

量子コンピューティング —回路アーキテクチャとデバイスの基礎—

雨宮好仁 北海道大学

Quantum Computation

—A guide to the quantum circuits and quantum logic devices—

Y. AMEMIYA *Hokkaido University*

1. はじめに

量子コンピューティング（量子計算）とは、量子力学的な波動関数の重ね合わせを利用して並列演算を行う手法のことをいう。その概念は1980年ごろからFeynmanらによって提案され、1985年になってDeutschにより「量子チューリング機械」として定式化された。量子チューリング機械は複数の入力データをコヒーレントな量子重ね合わせ状態で受け取り、そのデータ各々に対して同時に計算を実行する。したがって大規模な並列演算が可能となり、従来のコンピュータでは難しい問題、たとえば大きい整数の因数分解などを効率よく解くことができる。そのためRSA公開鍵暗号システムを破ることができる、ということで一躍有名になった。

本稿では、量子コンピューティングに興味をもつ電子工学エンジニアのために導入の解説を行う。エンジニアが計算システムの構造を把握しようとするときには、システムをトップダウン的に見ていくことが普通である。すなわち、①計算システムに要求される機能、②機能を出すためのアルゴリズム、③アルゴリズムを実行するための論理回路、④回路を構成する電子デバイス、という順序で追っていくと分かりやすい。本稿でもこの方針で解説を進める。そして量子計算の説明によく使われる「Deutsch-Jozsa例題」を例にとり、この問題を解くための量子計算システムを考える。

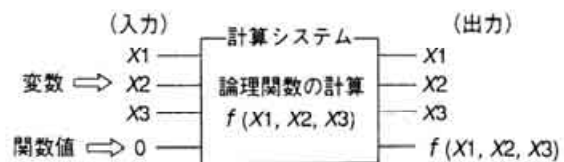
以下では、はじめにDeutsch-Jozsa例題の説明を行う（第3章）。そのあと、例題を解くアルゴリズム（第4章）から、アルゴリズムを実行する量子論理回路（第5章/第6章）、さらに回路構成のための量子デバイス（第7章/第8章）の順に説明を進める。イメージの把握を第1として、詳細は省略し数式もなるべく避けた。数理的な扱い

と物理実験の現状については末尾の文献を参照されたい。

本稿では、非チューリング系の量子コンピューティングについても述べる。一般に量子コンピューティングといえば量子チューリング機械のことを指すが、それ以外にも量子並列計算を行う計算モデルは存在する（第9章）。いくつかの例を挙げるとともに、電子デバイスによる具現化の案を述べる（第10章/第11章/第12章）。

2. 「量子重ね合わせ」による並列計算

量子計算システムの動作を模式的に描いて図1に示す。この図は、ある3変数デジタル関数 $f(X1, X2, X3)$ を計算するシステムの例である（変数 Xi と関数 f ともに1か0）。入力と出力にそれぞれ3つの変数ビットと1つの関数ビットがある。いま入力側の変数ビットに変数値 $(X1, X2, X3)$ を与え、関数ビットには0を与える。すると出力側の関数ビットに関数値 $f(X1, X2, X3)$ が



$$\begin{array}{l}
 \text{入力の重ね合わせ} \quad (\text{量子計算}) \quad \text{出力} \\
 X1 = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
 X2 = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
 X3 = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)
 \end{array}
 \Rightarrow
 \frac{1}{\sqrt{8}} \begin{pmatrix} f(0, 0, 0) + f(1, 0, 0) \\ + f(0, 0, 1) + f(1, 0, 1) \\ + f(0, 1, 0) + f(1, 1, 0) \\ + f(0, 1, 1) + f(1, 1, 1) \end{pmatrix}$$

図1 量子計算システムの動作。変数 $(X1, X2, X3)$ を入力として関数 $f(X1, X2, X3)$ を計算し出力する。1と0の重ね合わせ信号を扱うことができる。

現われる。出力側の変数ビットには、入力した変数値がそのまま現われる。

量子計算システムでは、入力ビットの個数と出力ビットの個数は必ず同じである。理由は次のことによる。量子計算システムでは1ビット情報を物理粒子1個の量子状態（電子のスピンなど）で表す。計算前の粒子の量子状態が入力であり、計算後の量子状態が出力である。計算途中で粒子の個数が変わることはないので、出力数は入力数に等しい。

いま入力変数 (X_1, X_2, X_3) の可能な組み合わせすべてについて関数 $f(X_1, X_2, X_3)$ を計算したい。変数が3つの場合、可能な変数組み合わせは8個 ($=2^3$ 個) である (すなわち $(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)$)。普通の計算システム (CMOSのLSIなど) であれば、1つの入力を与えて出力をみる、という操作を8回繰り返す必要がある。変数が N 個に増えると、必要な操作は 2^N 回と指数関数的に増加して膨大となる。

量子的な計算システムでは状況が異なる。量子計算では変数を粒子の量子状態で表すから、入力として $1(=|1\rangle)$ と $0(=|0\rangle)$ の重ね合わせ状態 ($(|1\rangle + |0\rangle)/\sqrt{2}$) を与えることができる。3つの変数にそれぞれ重ね合わせ状態を入力すれば、出力には8個の変数組み合わせに対する関数値が重ね合わせ状態で現われる。つまり8つの関数計算を1回で並列実行できる。変数が多くなっても関数計算は1回でよい。この性質を利用すれば大規模な並列演算が可能となる。

ただし量子計算では、計算結果が重ね合わせ状態で出力される。そのため、ある特定の入力に対する関数値を知ることにはできない。つまり量子並列計算は“癖”のある計算手法であって、問題を解くためのアルゴリズムに工夫を要する。現在までの研究により、いくつかの重要な問題について求解アルゴリズムが発明されている。主要なものには次の3つであり、それぞれ発明者の名を冠して呼ばれている。

(a) Deutsch-Jozsaのアルゴリズム

出題者が提示した関数の種別を解答者が当てる、という問題 (Deutsch-Jozsa例題と呼ばれるもの) を解くためのアルゴリズム。実用的な意味はないが、量子並列計算の説明によく使われる。本稿では、このアルゴリズムを例として量子計算のイメージを説明する。

(b) Shorのアルゴリズム

因数分解や離散対数問題を解くためのアルゴリズム。量子コンピューティングを一躍有名にしたものである。整数 N の因数分解を普通の方法で行うと、

$$2^{(\log N)^{1/2} (\log \log N)^{2/3}}$$

の計算量を要する。つまり整数 N の桁数 ($\log N$) に対して指数関数的に増加する膨大な計算量が必要である。しかし量子計算では、本アルゴリズムを用いて $\log N$ に比例する少ない計算量で因数分解できる。

(c) Groverのアルゴリズム

ファイル検索のためのアルゴリズム。いま番号を付けたファイルが (番号順でなく) ランダムに N 個並んでいるとする。ある番号が指定されたとき、その番号のファイルを引き当てたい。普通ならばファイル番号を順番に照合していくほかないので、だいたい N 回の操作が必要である。しかし量子計算では、本アルゴリズムを用いておよそ \sqrt{N} 回の操作で引き当てられる。本アルゴリズムはファイル検索以外の分野にも応用可能性がある。

