量子探索と量子ゲーム

情報基盤工学講座　　横井　稜

November 22, 2019

はじめに

背景

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.

本稿の目的

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. 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.

計算のモデル

説明

古典の計算機の本稿でのモデルが下の図 1 である．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．
x_1～x_n:入力ビット．y_1～y_3:出力ビット．
u_1^i～u_m^i:箱の入力．v_1^i～v_m^i:箱の出力．i:左から何ステップ目の箱かを表す．

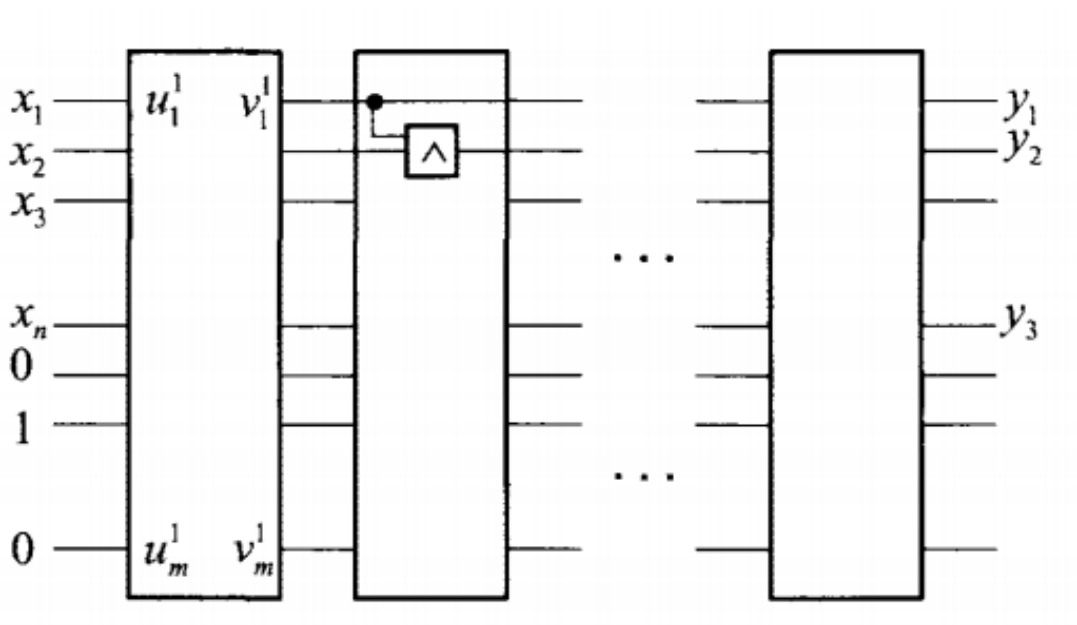


図 1　計算機のモデル

箱の入出力

箱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．$m = 2$ なら入出力の状態は $00, 01, 10, 11$．それぞれを縦ベクトル(状態ベクトルと呼ぶ)$(1,0,0,0)$,$(0,1,0,0)$,$(0,0,1,0)$,$(0,0,0,1)$ で表すことを仮定している．

図 2 の遷移行列について

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** だったとしたもの．

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

図 2　　$m = 2$ の時の遷移行列の例

図 2 の計算の例

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

図 3　　$m = 2$ の時の遷移行列の計算例 1

説明

この手法の長いところは，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．

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

図 4　　$m = 2$ の時の遷移行列の計算例 2

重ね合わせ状態

基礎

量子計算機のモデルも古典計算機のモデルと見かけ上は同じものを使用．古典計算ではレジスタの状態を 1 ビットの $0, 1$ 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．これを，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 $(1, 0)$ で，$|1\rangle$ は $(0, 1)$ である．

$$a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \tag{1}$$

a, b はそれぞれ $|0\rangle, |1\rangle$ の強さの比を表す係数（振幅）で以下を満たす．

$$|a|^2 + |b|^2 = 1 \tag{2}$$

ユニタリ変換

ユニタリ行列とは

ユニタリ行列 A とは $AA^\dagger = A^\dagger A = I$ を満たす行列.
$A^\dagger$ は A の共役転置行列，I は単位行列.

