レクチャーシリーズ 「知能コンピューティングとその周辺」〔第12回〕

量子探索と量子ゲーム

Quantum Search and Quantum Games

岩間 一雄 京都大学大学院情報学研究科
Kazuo Iwama School of Informatics, Kyoto University.
iwama@kuis.kyoto-u.ac.jp, http://www.lab2.kuis.kyoto-u.ac.jp/~iwama

Keywords: quantum algorithms, quantum search, quantum games.

1. はじめに

本稿の目的は量子計算の神秘の世界の一端を紹介することである．量子計算は，その存在は誰もが知っていても，どうも「敷居が高くて入りづらい」としり込みしている人や，「どうせ実現しないものを勉強しても仕方がない」というより積極的な反対派が大部分であろう．確かに量子計算の隅から隅までを自家薬籠中のものにするのは大変かもしれない．しかし，そんな人は世界中見回してもそれほど多いわけではなく，著者を含めて「自分の好きな部分を何となく理解して騙し騙し論文を書いている」という人が大部分なのではないだろうか．

したがって，ある程度具体的問題に絞って基本的成果を説明することは，（かなり専門化している）制約充足問題の最近の成果を説明するよりもむしろ簡単かもしれない．そこで，本稿では，比較的説明しやすく，かつ量子の効果がはっきりしている問題として，量子探索問題と，量子ゲーム（擬似テレパシー）を取り上げることにしよう．次の2章で最低限必要な量子計算の基礎を説明し，その後の二つの章で，それぞれの問題を取り上げる．

AIとの関係であるが，著者の乏しい経験によれば，AIの基本的アプローチはやはり実験で，理論的証明は行わないにもかかわらず，ある程度の普遍的事実を導き出すことを可能にする工夫の効いた実験データを取ることではないであろうか．本稿では実験は全くないし，すべて数学的モデル上での議論になる．ただし，上のようなどちらかといえば帰納的アプローチは私も好きで，本稿でも，例えば一般のnに対して成立する性質を$n=2$や3で説明して一般の場合を推測していただくという書き方を多用する．量子計算の解説にときどき現れる，式の変形を中心とした説明は（それはそれで大変美しいのであるが）できるだけ避けたい．

2. 量子計算の基礎

2·1 計算のモデル

量子計算に入る前に古典の計算機の本稿でのモデルを導入しておこう．図1に示すように，計算機はレジスタの値を演算によって（左から右へ）順次変えていくものとみなす．左のx_1からx_nまでが入力ビットで，ほかにも定数をいくらでも利用してよい．箱が1ステップの計算で，箱の中は適当な論理回路が入っていると思ってほしい．例えば2ステップ目では，レジスタの1と2の値のANDを取って，それをレジスタ2に格納している．出力は適当なレジスタの値を選択する．図ではレジスタの3ビットをy_1からy_3として選択している．

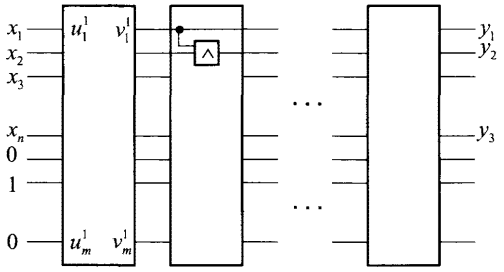

図1 計算機のモデル

1ステップの計算を示す一つの箱の中にどのくらい複雑な論理回路を入れることができるかという問題が生じるが，nの多項式程度としておこう（あまり重要ではない）．iステップ目の箱の入力をu_1^iからu_m^i，出力をv_1^iからv_m^iとしよう．箱の中身は単純な論理回路であるから，u_1^iからu_m^iの値が決まればv_1^iからv_m^iの値は一意に決まる．その入出力関係を示すのに$2^m \times 2^m$の行列（**遷移行列**）が使える．

例えば，$m=2$の場合を考えてみよう．入出力の状態としては00から11までの4状態ある．論理回路として，例えば出力の1ビット目が入力2ビットのAND，2ビット目が入力のORだったとしよう．すると，遷移行列Mは以下のようになる．

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

この遷移行列の意味は以下のように説明できる．今，入力状態が10であったとしよう．すると，出力の状態は上の論理回路から01になるが，それは以下のようにM

とベクトルの掛け算によって計算される．ただしここでは，状態00, 01, 10, 11はそれぞれ，縦ベクトル（**状態ベクトル**と呼ばれる）(1, 0, 0, 0), (0, 1, 0, 0), (0, 0, 1, 0), (0, 0, 0, 1) で表すことを仮定している．

$$\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&1&1&0\\0&0&0&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}0\\0\\1\\0\end{bmatrix}$$

この手法の良いところは，状態が決定的でなくて確率的に分布していてもそのまま使用できることである．例えば上の例で入力の状態が01と10にそれぞれ確率0.8と0.2で分布しているときの出力の状態は確率1.0で状態01になることが下の計算によってわかる．

$$\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&1&1&0\\0&0&0&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}0\\0.8\\0.2\\0\end{bmatrix}$$

2·2 重ね合わせ状態

さて，いよいよ量子計算の基礎の説明に移る．量子計算機のモデルも上の古典計算機のモデルと見掛け上は同じものを使用する．ただしいくつかの点で大きく異なる．第一にレジスタの状態である．古典計算では1ビットの情報は0または1であるが，量子計算ではレジスタの1ビットに，0と1が**重ね合わさった**状態を格納できる．このような状態を**キュービット**と呼び

$$a|0\rangle+b|1\rangle$$

で表す．ここで，$|0\rangle$ は状態ベクトル (1, 0) を表し，古典の状態0に対応する．$|1\rangle$ も同様である．したがって上の状態は状態ベクトル

$$\begin{bmatrix}a\\b\end{bmatrix}$$

で表してもよい．a と b は $|0\rangle$ と $|1\rangle$ の強さの比を表す係数で（**振幅**と呼ばれる），$|a|^2+|b|^2=1$ を満たす複素数である．例えば，二つの振幅が等しい場合は

$$\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle=\begin{bmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{bmatrix}$$

となる．

2ビット（本来は2キュービットというべきであるが，繁雑であるので以下では単にビットという）以上へ自然に拡張され，例えば2ビットなら，例として

$$\frac{1}{\sqrt{3}}|00\rangle+\frac{1}{\sqrt{3}}|01\rangle+\frac{1}{\sqrt{6}}|10\rangle+\frac{1}{\sqrt{6}}|11\rangle=\begin{bmatrix}1/\sqrt{3}\\1/\sqrt{3}\\1/\sqrt{6}\\1/\sqrt{6}\end{bmatrix}$$

といった状態が考えられる．ここで，例えば $|01\rangle$ は二つの縦ベクトル $|0\rangle$ と $|1\rangle$ のテンソル積であり，縦ベクトル (0, 1, 0, 0) になる，ほかも同様である．四つの振幅の絶対値の2乗の和が1に等しいことを確かめてほしい．