3. Deutsch-Jozsa例題とは

Deutsch-Jozsa例題とは、出題者と解答者による次のようなゲームである (図2)。

(1) はじめに出題者が任意のデジタル関数を考える (関数と変数ともに1か0)。この関数そのもの (関数計算の操作) は解答者に明かさない。ただし約束として、その関数は次の2種のいずれかとする。

(i) その関数は定数。つまり変数の値にかかわらず恒等的に1か0。(第1種の関数)

(ii) その関数は、可能な変数組み合わせの半数に対して1、他の半数では0。たとえば変数が10個の場合、可能な変数組み合わせは1024組 ($=2^{10}$ 組) であり、そのうち512組では関数値が1、残り512組では関数値が0。(第2種の関数)

(2) 解答者は、適当な変数組み合わせを選んで出題者に伝え、それに対する関数の値を教えてもらうことができる。この作業を「関数計算」と呼ぶ。1回の関数計算では、解答者が選んだ変数組み合わせ1個に対する関数値を出題者

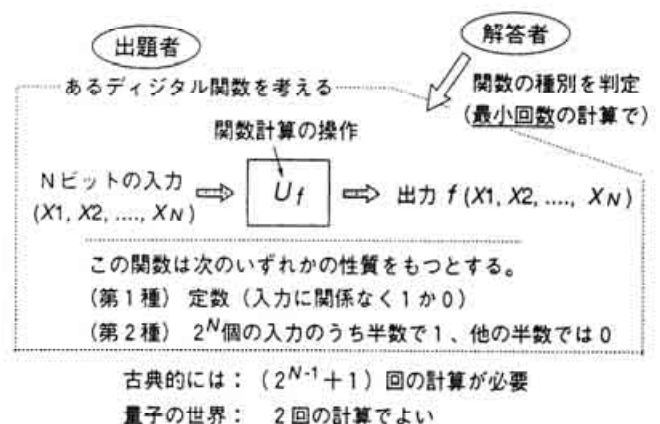


図2 Deutsch-Jozsa例題。出題者が想定した関数の種別を解答者が当てる、というゲームである。

が計算して解答者に教える。

(3) 出題者から教えられたデータをもとに、この関数の種別 (第1種であるか第2種か) を解答者が当てる。そのとき最小回数の関数計算で確実に当てたい。解答者はどのようにしたらよいか?

普通に考えると、求解に必要な関数計算は変数が N 個のとき $(2^{N-1}+1)$ 回である。なぜなら、解答者が適当に選んだ 2^{N-1} 個の変数組み合わせ (可能な組み合わせの半数) に対して関数値がすべて同一であった場合、さらにもう1つを見ないと関数の種別が判定できないからである。ところが、量子計算の世界では状況が異なる。変数の個数によらず2回だけの関数計算でよい。

4. Deutsch-Jozsa問題を解くための準備

次の第5章でDeutsch-Jozsa問題を解くための量子計算アルゴリズムを説明する。そのための準備事項を以下に述べる。

(1) ビット信号を載せる物理系 (図3)

量子計算システムでは、ビット信号の1-0情報を物理粒子の量子状態で表す。問題の関数がたとえば3変数関数ならば、用意すべき物理系は4粒子系である (変数ビット用に3粒子、関数値ビットの書き込み用に1粒子)。その量子状態を次のように表記する。

$$|X_1 X_2 X_3, f_{x_1 x_2 x_3}\rangle$$

X_1, X_2, X_3 : 変数ビットの値

$f_{x_1 x_2 x_3}$: 関数ビットの値

(表記例) $|101, 0\rangle, |110, 1\rangle$ など

(2) 関数計算の操作 (図4)

量子計算とは、上記の物理系に適切な操作 (目的に応じたユニタリ変換) を施して量子状態を変換することをいう。そのときの入力とは物理系の初期状態、出力は変換後の状態である。「関数を決める」ということは「ユニタリ変換の形を決める」ことに等しい。

ゲームの開始にあたって出題者が関数を決める。この関数システムを図に示す。 U_f は関数に対応するユニタリ変換であり、その内容は出題者しか知らない。先に示した図1と同じものであり、関数ビット入力に0を与えたとき関数値が出力される。なお、説明の都合上、関数ビット入力に1を与えたときは関数値の反転 (否定) が出力されるものとする。つまりそのような U_f を出題者が想定したとする。

(3) 入力の重ね合わせをつくる

粒子系の任意ビットに対して次のユニタリ変換 U_2 を行えるものとする。

$$\underbrace{|X_1\rangle \otimes |X_2\rangle \otimes |X_3\rangle}_{\text{変数ビット}} \otimes \underbrace{|f_{x_1 x_2 x_3}\rangle}_{\text{関数ビット}}$$

↓

$$|X_1 X_2 X_3, f_{x_1 x_2 x_3}\rangle \text{ と表記}$$

たとえば $|101, 1\rangle$

図3 ビット信号を載せる物理系。図例は3変数関数扱う場合であり、4粒子系を使用する。

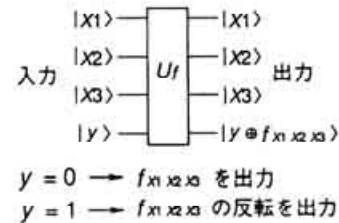


図4 関数の計算。量子計算とは物理系の状態を別の状態に変えるユニタリ変換 U_f のことである。

$$U_2 = (1/\sqrt{2}) \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

このユニタリ変換を状態 $|0\rangle$ にある変数ビットに施すと、次のように1と0の重ね合わせ状態が生成される。

$$|0\rangle \rightarrow (|1\rangle + |0\rangle)/\sqrt{2}$$

(4) 関数値が1のとき印をつける

粒子系の任意ビットに対して次のユニタリ変換 S を行えるものとする。

$$S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

このユニタリ変換を関数ビットに施すと、関数値が1のとき粒子系の波動関数にマイナス符号がつく。関数値が0のときは変化ない。

$$\text{(例)} \quad |110, 1\rangle \rightarrow -|110, 1\rangle$$

$$|101, 0\rangle \rightarrow |101, 0\rangle$$

5. Deutsch-Jozsa問題の求解アルゴリズム

関数の種別を2回の関数計算で判定する量子アルゴリズムは以下のようなものである。その流れを図5に示す。解答者の立場からみた作業を順に説明する。

(1) ビット信号の初期化 (この作業が済むと粒子系の波動関数は図5に示す Ψ_1 となる)

ビット信号を載せる粒子系を用意し、各粒子の状態をすべて0に初期化する。つまり波動関数 Ψ_1 を $|00\dots 0, 0\rangle$ に設定する。

(2) 重ね合わせ入力の書き込み (波動関数 Ψ_2)

