そこで状態を表すベクトルを情報と解釈すると、状態の推移はこの情報の加工、すなわち、「計算」と見なすことができるようになり、ユニタリ作用素は「計算機」と考えることができるようになる。

いま、量子システムの状態の集合である複素線形空間を  $W$  とし、 $W$  から  $W$  へのユニタリ作用素を  $U$  とする。 $W$  のベクトル  $|\varphi\rangle$  に  $U$  を施すとベクトル

$$(1.1) \quad |\psi\rangle = U|\varphi\rangle$$

が得られる。 $|\varphi\rangle$  を計算のための入力情報、 $|\psi\rangle$  を計算結果とそれぞれ考えるわけである。しかしながら、量子力学の法則により、 $|\psi\rangle$  自身を直接知ることはできない。いま、 $W$  の正規直交基底を  $|0\rangle, |1\rangle, \dots, |N-1\rangle$  とすると、 $|\psi\rangle$  はこれらの線形結合として

$$(1.2) \quad |\psi\rangle = w_0|0\rangle + \dots + w_{N-1}|N-1\rangle$$

と表されるが、このとき、エルミート作用素で表されるある観測量を観測すると、確率  $|w_k|^2$  で  $|\varphi_k\rangle$  が（正しくはエルミート作用素の固有値が観測値として）得られる。このように、量子計算では、計算結果は確率的に得られることになる。したがって量子計算でのプログラミングの基本方針としては、 $|\varphi_k\rangle$  が所望の結果（正しい結果）であるときには、 $|w_k|^2$  ができるだけ大きくな

るように設計することになる。

計算過程を生み出す道具  $U$  が線形であることから、自然な形で、並列計算が可能になり（量子並列性）、このことが計算の高速性を生み出すのではないかという期待がある。実際、ファイル検索や因数分解などの量子アルゴリズムが古典計算の速度を質的に凌駕できることが示されている（Shor, 1994; Grover, 1996）。

しかしながら、線形的な状態推移を引き起こす物理的リソースは古典の世界にも多く見受けられる。しかもそこでは観測によって状態が、したがって、計算結果が乱されるということはない。この小論では、古典物理の線形リソースの一つとして線形 2 端子回路網を取り上げ、それによって量子計算とある意味で相似な計算過程を構成したときに、どのような計算機械が得られるかを検討する。

**2. 線形 2 端子回路が定める写像** 線形素子であるインダクタンス、キャパシタンスおよびレジスタンスから成る 2 端子回路を考え、これに正弦波形（電圧） $x = e^{j\omega t}$  を印加すると正弦波形（電流） $y = a(\omega)e^{j\omega t}$  が出力されることは電気回路理論でよく知られている（Kiyasu et al., 1957）。ここに、 $j$  は虚数単位  $\sqrt{-1}$ 、 $\omega$  は角周波数である。また、 $a$  は回路の構造から定まる、 $j\omega$  の、有理関数であり、アドミタンスと呼ばれている。特に、複数の正弦波形

$$(2.1) \quad e_0 = e^{j\omega_0 t}, \dots, e_{N-1} = e^{j\omega_{N-1} t}$$

の線形結合で表される入力：

$$(2.2) \quad x = x_0 e_0 + \dots + x_{N-1} e_{N-1}$$

に対する出力は

$$(2.3) \quad y = x_0 a(\omega_0) e_0 + \dots + x_{N-1} a(\omega_{N-1}) e_{N-1}$$

で与えられる。このことから、2 端子回路は  $e_0, \dots, e_{N-1}$  で張られる複素線形空間  $V$  から  $V$  への線形写像として、基底  $e_0, \dots, e_{N-1}$  による表現行列が対角行列：

$$(2.4) \quad A = \begin{bmatrix} a(\omega_0) & & 0 \\ & \ddots & \\ 0 & & a(\omega_{N-1}) \end{bmatrix}$$

であるような写像を定めることがわかる。

**3.1 ビット演算と制御 NOT** 最も簡単な 1 ビットの演算として **NOT** を計算する線形回路を構成することから始めよう。量子計算では、 $2 \times 2$  のユニタリ行列  $U$  を用意して

$$(3.1) \quad U|0\rangle = |1\rangle, U|1\rangle = |0\rangle, \text{ただし, } U := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

のように状態推移を起こし、**NOT** が計算できたと考える。したがって、回路で同じことをするにはこの  $U$  を表す  $A$  を作ればよいが、 $A$  は対角なので、このままでは  $U$  を実現することができない。

