量子コンピュータ入門講座の開講へ向けて　II

Quantum Computing for Information Science Students　II

中島 由美*　　土屋 尚†

要旨

本学における量子コンピュータ入門の講義の開講へ向けた準備の第２回目である。前回、主として従来型コンピュータの働きを量子コンピュータの立場から書き直すことを行ったが、ここでは量子ビットについて詳説する。１量子ビットゲートと２量子ビットゲートの組み合わせにより任意の２量子ビット状態を作り出せることまでを示す。

1　はじめに

前年度の紀要において著者らは、本学における量子コンピュータに関する講義の開講の可能性を探り始めた [1]。量子力学の学習をしていない情報系の学生に対しても量子コンピューティングについて教えることは可能であるとするマーミンの考え [2] に従って、彼の考えをできるだけかみくだき紹介することにつとめた。しかしそこではページ数の制約もありほとんど量子コンピューティングに踏み込むことはできず、従来のコンピューティングの基礎であるビット、これを量子ビット (Q ビット) に対して古典ビット (C ビット) と呼ぶのであるが、これを量子力学の標準的な表記で書き直すことに終始せざるを得なかった。

本報告において本格的に量子ビットについて解説し始めることになる。前回紹介した古典的ビットを拡張したものである量子ビットを導入し、演算の初期状態を作り出すゲートの導入までを行う。参考にするのはもちろん文献 [2] であるが、そこでの量子ビット及び量子コンピュータに関する記述はあまりにもコンパクトにまとめられたものなので、彼自身による教科書 [3] とその邦訳 [4] を適宜参照することにする。さらに進んで学習したい人にも便利なはずである。

ここで我々が強調したいことは、日本語版が出ているからといって内容がやさしくなったり、量子力学のわかりにくさが軽減される訳ではないことである。計算の面倒さも依然として残っている。この報告では、前回と同様、そのギャップをできるだけ埋めることにつとめたつもりである。いかに丁寧に解説したり、式の導出をしたりしているかを実際に文献 [3] 及び [4] と対比させてみていただきたい。

本報告の構成は以下の通りである。次節で量子ビットとその状態について述べる。第３節で量子ビットに対する可逆演算操作について論じる。第４節は測定ゲートとボルンの規則という量子力学の基本事項を紹介しているが、そこで述べられていることはあまりに日常的経験からかけ離れているため、かなりとまどう読者もいるに違いない。我々は、これをゲームのルールとして受け入れることを提案する。

* 明星大学情報学部准教授
† 明星大学名誉教授

次に一般化されたボルンの規則として多くの量子ビットのある中の特定の 1 つの量子ビットに対する測定を行う場合を論じる。続いて測定ゲートと状態の準備を論じ、さらに第 5 節で 1 量子ビット及び 2 量子ビットの系に対し任意の状態を用意するにはどうすればよいかを具体的に示す。今回はここまでの解説で終らざるを得ない。

2　量子ビットとその状態

古典ビットのとりうるのは 2 次元ベクトル全体の中の $|0\rangle$ と $|1\rangle$ で表される直行する状態のみであった。量子ビットで表される状態 $|\psi\rangle$ は $|0\rangle$ と $|1\rangle$ とによってすべての複素数にわたって張られる 2 次元のベクトル空間のどんな単位ベクトルもとりうる。このように言葉でのべると抽象的になってかえってわかりにくい。次のように式で表す方がずっとすっきりするであろう。すなわち量子ビットの一般的な状態は

$$\begin{aligned}|\psi\rangle &= \alpha_0 |0\rangle + \alpha_1 |1\rangle \\ &= \alpha_0 \begin{pmatrix}1\\0\end{pmatrix} + \alpha_1 \begin{pmatrix}0\\1\end{pmatrix} \\ &= \begin{pmatrix}\alpha_0\\0\end{pmatrix} + \begin{pmatrix}0\\\alpha_1\end{pmatrix}\end{aligned} \tag{1}$$

である。α_0 と α_1 は規格化条件

$$|\alpha_0|^2 + |\alpha_1|^2 = 1 \tag{2}$$

を満たすということだけを条件づけられた複素数である。この条件は $|\psi\rangle$ が単位ベクトルでなければならないということからきている。つまり

$$\begin{aligned}\langle\psi|\psi\rangle &= \left(\alpha_0^* \langle 0| + \alpha_1^* \langle 1|\right)\left(\alpha_0 |0\rangle + \alpha_1 |1\rangle\right) \\ &= \alpha_0^*\alpha_0 \langle 0|0\rangle + \alpha_1^*\alpha_0 \langle 1|0\rangle + \alpha_0^*\alpha_0 \langle 0|1\rangle + \alpha_1 \langle 1|1\rangle \\ &= \alpha_0^*\alpha_0 + \alpha_1^*\alpha_1 = |\alpha_0|^2 + |\alpha_1|^2 = 1\end{aligned} \tag{3}$$

である。

状態 $|\psi\rangle$ は $|0\rangle$ と $|1\rangle$ の**重ね合わせ** (superposition) と呼ばれ、α_0 か α_1 のどちらかが 0 で他方が 1 になれば、古典ビットと一致する。