変数ビットの各粒子にユニタリ変換 U_2 を施す。変数が N 個の場合、 U_2 の操作は合計 N 回である。この操作

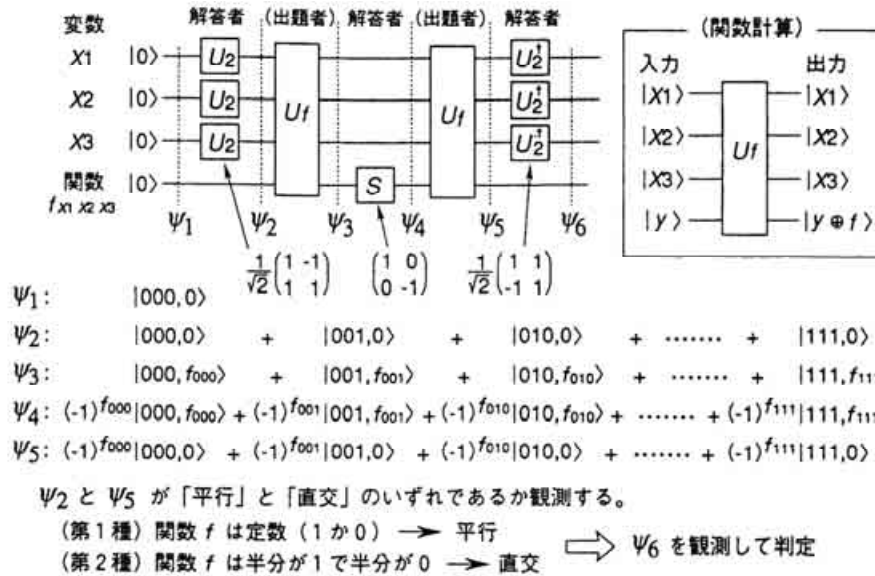


図5 Deutsch-Jozsa問題を解くためのアルゴリズム。各ステップにおける物理系の波動関数をあわせて示す。

によって、各変数ビットに1と0の重ね合せ状態を書き込む。

(3) 第1回目の関数計算 (波動関数 ψ₃)

重ね合せ入力変数を書き込んだ粒子系を出題者に渡して関数値を計算させる。そして結果を関数ビットに書き込ませる。つまり、粒子系に対してユニタリ変換 U_f を施してもらう。

(4) 波動関数の符号変換 (波動関数 ψ₄)

出題者から戻された粒子系の関数ビットにユニタリ変換 S を施す。それによって、粒子系の波動関数において関数ビットが1の成分だけにマイナス符号をつける。

(5) 第2回目の関数計算 (波動関数 ψ₅)

次に粒子系を再び出題者に渡して関数値を計算させ、その結果を関数ビットに書き込ませる。すなわちユニタリ変換 U_f をもう一度施してもらう。この操作によって、波動関数のすべての成分における関数ビットが0に戻る。(イメージ的には、関数計算というよりその逆操作である。)

(6) 関数種別の判定

波動関数 ψ₅ と ψ₂ が「平行」と「直交」のいずれであるか観測する。その結果が平行であれば関数は第1種(定数)、直交ならば第2種である。

理由を次に述べる。関数が第1種(定数)であれば「ψ₅ = ψ₂ (関数値が定数0のとき) または ψ₅ = -ψ₂ (関数値が定数1のとき)」であり、したがって「ψ₂ と ψ₅ は平行(内積が1または-1)」と観察される。関数が第2種であれば「ψ₅ の成分のうち半数がプラス符号(関数値が0のもの)で残り半数がマイナス符号(関数値が1のもの)

の)」であり、したがって「ψ₂ と ψ₅ は直交(内積が0)」と観察される。最初の約束により関数は第1種と第2種のいずれかなので、観測結果が平行なら第1種、直交なら第2種と判定できる。

(7) 平行と直交の判別 (波動関数 ψ₆)

ψ₅ と ψ₂ の平行/直交は次のように判別する。いま波動関数 ψ₅ の各変数ビットに U₂ の逆変換 U₂[†] を施す。

$$U_2^\dagger = (1/\sqrt{2}) \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

その後すべての変数ビットを観測する。ψ₅ が ψ₂ と平行であれば、すべての変数ビットの値が0と観測される。一方、直交であれば、すべての変数ビットの値が同時に0と観測されることはない(少なくとも1つの変数ビットは1と観測される)。

6. 量子計算のための基本ゲート

Deutsch-Jozsaアルゴリズムを実行するための量子論理回路を設計してみる。普通の論理回路と同じように、量子論理回路も基本ゲート(量子ゲート)を組み合わせて構成する。

(1) 基本量子ゲート

普通のデジタル演算が基本論理ゲートの組み合わせ(AND+NOTなど)で実現できるように、量子コンピューティングの演算も適切な量子ゲートの組み合わせで構成できる。代表例は次の量子ゲート2種の組み合わせである(図6)。

(i) 1ビット信号に対するユニタリ変換ゲート

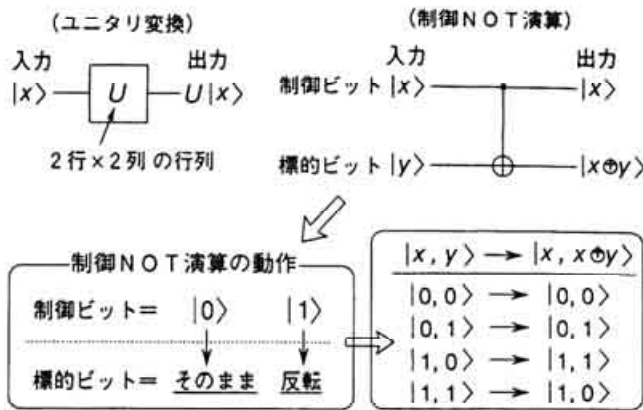


図6 量子計算のための基本ゲート。ユニタリ変換と制御NOT演算を組合せることで任意の量子計算を実行できる。

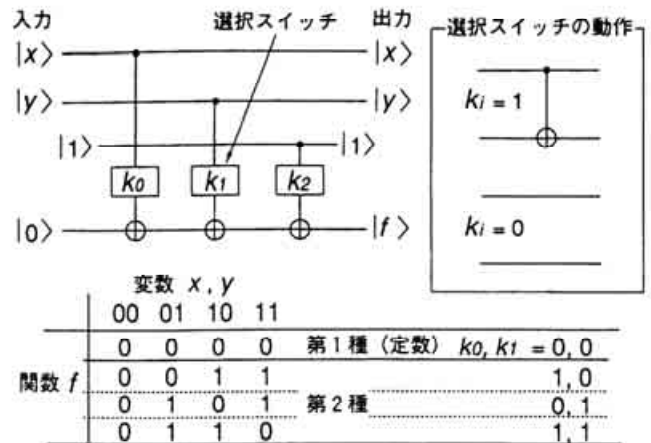


図7 Deutsch-Jozsa例題の関数を発生させる回路。例として2変数関数器を示す。関数の形を決める選択スイッチ信号 (k_0, k_1, k_2) は出題者が設定する。

