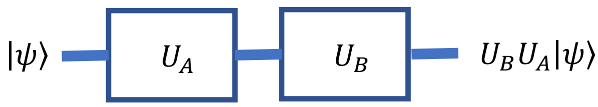
因果順序と量子情報処理

量子情報班（文責：吉田智治）

1　因果順序

情報処理を行う際、簡単な計算や通信を順番に行って行くことで複雑な処理を行います。(「因果順序と量子情報処理」のポスター参照）この実行する順番のことを**因果順序**と呼びます。例えば、量子状態 $|\psi\rangle$ にユニタリーゲート U_A をかけた後、ユニタリーゲート U_B をかける、などです。これを図で書くと下図のようになります。



通常は、このように因果順序は一つ定まっているのですが、二つ以上の因果順序を「量子的に」重ね合わせる、ということを考えることもできます。この重ね合わせを実現したものを**量子スイッチ**と呼びます。量子スイッチを使うと情報処理の際、計算量や通信量などを減らすことができると知られています。ここでは、量子スイッチを使った情報処理について解説していきます。

2　量子スイッチについて [1]

量子スイッチは、ユニタリーゲート 2 つを入力として受け取り、ユニタリーゲートを出力するものです。ユニタリーゲート U_A, U_B を入力としたときの出力を $S(U_A, U_B)$ と書きます。出力されたユニタリーゲートは、操作を加える量子状態 $|\psi\rangle$ と、制御ビットと呼ばれる量子状態 $|\psi_c\rangle$ の複合系に作用します。そして、制御ビットの状態が $|\psi_c\rangle = |0\rangle$ のとき、$|\psi\rangle$ にユニタリーゲートが U_A, U_B の順で、$|\psi_c\rangle = |1\rangle$ のとき、U_B, U_A の順で作用します。式で書くと、以下のようになります。

$$S(U_A, U_B)(|\psi\rangle \otimes |0\rangle) = U_B U_A |\psi\rangle \otimes |0\rangle \tag{1}$$

$$S(U_A, U_B)(|\psi\rangle \otimes |1\rangle) = U_A U_B |\psi\rangle \otimes |1\rangle \tag{2}$$

そして、制御ビットの状態を $|0\rangle$ と $|1\rangle$ の重ね合わせ状態にすると、因果順序の量子的重ね合わせが実現できます。例えば、$|\psi_c\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ にすると、以下のようになります。

$$S(U_A, U_B)\left(|\psi\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}}(U_B U_A |\psi\rangle \otimes |0\rangle + U_A U_B |\psi\rangle \otimes |1\rangle) \tag{3}$$

3　量子スイッチの応用例 [2]

量子スイッチを用いることで必要な通信量を減らすことができるタスクについて考えていきます。まず、設定として、Alice, Bob, Charlie の三人がいるものとします。Alice と Bob は、n 桁の 0/1 の数字の列 (Alice は $\boldsymbol{x}$、Bob は $\boldsymbol{y}$) と、2^n 桁の 0/1 の数字の列を一つずつ (Alice は $\boldsymbol{f}$、Bob は $\boldsymbol{g}$) 持っているものとします。$\boldsymbol{f}, \boldsymbol{g}$ の z 桁目の数字を f_z, g_z と書き、$\boldsymbol{x}, \boldsymbol{y}$ を 2 進数の数字だと思った時の数を x, y と書きます。この時、Alice, Bob, Charlie の三人が計算と量子状態の通信を行うことで、Charlie は $f_y + g_x$

を 2 で割った余り r を出力する、というのがタスクです。ただし、三人は十分な計算能力があり、通信は一方向のみしか行えないものとします。例えば、Alice から Bob に通信を行った場合、その後 Bob から Alice には通信することができません。通信量をできるだけ減らしたいものとします。

まず、因果順序が定まっている場合、$\boldsymbol{f}$ または $\boldsymbol{g}$ の情報を全て通信しなければならないことがわかります。つまり、2^n 桁の数字を通信する必要があり、通信量は最低でも 2^n bit 必要とわかります。量子状態を用いることでこの通信量を半分にすることはできますが、それでも 2^{n-1} qubit の通信量が必要です。

