Blind Quantum Computation

Feb 12, 2024

amakihc

Contents

1. Introduction

量子コンピュータが実用化されると、医療や金融、機械学習など、様々な分野で活躍することが期待されている。そこで、様々な個人や企業が量子コンピュータを用いたいと考えることになるが、量子コンピュータを自前で用意することは、その大きさや費用面から厳しいといえるだろう。量子コンピュータを自前で用意できない個人や企業が量子コンピュータを利用する方法として、外部の量子コンピュータをクラウドで利用することが挙げられる。しかし、外部に量子計算を委託するということは、外部に量子計算の内容が漏れてしまうリスクがある。このようなときに用いるのがブラインド量子計算のプロトコルであり、それにより利用者のプライバシーや企業秘密を守ったまま外部に量子計算を委託することができる。

2. Quantum Computation

2.1. Quantum Bits

1 量子ビットの状態は以下のように表される。

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle \tag{2.1}$$

上式では、$\{|0\rangle, |1\rangle\}$ を基底にとっている。 このような基底を計算基底という。 基底のとり方は計算基底のほかに Hadamard 基底があり、$\{|+\rangle, |-\rangle\}$ で表す。

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}} \tag{2.2}$$

2 量子ビットの状態は $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ の基底を用いて以下のように表せる。

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle \tag{2.3}$$

2.2. Quantum Gates

1 量子ビットに作用するゲートは、以下の通り。

Pauli ゲート

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.4}$$

Hadamard ゲート

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.5}$$

π/8 ゲート

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \tag{2.6}$$

回転ゲート

$$\begin{aligned} R_x(\theta) = e^{-i\theta X/2} &= \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \\ R_z(\theta) = e^{-i\theta Z/2} &= \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} \end{aligned} \tag{2.7}$$

$R_y(\theta)$ もあるが、今回は省略した。 回転ゲートの定義は上式であるが、グローバル位相は無視してよいので、計算の都合上、以下では

$$R_z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \tag{2.8}$$

とする。

2 量子ビットに作用するゲートは、以下の通り。

CNOT ゲート

$$U_{\mathrm{CN}} = \begin{pmatrix} I & O \\ O & X \end{pmatrix} \tag{2.9}$$

CZ ゲート

$$U_{\mathrm{CZ}} = \begin{pmatrix} I & O \\ O & Z \end{pmatrix} \tag{2.10}$$

ここではブロック行列で記述したが、実際は 4×4 の行列である。

3. Measurement Based Quantum Computation

3.1. Entanglement and Measurement

2 量子ビットの状態を 1 量子ビットの積で記述すると以下の通り。

$$(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle \tag{3.1}$$

ただし、これでは任意の 2 量子ビットの状態を表すことはできない。 例えば、$\dfrac{|00\rangle + |11\rangle}{\sqrt{2}}$ という状態を満たすような (a, b, c, d) の組は存在しない、すなわち積に分解することができないことがわかる。 このように、積に分解することができない状態をエンタングル状態という。

任意の量子状態 $|\psi\rangle = a|0\rangle + b|1\rangle$ を考える。 $|\psi\rangle$ と $|+\rangle$ の間に CZ ゲートをかけると、エンタングル状態になる。

$$U_{\mathrm{CZ}}|\psi\rangle|+\rangle = U_{\mathrm{CZ}}(a|0\rangle + b|1\rangle)|+\rangle = a|0\rangle|+\rangle + b|1\rangle|-\rangle \tag{3.2}$$

1 ビット目を $\{R_z(-\theta)|\pm\rangle\}$ に射影する測定を行う。

まず、$R_z(-\theta)|+\rangle$ に射影された場合を考える。 測定後の状態は以下の通り。

$$\begin{aligned} &\sqrt{2}\langle+|_1 R_z(-\theta)^\dagger \big(a|0\rangle_1|+\rangle_2 + b|1\rangle_1|-\rangle_2\big) \\ &= \sqrt{2}\langle+|_1 \big(a|0\rangle_1|+\rangle_2 + b|1\rangle_1|-\rangle_2\big) \\ &= a|+\rangle_2 + be^{i\theta}|-\rangle_2 \end{aligned} \tag{3.3}$$