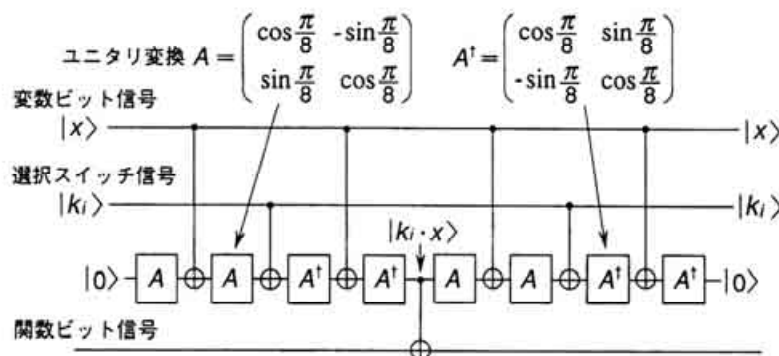


図8 量子回路による選択スイッチ。論理和の回路を使ったもの。

本ゲートは2行2列の行列で表されるユニタリ変換を行う。任意の2行2列ユニタリ変換を行える必要がある。

(ii) 2ビット信号に対する制御NOTゲート

本ゲートは入出力に制御ビットと標的ビットをもつ。制御ビットの値が1のときに標的ビットの値を反転させて出力する。制御ビットが0のときは標的ビットをそのまま出力する。制御ビット自体はそのまま出力される。言い換えると、制御ビット入力と標的ビット入力の排他的論理和を標的ビット出力として出す。重ね合せ入力に対しても動作する必要があるから、普通の電子回路ではもちろん構成できない。

(2) Deutsch-Jozsaアルゴリズムの回路

Deutsch-Jozsaアルゴリズムを回路化するとき、説明を要する部分は関数発生器である (他の部分はユニタリ変換ゲートで構成できる)。いま2変数の関数 $f(x, y)$ を例にとって、関数発生器の回路を図7に示す。3つの制御NOTゲートからなる。出題者が関数の形を選べるように、制御NOTゲートのそれぞれに選択スイッチを挿入する。

選択スイッチに要求される動作は次のことである。各

選択スイッチは外部から信号 (k_0, k_1, k_2) を受け、その信号が1ならば制御NOTゲートを動作させる。信号が0のときは制御NOTゲートの働きを停止する (制御NOTゲートがない場合と同じにする)。この選択スイッチは量子的な素子である必要はない。外部信号 (普通の電気信号など) によって制御NOTゲートの動作を設定・解除できる仕組みであればそれでよい。(選択スイッチも量子回路にしたいときは図8の構成とする。このときは選択スイッチ信号 k_i も量子ビット信号にする。)

以上の構成により、選択スイッチ信号 k_0 と k_1 が同時に0のときに第1種の関数 (定数) が発生し、それ以外の場合に第2種の関数が発生する。なお選択スイッチ信号 k_2 は関数値を反転させるもので、 k_0 および k_1 とともに関数形の選択に用いる ($k_2=1$ のときは、 $k_2=0$ のときの補関数を発生する)。出題者が選択スイッチ信号 k_0, k_1, k_2 を選んで関数の形を決める (解答者には知らせない)。

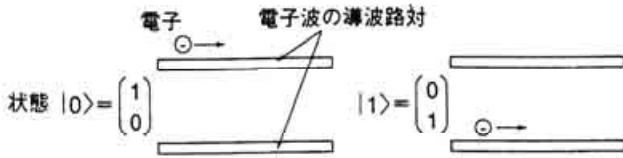


図9 電子波の導波路対による量子配線。上の導波路に電子が流れている状態を0, 下を流れている状態を1と定義する。

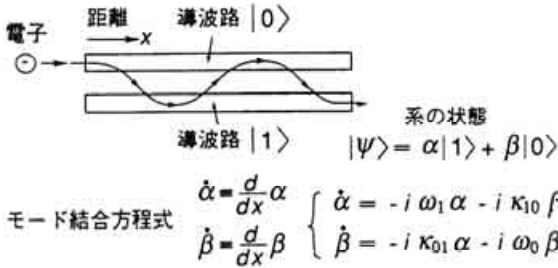


図10 結合導波路による重ね合せ状態の生成。モード結合方程式に従って重ね合せ状態が変化する。

1. 量子回路のための基本デバイス —電子波回路による構成—

量子論理回路を実際のデバイスで具現化する方法の例として、ここでは電子波回路による構成法を説明する。電子波回路は普通の電子回路のイメージに近いので、解説例として分かりやすい。

量子論理回路の基本要素は次の3つ、すなわち量子配線、ユニタリ変換デバイス、および制御NOTゲートデバイスである。以下に順を追って説明する。

(1) 量子配線

量子回路においてビット信号を伝送するための配線である。重ね合せ信号も伝送する必要がある。これを電子波の導波路で構成する。

いま信号1ビットに対して2本の導波路を用意する(図9)。この導波路は絶縁体または真性半導体からなり、電子を流すための電界がかけられているとする。そこに(1ビット信号あたり)電子を1個だけ流す。導波路の一方に電子が流れている状態を $|0\rangle$ (ビット信号0), 他方を流れている状態を $|1\rangle$ (ビット信号1)と定義する。すなわち2線式のビット表現を用いる。(付記: 以上は文献5の量子光学回路を参考にしたものである。)

この導波路対は重ね合せ信号も伝送できる。いま2本の導波路を近接させて、一方の導波路から他方に電子がトンネル効果で移動できるようにする(図10)。このように結合した2本の導波路の一方に電子を流すと、それは電子波のモード結合方程式に従って2つの導波路を渡り歩く。つまり $|1\rangle$ と $|0\rangle$ の2状態を交替する。いずれか

の状態から出発して適切な距離だけ電子を走行させれば重ね合せ状態が実現できる(たとえば $(|1\rangle + |0\rangle)/\sqrt{2}$ など)。走行距離に応じて任意の重ね合せ状態が得られる。途中で2つの導波路を引き離して結合を解除すれば、そのときの重ね合せ状態がそのまま保存されて伝わる。

(2) ユニタリ変換デバイス

この導波路対を使うとユニタリ変換を簡単に実現できる。図11には2種類のユニタリ変換デバイスを示した。1つは導波路対に位相シフトを付したもの、もう1つは方向性結合器である。それぞれ次のユニタリ変換を行う。

(位相シフト導波路対)	(方向性結合器)
$\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{i\psi} \end{pmatrix}$	$\begin{pmatrix} \cos\theta & -i\sin\theta \\ -i\sin\theta & \cos\theta \end{pmatrix}$
ϕ, ψ : 位相シフトの量	θ : 結合係数

この2種類のユニタリ変換を組み合わせると2行2列の任意のユニタリ変換が得られる。例として、重ね合せ入力をつくるユニタリ変換 U_2 の構成法を図12に示す。

(付記: ユニタリ変換に方向性結合器を使用することは田部道晴氏(静岡大学電子工学研究所)の示唆による。)

(3) 制御NOTデバイス

(a) 構造と動作

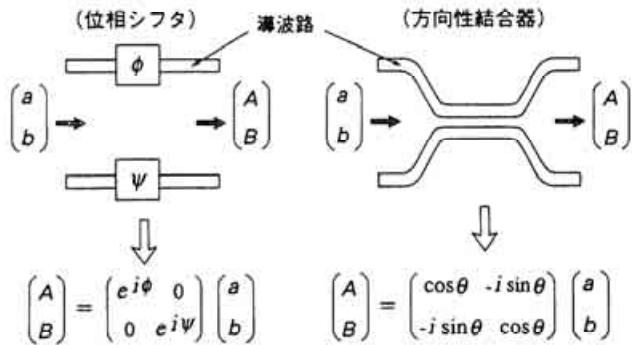


図11 電子波回路によるユニタリ変換デバイス。位相シフト(左)と方向性結合器(右)。

任意のユニタリ行列(2行×2列)

$$= \begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix} \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix} \begin{pmatrix} \cos\theta & -i\sin\theta \\ -i\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{pmatrix}$$