1 つの量子ビットの一般的な状態は (1) で与えたように 2 つの古典ビット状態の重ね合わせであった。2 つの量子ビットに対する一般的な状態も 4 つの直交する古典状態の規格化された重ね合わせ

$$|\Psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \tag{4}$$

で表される。課される条件は、複素振幅に対する規格化条件

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \tag{5}$$

のみである。

この状態はそれぞれの量子ビットが

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \tag{6}$$

及び

$$|\phi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle \tag{7}$$

をとっているものとして、これらのテンソル積をとって得られる状態とは違うことに注意しなければならない。実際に積をとってみよう。

$$\begin{aligned}|\psi\rangle \otimes |\phi\rangle &= (\alpha_0 |0\rangle + \alpha_1 |1\rangle) \otimes (\beta_0 |0\rangle + \beta_1 |1\rangle) \\ &= \alpha_0\beta_0 |0\rangle \otimes |0\rangle + \alpha_0\beta_1 |0\rangle \otimes |1\rangle + \alpha_1\beta_0 |1\rangle \otimes |0\rangle + \alpha_1\beta_1 |1\rangle \otimes |1\rangle \\ &= \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \end{aligned} \tag{8}$$

この状態は一般的な 2 つの量子ビット状態 (3) と比べて、明らかに係数の間に関係があるので、より制限された状態であることがわかる。これら 2 つの状態が等しくなるためには各係数間に $\alpha_{00} = \alpha_0\beta_0$, $\alpha_{01} = \alpha_0\beta_1$, $\alpha_{10} = \alpha_1\beta_0$, $\alpha_{11} = \alpha_1\beta_1$ が成り立っていなければならない。これら 4 つの関係式より

$$\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10} \tag{9}$$

という関係がなければ状態 (4) と状態 (8) が一致しないことがわかる。ところが一般的な 2 量子ビット状態の振幅 (係数) に課された条件は規格化条件 (5) だけであるから、今得られた条件 (9) を満たす必要などない。従って一般的 2 量子ビット状態は決して 1 量子ビット状態の積で表される状態ではないのである。

同様のことが n 量子ビットの系に対してもいえる。n 個の量子ビットの一般的な状態は 2^n 個の異なった古典状態の重ね合わせでありその振幅の 2 乗の和は 1 である。すなわち、式で表すと

$$|\Psi\rangle = \sum_{0 \leqq x < 2^n} \alpha_x |x\rangle_n \tag{10}$$

$$\sum_{0 \leqq x < 2^n} |\alpha_x|^2 = 1 \tag{11}$$

である。

今、2 量子ビットに対して行ったのと同じ考察から、n 量子ビットに対しても次のことがいえる。n 古典ビット系の一般的な状態は $|0\rangle$ と $|1\rangle$ の 2^n 個の積で表される状態の 1 つであるが、n 量子ビット系の一般的状態はこれら 2^n 個の状態の重ね合わせであり、1 つの量子ビットの状態の積としても表せるようなものでは（一般的には）ない。いいかえると n 量子ビット系の中の 1 つ 1 つの量子ビットはそれ自身の個別の状態というものを持つことはないのである。

このような 2 つあるいはそれ以上の量子ビットの積で表せない状態のことを**絡みあった**（entangled）状態という。

3　量子ビットに対する可逆演算

1 つの古典ビットに対する唯一の可能な可逆演算は NOT である。可逆という言葉の意味及び、この NOT を反転演算と呼び演算子 $\mathbf{X}$ で表して既に詳しく紹介してある（[1] の §3.1)。1 つの量子ビットに対して行うことのできる可逆演算はもっと多様である。単位ベクトルを単位ベクトルに変換するどのような線形変換であってもよいのである。そのような変換をユニタリー変換と呼び、演算子 $\mathbf{u}$ で表す。$\mathbf{u}$ は

$$\mathbf{u}\mathbf{u}^\dagger = \mathbf{u}^\dagger\mathbf{u} = \mathbf{1} \tag{12}$$

という関係を満たす。$\mathbf{u}$ は 2 行 2 列の単位行列を表す。ここで $\mathbf{u}^\dagger$ は $\mathbf{u}$ のアジョイント演算子と呼ばれる演算子を表し、$\mathbf{u}$ の行列の転置行列をとりさらに複素共役にした要素を持つ行列で表される。(12) の

関係から明らかなように $\mathbf{u}^\dagger$ は $\mathbf{u}$ の逆行列でもある。どんなユニタリー演算 $\mathbf{u}$ もユニタリーな逆演算子 $\mathbf{u}^\dagger$ をもつ訳であるから、量子ビットに対するユニタリーな演算は可逆なのである。

n 個の古典ビットの行う最も一般的な可逆演算は $(2^n)!$ 個の異なる置換である。一方、n 個の量子ビットに対して量子コンピュータができる可逆演算は

$$\mathbf{u}\mathbf{u}^\dagger = \mathbf{u}^\dagger\mathbf{u} = \mathbf{1}$$

を満たすどんな 2^n 次元のユニタリー変換であってもよい。

量子コンピュータ用のアルゴリズムはどんなものでも、1 つの量子ビットに対するゲート（1 量子ビットゲート）と 2 つの量子ビットに対するゲート（2 量子ビットゲート）の積で表し得ることが示されている。第 5 節でこの 2 量子ビットゲート等を作用させて任意の 2 量子ビット状態を作り出せることを示すが、そのためには日常経験とはかけはなれた量子の世界にまず慣れなければならない。次の第 4 節はそのためのものである。

4　測定ゲートとボルンの規則、状態準備

それぞれが 0 か 1 をとる古典ビットが n 個あるときその状態を読みとることには何の問題もない。そのことに我々は慣れきっている。さらに、古典コンピュータでは、当たり前のこととして触れられてもいないことであるが、古典ビットの状態は読み取りという操作により変えられることはない。

ところが量子ビットに対してはこの当たり前のことが通用しないのである。

4.1　ボルンの規則

まず 1 つの量子ビットについて、ボルンの規則として知られている、量子ビットの状態を知るとはどういうことかについて説明する。式 (1) で与えられる重ね合わせ状態にある 1 つの量子ビット、すなわち

