量子コンピュータ入門講座の開講へ向けて　III

Quantum Computing for Information Science Students　III

中島 由美*　　土屋 尚†

要旨

本学部の４年生及び大学院生に対する量子コンピュータ入門の講義内容の提案の第３回目である。基本的な量子計算の過程の一般論とドイチュの問題について解説する。

1　はじめに

本学における量子コンピュータ入門講座の開講へ向けての提案を [1]、[2] で行ってきたが、今回はその第３回目である。情報の専門家に対し、量子力学を学ぶ負担を軽くして量子コンピューティングの心髄を伝えることを目的としたマーミンの教科書 [3]、[4] を基にし、その内容をいかに本学のカリキュラムにつながるようにできるかに腐心し議論を進める。次節で量子コンピュータでの計算過程の基本的なことを一般論として述べ、第３節で量子計算の最も簡単な問題であるドイチュの問題について論じる。付録として II の正誤表を付加する。

2　計算過程の一般論

量子コンピュータにおける計算とはどうあるべきかという一般的な議論を本節で行う。量子コンピュータといえどもある数 x に対して、指定された関数 f によって処理し、新しい数 $f(x)$ を作り出さなければならない。この数 x をどう表現するかであるが、通常の古典コンピュータにおいても数はすべて非負の整数として表されている。負数にしろ小数にしろ、すべて正整数をどう解釈するかによって扱うことが可能になっているだけで、コンピュータの表し得るのは 0 と正の整数なのである。この状況は量子コンピュータにおいても変わりはしない。量子ビットを k 個用意し、その計算基底状態で 2^k 未満の負でない整数を表すのである。x を表す n 個の量子ビットを**入力レジスタ**と呼び、$f(x)$ を表す m 個の量子ビットを**出力レジスタ**と呼ぶ。つまり $(n+m)$ 個の量子ビットを使う。量子ビットの実現はおそらく大変なことであるに違いないのに、なぜ、入力レジスタと出力レジスタを別にするというもったいないことをするのだろうか。それは測定という操作以外の量子計算過程が可逆的に行われなければならないからである。入力レジスタに出力を書き込む方法では、２つの x の値に対して $f(x)$ の値が同じになったとしたら、計算を逆に行って元に戻すことはできなくなるから、この２重のレジスタのアーキテクチャ（dual-register architecture）が必要なのである。量子コンピュータは入力レジスタだけでなく出力レジスタにも操作が及ぶように設計されている。

* 明星大学情報学部准教授
† 明星大学名誉教授

もちろん一般的計算にはこの $(n+m)$ 個の量子ビットの他に多くの量子ビットを必要とするだろうが、我々はまずそれらを無視して、f の計算には入出力レジスタの $(n+m)$ 個の量子ビットに対するユニタリ変換 $\mathbf{U}_f$ 以外は必要ないとして話を進める。

変換 $\mathbf{U}_f$ をある計算基底状態を別の計算基底状態に変える可逆変換と定義する。入力レジスタと出力レジスタを構成する $(n+m)$ 個の量子ビットの計算基底に対する $\mathbf{U}_f$ の作用のしかたは、

$$\mathbf{U}_f \left(|x\rangle_n |y\rangle_m\right) = |x\rangle_n |y \oplus f(x)\rangle_m \tag{1}$$

となっているものとする。ここに現れた $\oplus$ という記号はすでに I の (37)[1] で紹介ずみの、ビットごとの和を 2 で割りその余りをとるという演算、つまりビットごとの排他的論理和 (XOR) 演算を表す。確認のための例を示しておこう。x と y が m ビットの整数でそれぞれの j 番目のビットを x_j、y_j とする。$x \oplus y$ は m ビットの整数でその j 番目のビットが $x_j \oplus y_j$ で決まるのである。$m=4$ で $x=1101$、$y=0111$ なら $x \oplus y = 1101 \oplus 0111 = 1010$ となる。