一方で、量子スイッチを用いると通信量を圧倒的に減らすことができます。具体的な構成法を示すために、以下のような略記法を用います。

$$|\boldsymbol{z}\rangle = |z_1\rangle |z_2\rangle \cdots |z_n\rangle \tag{4}$$

ただし、$\boldsymbol{z}$ は n 桁の 0/1 の数字の列。また、n 桁の 0/1 の数字の列全体の集合を $\mathbb{Z}_2^n$ と書きます。さらに、$\boldsymbol{x}, \boldsymbol{y} \in \mathbb{Z}_2^n$ に対して

$$\boldsymbol{x} \oplus \boldsymbol{y} = (x_1 \oplus y_1 \cdots x_n \oplus y_n) \tag{5}$$

と書きます。ただし、$x_i \oplus y_i$ は $x_i + y_i$ を 2 で割った余りを表します。

$\boldsymbol{x} = (x_1 \cdots x_n) \in \mathbb{Z}_2^n$ に対して

$$X(\boldsymbol{x}) = X^{x_1} \otimes \cdots \otimes X^{x_n} \tag{6}$$

と定義します。ただし、X は

$$|0\rangle \to |1\rangle \tag{7}$$
$$|1\rangle \to |0\rangle \tag{8}$$

というゲートです。この時、$\boldsymbol{z} \in \mathbb{Z}_2^n$ に対して

$$X(\boldsymbol{x}) |\boldsymbol{z}\rangle = |\boldsymbol{x} \oplus \boldsymbol{z}\rangle \tag{9}$$

となります。また、$\boldsymbol{h} \in \mathbb{Z}_2^{2^n}, \boldsymbol{z} \in \mathbb{Z}_2^n$ に対して

$$|\boldsymbol{z}\rangle \to (-1)^{h_z} |\boldsymbol{z}\rangle \tag{10}$$

というゲートを $D(\boldsymbol{h})$ と書きます。

$U_A = X(\boldsymbol{x})D(\boldsymbol{f}), U_B = X(\boldsymbol{y})D(\boldsymbol{g})$ と定義します。U_A, U_B はそれぞれ Alice, Bob が持っている情報のみで定義できることに注意しましょう。この時、$\mathbf{0} = 0 \cdots 0 (n$ 桁$)$ とすると、

$$U_A U_B |\mathbf{0}\rangle = (-1)^{f_y} |\boldsymbol{x} \oplus \boldsymbol{y}\rangle \tag{11}$$
$$U_B U_A |\mathbf{0}\rangle = (-1)^{g_z} |\boldsymbol{x} \oplus \boldsymbol{y}\rangle \tag{12}$$

となります。よって、$(U_A U_B + U_B U_A) |\mathbf{0}\rangle$ または $(U_A U_B - U_B U_A) |\mathbf{0}\rangle$ のいずれかは 0 で、前者が 0 のとき $r = 0$, 後者が 0 のとき $r = 1$ になります。従って、$(U_A U_B + U_B U_A) |\mathbf{0}\rangle = 0$ か $(U_A U_B - U_B U_A) |\mathbf{0}\rangle = 0$ のいずれになるかを Charlie が判定できればいいことになります。

ここで量子スイッチを用います。制御ビットは Charlie が持っているものとします。制御ビットは、はじめ $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ という状態にあるとし、操作を加える量子状態は $|\psi\rangle = |\mathbf{0}\rangle$ になっているものとします。そのとき、U_A, U_B を量子スイッチに入力したものをこれらの状態に加えると、

$$S(U_A, U_B)(|\mathbf{0}\rangle \otimes |+\rangle) = \frac{1}{\sqrt{2}} (U_B U_A |\mathbf{0}\rangle \otimes |0\rangle + U_A U_B |\mathbf{0}\rangle \otimes |1\rangle) \tag{13}$$