2·3 ユニタリ変換

次に1ステップの計算がどのように進行するかを述べる．古典の場合と同様に遷移行列で表現することができるが，その行列が**ユニタリ行列**でなければいけないという制限がある．この制限は量子力学の原理からきているもので，ここでは理由なしで受け入れていただきたい．ちなみにユニタリ行列 A とは

$$AA^\dagger=A^\dagger A=I$$

を満たす行列であることを思い出してほしい．ここで，$A^\dagger$ は A の共役転置行列，I は単位行列である．ユニタリ行列には以下の重要な性質がある．状態ベクトル $\boldsymbol{u}$ がユニタリ遷移行列 A によって $\boldsymbol{v}$ に変更されたとする．つまり

$$\boldsymbol{v}=A\boldsymbol{u}$$

である．このとき両辺に $A^\dagger$ を掛けることによって

$$\boldsymbol{u}=A^\dagger\boldsymbol{v}$$

が得られる．つまり，計算が**可逆**なのである．

ユニタリ遷移行列の例として最も重要なものに，**アダマール変換**と呼ばれるものがある．これは1ビットの状態に対しては

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}$$

で表され，状態 $|0\rangle$ と $|1\rangle$ を以下のように変換する（変換という意味を強調するために，このように左から右への矢印を使うこともある）．

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix}\Rightarrow\begin{bmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{bmatrix}=\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\1&-1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\Rightarrow\begin{bmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{bmatrix}=\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle$$

2ビット状態に対するアダマール変換はその各ビットにアダマール変換を施したものとして定義される．したがって，例えば $|00\rangle=|0\rangle|0\rangle$ に施すと状態は

$$\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)$$
$$=\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)$$

となって1ビットの場合と同様に四つの等しい振幅の状態に分かれる．なお，遷移行列は以下で表されることを確かめられたい．

$$\frac{1}{2}\begin{bmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{bmatrix}$$

3ビットの状態に対する図2のような1ステップの計算を考えてみよう．ここで3番目のビットに対する白丸はEXORを意味し，1番目と2番目の線に対する黒丸はANDを意味している．つまり，u_1 と u_2 がともに1の場合は縦の線の状態が1になって，u_3 の状態を反転（0を1に，1を0に）させるが，それ以外の場合（つまり u_1 と u_2 の少なくとも一方が0の場合）u_3 の状態は変化し

ない．このような「素子」を**制御NOT**と呼ぶ．

したがって，この計算では，状態 $|110\rangle$ は $|111\rangle$ に遷移し，逆に $|111\rangle$ は $|110\rangle$ に遷移する．ほかの状態は変化しない．よって，この計算の遷移行列は以下のようになることが容易にわかる．またこの行列は明らかにユニタリ行列である．つまり，量子計算として許されているのである．

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

しかし，例えば2·1節で出てきた遷移行列は明らかにユニタリ行列ではない．つまりそのような回路による計算は許されていないということである．

2·4　量子並列計算

図2の回路の入力状態として，u_1, u_2 の状態としては振幅の等しい四つの状態の重ね合わせ，u_3 の状態としては0を考える．すると全体の状態は

$$\frac{1}{2}|000\rangle+\frac{1}{2}|010\rangle+\frac{1}{2}|100\rangle+\frac{1}{2}|110\rangle$$

となる．そこで上の行列を掛けて，v_1, v_2, v_3 の状態を出してみてほしい（上の4状態以外は振幅を0にして，長さ8の縦ベクトル（1/2, 0, 1/2, 0, 1/2, 0, 1/2, 0）をつくってから行列を掛ける）．簡単な計算で以下の状態が得られる．

$$\frac{1}{2}|000\rangle+\frac{1}{2}|010\rangle+\frac{1}{2}|100\rangle+\frac{1}{2}|111\rangle$$

ここで注目してほしいのは，v_1, v_2, v_3 の3状態では1ビット目と2ビット目のANDが正確に計算されて3ビット目に反映されていることである．u_3 を0にしているので，制御NOTが上2ビットのANDを3ビット目に反映するということはわかるが，**1回**のAND計算で（図2の回路に対応する上記の遷移行列の**1回**の適用で），00, 01, 10, 11 のANDの値を同時に計算してしまったことになる．これはちょっと驚異である．量子計算の進行はあくまで遷移行列によって定義されるが，このように（古典の）論理回路の計算のような考え方も可能である．その際，状態が古典の状態なら問題はないが，いくつかの古典の状態が重ね合わさっている場合は，そのおのおのの（古典の）状態に対して論理演算を適用すればよい

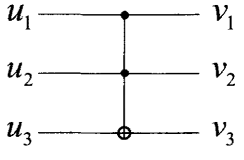

図2　制御NOT

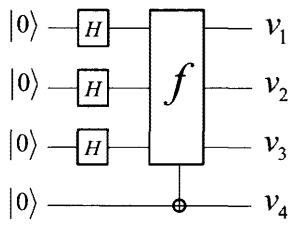

図3　量子並列計算

ことが上の説明でわかっていただけたと思うし，これが正しいことも証明できる．

より発展させて，図3のような回路を考えよう．ここで f は3変数の（古典の）論理関数である．つまり，上3ビットの値に対してその関数値を計算して，その値を4ビット目に反映させるというしくみである．今までは（図1や図2では）回路の入力はいくつかの論理変数であったが，図3では入力がすべて定数 $|0\rangle$ になっている．その理由はこの回路の目的が，上と同じように，関数 f のすべての異なった入力に対する値を並列に計算してしまおうということだからである．箱で囲った H はアダマール変換を表す．したがって，関数の箱の前の3ビットの状態は $|000\rangle$ から $|111\rangle$ まで等しい振幅の重ね合わせになっている．出力 v_1 から v_4 の状態は上の説明から

$$|000f(0,0,0)\rangle+|001f(0,0,1)\rangle+\cdots+|111f(1,1,1)\rangle$$

になることがわかる（各状態の振幅は $1/\sqrt{8}$ になるが，すべて等しい場合は省略してもよいことにする）．ここでも，関数 f を1回しか使っていないのに，8種類の値をすべて計算してしまっている．これを**量子並列計算**と呼ぶ．

f の引数の数はいくつでもよいし，実現する「回路」は通常簡単につくれる．例えば，n 変数の3CNF式（項のサイズがすべて3の和積標準形の論理式）なら，具体的つくり方は省略するが，制御NOTを多数使うことによってつくることができることはほぼ明らかであろう．この関数 f を図3の f と考えてほしい．前と同じように関数 f を1回使用するだけで，2^n 通りの関数値をすべて計算できる．こうして，f が充足可能であるなら，出力に最後のビットが1であるような状態が少なくとも一つはあるし，充足不能なら，出力の最後のビットはすべての状態において0である．このように，f の充足可能性·不能性を異なった二つの状態に対応させることができた．3CNF式の充足可能性問題は有名なNP完全問題であるが，こうしてたった1回の f の関数評価によってこの問題が解けてしまったことになる．本当であろうか….