変換 (1) は可逆である。つまり $\mathbf{U}_f$ を施した結果から、施す前の状態を得ることが可能であるということなのだが、実際、変換 (1) の場合は $\mathbf{U}_f$ はそれ自身の逆変換 $\mathbf{U}_f^{-1}$ に等しいのである。以下でそれを示そう。変換 (1) を施した結果にもう一度 $\mathbf{U}_f$ を施すと

$$\begin{aligned}\mathbf{U}_f \left\{\mathbf{U}_f \left(|x\rangle |y\rangle\right)\right\} &= \mathbf{U}_f \left(|x\rangle |y \oplus f(x)\rangle\right) \\ &= |x\rangle |(y \oplus f(x)) \oplus f(x)\rangle \\ &= |x\rangle |y \oplus f(x) \oplus f(x)\rangle\end{aligned}$$

となるが、どのようなビット列 z に対しても $z \oplus z = 0$ であるから $f(x) \oplus f(x) = 0$ となり

$$\begin{aligned}&= |x\rangle |y \oplus 0\rangle \\ &= |x\rangle |y\rangle\end{aligned}$$

となる。つまり入力レジスタと出力レジスタの任意の状態 $|x\rangle |y\rangle$ に $\mathbf{U}_f$ を続けて 2 度作用させると元の状態 $|x\rangle |y\rangle$ に戻ることがわかった。つまり

$$\mathbf{U}_f \mathbf{U}_f = \mathbf{1}$$

であるから、$\mathbf{U}_f$ は逆演算子の定義 $\mathbf{U}_f \mathbf{U}_f^{-1} = \mathbf{1}$ を満たす。すなわち

$$\mathbf{U}_f = \mathbf{U}_f^{-1} \tag{2}$$

となり、$\mathbf{U}_f$ はそれ自身の逆変換に等しい。もし出力レジスタの初期状態が 0、すなわち $y=0$ なら (1) は

$$\mathbf{U}_f |x\rangle_n |0\rangle_m = |x\rangle_m |f(x)\rangle_m \tag{3}$$

となり、$f(x)$ が直接出力レジスタに出るようにできる。

この事実を利用すれば、量子コンピュータの行う最も重要な計算とも言える次のことが可能になる。2 量子ビット状態 $|0\rangle |0\rangle (= |0\rangle \otimes |0\rangle)$ のそれぞれに対し、I の 3.3 節で紹介した 1 量子ビットアダマール変換 $\mathbf{H}$ を施したとすると

$$(\mathbf{H}_1 \otimes \mathbf{H}_0)(|0\rangle \otimes |0\rangle) = (\mathbf{H}_1 |0\rangle) \otimes (\mathbf{H}_0 |0\rangle)$$

となる。ここでの添字 1 と 0 は各々 1 番目及び 0 番目の量子ビットに作用するアダマール変換であることを示し、右辺は II の (38)[2] で示した公式を使った結果である。さらに I の (41)、(42)[1] で示したアダマール変換の具体的作用の結果を使うと上式の右辺は

$$
\begin{aligned}
&= \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right) \otimes \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle \right) \\
&= \frac{1}{2} \left(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \right) \\
&= \frac{1}{2} \left(|0\rangle |0\rangle + |0\rangle |1\rangle + |1\rangle |0\rangle + |1\rangle |1\rangle \right) \\
&= \frac{1}{2} \left(|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2 \right)
\end{aligned} \tag{4}
$$

となる。3 量子ビットの場合には

$$
\begin{aligned}
&\left(\mathbf{H}_2 \otimes \mathbf{H}_1 \otimes \mathbf{H}_0 \right) \left(|0\rangle \otimes |0\rangle \otimes |0\rangle \right) \\
&= \left\{ \left(\mathbf{H}_2 \otimes \mathbf{H}_1 \right) \left(|0\rangle \otimes |0\rangle \right) \right\} \otimes \left(\mathbf{H}_0 |0\rangle \right) \\
&= \mathbf{H}_2 |0\rangle \otimes \mathbf{H}_1 |0\rangle \otimes \mathbf{H}_0 |0\rangle \\
&= \frac{1}{2^{\frac{3}{2}}} \left(|0\rangle + |1\rangle \right) \otimes \left(|0\rangle + |1\rangle \right) \otimes \left(|0\rangle + |1\rangle \right) \\
&= \frac{1}{2^{\frac{3}{2}}} \left(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \right) \otimes \left(|0\rangle + |1\rangle \right) \\
&= \frac{1}{2^{\frac{3}{2}}} \left(|0\rangle \otimes |0\rangle \otimes |0\rangle + |0\rangle \otimes |0\rangle \otimes |1\rangle + |0\rangle \otimes |1\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \otimes |1\rangle \right. \\
&\quad \left. + |1\rangle \otimes |0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle \otimes |1\rangle + |1\rangle \otimes |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle \otimes |1\rangle \right) \\
&= \frac{1}{2^{\frac{3}{2}}} \left(|0\rangle_3 + |1\rangle_3 + |2\rangle_3 + |3\rangle_3 + |4\rangle_3 + |5\rangle_3 + |6\rangle_3 + |7\rangle_3 \right) \\
&= \frac{1}{2^{\frac{3}{2}}} \sum_{0 \le x < 2^3} |x\rangle_3
\end{aligned} \tag{5}
$$

