

# 量子情報処理へ向けた表計算プログラミング

伊集院 八郎 (近畿大学 産業理工学部)

量子重ね合わせや量子もつれなどの量子情報に特有な性質を理解しやすくするために、表計算ソフト上で簡単に量子計算をシミュレーションできるようにした。いろいろな量子計算に加えて、量子離散フーリエ変換や量子テレポーテーションを、わずかな操作で簡単にシミュレーションすることができる。

## Programming on the Spreadsheets toward Quantum Information Processing

Hachiro Ijuin (Faculty of Humanity-Oriented Science and Engineering, Kinki Univ.)

### Abstract

The simulation of quantum computation has been able to be carried out easily on the spreadsheets to make the property understandable peculiar to quantum information such as the quantum superposition and entanglement. In addition to the various quantum calculations, quantum discrete Fourier transform and the quantum teleportation would be simulated easily in the slight operation.

キーワード：表計算、量子情報、量子計算、量子離散フーリエ変換

( Spreadsheets, Quantum Information, Quantum Computation, Quantum Discrete Fourier Transform)

### 1. はじめに

量子物理と情報理論という異質の分野を土台にする量子情報は、多くの新しい概念を含み、全く新しい処理方法をとることから、その本質をとらえることが難しいとされている。また、その対象範囲は量子計算から量子情報通信まで多岐にわたっている。量子計算においては、計算の基底となる二つの状態だけでなく、その重ね合わせ状態が扱われるので、超並列計算が可能になる。量子状態はその複製が不可能なことから、量子通信において盗聴があればならずそれを検出できるので、安全な鍵配送が可能になる。送信側と受信側が量子もつれの状態を共有できれば、送信側で載せた情報を受診側へ量子テレポーテーションによって送ることができる。このような量子情報の重要な応用に関し、いつでもどこでもほとんど誰もが使える表計算ソフト上でシミュレーションすることを考えた。そのためには、まず、複素数やベクトルあるいは行列を不自由なく扱えるように表計算ソフトの機能を拡張した。

特に複素要素の行列計算を無理なく行えるようにすることが上記のシミュレーションを遂行するうえで不可欠である。次に、単一の量子ビットの状態をいわゆるブロッホ球によって可視化できるようにし、任意の重ね合わせ状態をとれるようにした。この状態に、量子計算の基本となるユニタリ変換を行なって新たな状態を求め、計算結果を示す別のブロッホ球に反映させられるようにした。ここでの1量子ビットのユニタリゲートと共に万能ゲートを構成する制御 NOT ゲートを2量子ビットに作用させて量子もつれの状態も実現できるようにした。量子暗号配送は1量子ビットによって実現でき、2量子ビットに拡張することによって量子離散フーリエ変換を、さらに3量子ビットに拡張することによって量子テレポーテーションを可能にした。そのほかにもいろいろな量子ゲートを配した量子回路に対する量子計算を実行可能にして、広く量子情報の処理および量子情報通信の原理や量子アルゴリズムの理解に役立てられるようにした。

## 2. 表計算ソフト上での複素行列の処理

表計算ソフトにおいて、行方向や列方向へならぶ一連のデータはベクトルや行列の要素と見ることができ、ベクトルの内積は、関数 SUMPRODUCT の引数に、行方向にならぶ一連のデータの二組みあるいは列方向にならぶ一連のデータの二組みを指定して任意のセルに結果を求めることができる。また、行列式の値は、その値を得るために用意された関数 MDETERM の引数に、正方行列の要素を囲うようにセル範囲を指定して与えれば求められる。しかしながら、それらに何らかの演算を施した結果がベクトルや行列となるときには、それをいわゆる配列数式として求めなければならない。たとえば、結果を求めるセル範囲をあらかじめ選択し、その状態で数式入力バーに必要な数式を入力後に、Shift キーと Ctrl キーを押したまま Enter キーを押すといった操作を行う。

	A	B	C	D
1	1	2	3	
2	4	5	6	
3	7	8	9	
4				
5	行ベクトルの内積		列ベクトルの内積	
6	=SUMPRODUCT(A1:C1,A2:C2)		=SUMPRODUCT(A1:A3,B1:B3)	
7	32		78	
8				
9	2×2行列の行列式		3×3行列の行列式	
10	=MDETERM(A1:B2)		=MDETERM(A1:B2)	
11	-3		6.66134E-16	
12				
13	ベクトルのスカラー倍	ベクトルの和と差	行列とベクトルの積	行列とベクトルの積
14	=10*C1:C3	=A1:A3+B1:B3-C1:C3	=MMULT(A1:B2,C1:C2)	=MMULT(A1:C3,A1:A3)
15	30	0	15	30
16	60	3	42	66
17	90	6		102
18				
19	行列と行列の積		行列の逆行列	
20	=MMULT(A1:B2,B2:C3)		=MINVERSE(A1:B2)	
21	21	24	-1.666666667	0.666666667
22	60	69	1.333333333	-0.333333333