ユニタリ行列の性質

状態ベクトル u がユニタリ遷移行列 A によって v に変更されたとする.

$$v = Au \tag{3}$$

両辺に $A^\dagger$ を掛けると次のようになる.

$$u = A^\dagger v \tag{4}$$

つまり，計算が可逆

アダマール変換

アダマール変換とは

ユニタリ遷移行列の例の中でも最も重要なもの．1 ビットの状態に対しては以下のように表される．

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{5}$$

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

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

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

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

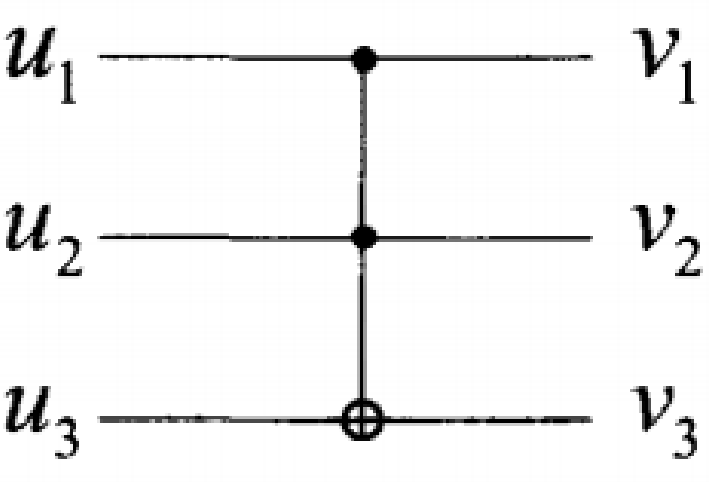
図 5　アダマール変換の例
（左 1 ビット，右 2 ビットの $|00\rangle$ に対して）

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

3 ビットの状態に対する 1 ステップの計算例

制御 NOT 素子

図 6 は，3 ビットの状態に対する 1 ステップの計算で，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．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 の状態を反転させる．
つまり，$|110\rangle$ と $|111\rangle$ はそれぞれ $|111\rangle$ と $|110\rangle$ になる．



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

図 6　制御 **NOT(3** ビット**)**

3 ビットの状態に対する 1 ステップの計算例（続き）

計算例

例えば以下のような式があったとする.

$$\frac{1}{2}|000\rangle + \frac{1}{2}|010\rangle + \frac{1}{2}|100\rangle + \frac{1}{2}|110\rangle = (\frac{1}{2}, 0, \frac{1}{2}, 0, \frac{1}{2}, 0, \frac{1}{2}, 0) \quad (6)$$

これを制御 **NOT** の遷移行列に掛けると次のようになる.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ \frac{1}{2} \\ 0 \\ 0 \\ \frac{1}{2} \end{bmatrix} \quad (7)$$

$$(\frac{1}{2}, 0, \frac{1}{2}, 0, \frac{1}{2}, 0, 0, \frac{1}{2}) = \frac{1}{2}|000\rangle + \frac{1}{2}|010\rangle + \frac{1}{2}|100\rangle + \frac{1}{2}|111\rangle \quad (8)$$

背景

図 7 の回路は，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．入力はすべて定数 $|0\rangle$.

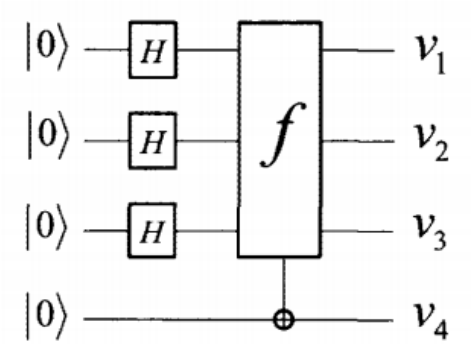


図 7　量子並列計算

f:3 変数の (古典の) 論理関数,H:アダマール変換,v_1〜v_4:出力

$$|000f(0,0,0)\rangle + |001f(0,0,1)\rangle + |010f(0,1,0)\rangle + |011f(0,1,1)\rangle$$
$$+|100f(1,0,0)\rangle + |101f(1,0,1)\rangle + |110f(1,1,0)\rangle + |111f(1,1,1)\rangle \quad (9)$$

この式は振幅 $\frac{1}{\sqrt{8}}$ は省略されている.