となる。よって n 量子ビットに対しても直ちに一般化できて

$$
\mathbf{H}^{\otimes n} = \mathbf{H} \otimes \mathbf{H} \otimes \cdots \otimes \mathbf{H} \qquad (n \text{ 個の } \mathbf{H}) \tag{6}
$$

という略記法を導入すれば

$$
\mathbf{H}^{\otimes n} |0\rangle_n = \frac{1}{2^{\frac{n}{2}}} \sum_{0 \le x < 2^n} |x\rangle_n \tag{7}
$$

である。よって、もし入力レジスタの初期状態が $|0\rangle_n$ で、その各々の量子ビットにアダマール変換を施せば、状態は n 個のビットの可能な状態の等しい重みでの重ね合わせ状態となる。それからその重ね合わせ状態に変換 $\mathbf{U}_f$ を施せば、そしてさらに出力レジスタが 0 に揃えられているとしたら、

$$
\mathbf{U}_f \left(\mathbf{H}^{\otimes n} \otimes \mathbf{1}_m \right) \left(|0\rangle_n |0\rangle_m \right)
$$

II の (38)[2] を使えば

$$
= \mathbf{U}_f \left(\mathbf{H}^{\otimes n} |0\rangle_n \right) \otimes \left(\mathbf{1}_m |0\rangle_m \right)
$$

(7) より

$$
\begin{aligned}
&= \mathbf{U}_f \left(\frac{1}{2^{\frac{n}{2}}} \sum_{0 \le x < 2^n} |x\rangle_n \right) \otimes (\mathbf{1}_m |0\rangle_m) \\
&= \mathbf{U}_f \left(\frac{1}{2^{\frac{n}{2}}} \sum_{0 \le x < 2^n} |x\rangle_n \right) \otimes |0\rangle_m \\
&= \frac{1}{2^{\frac{n}{2}}} \mathbf{U}_f \left(|0\rangle_n + |1\rangle_n + |2\rangle_n + \cdots + |2^n - 1\rangle_n \right) \otimes |0\rangle_m \\
&= \frac{1}{2^{\frac{n}{2}}} \mathbf{U}_f \left(|0\rangle_n \otimes |0\rangle_m + |1\rangle_n \otimes |0\rangle_m + |2\rangle_n \otimes |0\rangle_m + \cdots + |2^n - 1\rangle_n \otimes |0\rangle_m \right) \\
&= \frac{1}{2^{\frac{n}{2}}} \left(\mathbf{U}_f |0\rangle_n \otimes |0\rangle_m + \mathbf{U}_f |1\rangle_n \otimes |0\rangle_m + \mathbf{U}_f |2\rangle_n \otimes |0\rangle_m + \cdots + \mathbf{U}_f |2^n - 1\rangle_n \otimes |0\rangle_m \right) \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{0 \le x < 2^n} \mathbf{U}_f |x\rangle_n |0\rangle_m
\end{aligned}
$$

(3) より

$$
= \frac{1}{2^{\frac{n}{2}}} \sum_{0 \le x < 2^n} |x_n\rangle |f(x)\rangle_m \tag{8}
$$