図1 表計算ソフト上でのベクトルと行列の計算

図1には、ベクトルと行列に関するいろいろな演算結果を求める例を示している。幾種類か示された例のうち、セル範囲 B15:B17 には、ベクトルの加減算の結果が配列数式として示されている。このセル範囲に入力した数式を示すために、その直上のセル B14 には数式=A1:A3+B1:B3-C1:C3 を文字データにして格納してある。他の例も同様に示され、ベクトルのスカラー倍、2×2行列や3×3行列と列ベクトルの積、2×2行列どうしの積、2×2行列の逆行列などが求められている。ただし、3×3行列の行列式の値だけは、0で

あるべきところにきわめて小さな数値が示されている。図2では、すべての要素が $1/\sqrt{2}$ （ただし2行2列成分のみが負符号がつく）となるアダマール行列の要素をセル範囲 A1:B2 および A4:B5 におき、その行列によるセル範囲 D1:D2 および D4:D5 に要素をおいた基本ベクトルの変換例をF列に示している。

	A	B	C	D	E	F
1	0.707107	0.707107		1		0.707107
2	0.707107	-0.70711		0		0.707107
3						
4	0.707107	0.707107		0		0.707107
5	0.707107	-0.70711		1		-0.70711

図2 アダマール行列による基本ベクトルの変換

一方、表計算ソフトでは複素数も扱うことができる。そのセルへの入力、実部が  $a$  で虚部が  $b$  の複素数  $a+bi$  であれば、シングルクオート「'」を先頭に置いた ' $a+bi$ ' の形で入力する。あるいは、複素数を生成する関数を使用して数式 =COMPLEX(  $a$ ,  $b$  ) を入力する。複素数の四則演算には、+、-、\*、/ などの演算記号は使用できず、和、差、積、商のための関数 IMSUM, IMSUB, IMPRODUCT, IMDIV を使わなければならない。複素数を引数にできる関数には、上記のほかに IMABS, IMAGINARY, IMARGUMENT, IMCONJUGATE, IMCOS, IMEXP, IMLN, IMLOG10, IMLOG2, IMPOWER, IMREAL, IMSIN, IMSQRT などがある(1)。

量子計算では状態ベクトルのユニタリ変換が基本になる。状態ベクトルもユニタリ行列も一般には複素数要素になるので、表計算ソフト上での量子計算を考える場合には、複素数要素のベクトルや行列の演算が不自由なく行えなければならない。表計算ソフトには、必要な演算や処理を行うための関数を用意する機能があるので、これを利用すれば複素数要素のベクトルや行列の和や積のほか、テンソル積など量子計算で多用される演算のための関数を追加できる(2)。図1のアダマール行列は実数値行列なので、表計算ソフトにあらかじめ用意されている関数 MMULT を用いて基本ベクトルとの積を求めているが、これを新たに用意した複素行列用の関数 MATMUL を用いても同じ結果が得られる。

### 3. 量子状態と量子ビット

古典ビットを 0 と 1 の 2 状態を表すことに対応させて、量子計算の計算基底にも二つの状態を考える。それぞれを 2 次元の複素ヒルベルト空間のベクトル  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$

および  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  で表し、状態  $|0\rangle$  および状態  $|1\rangle$  とも表記する。

ただし、量子ビットには、二つの基底状態の重ね合わせ、つまり、複素係数  $\alpha$  と  $\beta$  (ただし、 $\alpha^2 + \beta^2 = 1$ ) に対し、 $\alpha|0\rangle + \beta|1\rangle$  と表される状態も含まれる (3) (4)。それゆえ、単一量子ビットの量子状態には無数の状態が存在することになり、古典ビットの単位 bit に対し、量子ビットは qubit をその単位とする。この 1 qubit の量子状態を視覚的に表現するには、図 3 に示されるブロッホ球がよく用いられる (5)。これは 3 次元座標空間の座標原点を中心とする半径 1 の球で、座標原点から球面上の点  $(x, y, z)$  に向かうベクトルによって 1 qubit の量子状態を表す。このベクトルはブロッホベクトルといい、量子状態を表すベクトル  $\begin{pmatrix} \sqrt{\frac{z+1}{2}} \\ \frac{x+iy}{\sqrt{2(z+1)}} \end{pmatrix}$  に

対応する。ここで、 $i = \sqrt{-1}$  であり、 $z = -1$  のとき  $\sqrt{\frac{x+iy}{2(z+1)}} = 1$  とする。ただし、全体にかかる位相因子は