となります。次に、制御ビットに Hadamard ゲート H というゲートを加えます。これは

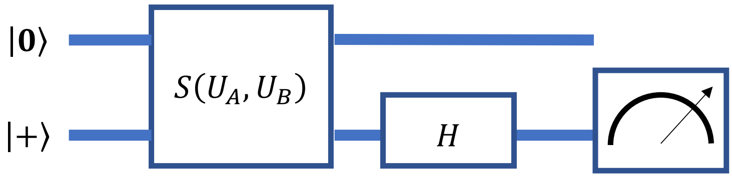
$$|0\rangle \to |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{14}$$

$$|1\rangle \to |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{15}$$

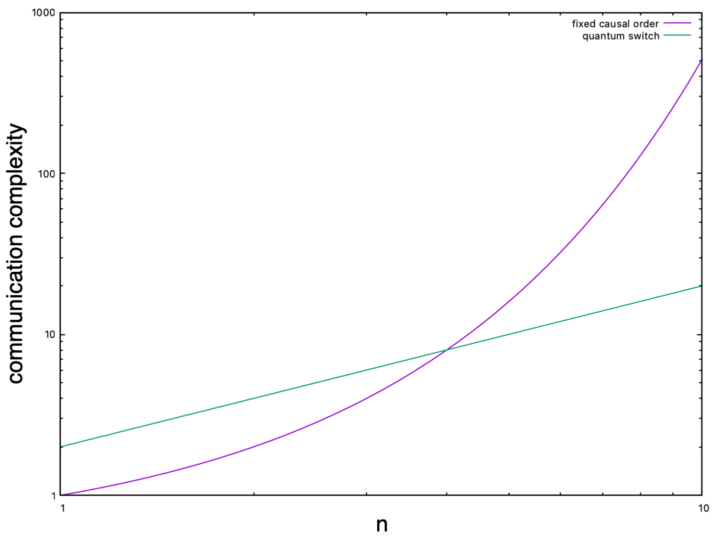
というゲートです。そのゲートをかけた後の状態は、

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\left(U_B U_A |\mathbf{0}\rangle \otimes |+\rangle + U_A U_B |\mathbf{0}\rangle \otimes |-\rangle\right) && (16)\\
&= \frac{1}{\sqrt{2}}\left(U_B U_A |\mathbf{0}\rangle \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} + U_A U_B |\mathbf{0}\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) && (17)\\
&= \frac{1}{2}\left((U_A U_B + U_B U_A) |\mathbf{0}\rangle \otimes |0\rangle - (U_A U_B - U_B U_A) |\mathbf{0}\rangle \otimes |1\rangle\right) && (18)\\
&= \begin{cases} -\frac{1}{2}(U_A U_B - U_B U_A) |\mathbf{0}\rangle \otimes |1\rangle & (r = 0) \\ \frac{1}{2}(U_A U_B + U_B U_A) |\mathbf{0}\rangle \otimes |0\rangle & (r = 1) \end{cases} && (19)
\end{aligned}$$

となります。よって、Charlie が制御ビットに $\{|0\rangle, |1\rangle\}$ の射影測定をして、測定結果が 0 ならば $r = 1$、1 ならば $r = 0$ と分かります。このとき、用いた通信について考えると、量子スイッチ一回につき ALice から Bob、Bob から Alice に通信を行っているので 2 回の通信を用いています。操作を加える量子状態 $|\psi\rangle$ は n 桁の 0/1 の数字の列なので、合計で $2n$ qubit の通信を行っています。以上の手続きを図にすると下のようになります。



ゆえに、量子スイッチを用いると、通信量が 2^{n-1} qubit から $2n$ qubit に減ることがわかります。これをグラフで図示すると下のようになり、n が大きくなるにつれて、量子スイッチを用いたほうが大きく改善していることが分かります。



参考文献

[1] Oreshkov, O., Costa, F., Brukner, Č. (2012). Quantum correlations with no causal order. *Nat. Comm.*, **3**(1), 1-8.

[2] Guérin, P. A., Feix, A., Araújo, M., Brukner, Č. (2016). Exponential communication complexity advantage from quantum superposition of the direction of communication. *Phys. Rev. Lett.*, **117**(10), 100502.