となる。

この結果は量子コンピューティングの不思議な面を表している。はじめに $|0\rangle_n$ の状態にあった入力レジスタに $\mathbf{U}_f$ を作用させる前に、1 つ 1 つの量子ビットにアダマール変換を施しておくと、計算の結果は関数 f の 2^n 個のすべての結果を知らないと指定できないような状態で記述されると言っているのである。よって入力レジスタがたった 100 個の量子ビットでできていたとしても、はじめは $|0\rangle_{100}$ という状態にあり、それぞれに 100 個のアダマール変換を作用させ次に $\mathbf{U}_f$ を作用させると最終状態は関数 f の $2^{100} \sim 10^{30}$ 回の評価の結果を含む形となるのである。この見かけ上のミラクルを**量子並列性**（quantum parallelism）と呼んでいるのである。

しかしこのミラクルの大部分は単なる見かけ上のものである。量子計算に携わる人の中にも不用意にそのように述べる人がいるのだが、計算の結果が f の 2^n 回の評価の結果とは言えないのである。言えることのすべては、計算の出力の状態を特徴づけるのはそのような評価だということだけである。我々の知らない状態にある量子ビットの集合があるときそれの状態が何かを見つけるための方法は測定を行うことしかないということを忘れてはならない。

(8) の状態にある $(n+m)$ 個の量子ビットを測定ゲートに送ると、入力レジスタの量子ビットは 2^n 未満の x の値のどれかである x_0 を等しい確率でとり、出力レジスタの測定結果はその特定の x_0 に対応した $f(0)$ の値を返すはずである。II の 4 節 [2] でのべたボルンの規則はそう告げるはずである。測定の後レジスタの状態は $|x_0\rangle |f(x_0)\rangle$ に移り、他の x の値に対する $f(x)$ の値を知る手だてはない。

出力状態の測定をする前に、出力状態のコピーを作ることが可能だとすれば、それらコピーを次々と測定にかけることにより計算結果に対する分布が得られ、その分布の中心からどの f が遂行されたかが高い確率でわかるであろう。しかしそのようなコピーを作ることは**複製禁止定理**（no-cloning theorem）によって禁じられている。その定理とは「任意の状態 $|\psi\rangle_n$ に対し、状態 $|\psi\rangle_n |0\rangle_n$ を $|\psi\rangle_n |\psi\rangle_n$ に変換するユニタリ変換は存在しない。」というものである。その証明は次のように線形性のみを使い簡単にできる。

任意の状態をコピーできるユニタリ変換 $\mathbf{U}$ があったとしたら

$$\begin{aligned}\mathbf{U}\left(|\psi\rangle|0\rangle\right) &= |\psi\rangle|\psi\rangle \\ \mathbf{U}\left(|\phi\rangle|0\rangle\right) &= |\phi\rangle|\phi\rangle\end{aligned} \tag{9}$$

である。コピーを作り出すのであるから元の状態 $|\psi\rangle$ はそのまま残すし、任意の状態をコピーできるのであるから元の状態は $|\psi\rangle$ でも $|\phi\rangle$ でもよい。$\mathbf{U}$ が線形の演算子であるという条件からは

$$\begin{aligned}\mathbf{U}\left(a|\psi\rangle + b|\phi\rangle\right) &= a\mathbf{U}|\psi\rangle|0\rangle + b\mathbf{U}|\phi\rangle|0\rangle \\ &= a|\psi\rangle|\psi\rangle + b|\phi\rangle|\phi\rangle\end{aligned} \tag{10}$$

という結果が得られる。しかし $\mathbf{U}$ は任意の状態をコピーできると仮定しているのであるから、これらの重ね合わせ状態 $(a|\psi\rangle + b|\phi\rangle)$ もそのままコピーできるはずで、その場合は

$$\begin{aligned}&\mathbf{U}\left(a|\psi\rangle + b|\phi\rangle\right)|0\rangle \\ &= \left(a|\psi\rangle + b|\phi\rangle\right)\left(a|\psi\rangle + b|\phi\rangle\right) \\ &= a^2|\psi\rangle|\psi\rangle + b^2|\phi\rangle|\phi\rangle + ab|\psi\rangle|\phi\rangle + ab|\phi\rangle|\psi\rangle\end{aligned} \tag{11}$$

という結果となる。しかし (11) は a か b のどちらかが 0 でない限り (10) と等しくはならない。つまりこのようなコピーのできる線形演算子 $\mathbf{U}$ は存在しないのである。