そこで正弦波形  $e_0 = e^{j\omega_0 t}, e_1 = e^{j\omega_1 t}$  で生成される線形空間を  $V$ 、 $|0\rangle, |1\rangle$  が張る線形空間を  $W$  とし、 $V$  から  $W$  へのある同形写像  $\varphi$  によってつぎのダイアグラムが可換になるように、 $A$  を定める

ことにする：

$$(3.2) \quad \begin{array}{ccc} V & \xrightarrow{A} & V \\ \varphi \downarrow & & \varphi \downarrow \\ W & \xrightarrow{U} & W \end{array} \quad U = \varphi \circ A \circ \varphi^{-1}.$$

それには、(3.2)の第2の式からわかるように、 $A$ が対角であったことに注意すれば、 $U$ を対角化すればよいことがわかる。実際、

$$(3.3) \quad a(\omega_0)=1, a(\omega_1)=-1, \quad \begin{cases} \varphi(e_0) = (|0\rangle + |1\rangle)/\sqrt{2} \\ \varphi(e_1) = (|0\rangle - |1\rangle)/\sqrt{2} \end{cases} \quad \begin{cases} \varphi^{-1}(|0\rangle) = (e_0 + e_1)/\sqrt{2} \\ \varphi^{-1}(|1\rangle) = (e_0 - e_1)/\sqrt{2} \end{cases}$$

ととれば、

$$(3.4) \quad (\varphi \circ A \circ \varphi^{-1})(|0\rangle) = |1\rangle, \quad (\varphi \circ A \circ \varphi^{-1})(|1\rangle) = |0\rangle$$

が成り立ち、回路によって NOT が計算できることがわかる。このとき、 $\varphi^{-1}$ と $\varphi$ はそれぞれビット情報と波形情報との間の符号化と復号化の役割を果たしていることになる。

つぎに基本的な量子ゲートである制御 NOT について考える。こんどは正弦波形  $e_0, e_1, e_2, e_3$  で生成される線形空間を  $V$ 、 $|00\rangle, |01\rangle, |10\rangle, |11\rangle$  が張る線形空間を  $W$  として、まえと同様に考える。

量子計算では、 $4 \times 4$  のユニタリ行列  $U$  を用意して

$$(3.5) \quad U|00\rangle = |00\rangle, \quad U|01\rangle = |01\rangle, \quad U|10\rangle = |11\rangle, \quad U|11\rangle = |10\rangle,$$

ただし、

$$(3.6) \quad U := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma, \quad \sigma := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

のように状態推移を起し、制御 NOT が計算できたと考える。この  $U$  を対角化することによって回路のアドミタンス関数と同形写像がつぎのように定まる：

$$(3.7) \quad a(\omega_0)=1, \quad a(\omega_1)=1, \quad a(\omega_2)=1, \quad a(\omega_3)=-1$$

$$(3.8) \quad \begin{cases} \varphi(e_0) = (|0,0\rangle + |0,1\rangle)/\sqrt{2} \\ \varphi(e_1) = (|0,0\rangle - |0,1\rangle)/\sqrt{2} \\ \varphi(e_2) = (|1,0\rangle + |1,1\rangle)/\sqrt{2} \\ \varphi(e_3) = (|1,0\rangle - |1,1\rangle)/\sqrt{2} \end{cases} \quad \begin{cases} \varphi^{-1}(|0,0\rangle) = (e_0 + e_1)/\sqrt{2} \\ \varphi^{-1}(|0,1\rangle) = (e_0 - e_1)/\sqrt{2} \\ \varphi^{-1}(|1,0\rangle) = (e_2 + e_3)/\sqrt{2} \\ \varphi^{-1}(|1,1\rangle) = (e_2 - e_3)/\sqrt{2} \end{cases}$$

まったく同様にして任意の 1 ビットのユニタリ行列で規定される量子計算を実行する回路を作ることができる。

一方、任意のビット数の任意のユニタリ行列は 1 ビットのユニタリ行列と制御 NOT で構成できることが知られている (Deutsch, 1985)。また、回路が物理的実在として存在するための条件はアドミタンスが、複素変数の関数として、実係数の有理関数で、実部が正である変数に対して正則であり、虚軸上で実部が非負であり、虚軸上の極は 1 位でその留数が正であることである (Kiyasu et al., 1957)。

ユニタリ行列の固有値は  $e^{j\theta}$  の形をしているから、われわれの回路のアドミタンスをこの条件を満たすようにとることができ、したがってつねに実在することになる。以上のことから、ただちにつぎの結果が得られる：