観測

観測方法

先ほどの式の出力は 8 通りの状態が混在．この 8 状態のいずれか 1 つがその状態の振幅の 2 乗の確率で得られる．

ジレンマ

1. ある NP 完全問題があったとする．
2. その NP 完全問題の答えがを導き出せる関数 f を使った計算を量子計算によってしたとする．
3. 「見るもの」を確率で選んでいる．
4. f についてすべて計算されているのに，重要な部分が見れない．
5. つまり，関数 f への割当ての 1 つをランダムに選んで解くのと同じ．

量子計算の優位性

ジレンマを乗り越える

次に 3 変数の論理関数 f を考える．ここで関数 f は f_0 か f_e のいずれかであることが分かっているとする．つまり，問題は今の関数が f_0 または f_e のいずれかであるかを判定することになる．
古典計算では 5 回以上関数値を評価する必要がある．
量子計算では図 8 の回路で解く．

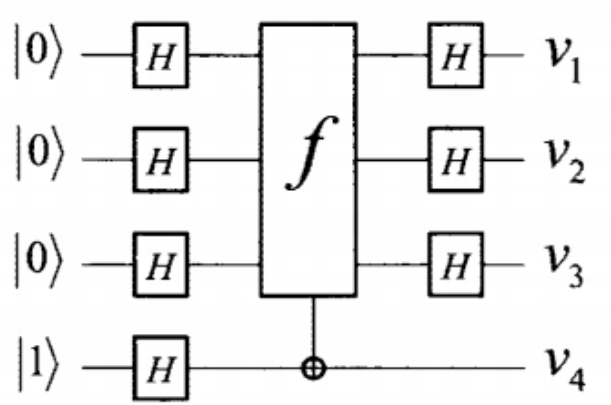


図 8　量子並列計算

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

量子計算の優位性 (続き)

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

左が関数 f_0，右が関数 f_e

$$|000\rangle(|0\rangle - |1\rangle) \quad \begin{aligned}&(|000\rangle + |001\rangle - |010\rangle - |011\rangle + |100\rangle - |101\rangle \\ &\quad - |110\rangle + |111\rangle)(|0\rangle - |1\rangle)\end{aligned}$$

遷移行列によって f_e の $|000\rangle$ は観測されなくなるので完全に分離できた．よって古典計算では 2^{n-1} 回の関数の評価が必要なところを量子計算では **1** 回でできる．

問題定義と古典計算の解答方法

問題定義

サイズ **1024** の配列があって，その各々に本のタイトルが順不同で入っているとする．そこで,「アルゴリズムサイエンス ー出口からの超入門ー」という本の配列のインデックスを求めたい.
これを前章と同じ論理関数の評価の問題に置き換えると，未知の n 変数論理関数 f 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になる．まず，$n = 2$ について議論する.

古典計算による解答方法

割当ては **00,01,10,11** の **4** 通りなので **4** 回評価すればいい.