2·5　観　　測

ここで量子計算の第3のルールを述べる．それは，レジスタの値をどのようにして得るかである．上で述べたように図3の出力は8通りの状態が「混在」している．この状態に関する情報を得るために我々ができることはこの状態を**観測**することだけである．その結果，何が得

られるかというと，この8状態のいずれか一つがその状態の振幅の2乗の確率で得られるのである．今の場合は振幅はすべて等しいので，八つのうちの一つがランダムに選ばれて得られる．

そこでもう1回上の充足可能性問題を考えてみよう．確かにn変数に対する2^n通りの割当てに対する関数値はすべて計算されている．しかし，出力の状態を観測したときに，その2^n通りの割当てに対する関数値の「いずれか一つ」が得られるに過ぎない．しかも，そのどれが得られるかは全くコントロールできず，完全にランダムである．これでは，例えば関数値が1になるのが，2^n通りの割当てのうちたった一つであったなら，それが選択される可能性は$1/2^n$でほとんどゼロである．さらにいうなら，古典的に2^n通りの割当ての一つをランダムに選んで，その関数値を計算するのと同じ成功確率である．関数値はすべて計算しているのに，その中の重要な部分を「見る」ことができないのである．大きなジレンマといってよい．

2・6 量子計算の優位性

このジレンマを乗り越える一つの方法を以下に与える．これは，量子計算が古典計算より本質的に高速である可能性を初めて示唆した結果で，その後の重要な結果（素因数分解など）の引き金になったといわれている．

図3のような3変数の論理関数fを考えるが，ここで，fは，すべての値が0の定数関数（f_0）か0と1を取る割当てがちょうど半々（つまりいずれも4個）であるような関数（f_e）のいずれかであることがわかっているとする．問題は今の関数がf_0またはf_eのいずれであるかを判定せよというものである．古典計算では，確実に判定するには5回以上関数値を評価する必要がある（4回では全部の関数値が0のときに，依然としてf_0とf_eの二つの可能性が残る）．

さて，量子計算の有利さを見るために図4の回路を考えよう．図3との違いは，第4ビットの初期値が$|1\rangle$でその後にアダマール変換が入っていることと，最初の3ビットに対して，関数評価の後にもアダマール変換を行っていることである．さて，関数の評価の直前の4ビットの状態は

$$\left(\frac{1}{\sqrt{2}}|0\rangle+\frac{1}{\sqrt{2}}|1\rangle\right)^{\otimes 3}\left(\frac{1}{\sqrt{2}}|0\rangle-\frac{1}{\sqrt{2}}|1\rangle\right)$$
$$=\frac{1}{4}(|000\rangle+\cdots+|111\rangle)(|0\rangle-|1\rangle)$$

である（ただし，$^{\otimes 3}$は，その状態を3回の繰り返すのを簡単に書くための記法である）．関数がf_0の場合は関数の評価後もこの状態は変化しない．したがって，最終的な状態は前半の3ビット$|000\rangle+\cdots+|111\rangle$にアダマール変換を施したものと最後の$|0\rangle-|1\rangle$の直積になる（ここはちょっと微妙である．本当は4ビット全体に対する遷移行列を求めて計算しないといけないが，このように状態が直積で書ける場合はそれぞれに対して独立に計算してその後で再び直積を考えても結果が同じになることが容易に示せる）．

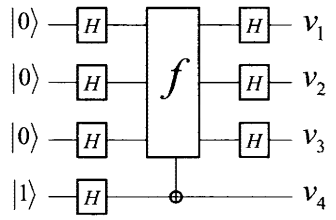

図4 量子計算の威力

ところで，3ビットに対するアダマール変換の遷移行列は

$$\frac{1}{\sqrt{8}}\begin{bmatrix}1&1&1&1&1&1&1&1\\1&-1&1&-1&1&-1&1&-1\\1&1&-1&-1&1&1&-1&-1\\1&-1&-1&1&1&-1&-1&1\\1&1&1&1&-1&-1&-1&-1\\1&-1&1&-1&-1&1&-1&1\\1&1&-1&-1&-1&-1&1&1\\1&-1&-1&1&-1&1&1&-1\end{bmatrix}$$

になる（これも簡単に導ける）．特色は最初の行はすべて1で，ほかの行は1と−1がちょうど半分ずつあることである．したがって，前半3ビットに対する変換の結果としては，今の状態に対する状態ベクトルが8個の1からなる縦ベクトルであることを考えると，最初の行に対応する状態$|000\rangle$だけが残ってほかはすべて振幅が打ち消して0になる．よって最終的状態は

$$|000\rangle(|0\rangle-|1\rangle)$$

となり，観測すれば0000の状態か0001の状態が等確率で得られる．いずれにしても最初の3ビットは必ず0である．

関数がf_eの場合は$|000\rangle$から$|111\rangle$のうちちょうど半分の関数値が1になる．例えば，$|011\rangle$の関数値が1になれば，4ビット目が反転されるので，状態$|0110\rangle$は$|0111\rangle$に，$|0111\rangle$は$|0110\rangle$になる．つまり

$$|011\rangle(|0\rangle-|1\rangle)$$

が

$$|011\rangle(|1\rangle-|0\rangle)=-|011\rangle(|0\rangle-|1\rangle)$$

に変化する．ほかにも$|010\rangle$，$|101\rangle$，$|110\rangle$の関数値が1になったとすると，結局最終的な状態は

$$(|000\rangle+|001\rangle-|010\rangle-|011\rangle+|100\rangle-|101\rangle$$
$$-|110\rangle+|111\rangle)(|0\rangle-|1\rangle)$$

になる．最初の3ビットと4ビット目の状態がこのように直積で書けているので，前述のように，それぞれ独立に遷移行列を適用しても問題ない．最初の3ビットに関してはちょうど半分の振幅が負である（ここもおもしろいところで，最初の3ビットに関しては何の演算も施されていないのに，状態が変化したように見える）．したがって，上の遷移行列をもう一回見てみるなら，第1行

に対応する振幅は打ち消して0になることがわかる．つまり，最初の3ビットが000の状態は絶対に観測されない．上で見たように，f_0の場合は最初の3ビットは常に000なので，完全に分離できたことになる．

この議論は関数の引数の個数が多くなっても全く同じである．したがって，n変数なら，古典で2^{n-1}回の関数の評価が必要なところを量子ではたった1回でできてしまうという信じられないような結果になるのである．

3. 量 子 探 索

3·1　問題の定義と古典アルゴリズム

サイズ1024の配列があって，そのおのおのに本のタイトルが入っているとしよう．ただしその順序は不同で何の情報もない．そこで，「アルゴリズムサイエンス―出口からの超入門―」という本の配列のインデックス（簡単のためこのタイトルは存在すると仮定する）を求めたい．これが本章で扱う問題であるが，より単純化して，前章で議論した論理関数の評価の問題に置き換えて論じることにする．つまり，未知のn変数論理関数f(ただし，ただ一つの割当てに対して関数値が1になることがわかっている）が与えられて，$f(a)=1$になる割当てaを求めよという問題である．ただし，この関数に対して我々ができることは具体的割当て$a\in\{0,1\}^n$に対して関数値を評価する（$f(a)$が得られる）ことだけである．

簡単のため，しばらくの間$n=2$の場合を議論する．割当ては{00, 01, 10, 11}の4通りしかないので，この四つの割当てに対して関数値を評価すれば簡単に解けるし，古典の場合はそれ以外のうまいやり方はなさそうである（乱数を利用するという考え方もあるが，ここでは確実に答えを求めることが要求されている）．量子の場合との比較を明確にするために，この問題を解く古典のアルゴリズムを前章のモデルで考えてみる．例えば図5のような回路でよいであろう．ここで，+1の箱は状態を2進数とみなして+1する回路である．ただし下からの入力が1の場合だけで，0の場合は何もしない．ちなみに箱の下に付いている小さな白丸は論理否定である．例えば$f(0,0)$の値が0なら，最初のfの評価の後の第3のビットの値は0であるから，次の+1の箱が働き，状態が00から01に変わる．もし$f(0,1)=1$なら，3番めのビットの値が1に変化し，それが2番目の+1の箱の働きを止めて，それ以降最初の2ビットの値は変化しない．こうして答えのy_1, y_2に01が得られるのである．明らかに関数値は4回評価している．