ただし、$\sqrt{2}$ は規格化定数である。 また、$R_z(-\theta)^\dagger = R_z(\theta)$ であることを用いた。 これは $HR_z(\theta)|\psi\rangle$ と一致することがわかる。

$$HR_z(\theta)|\psi\rangle = a|+\rangle + be^{i\theta}|-\rangle \tag{3.4}$$

同様にして、$R_z(-\theta)|-\rangle$ に射影された場合、$XHR_z(\theta)|\psi\rangle$ になることがわかる。

$$\begin{aligned} &\sqrt{2}\langle-|_1 R_z(-\theta)^\dagger \big(a|0\rangle_1|+\rangle_2 + b|1\rangle_1|-\rangle_2\big) \\ &= \sqrt{2}\langle-|_1 \big(a|0\rangle_1|+\rangle_2 + b|1\rangle_1|-\rangle_2\big) \\ &= a|+\rangle_2 - be^{i\theta}|-\rangle_2 \\ &= X\big(a|+\rangle_2 + be^{i\theta}|-\rangle_2\big) = XHR_z(\theta)|\psi\rangle \end{aligned} \tag{3.5}$$

演算子 X は余分な演算子である。 この場合、次の測定の角度に -1 をかけることで、X を打ち消すことができる。

$$\begin{aligned} & HR_z(-\varphi)XHR_z(\theta) \\ =\ & HXR_z(\varphi)HR_z(\theta) \\ =\ & ZHR_z(\varphi)HR_z(\theta) \end{aligned} \tag{3.6}$$