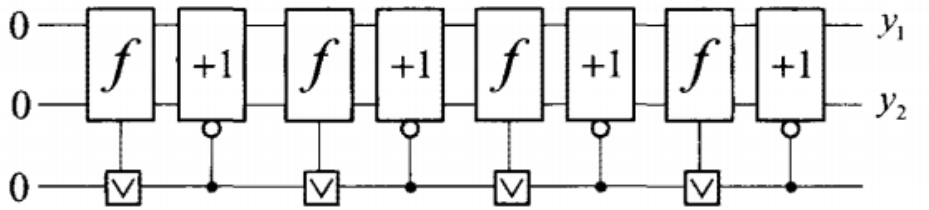


図 **9**　古典計算回路

量子計算の解答方法

素子の説明

X は否定素子で，$|0\rangle$ を $|1\rangle$ に，$|1\rangle$ を $|0\rangle$ にする．

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{10}$$

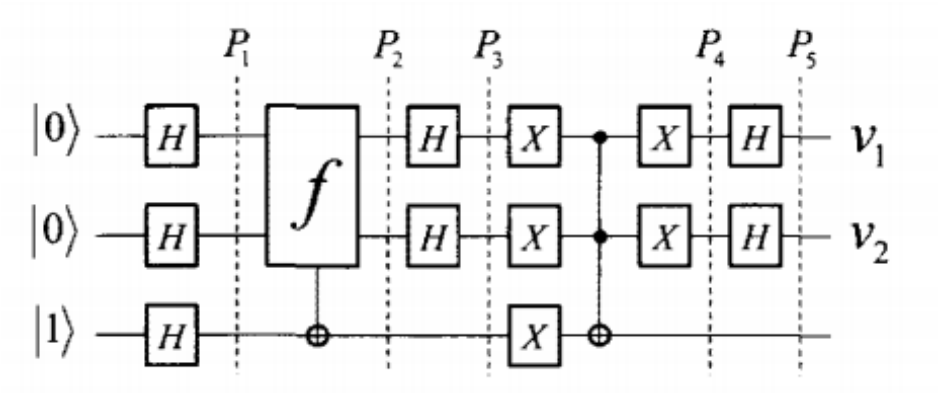


図 **10** 量子アルゴリズム

量子計算の解答方法

P_1 時点の状態は，$(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$，$P_2$ 時点の状態は，
$(-1)^{f(0,0)}|00\rangle + (-1)^{f(0,1)}|01\rangle + (-1)^{f(1,0)}|10\rangle + (-1)^{f(1,1)}|11\rangle$
$f(0,1) = 1$ でほかの割当てに対しては 0 とする．

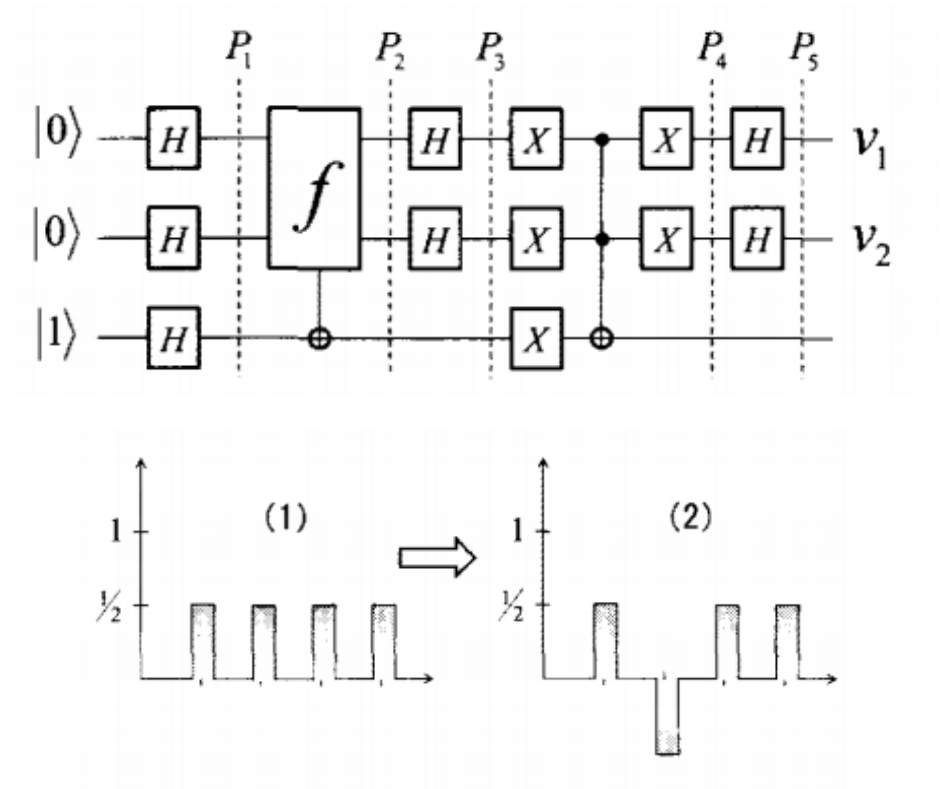


図 11　状態の変化 (1),(2)