従って量子コンピュータでも 1 度だけ走らせて、どの f が走ったかを知ることはできない。しかし次のようなことはできることがわかってきた。古典コンピュータでは何回も計算を行わないと知ることのできないような f の間の関係性についての情報を、量子コンピュータなら 1 度走らせて測定することで得られる。これが量子コンピューティングに対する最も大きな期待といえよう。しかしそのためには個々の x の値に対して $f(x)$ の値を知るという可能性を犠牲にしなければならないのであるが、このようにのべても抽象的すぎてわかりにくいので、次節でより具体的に解説する。

3　ドイチュの問題

ドイチュの問題というのは、ファインマンと共に量子計算の提唱者の一人と見なされているドイチュ（Deutsch）によって 1980 年代に出された問題である。関係性に関する情報を得るため、より具体的な情報を犠牲にする、量子計算の最も単純な例となっている。

入力レジスタも出力レジスタも 1 つの量子ビットよりなるとする。よって探求するのは 1 つの量子ビットを 1 つの量子ビットへ移す関数 f ということになる。表 1 に示すようにそのような関数は 4 つしかない。

表 1　1 ビットを 1 ビットへ移す 4 つの関数 $f(x)$

	$x=0$	$x=1$
$f_0(x)$	0	0
$f_1(x)$	0	1
$f_2(x)$	1	0
$f_3(x)$	1	1

ブラックボックス（中身のわからない箱）が与えられその中ではこれら 4 つの内の 1 つの計算が行われるとしよう。計算は前節で説明した量子計算のフォーマット (1) に従っているものとする。今の場合

入力レジスタも出力レジスタも 1 つずつであるから $n = m = 1$ で

$$\mathbf{U}_f \left(|x\rangle |y\rangle \right) = |x\rangle |y \oplus f(x)\rangle \tag{12}$$

である。ブラックボックス内では $\mathbf{U}_{f_0}$、$\mathbf{U}_{f_1}$、$\mathbf{U}_{f_2}$、$\mathbf{U}_{f_3}$ のどれか 1 つが遂行されるが、どれになるのかは知られていない。もちろん計算を 2 度行う（ブラックボックスを 2 回働かせる）とすれば答はわかる。つまり 1 度目は状態 $|0\rangle |0\rangle$ に対して、2 度目は入力レジスタが $|1\rangle$ である $|1\rangle |0\rangle$ という状態に対して働かせればよい。もしブラックボックスを働かせることができるのは 1 度だけとしたら、f について何がわかるだろうか。

答を先に言ってしまうと、f が入力の値によらず入力と同じ値を与えるか（これは f_0 と f_3 にあたる）、入力を反転させた値を与えるか（f_1 と f_2 に相当）という問いに答えられるというものである。次に、どうすれば量子コンピュータはこれを達成できるかを説明するのであるが、これは f の与える値自体に対しては何ももたらすことはないのである。これが、関係性についての情報を得るために、より具体的な情報を犠牲にする、ということなのである。

それでは以下でドイチュの問題すなわち「f が入力と同じ値を与えるか否かを 1 度だけブラックボックスを働かせることで決定せよ。」を量子計算的に解くことを考えよう。量子コンピューティングなのであるから、入力レジスタの状態を重ね合わせ状態にするということができるはずである。はじめ $|0\rangle |0\rangle$ にあった入力レジスタ、出力レジスタの内、出力レジスタはそのままにして入力レジスタのみにアダマール変換を施せば、重ね合わせ状態を得ることができる。式で表現すれば

$$(\mathbf{H} \otimes \mathbf{1}) \left(|0\rangle |0\rangle \right) = (\mathbf{H} \otimes \mathbf{1}) \left(|0\rangle \otimes |0\rangle \right)$$