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

の状態を知るためには**測定**（**観測**と訳してある文献も多い）と呼ばれる操作をしなければならない。測定を行えば $|0\rangle$ の状態にあるか、$|1\rangle$ の状態にあるかは決められる。この測定を十分数多く（理想的には無限回）行うと状態 $|0\rangle$ の場合が確率 $|\alpha_0|^2$ で、状態 $|1\rangle$ の場合が確率 $|\alpha_1|^2$ で得られる、とするのがボルンの規則というものである。式 (2) の規格化条件とはこの $|\alpha_0|^2$ と $|\alpha_0|^2$ が確率であることを保証するために必要だったのである。1 つの量子ビットの状態が確率的にしか決まらないということは、我々の日常生活から考えると大変不思議なことであるが測定に関する不思議さはこれにとどまらない。一度測定してしまえば、その量子ビットの状態は $|0\rangle$ か $|1\rangle$ に決定され、もとの重ね合わせ状態に戻ることはないのである。つまり、この測定という操作は**非可換**である。

測定をする前に量子ビットが状態 $|0\rangle$ または $|1\rangle$ にあった訳ではないことは前回の (39)〜(42) で導入したアダマール変換 $\mathbf{H}$ を使って示すことができる。状態が $|\phi\rangle = \dfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ である 1 つの量子

ビットに対してアダマール変換 $\mathbf{H}$ を作用させると（前回の (41)、(42) を使って)、

$$\begin{aligned}\mathbf{H}|\phi\rangle &= \frac{1}{\sqrt{2}}\mathbf{H}(|0\rangle + |1\rangle)\\ &= \frac{1}{\sqrt{2}}(\mathbf{H}|0\rangle + \mathbf{H}|1\rangle)\\ &= \frac{1}{\sqrt{2}}\left\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}\\ &= |0\rangle\end{aligned} \tag{13}$$

となる。よって $\mathbf{H}|\phi\rangle$ で表される状態を測定すればボルンの規則によって結果は確率 1 で 0 となる。

しかし、もし状態 $|\phi\rangle$ が確率 $\frac{1}{2}$ で状態 $|0\rangle$、確率 $\frac{1}{2}$ で状態 $|1\rangle$ にあったと仮定すれば、$\mathbf{H}$ を作用させれば（前回の (41)、(42) により)、$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ または $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ となることになる。これらの状態を測定すれば、等確率で 0 又は 1 が得られるはずで、この結果は明らかに (13) の結論すなわち必ず 0 とは矛盾する。よって $|0\rangle$ と $|1\rangle$ との重ね合わせ状態にある 1 量子ビットの状態はある確率であらかじめ $|0\rangle$ または $|1\rangle$ にあった訳ではないことがわかる。

n 個の量子ビットよりなる系から情報をとりだすためにもやはり測定が必要である。何らかの方法で 1 つ 1 つの量子ビットの状態を測定すれば、0 か 1 かの結果が得られる。しかしそうして得られた 0 と 1 の列は、可能な出力に対する確率を与えるだけである。n 個の量子ビットの状態が

$$|\Psi\rangle = \sum_{0\leqq x<2^n} \alpha_x |x\rangle_n \tag{14}$$

であったとすると、n 個の量子ビットに対する測定の結果得られる 0 と 1 の列、すなわち x の 2 進数展開の得られる確率が

$$p(x) = |\alpha_x|^2 \tag{15}$$

である。

この $x(0 \leqq x < 2^n)$ を得る確率は次のようにも表される。(14) より α_x を得るにはこれに左から $\langle x|$ を施し、規格直交性より

$$\begin{aligned}\langle x|\Psi\rangle &= \langle x|\left(\sum_{0\leqq x<2^n} \alpha_x |x\rangle_n\right)\\ &= \langle x|(\alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_x|x\rangle + \cdots + \alpha_{2^n-1}|2^n-1\rangle)\\ &= \alpha_x\langle x|x\rangle = \alpha_x\end{aligned} \tag{16}$$

となるから

$$p(x) = |\alpha_x|^2 = |\langle x|x\rangle|^2 \tag{17}$$

となる。さらに

$$\begin{aligned}\langle x|\Psi\rangle^2 &= \langle x|\Psi\rangle\,\overline{\langle x|\Psi\rangle}\\ &= \langle x|\Psi\rangle\langle\Psi|x\rangle\end{aligned} \tag{18}$$

であるが、ここで

$$\mathbf{P}_\Psi = |\Psi\rangle\langle\Psi| \tag{19}$$

という状態 $|\Psi\rangle$ への射影演算子を定義すれば

$$p(x) = \langle x|\mathbf{P}_\Psi|x\rangle \tag{20}$$

であり、また、

$$\begin{aligned} p(x) &= \langle x|\Psi\rangle \langle\Psi|x\rangle \\ &= \langle\Psi|x\rangle \langle x|\Psi\rangle \end{aligned} \tag{21}$$

で

$$\mathbf{P}_x = |x\rangle \langle x| \tag{22}$$

という状態 $|x\rangle$ への射影演算子を定義すれば

$$p(x) = \langle\Psi|\mathbf{P}_x|\Psi\rangle \tag{23}$$

と表されることがわかる。

ここで射影演算子について説明しておこう。2 つのベクトル $|\phi\rangle$ と $|\psi\rangle$ の外積をとってみよう。すなわち $|\phi\rangle \langle\psi|$ をとるのである。ケットベクトルは列ベクトル、ブラベクトルは行ベクトルであることを思い出せば、この積は行列となることは容易に理解できるだろう。行列で表現されるのは演算子であった ([1] の §3.1)。この外積は任意のベクトル $|\gamma\rangle$ を、ベクトル $|\phi\rangle$ の内積 $\langle\psi|\gamma\rangle$ で与えられる数倍したものに移す線形演算子なのである。実際

$$(|\phi\rangle \langle\psi|) |\gamma\rangle = |\phi\rangle (\langle\psi|\gamma\rangle) \tag{24}$$