量子計算の解答方法 (続き 2)

図 11 の分解して和で表したものが図 12

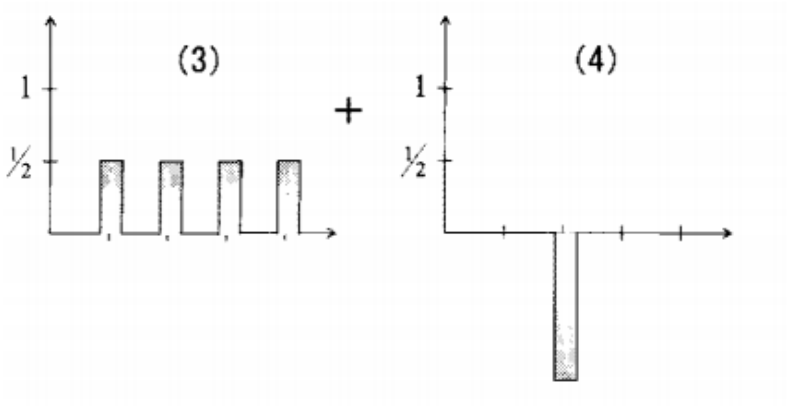


図 12　状態の変化 (3),(4)

P_3 時点の状態が図 13

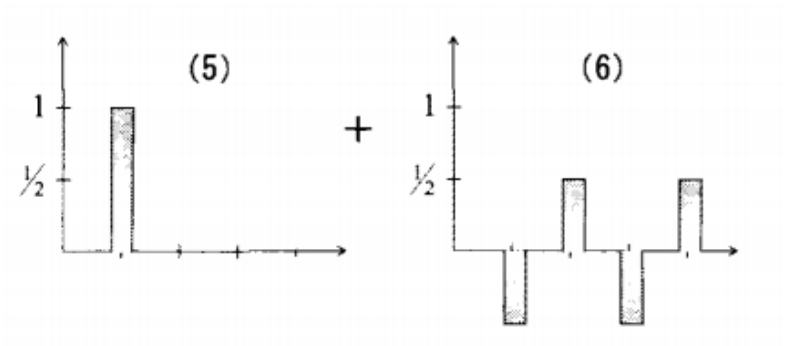


図 13　状態の変化 (5),(6)

量子計算の解答方法 (続き 3)

P_3 と P_4 の間の処理

P_3 の時点で $|00\rangle$ 以外の状態の時に振幅の正負を反転させる.

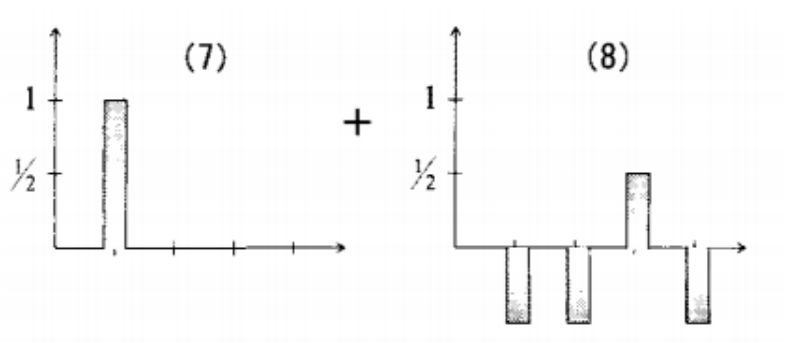


図 14　状態の変化 (7),(8)