観測上区別できないことから、状態  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  にかかる係数

$\sqrt{\frac{z+1}{2}}$  を非負の実数としている。

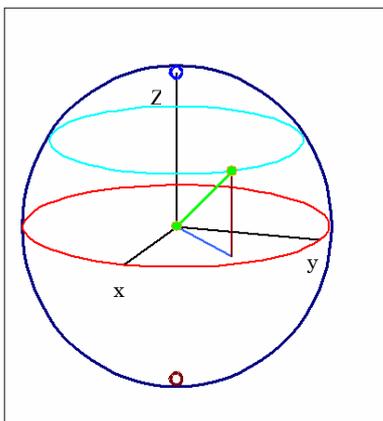


図 3 ブロッホ球

それゆえ、ブロッホベクトル  $(0, 0, 1)$  および  $(0, 0, -1)$  がそれぞれ状態  $|0\rangle$  および状態  $|1\rangle$  を表すことになる。また、z 軸から測る角度を  $\theta$ 、x-y 平面で x 軸から y 軸の方向へ図る角度を  $\varphi$  とすれば、

$$x = \cos \varphi \sin \theta, y = \sin \varphi \sin \theta, z = \cos \theta$$

であるから、1 qubit の単一量子状態を

$$\cos\left(\frac{\theta}{2}\right)\begin{pmatrix} 1 \\ 0 \end{pmatrix} + e^{j\varphi} \sin\left(\frac{\theta}{2}\right)\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (1)$$

とも表せる。ブロッホ球を地球儀に見立てると、量子計算の基底ベクトルの  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  および  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  は、それぞれが北極および南極を向くベクトルになる。また、 $\theta = \pi/2$

のときのベクトルは

$$\cos\left(\frac{\pi}{4}\right) = \cos\left(\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}} \text{ より、} \\ \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + e^{j\varphi} \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (2)$$

となり、赤道面内のベクトルになる。

	A	B	C	D	E	F	G	H	I	J
1										
2								th	phi	
3		0.349066	2.873793	0						eR
4		20	165	0				2.164208	5.480334	3
5										
6	0	1	PauliXNC	0.469472	0		0.469471562785891			
7	1	0		0.613347	-0.53514		0.61334636056076	-0.535139345156634i		
8										
9								rx	ry	
10		cos0	sin0	cos1	sin1	cos2	sin2		81	81
11	0	12.63839	20.58153	17.3162	-19.3416	17.31634	67.08137	0	121	40
12	1	28.86619	19.53434	30.76965	-20.2087	30.76971	66.21322	0.165347	119.8953	53.23216
13	29	-2.39258	22.47892	4.85496	-17.7685	4.855183	68.65437	4.795062	46.68893	-40.7233
14	30	12.63949	20.58142	17.31711	-19.3416	17.31726	67.08129	4.960409	59.88432	-38.5214
41		赤道面(z軸)		緯線(系列5)		緯線(系列6)		5.125756	72.53733	-34.1776
42		系列9(z軸)		系列9(緯線)		系列9(緯線)		5.291103	84.3028	-27.8105
44	cXY	40	40	40	40	40	40	5.45645	94.85981	-19.5936
45	cXY	40	117.2741	-20.5891	33.01786	69.07391	24.57147	5.621797	103.9204	-9.75123
46								5.787144	111.2374	1.448261
47		系列3(z軸)		系列10(緯線)		系列10(緯線)		5.952491	116.6112	13.6934
48	cXY	40	40	-20.5891	-10.193	69.07391	67.78342	6.117838	119.8953	26.66784
49	cXY	12.63839	20.54283	-20.5891	33.01786	69.07391	24.57147	6.283185	121	40
50										ブロッホ球(系列1)
51		系列4(z軸)		系列11(ブロッホ球)		系列11(ブロッホ球)				
52	cXY	40	40	40	40	40	40			
53	cXY	115.1755	32.91808	-20.5891	-10.193	69.07391	67.78342			

図 4 ブロッホ球を構成する Excel シート

図 4 には、ブロッホ球を描くための表計算ソフト Excel のシートを示している。セル範囲 B2:D4 には、ブロッホ球を見る視点を決める角度  $\alpha$ 、 $\beta$ 、 $\gamma$  を調整するためのスクロールバーと、その示す度数法および弧度法による角度を表示している。その右のセル範囲 H2:I4 には、(1) 式の  $\theta$ 、 $\varphi$  を変えるためのスクロールバーとそれが与える角度が表示されている。ブロッホ球は、入力量子ビット用と出力量子ビット用の二つ