(例) 重ね合せ状態をつくるユニタリ変換 $U_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$

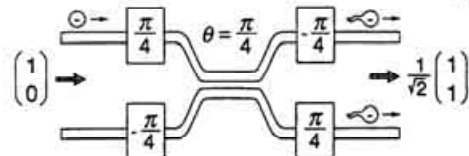


図12 重ね合せ入力をつくるユニタリ変換 U_2 の構成。

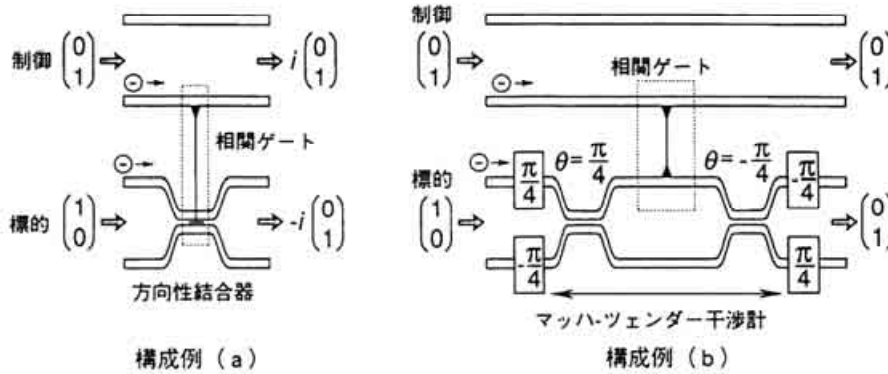


図 13 電子波回路による制御NOTデバイスの構成例。方向性結合器の結合係数を変えるタイプ（構成例 (a)）とマッハツェンダー干渉計を用いるタイプ（構成例 (b)）。

電子波回路による制御NOTデバイスの構成例を図 13 に示す。制御ビット用と標的ビット用の 2 対の導波路を持つ。そこに制御ビット信号の電子波と標的ビット信号の電子波を同時に流す。この 2 つの電子波の間に相互作用を持たせる。そのための仕組みを“相関ゲート”と呼ぶ。(標的ビット導波路と制御ビット導波路の間を電子が行き来することはないものとする。)

図 13(a) のデバイスでは、標的ビットの導波路対を近接させて方向性結合器をつくる。方向性結合器の結合係数 θ は 0 とする。その方向性結合器と制御ビットの導波路 $|1\rangle$ を相関ゲートで結合する。相関ゲートに必要な機能は「制御ビットの電子波が導波路 $|1\rangle$ を通過しているときに標的ビットの方向性結合器の結合係数 θ を 0 から $\pi/2$ に変化させる作用」である (このとき制御ビット信号には $\pi/2$ の位相シフトが生じるようにする)。それによって、制御ビット信号が 1 のときに標的ビット信号の 1-0 を反転させる。

なお説明の都合上、図では制御ビットの状態と標的ビットの状態を別々に記述してそれぞれに位相項 (i と $-i$) をつけてある。しかしこの系は 2 粒子系なので、実際

に意味のあるものは両信号の波動関数の直積で表された 2 粒子波動関数とその位相である。このことは次のデバイスでも同様である。

図 13(b) のデバイスでは、標的ビットの経路に方向性結合器を 2 つ挿入してマッハツェンダー干渉計を構成する。その干渉計の上側経路と制御ビットの導波路 $|1\rangle$ を相関ゲートで結合してある。この場合の相関ゲートに必要な機能は「制御ビットの導波路 $|1\rangle$ を通る電子波と干渉計の上側経路を通る電子波が互いに相手を $\pi/2$ だけ位相シフトさせる作用」である。正確にいうと「制御ビットの導波路 $|1\rangle$ と干渉計の上側経路とを同時に 2 つの電子波が通過したときに 2 粒子系の波動関数の符号を反転させる作用」である。それによって、制御ビット信号が 1 のときに標的ビット信号の 1-0 を反転させる。

(b) 相関ゲートをつくるには

制御NOTデバイスのキーポイントは相関ゲートであるが、これを実現する方法はまだ検討事項である。いま図(b)の構造を例にとると、たとえば次のような量子効果の利用を考えることができる (図 14)。