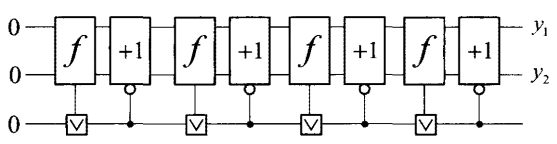

図5　古典計算回路

3·2　量子アルゴリズム

量子アルゴリズムは図6を見てほしい．新たにXという素子が出てきているが，これは**否定**素子で，その遷移行列は以下で与えられる．

$$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

$|0\rangle$を$|1\rangle$に，$|1\rangle$を$|0\rangle$に変換する働きがあることは容易にわかる．関数fはわずか1回しか評価していない．これで本当に答えが求まるのであろうか．

解析に当たっては，まず以下のことを注意したい．図のP_2のところまでは前の図4と同じである．そこで，もう1回2·6節の解説に戻ってほしいのだが，要するにfの値が0の場合は何もしないし，1の場合は4番目のビットの状態の振幅の正負を反転する効果があることに注意してほしい．このビットに対する振幅の正負反転は全体の振幅の正負反転と同じである．また，我々は図4の上3ビットの状態のみに興味があって，最後の状態には興味がない．したがって，最後のビットは完全に無視して，関数の値が1の場合は，上3ビット状態の振幅の正負が反転すると考えると解析が楽になる．要するに上の3ビットの状態のみ考えるのである．

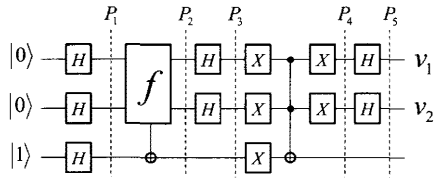

図6　量子アルゴリズム

図6も全く同様であって，以下では上2ビットのみ考える．すなわち，P_1の時点の状態は

$$(|00\rangle+|01\rangle+|10\rangle+|11\rangle)$$

であり，P_2の状態は

$$(-1)^{f(0,0)}|00\rangle+(-1)^{f(0,1)}|01\rangle+(-1)^{f(1,0)}|10\rangle+(-1)^{f(1,1)}|11\rangle$$

に変化することになる．

ここで，$f(0,1)=1$でほかの割当てに対しては0を取るものとしよう．そして，状態の変化を図7のように表す．図の（1）は$|00\rangle$をアダマール変換したP_1の状態であり，左から$|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$の振幅を棒グラフで示している．(2)はP_2の状態で，我々の$f(0,1)=1$という仮定から，$|01\rangle$の振幅が反転しているのがわかる．この（2）の状態は次の（3）と（4）の和の形で書けることが容易にわかるであろう（量子計算はすべて線形の世界なのでこういうときに便利である）．この状態で第2のアダマール変換に突入することになって，その結果は（5）と（6）のようになる．ここでアダマール変換はその逆変換がアダマール変換そのものであることに注意されたい．したがって，(5)のアダマール変換が(3)になることは以前に確認したが，そのことは（3）のア

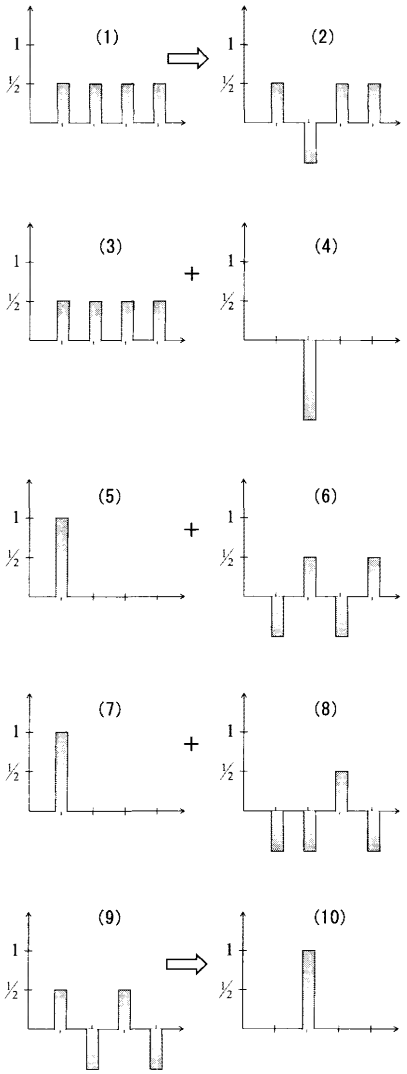

図7 状態の変化

ダマール変換が（5）になることも意味する．

ここで，図6のP_3とP_4に囲まれた部分の働きを見てみよう．まず確認してほしいのは，否定が2個続けて入っているので，それらの効果は打ち消されてしまうことに注意されたい．では，否定の間に挟まれている制御NOTはどのような役割をするのであろうか．このゲートは上の2ビットの値がP_3の時点で$|00\rangle$のときのみ（次の否定素子によって$|11\rangle$になるので）働く．そして，振幅の正負を逆転させるのであるが，よく見ると第3のビットにも否定素子が入っている．つまり，このことによって，全体が否定されてしまい，結局P_3の時点で$|00\rangle$以外の状態のときに振幅の正負が反転するのである．

そこで図7に戻ると，（5）と（6）の$|00\rangle$以外の状態の振幅のみが正負反転されて（7）と（8）になっている．ここで注意してほしいのは，（7）と（8）の合成は（9）で，これは（6）の正負反転である．さらに思い出してほしいのは，（6）は（4）のアダマール変換である．ということは，（6）の正負反転が図6の最後の段のアダマール変換に入るわけであるが，その結果は当然（4）

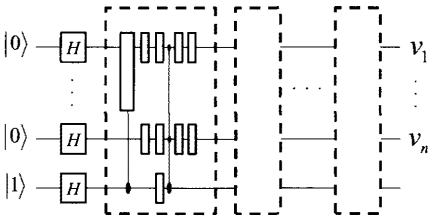

図8 一般の場合

の正負反転になるはずである．それが（10）の状態であり，これは紛れもなく$|01\rangle$である．こうして，図6のv_1とv_2を観測すれば01が得られることになって，これはまさしく我々がほしかった答えである．

$f(0,1)=1$以外の場合も確認してほしい．いずれの場合もみごとにほしい答えがたった1回の関数評価で出てくるのである．関数評価をすべての割当てに対応する重ね合わせの状態に対して行っているので当り前だと思われている方は前章の議論を思い出してほしい．ただ単に重ね合わせの状態に対して関数評価を行っただけでは古典的にランダムに状態を一つ選んでその一つの状態に対して評価することと変わらないのである．