を考慮するので、それぞれの球に共通な球の外郭および赤道面描画用データ（実際は円と楕円を描画）が、セル範囲 I11:J49 および B11:C41 に置かれている。セル範囲 D11:E41 および F11:G41 には、それぞれの球のブロッホベクトルの終点を通る緯線描画用データがある。 $x, y, z$  の座標軸用の描画データは、それぞれセル範囲 B48:C49、B52:C53 および B44:C45 に置かれている。ブロッホベクトルに対しては、それを描くためと、その終点から赤道面に下ろした垂線およびその足と原点を結ぶ線を描画するためのデータが、入力量子ビット用にセル範囲 D52:E53、D48:E49、D44:E45 に置かれ、出力量子ビット用にはセル範囲 F52:G53、F48:G49、F44:G45 に置かれている。他に、両極を示すためのデータもあるが、図には示されていない。

#### 4. 単一量子ビット状態とその変換

計算の基本モデルには、よくチューリングマシンがとりあげられる。それには決定論的なものだけでなく、確率論的なものも含まれ、いずれにも古典モデルと量子モデルが提唱されている。さらに、より具体的なものとして計算の回路モデルがある。回路はゲートを回線で結んで構成される。古典ゲートは、ブール代数演算を行うものとして、基本のものがいくつかある。たとえば、論理の和や積あるいは否定を演算するものとして、それぞれ OR、AND、NOT などの基本的なゲートがある。さらに、これらを組み合わせて論理の和や積の否定あるいは排他的論理和などの演算を行うゲートがある。ゲートへの入力を二方向に分岐（FUNOUT）できれば、NOT ゲートを NAND ゲートで構成できる。それゆえ、これらの組み合わせで、AND ほかの任意のゲートが構成できるので、FUNOUT と NAND ゲートは万能ゲートを構成する組みになっている。

一方、量子計算の回路モデルでは、量子状態をユニタリ変換するものとしてゲートを考える。状態を反転する NOT ゲートは、基底ベクトル  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  と  $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$  を互いに交換することから、このゲートにはユニタリ行列  $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  が対応する。単一量子ビットに対する量子ゲートとし

ての NOT ゲートは、ブロッホ球の  $x$  軸の周りの回転に関係している。つまり、NOT ゲートのユニタリ行列はパウリの  $x$  行列であるから  $\sigma_x$  と表し、 $2 \times 2$  単位行列を  $I$  とすれば、 $x$  軸の周りの角度  $\delta$  の回転は、

$$\cos \frac{\delta}{2} I - i \sin \frac{\delta}{2} \sigma_x \quad (3)$$

と表される。同様に、 $y$  軸や  $z$  軸の周りの角度  $\delta$  の回転は、パウリの  $y$  行列  $\sigma_y$  と  $z$  行列  $\sigma_z$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (4)$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (5)$$

を用いて、

$$\cos \frac{\delta}{2} I - i \sin \frac{\delta}{2} \sigma_y \quad (6)$$

$$\cos \frac{\delta}{2} I - i \sin \frac{\delta}{2} \sigma_z \quad (7)$$

と示される行列によってなされる (3) (6)。

	A	B	C	D	E	F	G	
1	$\alpha =$	0.523599	$\beta =$	1.047198	$\gamma =$	1.570796		
2		0.965926	-0.258819	0.866025	-0.5	0.7071067	0	
3		-0.258819	0.965926	0.5	0.866025	0	0.7071067	
4								
5		0.866025	-0.5	0.965926	-0.258819	0.8365163	-0.482962	
6		0.5	0.866025	-0.258819	0.965926	0.4829629	0.8365163	
7								
8		0.7071067	0	0.8365163	-0.482962	0.6830127	-0.5+0.183	
9		0	0.7071067	0.4829629	0.8365163	0.5+0.183	0.6830127	
10								
11		1	→	0.965926	→	0.8365163	→	0.6830127
12		0	→	-0.258819	→	0.4829629	→	0.5+0.183
13		$x$ 軸の周りの90°の回転		$y$ 軸の周りの60°の回転		$z$ 軸の周りの90°の回転		
14		0	→	-0.258819	→	-0.482962	→	-0.5+0.183
15		1	→	0.965926	→	0.8365163	→	0.6830127

図5 軸の周りの回転行列による変換

図5は、セル範囲 A1:B2、C1:D2、E1:F2 に、 $x$  軸の周りに  $\pi/6$ 、 $y$  軸の周りに  $\pi/3$ 、 $z$  軸の周りに  $\pi/2$  の回転を行う行列を配置し、互いに掛けていくことにより、基本のベクトルがどのように変換されるのかを示している。

図2のアダマール行列による基本ベクトルの変換は、単一量子ビット状態が基底の状態にある場合の変換も表している。この図の上半分に示される変換をブロッホ球で見ると、図6のようになる。左の球が入力状態