**定理 1** 2 端子回路による計算能力は量子計算のそれを下回らない。□

また、量子計算における計算量はその計算に要する 1 ビットのユニタリ行列と制御 NOT の個数によって評価できる (Ekert and Jozsa, 1996)。したがって、上でみたように、回路による計算は、量子計算における 1 ビットのユニタリ行列と制御 NOT の個数を、少なくとも上回ることなく、対応して構成できることから、つぎの結果も得られる：

**定理 2** 2 端子回路による計算量は量子計算のそれを上回らない。□

たとえば、量子計算によって多項式オーダーで解ける問題は 2 端子回路によっても多項式オーダーで解けるわけである。しかしながら、つぎの節で見ると、2 端子回路では周波数リソースの爆発が起きることに注意しなければならない。

**4. 周波数のリサイクルと多端子回路** 上の例からもわかるように、2 端子回路による計算では必要な波形（周波数）の種類はビット数の増加とともに指数関数的に増加する。これはサイズの大きな問題を解く際に、實際上、致命的な欠陥となる。この周波数リソースの爆発を回避する一般的な対策は、現在のところ明らかではないが、部分的にはつぎのようにして回避することができる。

その一つは周波数を再利用することである。たとえば、 $n$ 変数の

$$(4.1) \text{ AND: } x_1 \wedge \cdots \wedge x_n$$

を計算することを考える。量子計算では  $n+1$ 変数の Toffoli ゲートの  $n$  ビット目に  $|0\rangle$  を入力しておくことによって実現できる (Vedral et al., 1996; Uesaka, 2000)。これを上の 2 端子回路で実現しようとする、 $n+1$ ビットの計算であるから、 $2^{n+1}$ 種類の周波数が必要になる。

ところが、つぎのように構成すれば、 $n$ に無関係に、8 種類の周波数で事足りる。すなわち、まず 3 ビットの Toffoli ゲートを用いて  $x_1 \wedge x_2$  を求める。これに必要な周波数は  $2^3 = 8$ 種類である。この出力  $x_1 \wedge x_2$  と  $x_3$  をやはり 3 ビットの Toffoli ゲートに入力して  $x_1 \wedge x_2 \wedge x_3$  を得る。このときやはり  $2^3 = 8$ 種類の周波数を必要とするが、これは前の 8 種類の周波数と同じでも構わない。さらに  $x_1 \wedge x_2 \wedge x_3$  と  $x_4$  を 3 ビットの Toffoli ゲートに入力して  $x_1 \wedge x_2 \wedge x_3 \wedge x_4$  を得る。以下同様にして最後に  $x_1 \wedge \cdots \wedge x_n$  を得るが、必要な周波数はつねに同一の 8 種類で済むので、周波数の爆発は起きない。なお、このやり方は可逆な計算になっていないが、このことは一般には不都合な問題を引き起こすわけではない。

周波数の爆発を回避するもう一つの方法は 2 端子回路の代わりに**多端子回路**を用いることである。簡単のため、内部に線形素子を持ち、外部に 2 つの端子対（したがって 4 つの端子）を持つ回路を考える。各端子対に正弦波形（電圧）の線形結合：

$$(4.2) \quad x_1 = \alpha e_0 + \beta e_1 := \alpha e^{j\omega_0 t} + \beta e^{j\omega_1 t}, \quad x_2 = \gamma e_0 + \delta e_1 := \gamma e^{j\omega_0 t} + \delta e^{j\omega_1 t}$$

を印加すると正弦波形（電流）：

$$(4.3) \quad \begin{cases} y_1 = a_{11}(\omega_0)\alpha e_0 + a_{11}(\omega_1)\beta e_1 + a_{12}(\omega_0)\gamma e_0 + a_{12}(\omega_1)\delta e_1 \\ y_2 = a_{21}(\omega_0)\alpha e_0 + a_{21}(\omega_1)\beta e_1 + a_{22}(\omega_0)\gamma e_0 + a_{22}(\omega_1)\delta e_1 \end{cases}$$

が出力されることは電気回路理論でよく知られている (Kiyasu et al., 1957) . ここに  $a_{kl}$  は回路構造と回路定数で定まる,  $j\omega$  の, 実係数有理関数であり,  $a_{kl}$  を成分とする行列はこの 4 端子回路のアドミタンス行列と呼ばれている.