(i) アハラノフ-ボーム効果の利用

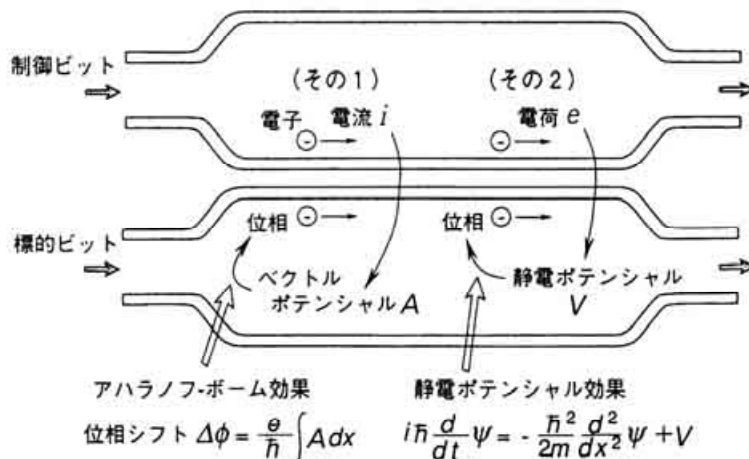


図 14 相関ゲートに利用できそうな物理現象。アハラノフ-ボーム効果と静電ポテンシャル効果。

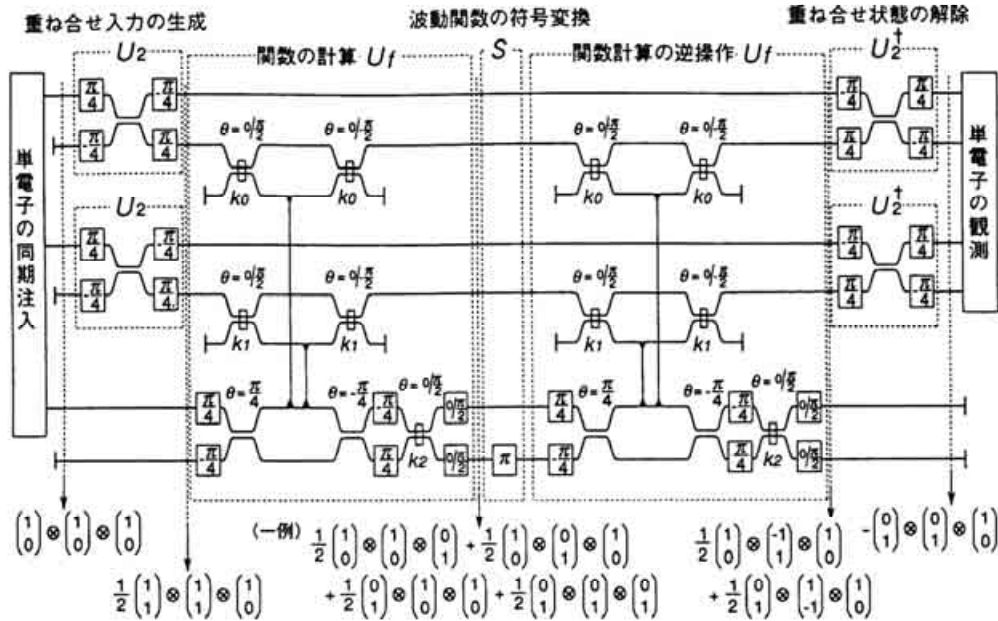


図 15 Deutsch-Jozsaアルゴリズムを実行するための電子波回路。電子の注入と観測には単電子回路を用いる。

制御ビットの導波路 $|1\rangle$ に電子波が通ると、その電流によって周辺にベクトルポテンシャルが発生する。それによって干渉計の上側経路を通る電子波の位相がシフトする。

(ii) 静電ポテンシャル効果の利用

制御ビットの導波路 $|1\rangle$ に電子波が通ると、電子電荷によって周辺に静電ポテンシャルが発生する。それによって、干渉計の上側経路を通る電子波の位相がシフトする。

ただしこれらの位相シフト効果はかなり小さいと予想されるので、実用のためには何らかの工夫を要する。位相シフト効果を高めるようなデバイス構造の開発が今後の研究課題である。

8. 量子計算システムの構成

Deutsch-Jozsaアルゴリズムを実行するための電子波回路を図 15 に示す (2 変数関数の例)。つぎのような構成をもつ。

- (i) 方向性結合器と位相シフタを用いて、重ね合せ生成のユニタリ変換 U_2 と重ね合せ解除のユニタリ変換 U_2' をつくる。
- (ii) 関数ビットの導波路 $|1\rangle$ に位相シフタ (シフト量: π) を付すことで、関数種別を分類するためのユニタリ変換 S をつくる。
- (iii) 関数発生器の主要部分は関数ビットに挿入した制御 NOT デバイスである。干渉計の上側経路に 2 つの相関

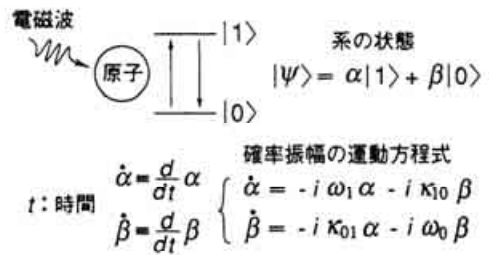


図 16 2 準位系における重ね合せ状態の生成。確率振幅の運動方程式に従って重ね合せ状態が変化する。

ゲートを付すことにより、1 つの干渉計に制御 NOT デバイス 2 個の働きをさせる。

- (iv) 関数の形を選択するスイッチ部分には方向性結合器を使用する。選択スイッチ信号 (k_0, k_1, k_2) により結合係数を変えて電子波の経路を切り換える。
- (v) 電子波回路の入力端から、変数ビットと関数ビットに各 1 個の電子を同時注入する。出力端の変数ビットで電子の流出を観測する。注入部と観測部には単電子回路を使用する。

ところで、電子波回路の他に 2 準位系を用いても量子論理回路が構成できる。すなわち、2 つのエネルギー状態をもつ原子や量子ドットに電磁波を照射すると、その系は確率振幅の運動方程式に従って 2 状態間を交替する (図 16)。確率振幅の運動方程式は (時間変数 t を距離変数 x に見立てれば) 前記のモード結合方程式と相似形である。したがって 2 準位系でも電子波回路と同じ動作を実現できる。実際の研究例はこの方が多い。2, 3 の例を

あげる。詳細は末尾の文献を参照されたい。

(i) 結合量子ドット形：結合した2つの量子ドットと電磁波の相互作用を用いる。

(ii) 核スピン形：液体や結晶の原子の核スピンと電磁波の相互作用を用いる。核磁気共鳴の装置をそのまま利用できる。簡単な量子計算の実験が行われている。

(iii) 巨視的量子ヒールス形：超伝導電子系で生じる巨視的量子効果と電磁波との相互作用を利用する。rf-SQUIDによる磁束量子形と単電子回路によるシングルエレクトロン形がある。

2準位系では、粒子系に載せたビット信号は空間的に静止しており、論理ゲート（論理操作）の方を動かしてビット信号の位置まで持ってくる。もしくは電磁波の周波数を変えることで任意の粒子に選択操作を加える。したがって電子波回路の「量子配線」に相当するものはない。

9. そのほかの量子計算システム —量子チューリング機械から離れて—

現在一般に量子コンピューティングという言葉が使われる場合、それは「量子チューリング機械」のことを指している。これはチューリング機械という計算モデルに量子並列性を導入したものである。ところで計算モデルにはチューリング機械の他にも多くの種類がある。例としてニューラルネットワーク、セルオートマトン、アナログコンピューティング（相似計算法）などが挙げられる（図17）。これらの計算モデルに量子並列性を導入することも今後の研究課題である。たとえば量子ニューラルネットワークや量子セルオートマトンというものが可能かもしれない。しかし、それらがどのようなものであつて、量子並列性が一体どのような形で利用されるのか、ということについてはほとんど検討されていない。次に非チューリング系の量子コンピューティングについて、

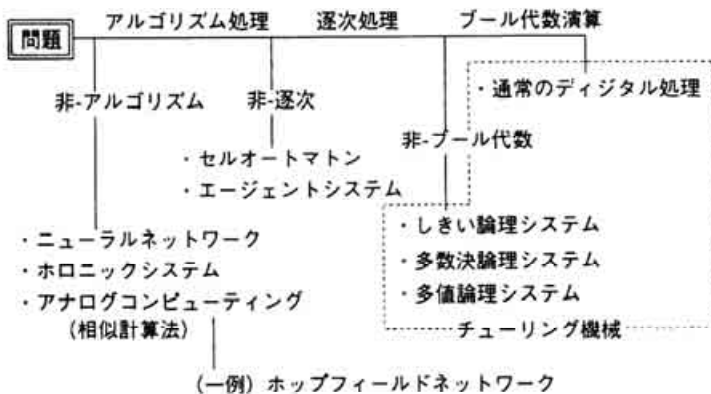


図17 与えられた問題を解くプロセスと各種の計算モデル。

著者の想像をまじえながら解説を加える。

10. 量子ホップフィールドネットワーク

概念がだいたい確立している例に量子ホップフィールドネットワークがある。これはホップフィールドネットワーク（HPネットワーク）という計算モデルに量子並列性を導入したものであつて、通常のHPネットワークでは避けられない問題「ローカルミニマム障害」がない。したがって、難しい組み合わせ問題を迅速に解くためのデバイスを開発できる可能性がある。以下に順を追って説明する。