ただし、$R_z(-\varphi)X = XR_z(\varphi),\ HZH = X$ を用いた。

演算子 Z も余分な演算子である。 この場合、次の測定の角度に π を足すことで、Z を打ち消すことができる。

$$HR_z(\varphi+\pi)ZHR_z(\theta) = HR_z(\varphi)HR_z(\theta) \tag{3.7}$$

とすればよい。 ただし、$R_z(\theta+\pi)Z = R_z(\theta)$ を用いた。

したがって、測定したい角度を θ 、実際にする測定の角度を θ' とすると、

$$\theta' = (-1)^{s_X}\theta + s_Z\pi \tag{3.8}$$

とすればよい。 ただし、s_i は前の測定で演算子 i がある場合は 1、ない場合は 0 を表す変数である。

3.2. Brickwork States

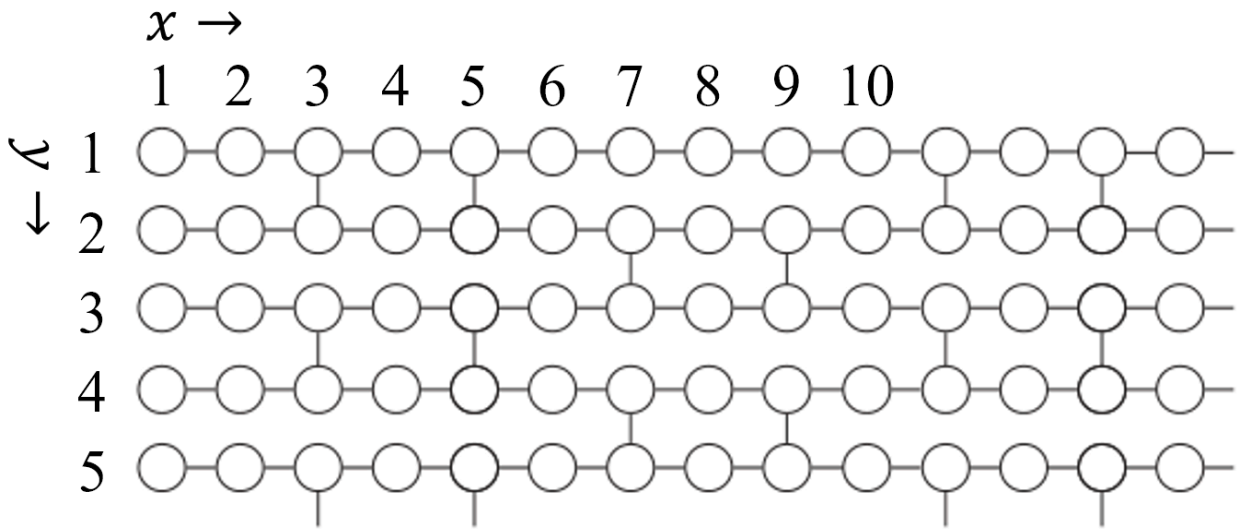

Figure 1: The brickwork state

Figure 1 のようなグラフ状態を brickwork state という。 この状態は、以下の手順によってつくられる。

1. $|+\rangle$ の状態の量子ビットを m 行 n 列の格子状に配置する。
2. それぞれの行に対して、(x, y) と $(x+1, y)$ の間に CZ ゲートをかける。
3. 奇数の行の、$x \equiv 3 \pmod 8$ に対して、(x, y) と $(x, y+1)$ の間に CZ ゲートをかける。また、$(x+2, y)$ と $(x+2, y+1)$ の間に CZ ゲートをかける。
4. 偶数の行の、$x \equiv 7 \pmod 8$ に対して、(x, y) と $(x, y+1)$ の間に CZ ゲートをかける。また、$(x+2, y)$ と $(x+2, y+1)$ の間に CZ ゲートをかける。

この状態を $|G\rangle$ とする。[1]

3.3. Universal Quantum Computation

brickwork state 上の計算は universal であることが以下のように示せる。 ただし、universal とは、任意の量子計算が（近似的に）可能であることである。 まず、$\{U_{\mathrm{CN}}, H, T\}$ は universal であることがわかっている。

U_{CN} は Figure 2 のような測定型で実現される。

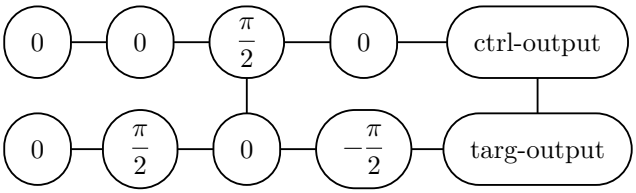

Figure 2: Implementation of U_{CN}

これが成り立つことは以下のように示せる。 この測定型は Figure 3 に示すゲート型と等価になる。

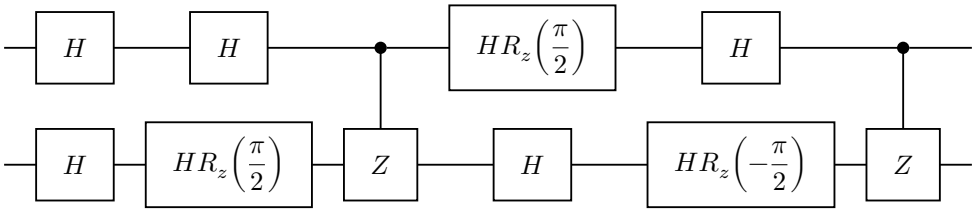

Figure 3: Gate notation of Figure 2

この回路を計算すると CNOT ゲートと一致することがわかる。

$$
\begin{aligned}
&U_{\mathrm{CZ}}\left(R_z\left(\frac{\pi}{2}\right)\otimes R_x\left(-\frac{\pi}{2}\right)\right)U_{\mathrm{CZ}}\left(I\otimes R_x\left(\frac{\pi}{2}\right)\right)\\
&=\begin{pmatrix} I & O \\ O & Z \end{pmatrix}\begin{pmatrix} R_x(-\frac{\pi}{2}) & O \\ O & e^{i\pi/2}R_x(-\frac{\pi}{2}) \end{pmatrix}\begin{pmatrix} I & O \\ O & Z \end{pmatrix}\begin{pmatrix} R_x(\frac{\pi}{2}) & O \\ O & R_x(\frac{\pi}{2}) \end{pmatrix} \qquad (3.9)\\
&=\begin{pmatrix} I & O \\ O & X \end{pmatrix}=U_{\mathrm{CN}}
\end{aligned}
$$