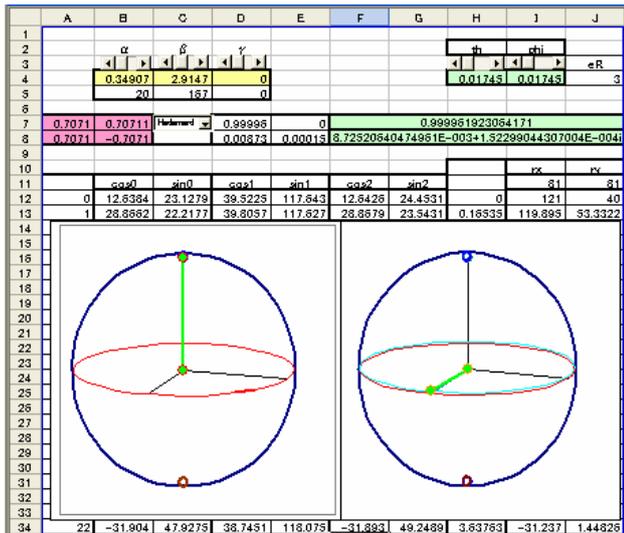


図6 基底状態のアダマール変換

を示し、ブロッホベクトルは北極（z 軸方向）を向いている。右の球が出力状態を示し、ブロッホベクトルは x 軸方向を向いている。この例は、一つの基底の状態が二つの基底状態の重ね合わさった状態になることを示している。

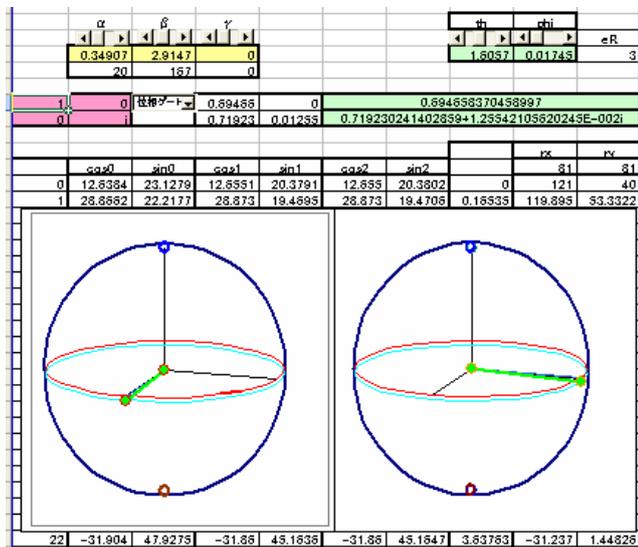


図7 アダマール変換後の位相変換

(1)式で与えられる任意の単一量子ビットの状態に、

複素行列  $\begin{pmatrix} 1 & 0 \\ 0 & e^{i\gamma} \end{pmatrix}$  を作用させると、明らかに状態

$$\cos\left(\frac{\theta}{2}\right)\begin{pmatrix} 1 \\ 0 \end{pmatrix} + e^{j(\varphi+\gamma)}\sin\left(\frac{\theta}{2}\right)\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (8)$$

に変わる。ここで、 $\gamma = \pi/2$  とすると、 $2 \times 2$  単位行列の 2 行 2 列成分だけを虚数単位とする行列が得られる。図 6 のアダマール変換後にこの位相変換行列によって状態に移した例を図 7 に示している。

### 5. 二量子ビット状態とその変換

2 qubit の二量子ビット状態は、二つの単一量子ビット状態の混合状態で、状態  $|00\rangle$ 、 $|01\rangle$ 、 $|10\rangle$ 、 $|11\rangle$  からなる。ただし、 $|ij\rangle$  はテンソル積  $|i\rangle \otimes |j\rangle$  を表すので、テンソル積を実行すれば

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

となる。2 量子ビット状態  $|00\rangle$ 、 $|01\rangle$ 、 $|10\rangle$ 、 $|11\rangle$  に対し、状態  $|00\rangle$  と  $|01\rangle$  は変えず、 $|10\rangle$  と  $|11\rangle$  を互いに交換

するユニタリ行列は、 $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$  になる。つまり、

二つの量子ビットの一方の状態が  $|1\rangle$  のときのみ他方を反転させる二量子ビットの排他的論理和を与えるものになる。二つの量子ビットの一方を制御ビット、他方を標的ビットといい、この変換を行うゲートを制御 NOT ゲートといい、単一量子ビットのユニタリ行列とで量子万能ゲートを構成することができる。

	A	B	C	D	E	F	G	H	
1	計算基底		2qubitゲート						
3	☒	1	0	1	0	0	0	0	
4			1	0	1	0	0	1	
5	☒	1	0	0	0	0	1	1	
6			1	0	0	1	0	0	
7		0	0						
8		1	0						
9		2	0						
10		3	1						