いま, 正弦波形  $e_0 = e^{j\omega_0 t}, e_1 = e^{j\omega_1 t}$  で生成される線形空間を  $V$  とし, 回路に入力  $x_1, x_2 \in V$  が印加されるとき出力として電流  $y_1, y_2$  が流れたとしよう. この現象を,  $V$  のテンソル積ベクトル空間  $V \otimes V$  のベクトル  $x_1 \otimes x_2$  を  $y_1, y_2$  のテンソル積  $y_1 \otimes y_2 \in V \otimes V$  に写す写像であると考え. すると, (4.3) からわかるように, この回路が定める  $V \otimes V$  上の線形変換  $A$  を, 基底  $e_0 \otimes e_0, e_0 \otimes e_1, e_1 \otimes e_0, e_1 \otimes e_1$  による表現行列で書くと

$$(4.4) \quad A = \begin{bmatrix} \alpha_{00} & 0 & 0 & 0 \\ a_{11}(\omega_0)a_{21}(\omega_0) & a_{11}(\omega_0)a_{22}(\omega_1) & a_{12}(\omega_1)a_{21}(\omega_0) & a_{12}(\omega_1)a_{22}(\omega_1) \\ a_{12}(\omega_0)a_{22}(\omega_0) & a_{12}(\omega_0)a_{21}(\omega_1) & a_{11}(\omega_1)a_{22}(\omega_0) & a_{11}(\omega_1)a_{21}(\omega_1) \\ 0 & 0 & 0 & \alpha_{33} \end{bmatrix}$$

となる. ここに

$$(4.5) \quad \alpha_{00} := (a_{11}(\omega_0) + a_{12}(\omega_0))(a_{21}(\omega_0) + a_{22}(\omega_0)),$$

$$(4.6) \quad \alpha_{33} := (a_{11}(\omega_1) + a_{12}(\omega_1))(a_{21}(\omega_1) + a_{22}(\omega_1)).$$

したがって, 2 ビットの量子計算をする  $4 \times 4$  のユニタリ行列  $U$  (たとえば, 制御 NOT) があれば,  $|0\rangle, |1\rangle$  が張る線形空間を  $W$  として,  $V \otimes V$  から  $W \otimes W$  へのある同形写像  $\varphi$  によってつぎのダイアグラム:

$$(4.7) \quad \begin{array}{ccc} V \otimes V & \xrightarrow{A} & V \otimes V \\ \varphi \downarrow & & \varphi \downarrow \\ W \otimes W & \xrightarrow{U} & W \otimes W \end{array} \quad U = \varphi \circ A \circ \varphi^{-1}$$

が可換になるように,  $A$  を定めれば,  $U$  と同じ計算をすることができる. このとき, 必要な周波数は 2 種類で済む. 同様にして, 任意のビット数の計算に対しても, この方式では 2 個の周波数で十分であり, 周波数リソースの爆発を避けることができる.

しかし, (4.4) から分かるように,  $A$  はもはや対角ではないので,  $A$  と  $\varphi$  を定めるのに単に  $U$  を対角化すればよいというわけにはいかない. 個々の計算内容に応じての工夫が一般に要求されるわけで,  $A$  と  $\varphi$  の組織的な決定方法を見いだすことが今後の課題となる.

ちなみに, 制御 NOT を実現する  $A$  と  $\varphi$  は, 初等的な計算から, たとえば, つぎのように取ればよいことがわかる:

$$(4.8) \quad \begin{cases} a_{11}(\omega_0) = a_{11}(\omega_1) = 0, a_{12}(\omega_0) = j, a_{12}(\omega_1) = -j \\ a_{21}(\omega_0) = -j, a_{21}(\omega_1) = j, a_{22}(\omega_0) = a_{22}(\omega_1) = 0 \end{cases}$$

$$(4.9) \quad \begin{cases} \varphi(e_0 \otimes e_0) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \varphi(e_0 \otimes e_1) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{-|0\rangle + |1\rangle}{\sqrt{2}} \\ \varphi(e_1 \otimes e_0) = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \varphi(e_1 \otimes e_1) = \frac{-|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \end{cases}$$

**5. 観測と NP 完全問題** 量子並列性によって指数関数のオーダの状態推移を多項式オーダで実現することができる。しかし、計算結果を得るには観測をする必要があり、それゆえ、指数関数オーダ個の中の一つが確率的に得られるにすぎない。ところが回路による計算では、観測によって系の状態を乱すことはないので、得られた状態推移の結果を壊すことなく、なんども観測をすることができ、指数関数オーダ個の中から任意個の状態を得ることができる。この事情は回路計算の大きな強みである。この間の事情を、NP 完全問題の一つである巡回セールスマン問題を例に考えてみよう。