H は Figure 4 のような測定型で実現される。

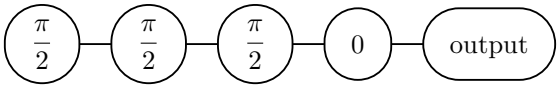

Figure 4: Implementation of H

T は Figure 5 のような測定型で実現される。

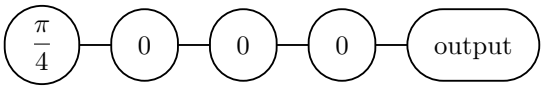

Figure 5: Implementation of T

したがって、brickwork state は universal であることが示せた。 さらに、測定の角度も $\left\{\frac{k\pi}{4} \mid k\in\mathbb{Z}\right\}$ だけでよいことがわかる。[1]

4. Blind Quantum Computation

4.1. Protocol

Alice が Bob に量子計算を依頼したいという場面を考える。 このとき、Alice にはどんなデバイスが要求されるだろうか。 結論、古典コンピュータと 1 量子ビット生成送信能力があれば実現できる。 当然、これは自身が量子コンピュータを持つよりもはるかに簡単に実現される。

m 行 n 列の brickwork state を用いて計算することを考える。 Alice は、以下の量子ビットを生成し、Bob に送る。

$$R_z(-\theta_{x,y})|+\rangle \tag{4.1}$$

ただし、(x,y) は brickwork state における座標である。 $\theta_{x,y} \in \left\{ \frac{k\pi}{4} \mid k \in \mathbb{Z} \right\}$ であり、k はランダムに選ぶ。

Bob は、受け取った量子ビットをグラフ $G=(V,E)$ に配置し、CZ ゲートを $e \in E$ に作用させる。

$$\begin{aligned} &\left(\bigotimes_{e \in E} U_{\mathrm{CZ}} \right) \left(\bigotimes_{(x,y)} R_z(-\theta_{x,y}) \right) \left(\bigotimes_{(x,y)} |+\rangle \right) \\ =& \left(\bigotimes_{(x,y)} R_z(-\theta_{x,y}) \right) \left(\bigotimes_{e \in E} U_{\mathrm{CZ}} \right) \left(\bigotimes_{(x,y)} |+\rangle \right) \\ =& \left(\bigotimes_{(x,y)} R_z(-\theta_{x,y}) \right) |G\rangle \end{aligned} \tag{4.2}$$

ただし、U_{CZ}, R_z が交換することを用いた。 この式から、回転された量子ビットを受け取ってそれを CZ でつなぐことと、$|+\rangle$ を CZ でつないでそれを回転させることは等しいことがわかる。

Alice は角度 $\varphi_{x,y}$ で測定したいとする。 しかし、測定型量子計算においては、測定の角度は計算内容そのものであるため、Bob に $\varphi_{x,y}$ をそのまま送ってはならない。 そこで、Alice は Bob に以下の古典情報を送る。

$$\delta_{x,y} = \theta_{x,y} + \varphi_{x,y} + \pi r_{x,y} \tag{4.3}$$

ただし、$r_{x,y} \in \{0,1\}$ はランダムに選ぶ。 Bob は角度 $\delta_{x,y}$ で測定する。

Bob は測定結果を Alice に送信し、Alice はそれをもとにまた角度を送信する、というのを繰り返すことが、このブラインド量子計算のプロトコルになる。[1], [2]