と確かめてみれば明らかである。では演算子 $|\psi\rangle \langle\psi|$ はどうなるであろうか。任意のベクトル $|\gamma\rangle$ にこれを作用させれば

$$(|\psi\rangle \langle\psi|) |\gamma\rangle = |\psi\rangle (\langle\psi|\gamma\rangle) \tag{25}$$

であるから、$|\gamma\rangle$ を $|\psi\rangle$ の方向へ $(\langle\psi|\gamma\rangle)$ 倍して移すことになる。つまり $|\gamma\rangle$ の $|\psi\rangle$ 方向への成分を表すことになる。すなわち $|\gamma\rangle$ の $|\psi\rangle$ 方向への射影をとる演算子を表しているのである。

4.2 状態準備

量子コンピュータにおいて、最終的な結果を与えるのに測定ゲートが重要であることは当然であるが、測定ゲートは計算を始める際にも重要な役割を演じるのである。いくつかの量子ビットの集まりは一般には絡みあった状態にあり特定の状態にそろっている訳ではない。いかにして計算に役立つ特定の状態に設定できるのだろうか。

答は測定にあるのである。n 個の量子ビットに対し測定を施せば結果は古典基底状態 $|x\rangle_n$ となる。そこで 1 となっている量子ビットに対し、1 量子ビット反転演算子 $\mathbf{X}$ を作用させ、0 となっている量子ビットには何もしなければ、結果としてすべて 0 にそろうから状態 $|0\rangle_n$ が得られることになる。

このような測定ゲートによる初期の状態の設定のことを状態準備という。

5 2 量子ビット状態の構成

非常に大まかないい方をすれば、量子コンピュータとは、1 量子ビットゲートと 2 量子ビットゲートよりなり、測定したとき意味のある情報を生み出すものということになる。1 量子ビットゲートを作ることはおそらくやさしいであろう。それらの単なるテンソル積ではない 2 量子ビットゲートを作るの

は多分ずっと難しいであろう。今集中的に研究されているのは cNOT ゲートである。([1] の §3.3 で制御 NOT 演算子としてその働きを詳しく紹介した。) 以下ではいかにして 1 量子ビットゲートと cNOT ゲートにより任意の状態を用意することができるかを示す。

つまり最終的に示したいのは $|00\rangle$ という状態に cNOT ゲートと 1 量子ビットゲートのみを作用させて、任意の 2 量子ビット状態ができることであるが、証明は逆に行われるので少しわかりにくいかもしれない。

どのような 1 量子ビット状態 $|\psi\rangle$ に対しても、状態 $|0\rangle$ を $|\psi\rangle$ に変換する 1 量子ビットゲート $\mathbf{u}$ が存在する。すなわち

$$|\psi\rangle = \mathbf{u}\,|0\rangle \tag{26}$$

である。絡みあっていない 2 量子ビット状態は 1 量子ビット状態のテンソル積であるから、1 量子ビットゲートをそれぞれの量子ビットに作用させれば作り出せる。しかし一般の 2 量子ビット状態は絡みあっており、その生成には 2 量子ビットゲートが必要である。これがいくつかの 1 量子ビットゲートと 1 つの cNOT ゲートの組み合わせでできるのである。

一般的な 2 量子ビット状態

$$|\Psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{27}$$

は

$$\begin{aligned} |\psi\rangle &= \alpha_{00}\,|0\rangle + \alpha_{01}\,|1\rangle \\ |\phi\rangle &= \alpha_{10}\,|0\rangle + \alpha_{11}\,|1\rangle \end{aligned}$$

を使えば

$$\begin{aligned} \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle &= \alpha_{00}\,|0\rangle \otimes |0\rangle + \alpha_{01}\,|0\rangle \otimes |1\rangle \\ &= |0\rangle \otimes (\alpha_{00}\,|0\rangle + \alpha_{01}\,|1\rangle) \end{aligned}$$

及び

$$\alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle = |1\rangle \otimes (\alpha_{10}\,|0\rangle + \alpha_{11}\,|1\rangle)$$

より

$$|\Psi\rangle = |0\rangle \otimes |\psi\rangle + |1\rangle \otimes |\phi\rangle \tag{28}$$

とも書けることに注意する。基底状態 $|0\rangle$ と $|1\rangle$ への効果が

$$\begin{aligned} &\mathbf{u}\,|0\rangle = a\,|0\rangle + b\,|1\rangle \\ &\mathbf{u}\,|1\rangle = -b^*\,|0\rangle + a^*\,|1\rangle \\ &|a|^2 + |b|^2 = 1 \end{aligned} \tag{29}$$

であるようなユニタリー変換 $\mathbf{u}$ （この $\mathbf{u}$ がユニタリーであることの確認は付録**A**にある）を使った $\mathbf{u} \otimes \mathbf{1}$ を $|\Psi\rangle$ に作用させてみよう。すると

$$\begin{aligned} (\mathbf{u} \otimes \mathbf{1})\,|\Psi\rangle &= (a\,|0\rangle + b\,|1\rangle) \otimes |\psi\rangle + (-b^*\,|0\rangle + a^*\,|1\rangle) \otimes |\phi\rangle \\ &= |0\rangle \otimes |\psi'\rangle + |1\rangle \otimes |\phi'\rangle \end{aligned} \tag{30}$$