$m$  個の都市から成る巡回セールスマン問題において、0 と 1 を値にとる  $n := m^2 + 1$  個の変数  $x := [x_1, \dots, x_n]$  を用いて巡回路を表すことにすると、その長さは  $x := [x_1, \dots, x_n]$  の 2 次形式：

$$(5.1) \quad f(x) = \frac{1}{2} \sum_{i,j=1}^n a_{ij} x_i x_j + c$$

によって表されることが知られており (Uesaka, 1993), また,  $2^n$  個の  $x := [x_1, \dots, x_n]$  に対する  $f$  の値を、量子計算によって多項式オーダで計算できることが知られている (Suyari and Uesaka, 1998) .

したがって、上に議論したことにより、回路によっても  $2^n$  個の  $x := [x_1, \dots, x_n]$  に対する  $f$  の値を多項式オーダで計算できる。その結果得られる状態は、ダミーのビットと係数を省略すれば、

$$(5.2) \quad |out\rangle := \sum_{x_1, \dots, x_n=0}^1 |x_1, \dots, x_n, f(x_1, \dots, x_n)\rangle = \sum_{x_1, \dots, x_n=0}^1 |x_1, \dots, x_n, f_1(x), \dots, f_r(x)\rangle$$

という形をしている。ここに  $f_1(x), \dots, f_r(x)$  は  $f(x_1, \dots, x_n)$  の 2 進数表示であり、 $f_1(x)$  が最上位ビットである。

ここで  $|out\rangle$  につぎのようなエルミート行列：

$$(5.3) \quad H_1 := \underbrace{I \otimes \dots \otimes I}_n \otimes |0\rangle\langle 0| \otimes \underbrace{I \otimes \dots \otimes I}_{r-1}$$

を施すと

$$(5.4) \quad H_1 |out\rangle = \sum_{x \in \{x | f_1(x)=0\}} |x_1, \dots, x_n, 0, f_2(x), \dots, f_r(x)\rangle$$

なる出力が得られ、 $f_1(x)=0$  を満たす情報だけが残る。そのような情報が存在しないとき、すなわち、 $H_1 |out\rangle$  が零ベクトルならば、すべての  $x := [x_1, \dots, x_n]$  に対して  $f_1(x)=1$  である。したがって、 $H_1 |out\rangle$  が零ベクトルであるかないかによって、最短距離の最上位ビットが 1 であるか 0 であるを判定できることになる。 $H_1 |out\rangle$  が零ベクトルであるかどうかを判定することは、量子計算の場合には不可能であるが、回路では出力が零であるかどうかによって判定することに注意せよ (これが回路、つまり、古典系における観測が優れている点である)。

つぎに、 $H_1 |out\rangle$  が零ベクトルのときは

$$(5.5) \quad \sum_x |x_1, \dots, x_n, 1, f_2(x), \dots, f_r(x)\rangle$$

に、また零ベクトルでないときには  $H_1 |out\rangle$  に、それぞれつぎのエルミート行列：

$$(5.6) \quad H_2 := \underbrace{I \otimes \dots \otimes I}_n \otimes |0\rangle\langle 0| \otimes \underbrace{I \otimes \dots \otimes I}_{r-2}$$

を施すと、まえと同様にして、その結果が零ベクトルであるかないかによって、最短距離の第 2 ビットが 1 であるか 0 であるかを判定できることになる。

以下このようにしてエルミート行列を順次施していくことによって、 $r$  回の (古典的な) 観測によって最短距離とそれを与える巡回路、すなわち、最適解が得られる。ここに  $r$  は巡回路の長さを表す 2 進数のビット数であるが、これは明らかに巡回セールスマン問題のサイズの多項式オーダーである。したがって、 $|out\rangle$  を得るのに要する計算量が多項式オーダーであったことに注意すれば、もし上のエルミート行列を回路で実現することができれば、巡回セールスマン問題は多項式オーダーで解けることになる。