3·3 一般の場合

一般のnの場合にはこれほど簡単ではない．$N=2^n$と置くと，古典ではN回の関数評価が必要である．量子では，これがおおよそ$\sqrt{N}$回の関数評価で実行できるのである．これが有名な**グローバー探索** [Grover 96] でショアの素因数分解アルゴリズム [Shor 94] とともに量子アルゴリズムの双璧をなしている．グローバー探索は非常に一般性の高いアルゴリズムで，数多くの応用や発展が知られている．

さて，Nが$\sqrt{N}$になる原理であるが，基本的には繰り返しである．まず古典の場合を考えて見よう．$N=2^n$の割当ての中からランダムに選んでfの値を評価すれば，およそ$1/N$の確率で答え（関数値が1になる割当て）にヒットする．2回やればこの確率が2倍，3回やれば3倍というのが直観的説明である．量子の場合は，アダマール変換して関数の評価を行えば，正しい答えの振幅として（ほかの正しくない状態の振幅と同じ）$1/\sqrt{N}$が得られる．この振幅が平方根になっているところがみそである．つまり，適当なうまい繰返しを開発して，前の古典のように，この振幅を2回の繰返しで2倍以上，3回で3倍以上にすることができれば，およそ$\sqrt{N}$回の繰返しで高い確率で答えが求まることになる．

アルゴリズムは図6のP_1から最後のP_5までを図8のようにおよそ$\sqrt{N}$回の繰り返すだけである（しかし，もちろんレジスタは$n+1$ビットを用意しなければならない）．そこで最初の1回の繰返しでの振幅の変化を見てみよう．図9である．前と同様に最初のアダマール変換によって，（1）のようにすべての状態の重ね合わせになり，次に関数値が1の状態のみ振幅の正負が反転して，

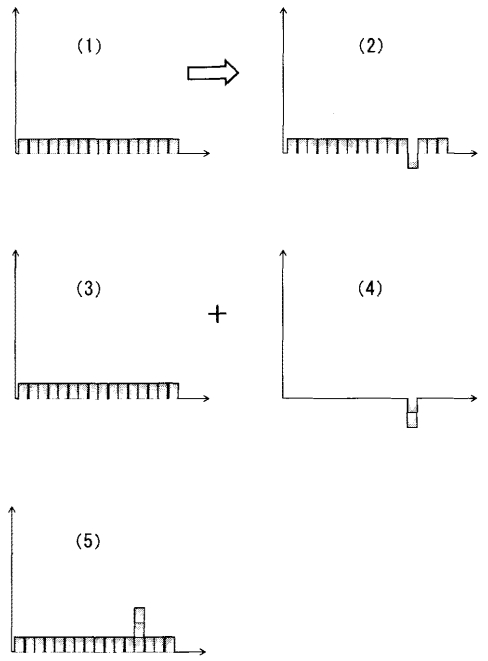

図9　一般の場合の動作

(2) のようになる．この (2) の状態は前と同様に (3) と (4) の和の形で書ける．まず (3) の成分であるが，次のアダマール変換で P_3 の時点では高さ1の $|00\rangle$ に戻り，次の P_3 から P_4 の間の回路では何の変更も受けない．したがって，また最後のアダマール変換で (3) の状態に戻ることになる．

次に (4) の成分を考えよう．この成分の振幅は $2/\sqrt{N}$ ということで小さい．これを P_3 の後ろでアダマール変換すると，さらに微小な振幅 $(2/N)$ のあらゆる状態が出てくる（ただし，振幅の正負は半分ずつで混在している）．これを次の P_3 から P_4 の間の回路で処理することになるが，そこで $|00\rangle$ 以外の振幅がすべて正負反転する．しかし，$|00\rangle$ の寄与は全体の $1/N$ しかないので，ほとんど無視してもよい．つまり，全部が反転してしまうと考えても大きな間違いではない．それをさらに最後のアダマール変換にかけるので，最終的には (4) の状態の正負反転したものが現れることになる．結局最終的な状態はこれと (3) の和になるので，図の (5) のようになる．答えに対応する状態の振幅がおよそ3倍になっていることがわかるであろう．ただし，上で無視した部分を厳密に考えるとこの倍率よりは若干悪くなることがわかる．

次の繰返しではこの3倍になった部分が反転される（図の (2) の部分に戻る）ことになり，同様に考えると最終的には5倍に大きくなることがわかる．このように，前に期待した「2回で2倍以上，3回で3倍以上」には十分過ぎる数字であるが，前述のように無視した部分があるのでこの倍率はだんだん鈍ってくる．

最終的におよそ $\sqrt{N}$ 回の繰返し，つまり $\sqrt{N}$ 回の関数の評価によって，前の図7の場合のように答えの状態のみが突出するのであるが，その数学的証明は若干専門的になってくるので，ここでは述べない．

4. 量子ゲーム

4·1　ゲームのモデル

ここで扱うのはいわゆるテレパシーゲームと呼ばれるものである．2人（以上）が関与するので，仮に太郎と花子としよう．さらに有限集合 X, Y, A, B とそれらの間の関係 $R \subseteq X \times Y \times A \times B$ が定まっている．太郎と花子は距離的に離れた場所にいて，互いの通信はできない（ので情報を交換したとすればテレパシーしか考えられない）．ゲームの一般的形態は以下のようなものである．ゲームの審判から太郎に何か X の要素 x が与えられ，花子には Y の要素 y が与えられる．太郎は x に対する何らかの答え $a \in A$ を出力する必要があり，花子もまた Y に対する答え $b \in B$ を出力する必要がある．もし，(x, y, a, b) が R に入っていれば太郎と花子の勝ちである．入っていなければ負けである．

例えば $X=Y=\{$りんご, バナナ$\}$, $A=B=\{0, 1\}$ を考えよう．太郎と花子が勝つ条件は審判から同じもの（りんごとりんご，バナナとバナナ）を提示されたときはともに1を出力し，違うものを提示されたときはともに0を出力することである．例えば太郎がりんごを提示されたとき，彼が知りたいのは花子が提示されたのがりんご（$a=1$ を出すべき）なのかバナナ（$a=0$ を出すべき）なのかという情報であるが，通信ができないので無理であろう．通常このように，勝つためには通信が必要に見えるゲームを考える．

太郎と花子はゲームが始まる前にはその戦略について，いくらでも相談できる．例えば今の場合でいえば，互いにりんごが来てもバナナが来ても常に0を出そうという戦略である．この戦略は，とても戦略とはいえないが，それほど悪くはない．もしりんごとバナナが確率1/2でランダムに与えられるなら，1/2の確率で勝利する．さらに，全く通信ができないという状況のもとではこれより本質的に高い確率で勝利するということはとても不可能に見える．本章の目的はこの不可能に見えることを量子の力で可能にしてしまうことである．

さてこのゲームに対する太郎と花子の行動（計算）のモデルであるが，前節のモデルを少し変形したものを使おう．図10を見てほしい．太郎も花子も基本的には論理関数 f と g を計算するだけである．そのための入力は太郎はゲームの審判からの $x \in X$ と「戦略」という箱からのビット情報であり，花子も同様である．この戦略ボックスからの情報の流れ（実際に信号線があるわけではなく，以前と同様，レジスタの値が変化するときの順番と読んでほしい）が存在することは，太郎と花子が事前にいくらでも戦略に関して相談できるということに対応している．例えば，太郎と花子は事前に十分に長い0と

