情報系の物理学　演習問題７’

G99P139-7 森 紘一郎

出題日：2000 年 12 月 6 日
提出期限：2001 年 1 月 10 日
提出日：2001 年 1 月 1 日

問題

量子コンピュータによる計算を適当な例をもとに説明せよ。

方針

XOR を計算する量子コンピュータを考える。ただし、一から考えるのは難しかったので、上坂吉則著「量子コンピュータの基礎数理」の P.76 にある量子コンピュータがどのように計算されるのかを詳しく追っていくことにした。

解答

XOR を計算する量子コンピュータ

次のような論理関数

$$\forall x, y = 0, 1, \quad f(x, y) := (x, x \oplus y) = (x, XOR(x, y))$$

を計算する量子コンピュータは

$$U := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma$$

で与えられる。すなわち

$$\forall x, y = 0, 1, \quad U|x, y\rangle = |x, x \oplus y\rangle$$

が成り立つ。ここで

$$\sigma := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$\forall x, y = 0, 1, \quad XOR(x, y) := x \oplus y := \begin{cases} 0 & (x = y \text{ のとき}) \\ 1 & (x \neq y \text{ のとき}) \end{cases}$$

である。

なぜ、これで XOR が計算できるのかを説明しようと思う。
量子コンピュータの定義より、U はユニタリ作用素でなければならない。つまり、

$$UU^* = I$$

を満たさなければならない。(*は共役転置、I は単位行列)

$$\begin{aligned} U &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma \\ &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{aligned}$$

ここで、2×2 のテンソル積は次のように計算できる。
命題
A_1, A_2 を C^2 上の線形作用素とする。このとき

$$A := A_1 \otimes A_2$$

の (i, j) 成分 a_{ij} は

$$a_{ij} = \langle i_1|A_1|j_1\rangle\langle i_2|A_2|j_2\rangle$$

で与えられる。ここで

$$i := 2i_1 + i_2, \quad i_1, i_2 = 0, 1$$

$$j := 2j_1 + j_2, \quad j_1, j_2 = 0, 1$$

である。
この命題を使うと、

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

となる。計算してみると、$U^* = U$ なので、

$$UU^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = I$$

となり、U はユニタリ行列であることが示された。次に、

$$U|x, y\rangle = |x, x \oplus y\rangle$$

となることを示す。U は線形性を持つので、

$$U|x, y\rangle = (|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma)|x, y\rangle$$

$$= (|0\rangle\langle 0| \otimes I)|x, y\rangle + (|1\rangle\langle 1| \otimes \sigma)|x, y\rangle$$

ここで、

命題

A_1, A_2 と B_1, B_2 を C^2 上の作用素とする。このとき、

$$(A_1 \otimes A_2)(B_1 \otimes B_2) = (A_1 B_1) \otimes (A_2 B_2)$$

が成り立つ。

という命題を使うと、

$$= (|0\rangle\langle 0|)|x\rangle \otimes I|y\rangle + (|1\rangle\langle 1|)|x\rangle \otimes \sigma|y\rangle \tag{1}$$

ここで、

$$(|0\rangle\langle 0|)|x\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} |x\rangle$$

であり、$x = 0, 1$ より、

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} |0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle \quad (x = 0 \text{ のとき})$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} |1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} = 0 \quad (x = 1 \text{ のとき})$$

よって、

$$(|0\rangle\langle 0|)|x\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} |x\rangle = (1 - x)|x\rangle$$

同様に

$$(|1\rangle\langle 0|)|x\rangle = x|x\rangle$$

$$\sigma|x\rangle = |1 - x\rangle$$

よって、式 (1) は、

$$= (1 - x)|x\rangle \otimes |y\rangle + x|x\rangle \otimes |1 - y\rangle$$

$$= |x\rangle \otimes ((1 - x)|y\rangle + x|1 - y\rangle)$$

$$= |x\rangle \otimes |x \oplus y\rangle$$

$$= |x, x \oplus y\rangle \tag{2}$$

よって、出力の第 2 キュービットを観測すれば、XOR(x,y) を得ることができる。
最後に、どのようなエルミート作用素を使って、観測するかを考える。
命題
U によって推移した状態から、観測によって計算結果を取り出す。入力 $|i_1, i_2\rangle$ に対する U による出力は

$$U|i_1, i_2\rangle = |f_1, f_2\rangle$$

となる。ここで、第 2 キュービットを観測して、観測値 f_2 が確率 1 で得られるようにするための観測量は、2 番目が $|1\rangle\langle 1|$ であり、残りがすべて I であるようなエルミート作用素