という結果となる。ここに

$$\begin{aligned} |\psi'\rangle &= a\,|\psi\rangle - b^*\,|\phi\rangle \\ |\phi'\rangle &= b\,|\psi\rangle + a^*\,|\phi\rangle \end{aligned} \tag{31}$$

である。(この導出については付録 B を参照してほしい。)

$|\psi'\rangle$ と $|\phi'\rangle$ を直交状態に保っておくために複素係数 a と b はどのように選べばよいだろうか。内積 $\langle\phi'|\psi'\rangle$ は (29) より

$$\begin{aligned} \langle\phi'|\psi'\rangle &= (b^*\,\langle\psi| + a\,\langle\phi|)(a\,|\psi\rangle - b^*\,|\phi\rangle) \\ &= a^2\,\langle\phi|\psi\rangle - b^{*2}\,\langle\psi|\phi\rangle + ab^*(\langle\psi|\psi\rangle - \langle\phi|\phi\rangle) \end{aligned} \tag{32}$$

直交条件を使えば、すなわち $\langle\phi'|\psi'\rangle = 0$ とおけば、a と b に対する条件が得られる。$|\psi\rangle = \alpha_{00}\,|0\rangle + \alpha_{01}\,|1\rangle$、$|\phi\rangle = \alpha_{10}\,|0\rangle + \alpha_{11}\,|1\rangle$ であったから

$$\begin{aligned} 0 = {} & a^2\,(\langle 0|\,\alpha_{10}^* + \langle 1|\,\alpha_{11}^*)\,(\alpha_{10}\,|0\rangle + \alpha_{01}\,|1\rangle) \\ & -b^{*2}\,(\langle 0|\,\alpha_{00}^* + \langle 1|\,\alpha_{01}^*)\,(\alpha_{10}\,|0\rangle + \alpha_{11}\,|1\rangle) \\ & +ab\,\{(\langle 0|\,\alpha_{00}^* + \langle 1|\,\alpha_{01}^*)\,(\alpha_{00}\,|0\rangle + \alpha_{01}\,|1\rangle) \\ & -(\langle 0|\,\alpha_{10}^* + \langle 1|\,\alpha_{11}^*)\,(\alpha_{10}\,|0\rangle + \alpha_{11}\,|1\rangle)\} \end{aligned} \tag{33}$$

である。これをまとめなおすと

$$\begin{aligned} 0 = {} & \left(\frac{a}{b^*}\right)^2 (\alpha_{10}^*\alpha_{00} + \alpha_{11}^*\alpha_{01}) \\ & + \frac{a}{b^*}\left\{|\alpha_{00}|^2 + \,|\,\alpha_{01}|^2 - |\alpha_{10}|^2 - |\alpha_{11}|^2\right\} - (\alpha_{00}^*\alpha_{10} + \alpha_{01}^*\alpha_{11}) \end{aligned} \tag{34}$$

となり $\left(\dfrac{a}{b^*}\right)$ に関する 2 次方程式が得られる。その解は一般に 2 つの複素数である。もし (27) の a がある 0 でない複素数であれば、複素解の内の 1 つが b^*（すなわち b）を決定する。a と共にそれが 1 量子ビット変換 $\mathbf{u}$ を与えることになる。その $\mathbf{u}$ は

$$(\mathbf{u}\otimes\mathbf{1})\,|\Psi\rangle = |0\rangle\otimes|\psi'\rangle + |1\rangle\otimes|\phi'\rangle \tag{35}$$

のように働き $|\psi'\rangle$ と $|\phi'\rangle$ は直交している。

次に規格化条件を満たすことを考えると、正の数 λ と μ をとり

$$|\psi''\rangle = \frac{|\psi'\rangle}{\lambda}$$

と

$$|\phi''\rangle = \frac{|\phi'\rangle}{\mu}$$

が単位ベクトルになるように選ぶことは常に可能である。よって $|\psi''\rangle$ と $|\phi''\rangle$ は基底 $|0\rangle$ と $|1\rangle$ から、ある変換 $\mathbf{v}$ によって

$$|\psi''\rangle = \mathbf{v}\,|0\rangle\ ,\ |\phi''\rangle = \mathbf{v}\,|1\rangle \tag{36}$$

のように作り出すことができる。$|\psi''\rangle$ $|\phi''\rangle$ の直交性は $|\psi'\rangle$ と $|\phi'\rangle$ のそれより保証されているから、一方が基底 $|0\rangle$ より変換 $\mathbf{v}$ によって得られるなら他方は同じ変換で得られる訳である。

そうすると

$$\begin{aligned}(\mathbf{u}\otimes 1)\,|\Psi\rangle &= |0\rangle\otimes|\psi'\rangle + |1\rangle\otimes|\phi'\rangle \\ &= |0\rangle\otimes(\lambda\,|\psi''\rangle) + |1\rangle\otimes(\mu\,|\phi''\rangle) \\ &= \lambda\,|0\rangle\otimes(\mathbf{v}\,|0\rangle) + \mu\,|1\rangle\otimes(\mathbf{v}\,|1\rangle) \\ &= \lambda\,(\mathbf{1}\,|0\rangle)\otimes(\mathbf{v}\,|0\rangle) + \mu\,(\mathbf{1}\,|1\rangle)\otimes(\mathbf{v}\,|1\rangle)\end{aligned} \tag{37}$$

となり、公式 (付録 C を参照)

$$\mathbf{a}\,|x\rangle\otimes\mathbf{b}\,|y\rangle = (\mathbf{a}\otimes\mathbf{b})\,(|x\rangle\otimes|y\rangle) \tag{38}$$