(1) HPネットワークの動作概念

HPネットワークはアナログコンピューティング（相似計算法）の一種である。多数のしきい要素からなる特殊な帰還形ネットワーク（図18）の動作を利用して組合せ問題を解く計算手法のことをいう。（組合せ問題とは、ある制約条件のもとで、与えられた目標関数を最小とする変数値の組合せを求める問題のこと。）このネットワークは多くのしきい要素と結合からなる。各結合の重み W_{ij} と θ_i は正負いずれの値にも設定できる（ただし $W_{ii} = W_{ji}$ かつ $W_{ii} = 0$ ）。各しきい要素 i の出力 V_i は帰還してネットワークの入力となる。各しきい要素 i は入力の重みつき総和に応じて1と0のいずれかを出力するものとする。つまり重みつき総和 $(\sum_k W_{ki} V_k + \theta_i)$ が正なら出力 V_i は1、負なら出力 V_i は0である。

このネットワークの特徴は次の性質を持つことにある。すなわち、任意の初期状態から出発して、下式で定義されるエネルギー関数 E の値を最小とする方向に状態（各しきい要素の1-0出力の組合せ）を変えていく。

$$E = -(1/2) \sum_i \sum_j W_{ij} V_i V_j - \sum_i \theta_i V_i$$

ネットワークの結合重みを適切に設定すれば、このエネルギー関数を与えられた組合せ問題の目標関数に対応させることができる。つまり、組合せ問題を解くことがネッ

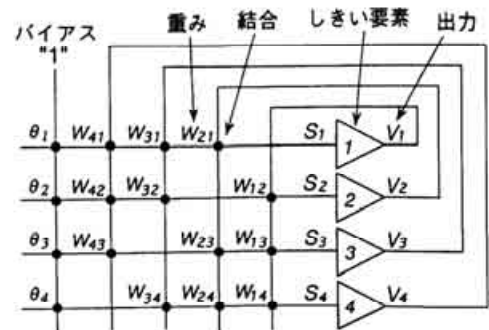


図18 ホップフィールドネットワークの概念。多数のしきい要素と重み結合からなる帰還形ネットワーク。

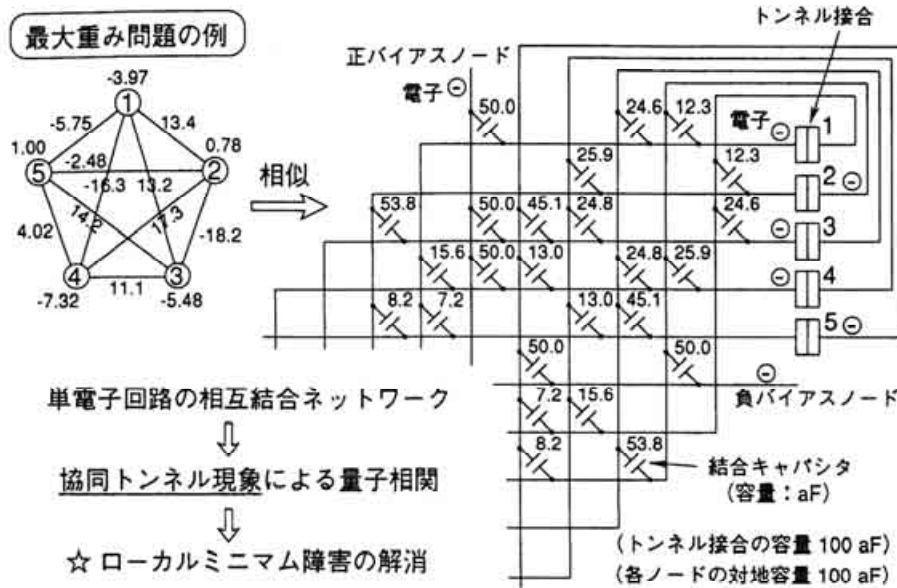


図 19 単電子回路による量子ホップフィールドネットワーク。図例は最大重み問題を解くためのもの。最大重み問題とは、節点と枝の両方に重みのついた完全グラフから、重み総和が最大となる完全部分グラフを抜き出す問題である。

トワークの最小エネルギー状態を見つけることに置き換えられる。したがって、ネットワークの収束状態を観測することで組合せ問題の解を求めることができる。HPネットワークでは問題自体がネットワーク上に載っており、そのネットワーク全体が一体のまま並列的に動作して解に到達する。そのため問題のサイズに関係なく高速に解を求められる可能性がある。

ところが残念なことに、既存のホップフィールドネットワークにおいては、必ず正解が得られるとは保証できない。その理由は、エネルギー関数が多くのローカルミニマムを持つことによる。ほとんどの場合にネットワークはローカルミニマム状態に落ち込んで停止し、最小エネルギー状態（すなわち正解）には到達できない。このローカルミニマム障害は各しきい要素の状態変化が互いに独立であることに起因しており、HPネットワークの既存概念に従うかぎり避けることができない。

このローカルミニマム現象は、HPネットワークで問題を解こうとするとき、極めて都合の悪いものである。我々はネットワークが停止したところを最小エネルギー状態とみなして問題を解くのであるが、それが真に最小エネルギー状態かどうかを確認することはできない。したがって、ローカルミニマムで停止する可能性がある以上、得られた解が正解とは確信できない。これはHPネットワークにおける最大の問題点であり、その応用分野を限られた範囲にとどめている阻害要因でもある。

(2) 量子相関の導入

ローカルミニマムが生じる理由は、従来のHPネットワークでは個々のしきい要素が互いに相関なく状態変化

するからである。ローカルミニマムを回避するためには次のような動作をさせたい。

「複数のしきい要素が同時に状態を変えるとネットワークエネルギーが減少するような場合には、実際に複数のしきい要素が相関して一斉に状態を変える」

このような状況を実現できれば、そのときにはローカルミニマムのないHPネットワークができる。一案として、複数のしきい要素を量子効果により相関動作させることを考える。このようなHPネットワークを量子ホップフィールドネットワーク（量子HPネットワーク）という。量子HPネットワークでは、任意の初期状態から出発して、必ず最小エネルギー状態に収束することが保証される。そのような量子HPネットワークは、たとえば単電子回路で構成することができる。

(3) 単電子回路による構成

単電子回路はその自由エネルギーを減少させるように状態を変える。この性質を利用すると、単電子回路でHPネットワークを構成することができる。いまトンネル接合をしきい要素として使用し、単電子の存在位置（電子が接合の右側にあるか左側にあるか）によってしきい要素の1-0状態を定義する。トンネル接合と重み結合キャパシタンでHPネットワーク回路を構成する。図19には最大重み問題を解く場合の回路例を示した。

単電子HPネットワークは、既存のHPネットワークの動作に加えて量子的な性質をもつ。すなわち、2つかそれ以上の複数接合で電子トンネル事象が同時に相関して生じる現象（協同トンネル現象）がある。言い換えると、単電子回路においては、幾つかのトンネル事象（状態遷