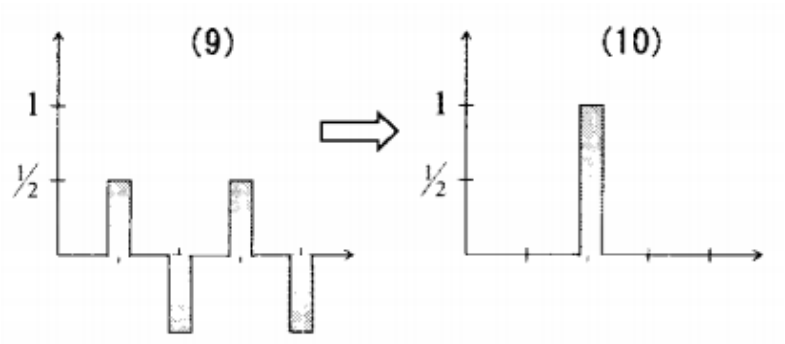


図 15　状態の変化 (9),(10)

一般の場合

グローバー探索

一般の n の場合にはこれほど簡単ではない．$N = 2^n$ 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というもの．

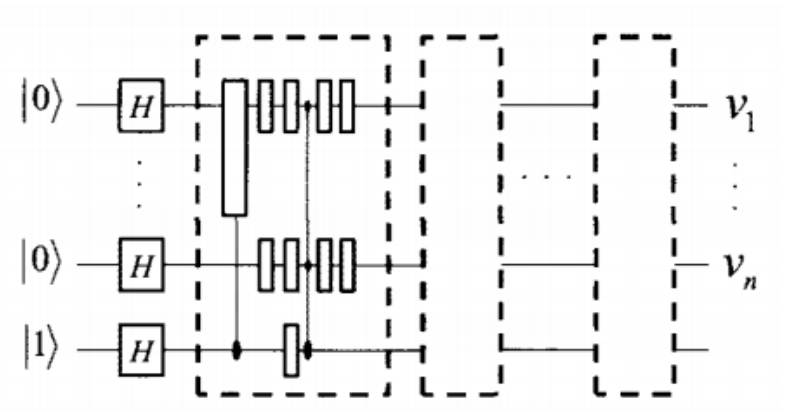


図 16　一般の場合の回路

一般の場合

グローバー探索

一般の n の場合にはこれほど簡単ではない．$N = 2^n$ 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というもの．

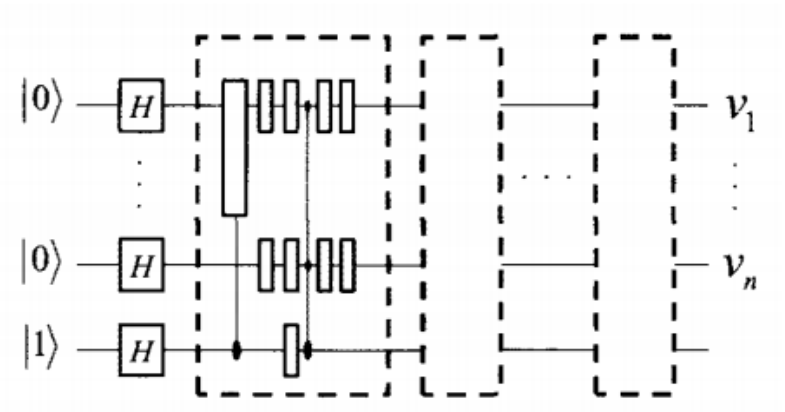


図 16　一般の場合の回路

一般の場合 (続き)