を用いて整理すると、

$$(\mathbf{u}\otimes\mathbf{1})\,|\Psi\rangle = (\mathbf{1}\otimes\mathbf{v})\,(\lambda\,|0\rangle\otimes|0\rangle + \mu\,|1\rangle\otimes|1\rangle) \tag{39}$$

となる。よって

$$|\Psi\rangle = (\mathbf{u}\otimes\mathbf{1})^{\dagger}\,(\mathbf{1}\otimes\mathbf{v})\,(\lambda\,|0\rangle\otimes|0\rangle + \mu\,|1\rangle\otimes|0\rangle) \tag{40}$$

となる。ここで一般に成り立つ関係式

$$(\mathbf{u}\otimes\mathbf{1})^{\dagger} = \left(\mathbf{u}^{\dagger}\otimes\mathbf{1}\right) \tag{41}$$

を使えば

$$|\Psi\rangle = \left(\mathbf{u}^{\dagger}\otimes\mathbf{1}\right)(\mathbf{1}\otimes\mathbf{v})\,(\lambda\,|0\rangle\otimes|0\rangle + \mu\,|1\rangle\otimes|1\rangle)\,, \tag{42}$$

さらに公式 (付録 C を参照)

$$(\mathbf{a}\otimes\mathbf{b})\,(\mathbf{c}\otimes\mathbf{d}) = (\mathbf{ab}\otimes\mathbf{bd}) \tag{43}$$

を使うと

$$\begin{aligned}|\Psi\rangle &= \left(\mathbf{u}^{\dagger}\mathbf{1}\right)\otimes(\mathbf{1v})\,(\lambda\,|\otimes\rangle\,|0\rangle + \mu\,|1\rangle\otimes|1\rangle) \\ &= \left(\mathbf{u}^{\dagger}\otimes\mathbf{v}\right)(\lambda\,|0\rangle\otimes|1\rangle + \mu\,|1\rangle\otimes|1\rangle)\end{aligned} \tag{44}$$

となる。これはさらに

$$\begin{aligned}|\Psi\rangle &= \left(\mathbf{u}^{\dagger}\otimes\mathbf{v}\right)(\lambda\,|0\rangle\,|0\rangle + \mu\,|1\rangle\,|1\rangle) \\ &= \left(\mathbf{u}^{\dagger}\otimes\mathbf{v}\right)(\lambda\,|0\rangle\,|0\oplus 0\rangle + \mu\,|1\rangle\,|0\oplus 1\rangle)\end{aligned}$$

でもあり [1] の (37) より

$$\begin{aligned}&= \left(\mathbf{u}^{\dagger}\otimes\mathbf{v}\right)(\lambda\mathbf{C}_{10}\,|0\rangle\,|0\rangle + \mu\mathbf{C}_{10}\,|1\rangle\,|0\rangle) \\ &= \left(\mathbf{u}^{\dagger}\otimes\mathbf{v}\right)\mathbf{C}_{10}\,(\lambda\,|0\rangle + \mu\,|1\rangle)\otimes|0\rangle\end{aligned} \tag{45}$$

となる。$|\Psi\rangle$ は単位ベクトルであり、変換は単位ベクトルを単位ベクトルに変換するから、この式で $(\lambda\,|0\rangle + \mu\,|1\rangle)$ は単位ベクトルでならなければならないことがわかる。よってそれは基底 $|0\rangle$ よりある変換 $\mathbf{w}$ によって得られるはずである。つまり

$$\begin{aligned}|\Psi\rangle &= \left(\mathbf{u}^{\dagger}\otimes\mathbf{v}\right)\mathbf{C}_{10}\,(\mathbf{w}\,|0\rangle)\otimes|0\rangle \\ &= \left(\mathbf{u}^{\dagger}\otimes\mathbf{v}\right)\mathbf{C}_{10}\,(\mathbf{w}\,|0\rangle)\otimes(\mathbf{1}\,|0\rangle)\end{aligned}$$

公式を使えば

$$= \left(\mathbf{u}^{\dagger} \otimes \mathbf{v}\right) \mathbf{C}_{10} \left(\mathbf{w} \otimes \mathbf{1}\right) \left(|0\rangle \otimes |0\rangle\right) \tag{46}$$

よって全体として

$$|\Psi\rangle = \left(\mathbf{u}^{\dagger} \otimes \mathbf{v}\right) \mathbf{C}_{10} \left(\mathbf{w} \otimes \mathbf{1}\right) \left(|0\rangle \otimes |0\rangle\right) \tag{47}$$

となるから、$|00\rangle$ という状態に cNOT ゲート $\mathbf{C}_{10}$ 及びいくつかの 1 量子ゲートだけを作用させて任意の 2 量子状態 $|\Psi\rangle$ を生成できることを示すことができた。

6　まとめ

文献 [1] と本稿で著者らは量子コンピュータを論ずる際の基礎となる、量子ビットの取り扱いについて紹介してきた。その結果、2 量子ビットに対し何らかの計算を行う、すなわち何らかのゲートを作用させるための準備を行う所まできた。[2] で紹介された、計算機の専門家に対する量子コンピュータの考え方の紹介については、本稿までで、詳細な解説をつけ加えてほぼ網羅できたことになる。

参考文献

[1] 中島由美, 土屋尚, 量子コンピュータ入門講座の開講へ向けて, 明星大学情報学部研究紀要第 19 号, pp.21-39 (2011)

[2] D.Mermin, *From Cbits to Qbits: Teaching Computer Scientists Quantum Mechanics* , Am. J. Phys. **71**, (1), pp.23-30 (2003)