図8 2qubit の量子計算の例 (CNOT)

図 8 は、2 qubit の量子計算の例として、制御 NOT による基底状態の変換を示している。A 列のチェックボックスは、状態  $|0\rangle$  または  $|1\rangle$  を簡単に切り替えられ

るようにするためのものである。セル範囲 C7:C10 には、選ばれた計算基底のテンソル積を求めている。さらに、セル範囲 D3:G6 に置いた 2 qubit に対する CNOT ゲートによる変換を H 列に求めている。

計算基底	1qubitゲート	2qubitゲート
0	0	1 0 0 0
1	0.707107 0.707107	0 1 0 0
2	0.707107 -0.707111	0 0 1 0
3	0	1 0 0 1

図9 量子もつれの例  
(アダマールゲートと CNOT ゲート)

図8に示す制御 NOT ゲートは、2 qubit に作用し、基底の状態を変換するものであったが、重ね合わさった状態に作用するときには、図9に示すような量子もつれが現れる。つまり、アダマールゲートによって重ね合わせの状態を作り、続いてそれを制御ビットとした制御 NOT ゲートを作用させると、結果の状態は

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (9)$$

となって、もはや基底状態のテンソル積に分解できない。この状態は、2 qubit の状態の一方が決まれば他方も決まるという互いにもつれた状態になっている。

二量子ビットに作用するゲートとして、他に制御位相ゲートがある。これは、図10に示されるように、制御ビットの状態が  $|1\rangle$  のときのみ標的ビットを位相ゲートで変換する。

計算基底	1qubitゲート	2qubitゲート
0	0	1 0 0 0
1	0	0 1 0 0
2	0.707107 0.707107	0 0 1 0
3	0.707107 -0.707111	0 0 0 1

図10 制御位相ゲートによる変換

量子計算は、計算量的に解くことの難しい大きな数の素因数分解を、短時間で解くことのできる量子アルゴリズムが発表されたことにより、大きく注目される

ようになった。その核心は、ある数  $N$  と互いに素でそれより小さい数  $x$  の  $r$  乗  $x^r$  を  $N$  で割った剰余の列に周期性があり、その周期を量子離散フーリエ変換によって素早く求めることができることである。

図11は、整数  $N$  を 35 として、これと互いに素となる数  $x$  を 2, 3, 4 などを選び、その  $r$  乗 ( $r=0, 1, 2, \dots$ ) を  $N$  で割った余りを順番に並べた表と、この表の  $x = 2, 3$  に対する余りをグラフ表示したものである。周期性とその周期が明らかにされている。ここで、余りが 1 となる最小の正の整数は  $r=12$  である。 $x = 2$  に対しては、 $x^{r/2} - 1 = 63$  なので、これと  $N = 35$  との最大公約数は 7 になる。一方、 $x^{r/2} + 1 = 65$  なので、これと  $N = 35$  との最大公約数は 5 になる。よって 35 は 5 と 7 を因数に持つことになる。同様に、 $x = 3$  に対しては、728 と 35 の最大公約数から 7、730 と 35 の最大公約数から 5 が共に 35 の約数として求まる。

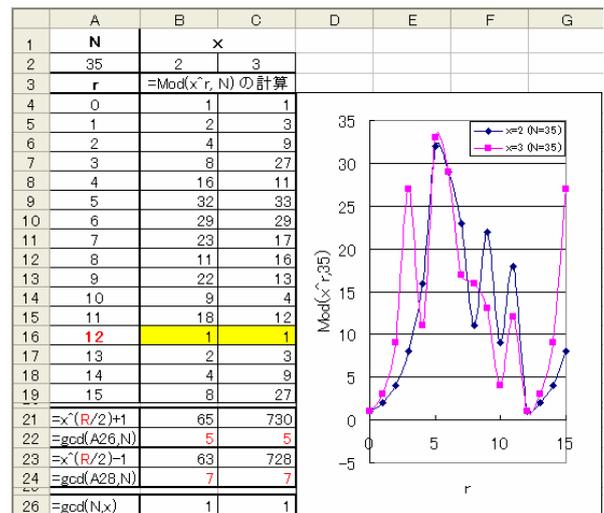


図11 整数  $N$  と互いに素でそれより小さい数  $x$  の  $r$  乗を  $N$  で割った剰余

$s$  キュービットの量子系には  $M = 2^s$  の異なる量子状態が含まれるので、このような系の量子離散フーリエ変換は、

$$|j\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{2\pi i j k / M} |k\rangle \quad (10)$$