$$A_2 = I \otimes |1\rangle\langle 1|$$

である。
この命題を使うと、式（2）の第 2 キュービットを観測したいのだから、エルミート作用素は、

$$A_2 = I \otimes |1\rangle\langle 1|$$

でよい。ここで、作用素 I、$|1\rangle\langle 1|$ の固有値と固有ベクトルについて次のことが成り立っている。
　I の固有ベクトル $|0\rangle, |1\rangle$ はそれぞれ固有値 1 に対応
　$|1\rangle\langle 1|$ の固有ベクトル $|0\rangle, |1\rangle$ はそれぞれ固有値 0,1 に対応
命題
A,B を C^2 上の作用素とする。A の固有値とそれに対応する固有ベクトルをそれぞれ

$$a_1, a_2; |a_1\rangle, |a_2\rangle$$

とし、B の固有値とそれに対応する固有ベクトルをそれぞれ

$$b_1, b_2; |b_1\rangle, |b_2\rangle$$

とする。このとき、$A \otimes B$ の固有値とそれに対応する固有ベクトルはそれぞれ

$$a_1 b_1, a_1 b_2, a_2 b_1, a_2 b_2$$

$$|a_1, b_1\rangle, |a_1, b_2\rangle, |a_2, b_1\rangle, |a_2, b_2\rangle$$

で与えられる。
この命題によると、A_2 の固有値と固有ベクトルに関して

A_2 の固有ベクトル $|0,0\rangle, |1,0\rangle$ は固有値 0 に対応し、
A_2 の固有ベクトル $|0,1\rangle, |1,1\rangle$ は固有値 1 に対応する
ことがわかる。
入力が $|0,0\rangle$ のとき、出力は

$$U|0,0\rangle = |0,0\rangle = 1|0,0\rangle + 0|1,0\rangle + 0|0,1\rangle + 0|1,1\rangle$$

であるので、観測の規約より、確率 $|1|^2 + |0|^2 = 1$ で 0 が観測される。
入力が $|0,1\rangle$ のとき、出力は

$$U|0,1\rangle = |0,1\rangle = 0|0,0\rangle + 0|1,0\rangle + 1|0,1\rangle + 0|1,1\rangle$$

であるので、観測の規約より、確率 $|1|^2 + |0|^2 = 1$ で 1 が観測される。
入力が $|1,0\rangle$ のとき、出力は

$$U|1,0\rangle = |1,1\rangle = 0|0,0\rangle + 0|1,0\rangle + 0|0,1\rangle + 1|1,1\rangle$$

であるので、観測の規約より、確率 $|0|^2 + |1|^2 = 1$ で 1 が観測される。
入力が $|1,1\rangle$ のとき、出力は

$$U|1,1\rangle = |1,0\rangle = 0|0,0\rangle + 1|1,0\rangle + 0|0,1\rangle + 0|1,1\rangle$$

であるので、観測の規約より、確率 $|0|^2 + |1|^2 = 1$ で 0 が観測される。
以上の結果をまとめると、
観測値が 0 ならば 計算結果は $XOR(x,y) = 0$ であり、
観測値が 1 ならば 計算結果は $XOR(x,y) = 1$ である。
たとえば、入力として $|0,1\rangle$ を量子コンピュータ U に入れ、エルミート作用素 A_2 によって観測すると 1 が 100%観測される。よって、観測値が 1 なので $XOR(0,1) = 1$　だということが分かる。

考察

参考文献によると、ユニタリ作用素は正方行列であるため、論理関数 XOR を計算するような量子コンピュータは存在しないらしい。しかし、出力を 2 キュービットにして、そのうちの 1 つが求める計算結果が出るようにし、それを観測すれば、XOR が計算できる。上で求めたのも、第 1 キュービットは適当でよく、行列の計算上付け足したものであることが分かる。量子コンピュータではこのようにすることがよくあるらしい。

感想

ユニタリ作用素のことを量子コンピュータと呼ぶところが面白いと思った。前から量子コンピュータという言葉を聞いていたが、ハードのことばかり想

像していたので、このような数学的なものだと知ってとても面白い考え方だと思った。NOT や XOR など簡単な量子コンピュータを見てきたが、観測という概念がいまいち分からなかった。なぜ、観測をしないと計算結果が分からないのか不思議に思った。量子力学をもっと勉強すれば分かると思うので、今後も勉強していきたい。また、確率が 1 のときばかりだったが、1 以外になるような例にも興味が起きた。

参考文献

上坂吉則著「量子コンピュータの基礎数理」