[3] D. Mermin, Quantum Computer Science - An Introduction , Cambridge UP (2007)

[4] マーミン著, 木村元訳, 量子コンピュータ科学の基礎, 丸善株式会社 (2009)

付録 A

式 (29) で定義した変換 $\mathbf{u}$ がユニタリーであることを確認する。(29) すなわち

$$\mathbf{u}\,|0\rangle = a\,|0\rangle + b\,|1\rangle\,,\ \mathbf{u}\,|1\rangle = -b^*\,|0\rangle + a^*\,|1\rangle\,,\ |a|^2 + |b|^2 = 1$$

に対し演算子 $\mathbf{u}^\dagger\mathbf{u}$ の各行列成分を計算すると

$$\begin{aligned}\langle 0|\,\mathbf{u}^\dagger\mathbf{u}\,|0\rangle &= (\langle 0|\,a^* + \langle 1|\,b^*)\,(a\,|0\rangle + b\,|1\rangle)\\ &= \langle 0|\,a^*a\,|0\rangle + \langle 1|\,b^*b\,|1\rangle\\ &= a^*a\,\langle 0|0\rangle + b^*b\,\langle 1|1\rangle\\ &= a^*a + b^*b = |a|^2 + |b|^2 = 1\end{aligned}$$

$$\begin{aligned}\langle 1|\,\mathbf{u}^\dagger\mathbf{u}\,|1\rangle &= (\langle 0|\,(-b) + \langle 1|\,a)\,(-b^*\,|0\rangle + a^*\,|1\rangle)\\ &= \langle 0|\,bb^*\,|0\rangle + \langle 1|\,aa^*\,|1\rangle\\ &= bb^*\,\langle 0|0\rangle + aa^*\,\langle 1|1\rangle\\ &= |b|^2 + |a|^2 = 1\end{aligned}$$

$$\begin{aligned}\langle 0|\,\mathbf{u}^\dagger\mathbf{u}\,|1\rangle &= (\langle 0|\,a^* + \langle 1|\,b^*)\,(-b^*\,|0\rangle + a^*\,|1\rangle)\\ &= -a^*b^*\,\langle 0|0\rangle - (b^*)^2\,\langle 1|0\rangle + (a^*)^2\,\langle 0|1\rangle + b^*a^*\,\langle 1|1\rangle\\ &= -a^*b^* + a^*b^* = 0\end{aligned}$$

$$\begin{aligned}\langle 1|\,\mathbf{u}^\dagger\mathbf{u}\,|0\rangle &= (\langle 0|\,(-b) + \langle 1|\,a)\,(a\,|0\rangle + b\,|1\rangle)\\ &= -ab\,\langle 0|0\rangle - a^2\,\langle 1|0\rangle - b^2\,\langle 0|1\rangle + ab\,\langle 1|1\rangle\\ &= -ab + ab = 0\end{aligned}$$

となる。よって $\mathbf{u}^\dagger\mathbf{u} = \mathbf{1}$ である。$\mathbf{u}^\dagger\mathbf{u}$ も同様に示すことができる。従って、(29) で定義した $\mathbf{u}$ はユニタリーである。

付録 B

式 (30) の導出について補足する。(28) より

$$\begin{aligned}(\mathbf{u}\otimes\mathbf{1})\,|\Psi\rangle &= (\mathbf{u}\otimes\mathbf{1})\,(|0\rangle\otimes|\psi\rangle + |1\rangle\otimes|\phi\rangle)\\ &= (\mathbf{u}\otimes\mathbf{1})\,(|0\rangle\otimes|\psi\rangle) + (\mathbf{u}\otimes\mathbf{1})\,(|1\rangle\otimes|\phi\rangle)\end{aligned}$$

となる。ここで公式 (付録 C 参照)

$$(\mathbf{a}\otimes\mathbf{b})\,(|x\rangle\otimes|y\rangle) = \mathbf{a}\,|x\rangle\otimes\mathbf{b}\,|y\rangle$$

を思い出すと、$\mathbf{a}$ を $\mathbf{u}$、$\mathbf{b}$ を $\mathbf{1}$、$|x\rangle$ を $|0\rangle$ または $|1\rangle$、$|1\rangle$ を $|\psi\rangle$ または $|\phi\rangle$ とすればよいから、

$$\begin{aligned}(\mathbf{u}\otimes\mathbf{1})\,(|0\rangle\otimes|\psi\rangle) &= \mathbf{u}\,|0\rangle\otimes\mathbf{1}\,|\psi\rangle\\ (\mathbf{u}\otimes\mathbf{1})\,(|1\rangle\otimes|\phi\rangle) &= \mathbf{u}\,|1\rangle\otimes\mathbf{1}\,|\phi\rangle\end{aligned}$$

となり、さらに (29) より

$$\begin{aligned}\mathbf{u}\,|0\rangle = a\,|0\rangle + b\,|1\rangle\,,\ \mathbf{1}\,|\psi\rangle = |\psi\rangle\\ \mathbf{u}\,|1\rangle = -b^*\,|0\rangle + a^*\,|1\rangle\,,\ \mathbf{1}\,|\phi\rangle = |\phi\rangle\end{aligned}$$

であるから

$$\begin{aligned}(\mathbf{u}\otimes\mathbf{1})\,(|0\rangle\otimes|\psi\rangle) &= (a\,|0\rangle + b\,|1\rangle)\otimes|\psi\rangle\\ (\mathbf{u}\otimes\mathbf{1})\,(|1\rangle\otimes|\phi\rangle) &= (-b^*\,|0\rangle + a^*\,|1\rangle)\otimes|\phi\rangle\end{aligned}$$