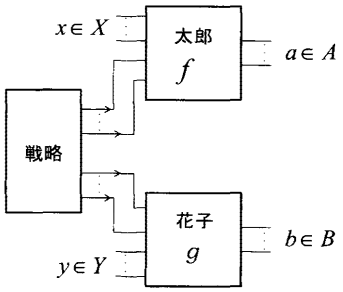

図10 ゲームのモデル

1の乱数列 $r_1, \cdots, r_m$ を生成し，各 r_i のコピーを f と g の計算に使うことができる．上のりんごとバナナのゲームでは，例えば審判からの i 回目の提示に対してはともに r_i を答えにするという戦略が取れる（つまり，太郎と花子の答えは常に同じ値になるが，その値は0と1がランダムに現れる）．この戦略の良いところは，たとえ，審判の提示がどのような分布でも（前の戦略では審判からの提示が常に同じであったら勝利の確率が0になってしまう）1/2の確率で勝利できることである．

4·2 量子戦略

りんごとバナナのゲームは残念ながら量子の力を使っても勝利の確率を上げることはできない．そこで，ちょっと違った以下のようなゲームを考えよう．

$$X=Y=A=B=\{0,1\},$$
$$R=\{(x,y,a,b) \mid x\wedge y=a\oplus b\}$$

つまり勝利するためには，一つでも0が提示されれば同じ値を出す必要があり，ともに1が提示されたら異なった値を出す必要がある．CHSHゲームと呼ばれる有名なゲームである [Clauser 69].

まず古典のアルゴリズムを考えておこう．この場合太郎も花子も無条件で0を出力するのがよい．審判の提示が一様ランダムであるなら，3/4の確率で勝てる．これ以上良い（たとえ乱数を使っても）アルゴリズムがないことがわかっている．

次に量子戦略であるが，ここで，以前に述べた量子状態の観測に関して若干の補足をしておこう．1ビットの状態

$$a|0\rangle + b|1\rangle$$

を観測したときは，確率 $|a|^2$ で状態 $|0\rangle$ が得られ，確率 $|b|^2$ で状態 $|1\rangle$ が得られるというのが観測の基本である．しかし，今までいわなかったのであるが，観測するときは，必ず直交する基底を指定することになっていて，結果はそのいずれかの基底として得られる．上の場合は，$|0\rangle$ と $|1\rangle$ が確かに直交する基底なので問題ない．しかし直交する基底を，例えば

$$\varphi=\frac{\sqrt{3}}{2}|0\rangle+\frac{1}{2}|1\rangle \quad と \quad \psi=\frac{1}{2}|0\rangle-\frac{\sqrt{3}}{2}|1\rangle$$

に取った場合を考えよう（直交することは，両者を縦ベクトルに直して，内積を取ると0になることでわかる）．この直交基底のもとで，例えば状態 $|0\rangle$ を観測するとどうなるか調べよう．

そのためには，$|0\rangle$ を φ と ψ の成分に分けて考えればよい．つまり

$$|0\rangle=\frac{\sqrt{3}}{2}\left(\frac{\sqrt{3}}{2}|0\rangle+\frac{1}{2}|1\rangle\right)+\frac{1}{2}\left(\frac{1}{2}|0\rangle-\frac{\sqrt{3}}{2}|1\rangle\right)$$

と書けるので（図11参照），確率3/4で状態 φ が得られ，確率1/4で状態 ψ が得られる．「どのようにして」得られるかと聞かれると困るのであるが，まあどちらかのランプが点く（つまり古典情報）とでも考えてほしい．さらに，重要なことであるが，観測した後のレジスタの状態はその得られた状態になる．観測の結果状態 φ が得られれば，その後の状態はもとの状態にかかわらず φ である．

2ビットの状態も通常は最も基本的な直交基底である $|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$ のもとで観測する．ここで興味深いのは2ビットのうち1ビットだけ観測することも許されている．2ビットの状態

$$a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle$$

の第1ビットを観測するとどうなるのであろうか．それは，確率 $|a|^2+|b|^2$ で状態 $|0\rangle$ が得られ，確率 $|c|^2+|d|^2$ で状態 $|1\rangle$ が得られる．前者の場合（後者も同様）は観測した後の状態は

$$\frac{a}{\sqrt{|a|^2+|b|^2}}|0\rangle|0\rangle+\frac{b}{\sqrt{|a|^2+|b|^2}}|0\rangle|1\rangle$$

になる．つまり，観測されなかった第1ビットが $|1\rangle$ の成分はすべて消え去り，観測された状態の成分がもとの大きさの比を保って残る．なお，以上はすべて約束（定義）なので無条件で受け入れてほしい．

さて，量子戦略である．図12を見てほしい．戦略回路はアダマール変換と制御NOT（ただし，ここでは制御部分が1個だけになっている）だけからなる簡単なものであるが，これが重要である．この戦略回路から得られる2ビット $|u\rangle$ と $|v\rangle$ の状態は

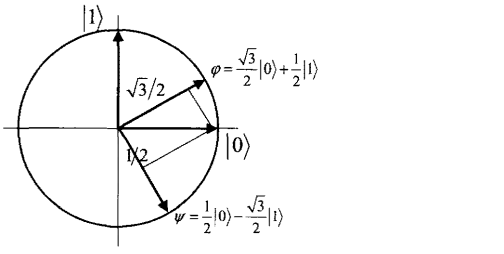

図11 直交基底

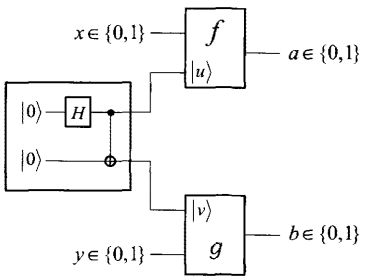

図12 CHSHゲームに対する量子戦略

$|00\rangle + |11\rangle$

であることを確認してほしい．太郎の計算 f は簡単で，（i）$x=0$ の場合はビット $|u\rangle$ を通常の（$|0\rangle$, $|1\rangle$）基底で観測する．状態 $|0\rangle$ が得られれば 0 を出力し，$|1\rangle$ が得られれば 1 を出力する．（ii）$x=1$ の場合は $|u\rangle$ を（$|+\rangle$, $|-\rangle$）基底で観測する．ここで，状態 $|+\rangle$, $|-\rangle$ は以下で定義される（図 13）．

$$|+\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ |-\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$

状態 $|+\rangle$ が得られれば 0 を出力し，$|-\rangle$ が得られれば 1 を出力する．

この段階の状況を整理しておこう．まず $x=0$ の場合を見てみよう．（i）によって，太郎は $|00\rangle+|11\rangle$ を（$|0\rangle$, $|1\rangle$）基底で観測する．第 1 ビットが 0 の状態と 1 の状態の強さが同じなので，補強された観測のルールによって，結果として等確率で $|0\rangle$ か $|1\rangle$ を得る．$|0\rangle$ を得た場合は $a=0$ である．このときは，観測後の 2 ビットの状態は $|00\rangle$ になっていて，当然花子の見ている 2 ビット目の $|v\rangle$ は $|0\rangle$ である．$|1\rangle$ を得た場合は $a=1$ で花子の $|v\rangle$ は $|1\rangle$ である．次に $x=1$ の場合である．簡単な計算で

$$|00\rangle + |11\rangle = |++\rangle + |--\rangle$$

であることがわかる．つまり，（ii）で $|00\rangle+|11\rangle$ を（$|+\rangle$, $|-\rangle$）基底で観測することは，$|++\rangle+|--\rangle$ を（$|+\rangle$, $|-\rangle$）基底で観測することと同じで，上と全く同様に等確率でいずれかを得る．$|+\rangle$ を得た場合は $a=0$ で，花子の $|v\rangle$ は $|+\rangle$，$|-\rangle$ を得た場合は $a=1$ で，花子の $|v\rangle$ は $|-\rangle$ である．