となる(6)。  $j=0,1$  の 1 qubit の基底状態に対しこれはアダマール変換を表している。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	計算基底	1qubitゲート									1qubitゲート			
3	0	1				1	0	0	0	0	0.7071068	0.7071068	0.7071068	0.7071068
4	0	0				0	1	0	0	0	0.7071068	-0.707107	0.7071068	0.7071068
5	0	1	0.707107	0.707107	0.7071067	0	0	1	0	0.70710678118				0.707106781186547
6	0	0	0.707107	-0.70711	0.7071067	0	0	0	0	0.70710678118				0.707106781186547
7	0	0	1			0.7071067								0.4899999999999999
8	2	1	0			0.7071067								0.4899999999999999
9	1	2	0			0								0.4899999999999999
10	3	3	0			0								0.4899999999999999
12	0	1				0	1	0	0	0	0.7071068	0.7071068	0.7071068	0.7071068
13	1	1				1	0	1	0	1	0.7071068	-0.707107	-0.7071068	0.7071068
14	0	1	0.707107	0.707107	0.7071067	0	0	1	0	0.70710678118				0.707106781186547
15	0	0	0.707107	-0.70711	0.7071067	0	0	0	0	0.70710678118				0.707106781186547
16	0	0	0			0								0.4899999999999999
17	2	1	1			0.7071067								-0.4899999999999999
18	1	2	0			0								0.4899999999999999
19	3	3	0			0.7071067								-0.4899999999999999
21	0	1				1	1	0	0	0	0.7071068	0.7071068	0.7071068	0.7071068
22	1	1				0	0	1	0	0	0.7071068	-0.707107	-0.7071068	0.7071068
23	0	1	0.707107	0.707107	0.7071067	0	0	1	0	0.70710678118				0.707106781186547
24	1	1	0.707107	-0.70711	-0.707106	0	0	0	0	-0.70710678118				-0.707106781186547
25	0	0	0			0.7071067								0.4899999999999999
26	2	1	0			-0.707106								0.4899999999999999
27	1	2	0			0								-0.4899999999999999
28	3	3	0			0								-0.4899999999999999
30	0	1				0	1	0	0	0	0.7071068	0.7071068	0.7071068	0.7071068
31	1	1				1	0	1	0	1	0.7071068	-0.707107	-0.7071068	0.7071068
32	0	1	0.707107	0.707107	0.7071067	0	0	1	0	0.70710678118				0.707106781186547
33	1	1	0.707107	-0.70711	-0.707106	0	0	0	0	-0.70710678118				-0.707106781186547
34	0	0	0			0								0.4899999999999999
35	2	1	0			0.7071067								-0.4899999999999999
36	1	2	0			0								0.4899999999999999
37	3	3	1			-0.707106								-0.4899999999999999

図12 二量子ビットの量子離散フーリエ変換

図12は、アダマール変換、位相変換、アダマール変換をこの順に、二量子ビットの基底の状態に作用させた結果である。得られた結果にビット反転操作をすれば、

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

$$|01\rangle \rightarrow \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle) \quad (12)$$

$$|10\rangle \rightarrow \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \quad (13)$$

$$|11\rangle \rightarrow \frac{1}{2}(|00\rangle - i|01\rangle - |10\rangle + i|11\rangle) \quad (14)$$

となる。これは、二量子ビットの状態に対し、式(10)を計算したものと同一結果を与えるので、図12によって二量子ビットの量子離散フーリエ変換がなされていることがわかる。

## 6. 多キュービット量子状態とその変換

三量子ビット以上の量子系に対しても、一般の量子計算だけでなく、量子離散フーリエ変換を拡張できる。ここでは、三量子ビットの系で実現できる量子テレポーテーションを考える。量子情報通信における量子計算は、送る側の情報を受ける側に移す恒等変換といえる。ただし非クローン化定理の制約があるので、この制約内での変換になる。実際の量子テレポーテーションは、送信側の測定系に関する情報を古典通信路を通

して伝える必要があるため、光速以上の通信速度は得られず、量子系のみでは構成できないことになる。それでも以下のような量子回路は、量子テレポーテーションの原理を理解する助けになる。

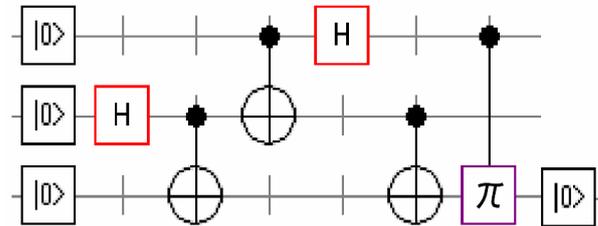


図13 量子テレポーテーション理解のための量子回路

図13は、上段が送信信号、中段は送信側、下段は受信側のそれぞれの状態に関わる配線と見ることができる。まず、送受信双方の重ね合わせの状態から量子もつれの状態をつくり、続いて送信側と送信信号の間に量子もつれの状態を生じさせて、以後は受信側での受信のための手順を踏んでいく流れになっている。表計算ソフトでは、送受信側を基底状態にして送信情報を準備したあと、これまでのフーリエ変換などと同様の必用な変換を、各段階ごとに施していくことになる。