である。再び直積に関する公式、II の (38)[2] を使えば

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

ということである。このように話や計算を進めるのは一筋道で大変わかりやすいのであるが、実際に答を正しく得るためにはもうひとひねりする必要があることがわかってきたのである。それは $|0\rangle |0\rangle$ から出発するのはもちろんであるが、まず入力レジスタ、出力レジスタの両方に NOT 演算子 $\mathbf{X}$ を施し、しかる後両方にアダマール変換を施す、つまり

$$(\mathbf{X} \otimes \mathbf{X}) |0\rangle |0\rangle = |1\rangle |1\rangle$$

に対してアダマール変換を施すと

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

という状態が得られる。この状態に $\mathbf{U}_f$ を一度だけ作用させると $\mathbf{U}_f$ は線形演算子であるから

$$\frac{1}{2} \mathbf{U}_f \left(|0\rangle |0\rangle - |1\rangle |0\rangle - |0\rangle |1\rangle + |1\rangle |1\rangle \right) = \frac{1}{2} \left(\mathbf{U}_f |0\rangle |0\rangle - \mathbf{U}_f |1\rangle |0\rangle - \mathbf{U}_f |0\rangle |1\rangle + \mathbf{U}_f |1\rangle |1\rangle \right) \tag{14}$$

となる。項別に (9) を考慮しながら計算すると

$$\begin{aligned}
\mathbf{U}_f\left|0\right\rangle\left|0\right\rangle &= \left|0\right\rangle\left|0\oplus f(0)\right\rangle = \left|0\right\rangle\left|f(0)\right\rangle \\
\mathbf{U}_f\left|1\right\rangle\left|0\right\rangle &= \left|1\right\rangle\left|0\oplus f(1)\right\rangle = \left|1\right\rangle\left|f(1)\right\rangle \\
\mathbf{U}_f\left|0\right\rangle\left|1\right\rangle &= \left|0\right\rangle\left|1\oplus f(0)\right\rangle = \left|0\right\rangle\left|\tilde{f}(0)\right\rangle \\
\mathbf{U}_f\left|1\right\rangle\left|1\right\rangle &= \left|1\right\rangle\left|1\oplus f(1)\right\rangle = \left|1\right\rangle\left|\tilde{f}(1)\right\rangle
\end{aligned}$$

ここで $\tilde{f}$ という記号を導入したが、これは

$$\tilde{f}(x) = 1 \oplus f(x) \tag{15}$$

という意味の略記法である。よって (14) は

$$\frac{1}{2}\mathbf{U}_f\left(\left|0\right\rangle\left|0\right\rangle - \left|1\right\rangle\left|0\right\rangle - \left|0\right\rangle\left|1\right\rangle + \left|1\right\rangle\left|1\right\rangle\right) = \frac{1}{2}\left(\left|0\right\rangle\left|f(0)\right\rangle - \left|1\right\rangle\left|f(1)\right\rangle - \left|0\right\rangle\left|\tilde{f}(0)\right\rangle + \left|1\right\rangle\left|\tilde{f}(1)\right\rangle\right) \tag{16}$$

となる。$f(0) = f(1)$ だとしたら、これは

$$\frac{1}{2}\left(\left|0\right\rangle\left|f(0)\right\rangle - \left|1\right\rangle\left|f(0)\right\rangle - \left|0\right\rangle\left|\tilde{f}(0)\right\rangle + \left|1\right\rangle\left|\tilde{f}(0)\right\rangle\right) = \frac{1}{2}\left(\left|0\right\rangle - \left|1\right\rangle\right)\left(\left|f(0)\right\rangle - \left|\tilde{f}(0)\right\rangle\right) \tag{17}$$

となる。$f(0) \neq f(1)$ だとすると、すぐ確かめられるように $f(1) = \tilde{f}(0)$、$\tilde{f}(1) = f(0)$ であるから、(16) は

$$\begin{aligned}
&\frac{1}{2}\left(\left|0\right\rangle\left|f(0)\right\rangle - \left|1\right\rangle\left|f(1)\right\rangle - \left|0\right\rangle\left|\tilde{f}(0)\right\rangle + \left|1\right\rangle\left|\tilde{f}(1)\right\rangle\right) \\
=\ &\frac{1}{2}\left(\left|0\right\rangle\left|f(0)\right\rangle - \left|1\right\rangle\left|\tilde{f}(0)\right\rangle - \left|0\right\rangle\left|\tilde{f}(0)\right\rangle + \left|1\right\rangle\left|f(0)\right\rangle\right) \\
=\ &\frac{1}{2}\left(\left|0\right\rangle + \left|1\right\rangle\right)\left(\left|f(0)\right\rangle - \left|\tilde{f}(0)\right\rangle\right)
\end{aligned} \tag{18}$$