結局花子の $|v\rangle$ 状態は図 14 のようになる．花子はもし太郎への審判からの提示（つまり x の値）と太郎が何を出力したか（つまり a の値）がわかれば完全に勝利できる．太郎と花子は今の段階で何も通信していないことを思い出してほしい．それにもかかわらず，図 14 に示されるように，花子は彼女が欲しい情報が $|v\rangle$ の状態の違いによって得られているのである．量子の力そのもの（後でより詳しく述べる）といってよいが，残念ながら花子は，この 4 種類の状態の違いを完全に識別することはできない．しかし，よく考えてみれば，以下のように完全に識別する必要はないことがわかる．

花子の審判からの提示が $y=1$ であったとしよう．そのとき，花子が出力すべき正しい b の値は図 15 のようになる（例えば，$x=0, a=0$ のときは，$x\wedge y=a\oplus b$ を満足させるためには $b=0$，ほかも同様）．このように $|1\rangle$ と $|+\rangle$ に対しては同じ b の値を出せばよいので，これらの状態の違いを識別する必要はない．つまり，現在の状態が（1）$|+\rangle$ または $|1\rangle$ であるか，（2）$|0\rangle$ または $|-\rangle$ であるかの（1）と（2）を識別したい．そのためには，図 16 に示すように

$$(|\theta_{-\pi/8}\rangle,\ |\theta_{3\pi/8}\rangle)$$

基底で観測し，$|\theta_{-\pi/8}\rangle$ を得れば $b=0$，$|\theta_{3\pi/8}\rangle$ を得れば $b=1$ を出力すればよい．なお，$|\theta_\alpha\rangle$ は，$|0\rangle$ を左に α 回転させたベクトルに対応する状態であり，正確には

$$|\theta_\alpha\rangle = (\cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle)$$

である．

例えば現在の状態が $|-\rangle$ であるなら，それの $|\theta_{-\pi/8}\rangle$ への射影を考えて，確率

$$(\cos\pi/8)^2 \approx 0.85$$

で $|\theta_{-\pi/8}\rangle$ を得るので，その確率で成功する．現在の状態が $|0\rangle$ の場合も同じ．現在の状態が $|+\rangle$ または $|1\rangle$ の場合は同じ確率で $|\theta_{3\pi/8}\rangle$ を得て成功する．このアイディアは量子の世界ではよく知られていて，ほかにも多くの応用がある．未だ成功確率は 1 ではないが古典の場合の 0.75 よりはずっと良い．

$y=0$ の場合は図 15，図 16 が図 17，図 18 のように変

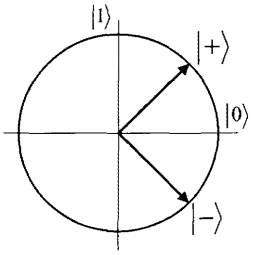

図 13　（$|+\rangle$, $|-\rangle$）基底

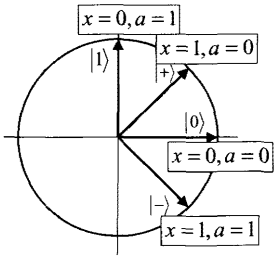

図 14　花子の $|v\rangle$ 状態

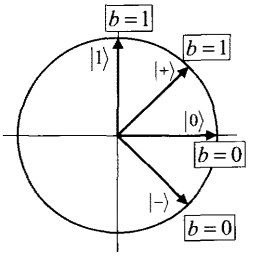

図 15　花子の必要な情報

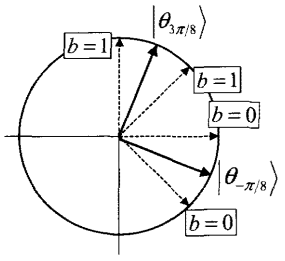

図 16　（$|\theta_{-\pi/8}\rangle$, $|\theta_{3\pi/8}\rangle$）基底

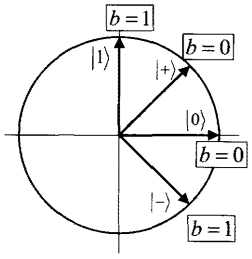

図17 $y=0$ の場合

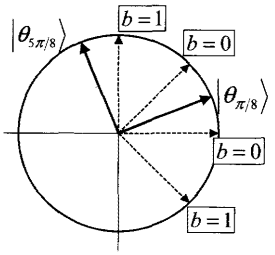

図18 （$|\theta_{\pi/8}\rangle$, $|\theta_{5\pi/8}\rangle$）基底

化するだけである（つまり花子は太郎の a の値と同じ値を出力したい）．今回は花子は

（$|\theta_{\pi/8}\rangle$, $|\theta_{5\pi/8}\rangle$）

基底を用いる．$b=1$ の場合がちょっとわかりにくいかもしれないが，振幅の正負は（どうせ2乗してしまうので）結果の確率に影響を与えないことを思い出してほしい．結局前と同じ確率 0.85 で勝利する．なお，ここでは太郎が先に観測して次に花子が観測するように書いたが，逆の順番であっても，同時でも結果に違いは生じない．

量子のトリックは何なのであろうか．それは，戦略ボックスで作成した

$$|00\rangle+|11\rangle$$

という状態なのである．この状態を太郎側で観測したとき，太郎が得るのは単に半々の確率で $|0\rangle$ か $|1\rangle$ であって，おもしろくも何ともない．しかし，$|0\rangle$ を得たときは観測の後の状態が $|00\rangle$ になってしまい，花子も必然的に $|0\rangle$ を観測する．これが重要なのである．太郎は「自分が $|0\rangle$ を得た」という情報を花子に伝えているように見えるが，両者はいっさい通信をしていないのである．戦略ボックスで上の状態を作成した後，太郎はレジスタの前半分をもって，花子は後ろ半分をもって，両者は遠く離れてしまう．太郎のレジスタの中身は $|0\rangle$ と $|1\rangle$ が同じ強さで，花子のレジスタの中でも同様である．しかし，両者の $|0\rangle$ と $|0\rangle$ が，また $|1\rangle$ と $|1\rangle$ が強く結合していると解釈できる．このような状態を**エンタングル**した状態と呼んでおり，量子計算では非常に重要な概念である．

このようにエンタングルした状態が本当に物理的に存在するのかどうか（存在するらしい）は物理学の研究者にとっては大きな問題であるが，私にとっては完全なブラックボックスである．これ以上の説明はいっさいできないのをお許しいただきたい．