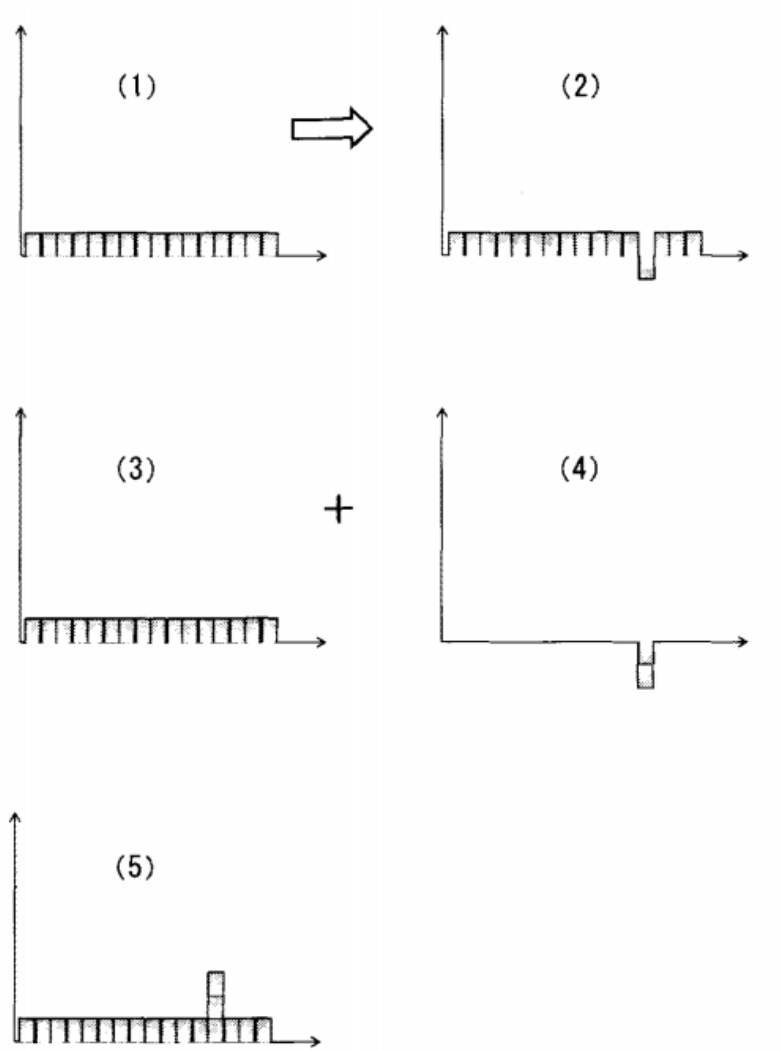


図 17　一般の場合の状態変化

量子ゲームのモデル

ゲームのモデル

扱うものはテレパシーゲーム．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．

ゲームの勝利条件

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 0 を出力し，違うものを提示されたときはともに 1 を出力することである．

古典戦略と量子戦略の比較

古典戦略の場合は，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 $1/2$ で勝利できる．量子戦略の場合は，ある 0 と 1 の乱数列 $r_1, \cdots, r_m$ を生成し，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．

CHSH ゲーム

CHSH ゲーム

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．古典戦略の場合は無条件に 0 を出力することで $3/4$ で勝てる．

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

今までの量子状態の観測の補足

1 ビットの状態の $a|0\rangle + b|1\rangle$ を観測したときには，確率 $|a|^2$ で状態 $|0\rangle$，確率 $|b|^2$ で状態 $|1\rangle$ が得られる．

量子観測の変更

観測する時にすること

観測する時は，必ず直交する規定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．

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

直交する規定を上のように取った場合に状態 $|0\rangle$ を観測すると，次のように書ける．

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

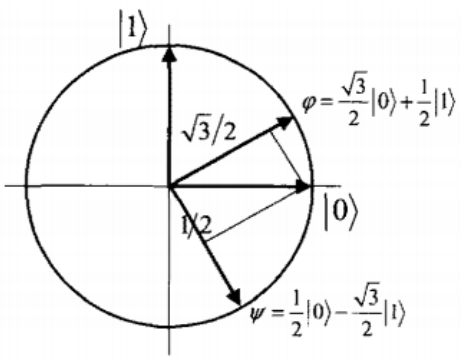


図 18　直交基底

一般の場合

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \quad \frac{a}{\sqrt{|a|^2+|b|^2}}|0\rangle|0\rangle + \frac{b}{\sqrt{|a|^2+|b|^2}}|0\rangle|1\rangle$$