となる。最後に入力レジスタに対しアダマール変換を施すと (17) と (18) はそれぞれ

$$\mathbf{H}\frac{1}{2}\left(\left|0\right\rangle - \left|1\right\rangle\right)\left(\left|f(0)\right\rangle - \left|\tilde{f}(0)\right\rangle\right) = \frac{1}{\sqrt{2}}\left|1\right\rangle\left(\left|f(0)\right\rangle - \left|\tilde{f}(0)\right\rangle\right) \tag{19}$$

$$\mathbf{H}\frac{1}{2}\left(\left|0\right\rangle + \left|1\right\rangle\right)\left(\left|f(0)\right\rangle - \left|\tilde{f}(0)\right\rangle\right) = \frac{1}{\sqrt{2}}\left|0\right\rangle\left(\left|f(0)\right\rangle - \left|\tilde{f}(0)\right\rangle\right) \tag{20}$$

となる。まとめると

$$\begin{aligned}
&\left(\mathbf{H}\otimes\mathbf{1}\right)\mathbf{U}_f\left(\mathbf{H}\otimes\mathbf{H}\right)\left(\mathbf{X}\otimes\mathbf{X}\right)\left|0\right\rangle\left|0\right\rangle \\
=\ &\begin{cases}
\left|1\right\rangle\dfrac{1}{\sqrt{2}}\left(\left|f(0)\right\rangle - \left|\tilde{f}(0)\right\rangle\right), & f(0) = f(1) \\
\left|0\right\rangle\dfrac{1}{\sqrt{2}}\left(\left|f(0)\right\rangle - \left|\tilde{f}(0)\right\rangle\right), & f(0) \neq f(1)
\end{cases}
\end{aligned} \tag{21}$$

ということになる。つまり、$f(0) = f(1)$ ならば入力レジスタが最終的に $\left|1\right\rangle$ に、$f(0) \neq f(1)$ ならば $\left|0\right\rangle$ になる。よって入力レジスタを測定することで、確かに $f(0)$ と $f(1)$ が同じか同じでないかという問いに答えられるのである。

どちらの場合も出力レジスタの状態は $\frac{1}{\sqrt{2}}\left(|f(0)\rangle - |\tilde{f}(0)\rangle\right)$ である。この重ね合わせ状態の 2 項の重みは $\frac{1}{\sqrt{2}}$ と $-\frac{1}{\sqrt{2}}$ で、測定すると $f(0)$ と $\tilde{f}(0)$ が共に確率 $\frac{1}{2}$ で現れ、$f(0)$ の具体的な値については何も知ることはできない。つまり出力レジスタは（今回の問いに対して）有益な情報は何も持っていないとも言えるし、$f(0) = \begin{cases} 0 \\ 1 \end{cases}$ に従って出力レジスタは $\pm\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ になることがわかるだけである、と言ってもよい。

4　まとめ

シリーズの第 3 回目として量子計算過程の一般論と、その具体的な例として歴史的にも最初のものであるドイチュの問題をマーミンの教科書 [3] を読み解く形で紹介した。マーミンも認めていることであるが、ドイチュの問題はいかにも問題のために無理に作られた問題という感じが強く、別にそれが解けたからといって何のためになるのかはわかりにくい。しかも出力レジスタを用意してあるにもかかわらず、入力レジスタの結果を見に行くことで答えられる問題があるということなので、だまされたような気になる読者も多いことだろう。さらにその答を得るためには NOT やアダマール変換を施さねばならないのであるから、その手間の方が系を 2 度走らせる手間より大変なのではなかろうかと心配にすらなる。しかしここで重要なのは原理的なことで、量子コンピュータを 1 度だけ走らせて、古典では答えられない問題に答えられる例が存在するということなのである。

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] 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 II, 明星大学情報学部研究紀要第 20 号, pp.75-88 (2012)
[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

II [2] の正誤表

	誤	正
p.77　6 行目	状態 (3)	状態 (4)
p.77　下から 2 行目	**u** は 2 行 2 列の	**1** は 2 行 2 列の
p.78　下から 3 行目	非可換	非可逆