となり

$$\begin{aligned}(\mathbf{u}\otimes\mathbf{1})\,|\Psi\rangle &= a\,|0\rangle\otimes|\psi\rangle + b\,|1\rangle\otimes|\psi\rangle - b^*\,|0\rangle\otimes|\phi\rangle + a^*\,|1\rangle\otimes|\phi\rangle\\ &= |0\rangle\otimes(a\,|\psi\rangle) + |1\rangle\otimes(b\,|\psi\rangle) + |0\rangle\otimes(-b^*\,|\phi\rangle) + |1\rangle\otimes(a^*\,|\phi\rangle)\\ &= |0\rangle\otimes(a\,|\psi\rangle - b^*\,|\phi\rangle) + |1\rangle\otimes(b\,|\psi\rangle + a^*\,|\phi\rangle)\end{aligned}$$

となる。さらに (31) より

$$= |0\rangle\otimes|\psi'\rangle + |1\rangle\otimes|\phi'\rangle$$

となる。

付録 C

公式 (38)

$$\mathbf{a}\left|x\right\rangle \otimes \mathbf{b}\left|y\right\rangle = \left(\mathbf{a}\otimes\mathbf{b}\right)\left(\left|x\right\rangle \otimes \left|y\right\rangle\right)$$

の証明を示す。ここでは $\mathbf{a},\mathbf{b}$ を 2 行 2 列の行列、$\left|x\right\rangle, \left|y\right\rangle$ を 2 行 1 列のベクトルとすれば十分であるから

$$\mathbf{a} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},\ \mathbf{b} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix},\ \left|x\right\rangle = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},\ \left|y\right\rangle = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

とする。

$$\begin{aligned} \mathbf{a}\otimes\mathbf{b} &= \begin{pmatrix} a_{11}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{12}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ a_{21}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{22}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix} \end{aligned}$$

$$\left|x\right\rangle \otimes \left|y\right\rangle = \begin{pmatrix} x_1\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ x_2\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_1y_1 \\ x_1y_2 \\ x_2y_1 \\ x_2y_2 \end{pmatrix}$$

$$\begin{aligned} \left(\mathbf{a}\otimes\mathbf{b}\right)\left(\left|x\right\rangle \otimes \left|y\right\rangle\right) &= \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix} \begin{pmatrix} x_1y_1 \\ x_1y_2 \\ x_2y_1 \\ x_2y_2 \end{pmatrix} \\ &= \begin{pmatrix} a_{11}b_{11}x_1y_1 + a_{11}b_{12}x_1y_2 + a_{12}b_{11}x_2y_1 + a_{12}b_{12}x_2y_2 \\ a_{11}b_{21}x_1y_1 + a_{11}b_{22}x_1y_2 + a_{12}b_{21}x_2y_1 + a_{12}b_{22}x_2y_2 \\ a_{21}b_{11}x_1y_1 + a_{21}b_{12}x_1y_2 + a_{22}b_{11}x_2y_1 + a_{22}b_{12}x_2y_2 \\ a_{21}b_{21}x_1y_1 + a_{21}b_{22}x_1y_2 + a_{22}b_{21}x_2y_1 + a_{22}b_{22}x_2y_2 \end{pmatrix} \end{aligned} \tag{C.1}$$

一方

$$\begin{aligned} \mathbf{a}\left|x\right\rangle \otimes \mathbf{b}\left|y\right\rangle &= \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ &= \begin{pmatrix} a_{11}x_1 + a_{12}x_2 \\ a_{21}x_1 + a_{22}x_2 \end{pmatrix} \otimes \begin{pmatrix} b_{11}y_1 + b_{12}y_2 \\ b_{21}y_1 + b_{22}y_2 \end{pmatrix} \\ &= \begin{pmatrix} a_{11}x_1 + a_{12}x_2\begin{pmatrix} b_{11}y_1 + b_{12}y_2 \\ b_{21}y_1 + b_{22}y_2 \end{pmatrix} \\ a_{21}x_1 + a_{22}x_2\begin{pmatrix} b_{11}y_1 + b_{12}y_2 \\ b_{21}y_1 + b_{22}y_2 \end{pmatrix} \end{pmatrix} \\ &= \begin{pmatrix} a_{11}b_{11}x_1y_1 + a_{11}b_{12}x_1y_2 + a_{12}b_{11}x_2y_1 + a_{12}b_{12}x_2y_2 \\ a_{11}b_{21}x_1y_1 + a_{11}b_{22}x_1y_2 + a_{12}b_{21}x_2y_1 + a_{12}b_{22}x_2y_2 \\ a_{21}b_{11}x_1y_1 + a_{21}b_{12}x_1y_2 + a_{22}b_{11}x_2y_1 + a_{22}b_{12}x_2y_2 \\ a_{21}b_{21}x_1y_1 + a_{21}b_{22}x_1y_2 + a_{22}b_{21}x_2y_1 + a_{22}b_{22}x_2y_2 \end{pmatrix} \end{aligned}$$

これはまさに (C.1) であるから (38) は確かめられた。

また、公式 (43)

$$(\mathbf{a} \otimes \mathbf{b})\,(\mathbf{c} \otimes \mathbf{d}) = (\mathbf{ab} \otimes \mathbf{cb})$$

は (38) の $|x\rangle$ を $\mathbf{c}$、$|y\rangle$ を $\mathbf{d}$ としたものであるから、上の証明で $|x\rangle$ を

$$\mathbf{c} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

$|y\rangle$ を

$$\mathbf{d} = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}$$

と拡張すれば確かめられる。