図14 量子テレポーテーション理解のための表計算

図14は、三量子ビットの系で構成する量子テレポーテーションを理解するための量子回路を表計算ソフトで表現し、量子テレポーテーションのシミュレーション

ョンが行えるようにしたものである。途中で重ね合せや量子もつれの状態がありながら、最終的には受信側に送信情報が現れている。この量子回路は、量子計算の結果を読み出すときの観測法にも深く関連している。

## 7. 検討とまとめ

集積回路の配線や部品のサイズがナノスケールオーダーになると、量子効果が顕在化するようになり、大概はそれが特性に悪影響を及ぼす。しかしながら、開き直ってその量子効果を積極的に利用することにすれば、むしろ全く新しい物理法則による優れた特性が導かれる例も増えている。その大きな可能性が量子物理と情報理論に支えられる量子情報や量子情報通信の分野に見出され、大きな広がりを見せ始めたといえる。しかしながらこの異質の分野の融合ゆえに、その基本の理解にも困難が伴う。さらに、量子物理の魅力的な部分は、日常とはかけ離れたむしろ奇異に思えることばかりと言えることから、いよいよその原理さえも捉えにくいものになっている。

そこで、ほとんど誰もがいつでもどこでも手軽に使うことのできる表計算ソフトを活用して、量子情報に馴染める工夫を考えた。いずれにしても、一般に表計算ソフトでは余り使われることのない、複素数や行列の使い方に習熟することがまず望まれる。その上で、さらに複素数を要素とするベクトルや行列を使いこなすことになるが、このあたりから表計算ソフトにはいろいろな制約が目立つようになる。それゆえ、その機能の補完や充実のためのプログラミング環境を利用して、複素行列を不自由なく使えるようにした。

具体的には、基本的な複素行列の演算が行えるようにするための関数を複数用意した。表計算は、ほとんどいつでもインタラクティブな操作を通して行うので、関数の引数はセルやセル範囲を指定するものとした。必要な数値データの取り込みには、チェックボックス、スクロールバー、コンボボックスなどの視覚的オブジェクトも使えるようにした。また、グラフ描画機能を、ブロッホ球のような動きのある図を構成するのに利用した。

ベクトルや行列を返す関数に対しては、結果を配列

数式として求めなければならず、そのためには操作手順をあらかじめ熟知しておく必要がある。配列数式はその一部の値の修正は不可能で、全体を消去するか、再度上書きするかしなければならないこと、あるいはそのコピー操作がセル範囲などとは異なることなどへの注意が必要になる。

単一量子ビットの状態に対しては、基底の2状態だけでなく、その重ね合わせの無数の状態があることを直感できるようにブロッホ球を用意した。それを見る視点の方向を大きく変えられるようにしたものの、ブロッホベクトルを空間的に正しく捉えやすくするためにはさらに工夫が必要である。ただし、複素行列を利用できるようにするための関数と量子計算用の関数以外は、シート上のセルに埋め込まれたわずかの数式があるだけにし、全体を極めて少ないプログラムコードに留めるようにしている。

多キュービットの量子系に対しては、表計算ソフトのシート上に、ユニタリ行列の要素を順序正しく配置すれば、あとは入力基底の状態変化によって量子計算が進むようにした。得られる量子情報を分かりやすく表現することやゲートをマウス操作で操作して簡単に回路を構成できるようにすることが課題になる。

## 参考文献

- (1) 伊集院八郎：表計算ソフト上での複素数とベクトルの処理, 応用物理教育, 34, No. 2, pp3-8, 2010.
- (2) 伊集院八郎：表計算ソフト上での複素行列の処理, 応用物理教育, vol. 32, no. 2, pp. 9-14, 2010.
- (3) 宮野健次郎、古澤明：量子コンピュータ入門, 日本評論社, 2008.
- (4) 伊集院八郎：表計算ソフト上での複素行列応用のためのプログラミング, 2010 夏のプログラミングシンポジウム報告集, pp. 21-28, 2010.
- (5) G. ベネンティ、G. カザーティ、G. ストゥリーニ (著)、廣岡一 (訳)、量子計算と量子情報の原理、シュプリンガー・ジャパン、2009
- (6) Michael A. Nielsen, Issac L. Chuang (著)、木村達也 (訳)、量子コンピュータと量子通信 I・II・III、Ohmsha, 2005.