4·3 Mermin-GHZ ゲーム

前節のゲームでは，量子の力を発揮はしたが，まだ完全な勝利は得られなかった．ここでは，量子の力によって，100%の成功確率が得られる例を紹介する [Mermin 90]．プレーヤは3名で，太郎，花子，ポチとしよう．提示されるのは，前と同じ各1ビットで，それぞれ $x, y, z \in \{0, 1\}$，出力するのも1ビットで，それぞれ $a, b, c \in \{0, 1\}$ である．今回は提示される3ビットには制限が付いていて，「$x+y+x$ は偶数」（つまり和の値は0または2）という制限を常に満たすものとする．勝利の条件は

$$x+y+z=2 \Rightarrow a+b+c=1 \text{ or } 3$$
$$x+y+z=0 \Rightarrow a+b+c=0 \text{ or } 2$$

というものである．

まず古典戦略を考えよう．簡単のために，戦略ボックスの情報を使わないと仮定する．その場合，太郎の論理関数 f が出力を $a=f(x)$ で決める．花子の論理関数 g，ポチの論理関数 h も同様である．すると，3人が常に勝利するためには，上の第二の条件から

$$f(0)+g(0)+h(0)\equiv 0$$

でなければならない（ただし，$\equiv$ は法2のもとでの合同を表す）．同様に上の第一の条件から

$$f(0)+g(1)+h(1)\equiv 1$$
$$f(1)+g(0)+h(1)\equiv 1$$
$$f(1)+g(1)+h(0)\equiv 1$$

でなければならない．しかし，この4式を満たす f は存在しない（上2式の和をとれば $g(0)+h(0)+g(1)+h(1)$ が奇数という式が得られ，下2式の和をとれば全く同じ和が偶数という式が得られる）．よって，古典で常勝の戦略は存在しない．これは戦略ボックスからの情報を使ったとしても変化しない（戦略は審判からの提示の前に決めなければならないので，それで常勝になる値があるなら，その値を単に f, g, h に組み込んでしまえばよい）．乱数を利用しても，異なった提示に対する平均を取る効果しかないので，常勝にはできない．

さて，量子の戦略である．前と同様に，戦略ボックスからは太郎，花子，ポチに1ビットずつ配給し，それぞれを $|u\rangle$, $|v\rangle$, $|w\rangle$ とする．仕込む状態としては前と同様にエンタングルした状態

$$|u\rangle|v\rangle|w\rangle=|000\rangle+|111\rangle$$

を用いる（戦略ボックスのつくり方は簡単にわかるであろう）．太郎の操作は簡単で，まず提示された値が $x=1$ なら，$|u\rangle$ に対してユニタリ変換

$$\begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}$$

を適用する（ただし，$i=\sqrt{-1}$）．$x=0$ なら何も行わない．その後で，このビットにアダマール変換を施し，通常の（$|0\rangle$, $|1\rangle$）基底で観測してそのまま答えとする．花子もポチも全く同様である．

ここで上の奇妙なユニタリ変換（これがユニタリ変換であることは容易にチェックできる）が何を意味する

か見てみよう．上の遷移行列から明らかなように，$|0\rangle$ に適用しても何の変化も起きない．$|1\rangle$ に適用すると

$$\begin{bmatrix}0\\1\end{bmatrix}\rightarrow\begin{bmatrix}0\\i\end{bmatrix}=i\begin{bmatrix}0\\1\end{bmatrix}$$

と変化する．では $|111\rangle$ の最初の2ビットに適用するとどうなるであろうか．

$$\begin{bmatrix}0\\i\end{bmatrix}\begin{bmatrix}0\\i\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}=i^2\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix}=-|1\rangle|1\rangle|1\rangle$$

であり，これは後ろの2ビットでも，両端の2ビットでも結果は全く同じものになる．

さて，x, y, z に1が2個ある場合を先に考えよう．直前に見たとおり，その2個がどのビットであろうとも，問題のユニタリ変換の後の状態は

$$|000\rangle - |111\rangle$$

となり，この状態に3ビットアダマール変換（2·6節に遷移行列があるので実際に確かめてほしい）を施すと

$$|001\rangle + |010\rangle + |100\rangle + |111\rangle$$

となる．観測結果は単純にこの四つのうちの一つであるから，1の数は奇数という勝利条件を満たす．x, y, z に1が0個の場合は，問題のユニタリ変換はどのビットにも適用されないので，状態はもとのままの

$$|000\rangle + |111\rangle$$

であり，アダマール変換の後は

$$|000\rangle + |011\rangle + |101\rangle + |110\rangle$$

で，やはり勝利の条件（1の数が偶数）を満たしている．結局量子は常に勝利するのである．量子の力でテレパシーを完全に模倣できるという意味で，擬似テレパシーと呼ばれている．

5. ま　と　め

量子計算の神秘を紹介すると最初にいったが，神秘というよりも「かなりインチキ臭い」と思われた方が多いかもしれない．もしそれが事実なら，それは単に著者の力不足であり，斯界にとっても損失である．しかし，最初にも述べたとおり，数学的モデルは一点の曇りもなく確定したものになっており，それを利用（悪用？）しておもしろい結果を出すのはどこでもやられていることである．おもしろいと思って下さった読者の方が少しでもいらっしゃれば無上の幸せである．

量子計算の最初の入門としては [西野 97] をお薦めする．著者は我が国における量子計算研究の草分けといってよい．より本格的に勉強されるなら [Nielsen 00] であるが，残念ながら，まだ日本語の良い解説書が出ていないようである．量子計算一般の，特にエンタングルメントの，物理の面からの解説に興味をお持ちの方も多いと思われるが，残念ながら著者の全くの守備範囲外である．しかし，我が国のレベルは質量ともにかなり高いので，周辺に必ず適当な研究者がおられるに違いない．助けを求めてほしい．

◇ 参 考 文 献 ◇

[Clauser 69] Clauser, J., Horne, M., Shimony, A. and Holt, R.: Proposed experiment to test local hidden-variable theories, *Phys. Rev. Lett.*, Vol. 23, No. 15, pp. 880-884 (1969)

[Grover 96] Grover, L.: A fast quantum mechanical algorithm for database search. *Proc. Annual ACM Symposium on Theory of Computing* (*STOC 96*), pp. 212-219 (1996)

[Mermin 90] Mermin, N.: Extreme quantum entanglement in a superposition of macroscopically distinct states, *Phys. Rev. Lett.*, Vol. 65 pp. 1838-1840 (1990)

[Nielsen 00] Nielsen, M. and Chuang, I.: *Quantum Computation and Quantum Information*, Cambridge University Press (2000) (邦訳：木村達也 訳：量子コンピュータと量子通信，Ⅰ-Ⅲ，オーム社 (2004, 2005))

[西野 97] 西野哲朗：量子コンピュータ入門，東京電機大学出版局 (1997)

[Shor 94] Shor, P.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *Proc. Annual IEEE Symp. on Foundations of Computer Science* (*FOCS 94*), pp. 124-134 (1994)

2008年10月28日　受理

著 者 紹 介

岩間　一雄

1973年京都大学工学部電気工学科卒業．1980年同大学院博士課程修了．工学博士．1978年より京都産業大学理学部講師，助教授．1983-84年までカリフォルニア大学バークレー客員准教授．1990年九州大学工学部助教授，1992年同教授を経て，1997年京都大学大学院工学研究科教授．現在同大学大学院情報学研究科教授．ラトビア大学名誉博士．アルゴリズムと計算の複雑さの理論の研究に従事．