実際、上のエルミート行列はつぎのようにして 2 端子回路で実現できる。簡単のため、 $H_1$  について考えよう。表記を簡潔にするため、2 進数  $x_1 \cdots x_n y_1 y_2 \cdots y_r$  を  $x_1 y$  と書くことにする。ここに  $x=0, \dots, 2^n-1$ ,  $y=0, \dots, 2^{r-1}-1$  である。さて波形：

$$(5.7) \quad e_{x_0 y} := e^{j\omega_{x_0 y} t}, e_{x_1 y} := e^{j\omega_{x_1 y} t}, \quad x=0, 1, \dots, 2^n-1, y=0, 1, \dots, 2^{r-1}-1$$

を用意し、これらで張られる線形空間  $V$ ：

$$(5.8) \quad V := \left\langle \bigcup_{x=0}^{2^n-1} \bigcup_{y=0}^{2^{r-1}-1} \{e_{x_0 y}, e_{x_1 y}\} \right\rangle$$

と  $\underbrace{|0 \cdots 0\rangle}_{n+r}, \dots, \underbrace{|1 \cdots 1\rangle}_{n+r}$  が生成する線形空間  $W$  を考える。これまでの回路の構成の仕方と同様にして、

$$(5.9) \quad \begin{array}{ccc} V & \xrightarrow{A} & V \\ \varphi \downarrow & & \varphi \downarrow \\ W & \xrightarrow{H_1} & W \end{array} \quad \text{すなわち} \quad H_1 = \varphi \circ A \circ \varphi^{-1}$$

が成り立つように、 $A$  と  $\varphi$  を定めればよい。それには、 $A$  が対角であることに注意して、 $H_1$  を対角化すればよい。 $H_1$  はエルミートであるから、容易に対角化できて、回路のアドミタンス関数と  $\varphi$  は

$$(5.10) \quad a(\omega_{x_0 y}) := 1, \quad a(\omega_{x_1 y}) := 0 \quad (x=0, \dots, 2^n-1, y=0, \dots, 2^{r-1}-1),$$

$$(5.11) \quad \varphi(e_{x_0 y}) := |x_0 y\rangle, \quad \varphi(e_{x_1 y}) := |x_1 y\rangle \quad (x=0, \dots, 2^n-1, y=0, \dots, 2^{r-1}-1)$$

と得られる。実際、このとき、

$$(5.12) \quad |x_0 y\rangle \xrightarrow{\varphi^{-1}} e_{x_0 y} \xrightarrow{A} a(\omega_{x_0 y}) e_{x_0 y} = e_{x_0 y} \xrightarrow{\varphi} |x_0 y\rangle,$$

$$(5.13) \quad |x_1 y\rangle \xrightarrow{\varphi^{-1}} e_{x_1 y} \xrightarrow{A} a(\omega_{x_1 y}) e_{x_1 y} = 0 \cdot e_{x_1 y} = 0 \xrightarrow{\varphi} 0$$

となることから、この回路によって上の  $H_1$  が実現できていることがわかる。

以上の考察と巡回セールスマン問題が NP 完全問題の一つであることから、結局、つぎのことがいえる：

**定理 3** すべての NP 問題は、2 端子回路による計算においては、P 問題である。□

しかし、この結果は、チューリング機械をベースとした計算量の理論において、 $NP=P$  だとい

っているわけではないことに注意すべきである。また、2端子回路を用いていることから、「周波数リソースの爆発を除いて」という条件付きでの話である。周波数リソースの爆発を回避するには3節で述べた方法などをさらに検討していく必要があり、これらは今後の課題である。

**参考文献：**

Barenco, A. et al. (1995) : Elementary gates for quantum computation, *Physical Review A*, 52, 5, 3457-3467.

Deutsch, D. (1985) : Quantum theory, the Church-Turing principle and the universal quantum computer, *Proc. R. Soc. Lond. A*400, 97-117.

Ekert, A. and Jozsa, R. (1996) : Quantum computation and Shor's factoring algorithm, *Reviews of Modern Physics*, 68, 3, 733-753.

Grover, L.K. (1996) : A fast quantum mechanical algorithm for database search, *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*.

喜安善市ほか (1957) : 回路網理論, 岩波講座現代応用数学 B.8-a, 岩波書店.

Shor, P.W. (1994) : Algorithms for Quantum Computation, Discrete Logarithms and Factoring, *Proc. 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.)*, IEEE Computer Society Press, 124-134.

須鎗弘樹, 上坂吉則 (1998) : 組合せ最適化問題の目的関数を計算する量子回路の一構成法, *電子情報通信学会*, J81-A, 12, 1722-1727.

上坂吉則 (1993) : ニューロコンピューティングの数学的基礎, 近代科学社.

上坂吉則 (2000) : 量子コンピュータの基礎数理, コロナ社.