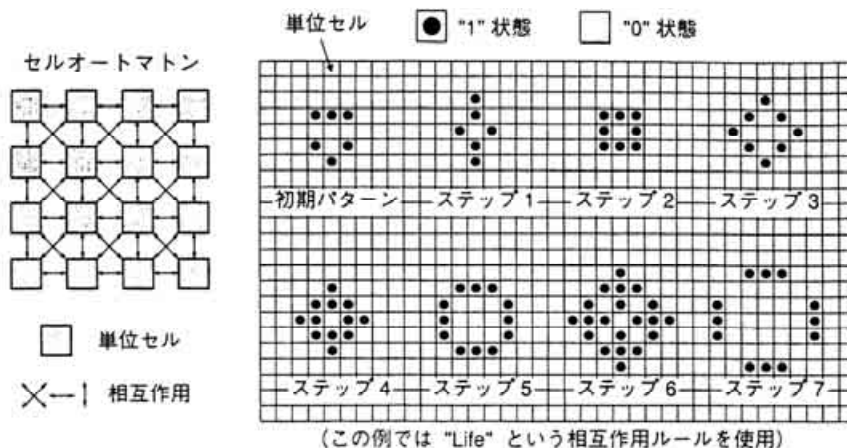


図 20 セルオートマトンの概念。単位セル間の相互作用による並列分散形の情報処理システムである。2次元パターン変換に利用できる。

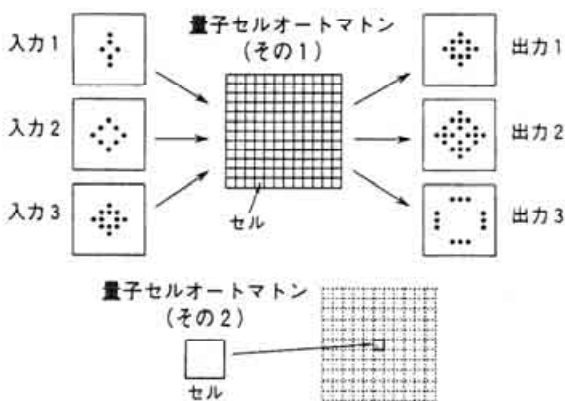


図 21 量子セルオートマトンの例。複数のパターンを重ね合せ状態で一齐に処理する(その1)、あるいは、1つのセルだけでセルオートマトン全体の動作を行う(その2)。

移) がまとまって生じるとエネルギーが減少するような状況であれば、そのような一連のトンネル事象が実際に生じる。このため単電子回路のHPネットワークは(普通のHPネットワークとは異なり)量子HPネットワークとして動作する。シミュレーションにより、任意の初期状態から始めて必ず最小エネルギー状態(正しい解)に収束することが確認されている。

11. 量子セルオートマトン

セルオートマトンは並列分散形の情報処理システムの一つである。近接相互作用を行う単位セルをマトリクス配列した構造を持つ(図 20)。各セルは2値(あるいは3値以上)の状態をとり、時間ステップごとに一齐にその状態を変える。あるセルの次の状態は「現在の自分の状態」と「隣接8セルの現在状態」をもとに決まる。その決定則を相互作用ルールという。

各セルを画素とみなせば、セルオートマトンの動作は2次元画像パターンの変換である。与えられた初期パターンを処理して(所定のステップ後に)出力パターンを生成する。適切な相互作用ルールを用いることで、各種の有用な画像処理を行うことができる。その動作は本質的に並列処理であり、高速の画像処理が可能である。

量子セルオートマトンがどのようなものであるか、ということは現在のところよく分からない。次に1, 2の案を記した(図 21)。

- (i) 量子セルオートマトンとは「複数の初期パターンを重ね合せ状態で受け取り、それらを同時に処理して各出力パターンを一齐に生成する」ような超並列システムである(図 21(その1))。
- (ii) 量子セルオートマトンとは「全セルの情報が一つのセルに込められていて、その1セルだけでセルオートマトンの動作を行える」ような超並列システムである(図 21(その2))。

12. 量子ニューラルネットワーク

ニューラルネットワークは学習と自己組織化を特徴とする情報処理システムである。そのうち応用範囲の最も広いものはバックプロパゲーション形ニューラルネットワーク(BPニューラルネットワーク)と呼ばれるものである。

BPニューラルネットワークは多数のしきい要素を層状に結合した構造をもつ。結合の重みを目的に応じて適切に設定すれば、与えられた入力信号を有用な出力信号に変換する情報処理システムができる。必要な結合重みを理論的に決めることは困難であり、実際には学習操作によって重み設定を行う。学習操作とは、教師信号(「入

力値」と「出力期待値」の組)をネットワークに提示して結合重みを調整することである。一般的に、教師信号として多数の組(数十組~数万組)を必要とする。しかもその全体を繰り返して(数百回~数万回)提示しなくてはならない。したがって、学習操作は非常に時間のかかる作業である。加えて学習過程で生じるローカルミニマム現象のために、学習が進まないことも多い。

学習操作を迅速に行うには、教師信号のすべての組を重ね合せて1回で提示できればよい(重ね合せた「入力値」と重ね合せた「出力期待値」を提示する)。その場合のBPニューラルネットワークは、重ね合せ教師信号を処理できるものでなくてはならない。あわせて(量子相関を利用することにより)前記のローカルミニマム学習停滞を回避できるようなものであって欲しい。そのようなBPニューラルネットワークが開発できれば、それを量子BPニューラルネットワークと呼ぶことができる。

参考文献

- はじめに量子チューリング機械についての原著論文を挙げる。(わかりやすい記述とはいえないので、最初は文献2)-4)を読む方がよい。
- 1) Deutsch, D.: "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proc. of the Royal Society of London, A* 400, 97-117 (1985)
- 入門解説書として次の書籍が薦められる。量子計算の概念とDeutsch-JozsaアルゴリズムおよびShorの因数分解アルゴリズムを詳細に解説してある。
- 2) 西野哲朗:「量子コンピュータ入門」東京電機大学出版局(1997)。
- 次の文献は、量子計算の数理モデルからハードウェア化の実験にわたる幅広い解説記事である。引用文献も多い。

Groverのアルゴリズムの解説もある。

- 3)「特集:量子コンピュータ」数理科学(サイエンス社), 36(10), 5-50 (1998)
- ハードウェア化の研究動向について、次の文献が参考になる。同じ著者による文献3)中の解説記事もあわせて参照されたい。
- 4) 竹内繁樹:「21世紀、量子猫は計算をするか?」日本物理学会誌, 54(4), 263-273 (1999)
- 現時点で実験が最も進展している量子計算デバイスは、核スピン系を核磁気共鳴で制御するものである。これについては北川勝浩氏による解説記事「NMR量子コンピュータ」が文献3)の中にある。
- 本稿の電子波回路で採用した2線式の量子配線方式は下記文献の量子光学回路を参考にしたものである。
- 5) I.L. Chuang and Y. Yamamoto: "Simple quantum computer," *Phys. Rev. A*, 52(5), 3489-3496(1995)
- 量子ホップフィールドネットワークの文献を挙げる。
- 6) 赤澤正道, 雨宮好仁:「単電子回路による量子ホップフィールドネットワーク—ローカルミニマム問題のないホップフィールドネットワーク」電子情報通信学会-技術研究報告, NC 97-173(1998), 徳田恵理子, 朝日昇, 赤澤正道, 雨宮好仁:「量子ホップフィールドネットワークによる最適化問題の求解」電子情報通信学会-技術研究報告, NC 98-163 (1999)