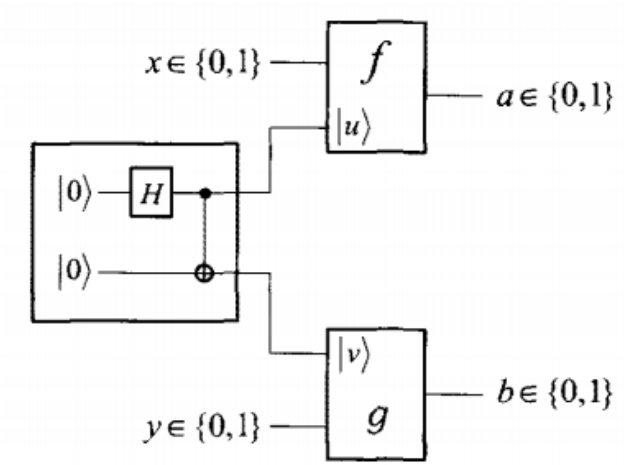


図 19　CHSH ゲームの量子戦略

量子戦略

この戦略回路から得られる 2 ビット $|u\rangle, |v\rangle$ の状態は $|00\rangle + |11\rangle$ である.

太郎の解答

$x = 0$ の場合

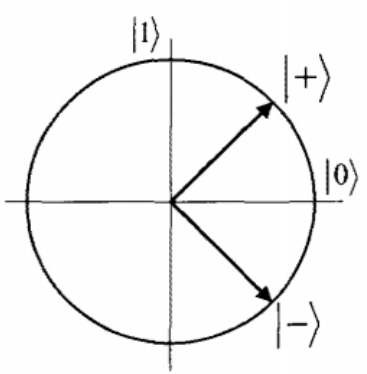
$x = 0$ の場合はビット $|u\rangle$ を通常の $(|0\rangle, |1\rangle)$ 基底で観測する．状態 $|0\rangle$ が得られれば 0 を出力し，$|1\rangle$ が得られれば 1 を出力する．

$x = 1$ の場合

$|u\rangle$ を $(|+\rangle, |-\rangle)$ 基底で観測する．

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

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．



花子の解答 $y = 1$

$y = 1$ の場合

$y = 1$ の場合は b の値は図のようになる．0.85 の確率で成功する．

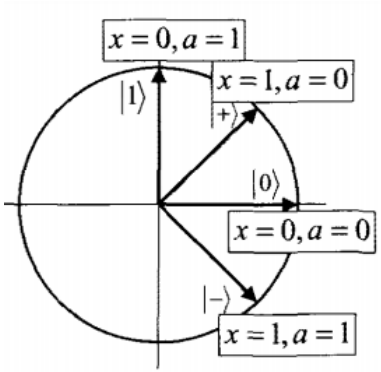


図 14　花子の $|v\rangle$ 状態

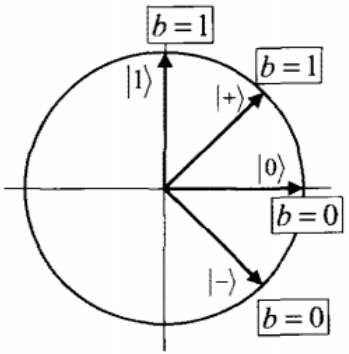
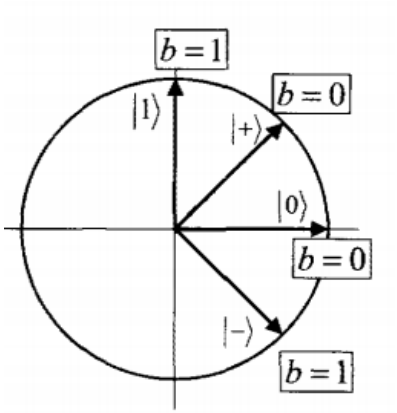


図 15　花子の必要な情報

花子の解答 $y = 0$

$y = 0$ の場合

0.85 の確率で成功する．太郎と花子は通信をしている訳ではないのに古典計算の確率 0.75 よりも 0.1 も高くなっている．であるから，テレパシーができているのではないかと言える



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．

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．