4.2. Correctness

correctness の定義は、Bob が悪者でない場合に Alice が正しい計算結果を得ることができることである。

以下に、δ の測定が φ の測定と本質的に等価であることを示す。 brickwork state において、(a,b) のビットを測定することを考える。

$$\begin{aligned} &\langle \pm | R_z(\delta_{a,b}) \left(\bigotimes_{(x,y)} R_z(-\theta_{x,y}) \right) |G\rangle \\ =& \langle \pm | R_z(\varphi_{a,b} + \pi r_{a,b}) \left(\bigotimes_{(x,y) \neq (a,b)} R_z(-\theta_{x,y}) \right) |G\rangle \end{aligned} \tag{4.4}$$

$r_{a,b}=0$ のときは、明らかに φ の測定になっている。 $r_{a,b}=1$ のときは以下の通り。

$$
\begin{aligned}
&\langle \pm | R_z(\varphi_{a,b} + \pi) \left(\bigotimes_{(x,y)} R_z(-\theta_{x,y}) \right) |G\rangle \\
&= \langle \pm | \big(|0\rangle\langle 0| - e^{i\theta_{a,b}} |1\rangle\langle 1| \big) \left(\bigotimes_{(x,y)\neq(a,b)} R_z(-\theta_{x,y}) \right) |G\rangle \\
&= \langle \mp | \big(|0\rangle\langle 0| + e^{i\theta_{a,b}} |1\rangle\langle 1| \big) \left(\bigotimes_{(x,y)\neq(a,b)} R_z(-\theta_{x,y}) \right) |G\rangle \\
&= \langle \pm | R_z(\varphi_{a,b}) \left(\bigotimes_{(x,y)} R_z(-\theta_{x,y}) \right) |G\rangle
\end{aligned}
\tag{4.5}
$$

したがって、この場合は測定結果を逆に解釈すればよいことがわかる。

4.3. Blindness

blindness の定義は、Bob が悪者でも Alice の秘密が守られることである。

θ の必要性については、以下のように説明できる。 もし θ がなくても安全に計算できるのであれば、量子通信は必要ない。 そのため、θ が必要かどうかは、量子通信が必要かどうかという問題と等価である。 結論、Alice が古典通信しかできない場合は、情報理論的安全性が保たれない可能性があることがわかっている。

情報理論的安全性とは、攻撃者の計算能力の高さによらず情報が手に入らないことである。 計算量的安全性とは、情報を得るための計算量が多項式時間を超えることである。

もし BQP $\subseteq$ NP ならば、Alice は古典通信しか用いることができなくとも情報理論的安全性が保障されることがわかっている。 ここで、BQP とは、量子コンピュータによって誤り確率が高々 1/3 で多項式時間で解ける計算量クラスであり、NP とは、答えが yes となるような問いに対して、多項式時間で検証できる計算量クラスである。 しかし、現在では BQP $\not\subseteq$ NP であると考えられている。 そのため、古典通信のみでブラインド量子計算を行うことは推奨されない。[(1)]

r の必要性については、以下のように説明できる。 r という変数をなくし $\delta = \theta + \varphi$ を Bob に送信することを考える。 Bob が悪者で、Alice が送信した量子ビットを無断で測定し、θ に関する情報を 1 ビット得たとする。 Bob にとって δ は当然既知なので、φ に関する情報を手に入れてしまうことになる。 情報理論的安全性では、情報が手に入らないことが条件となるため、新たに 1 ビットの変数 r を足すことによって、Bob が手に入れた 1 ビットの情報が打ち消され、φ に関する情報は手に入らず、条件を満たすことができる。[2]

4.4. Verifiability

verifiability の定義は、Alice が Bob のした量子計算が正しいか検証することができることである。 このプロトコルでは、Bob が正しく計算しているか確認する術がないため、検証性は満たすことができない。

Bibliography

[1] A. Broadbent, J. Fitzsimons, and E. Kashefi, “Universal Blind Quantum Computation”, arXiv:0807.4154v3, 2009.

[2] 小柴健史, 藤井啓祐, and 森前智之, 観測に基づく量子計算. コロナ社, 2017.

[(1)] この話は私は全く理解していません。 当時はモヤモヤしましたが今となっては興味ありません。