Quantum Computing

Part II: Quantum Algorithms

Jamal Slim

FTX - SFT Group

jamal.slim@desy.de

Regular Group Meeting
September 29, 2022

Presentation Overview

- No-cloning algorithm
- Quantum teleportation algorithm
- Quantum Fourier transform algorithm

No-Cloning Algorithm

- At the very basic level of classical computing, bits/data are written/read/copied between registers.
- This is not allowed arbitrary in quantum computing.
- Important results from QM, not all quantum states can be cloned or copied to another identical system.
    - Classically, information is copied but not the system.
- Applications of the "No-cloning" algorithm in quantum computing and quantum communications
    - Eavesdropping cannot copy messages
        - Messages will be destroyed
    - Secure quantum channels

No-Cloning Algorithm

- Let A and B be 2 electrons with initial states $|\Psi\rangle_{\mathrm{A}} = \alpha\,|0\rangle_{\mathrm{A}} + \beta\,|1\rangle_{\mathrm{A}}$ and $|0\rangle_{\mathrm{B}}$
- Cloning must be done though an operation not a measurement.
- Reading (measuring) collapses the state of the electron to $|0\rangle$ or $|1\rangle$
- Let the cloning operator be called $\mathcal{L}$ with

$$\mathcal{L}(|\Psi\rangle_{\mathrm{A}}\,|0\rangle_{\mathrm{B}}) = |\Psi\rangle_{\mathrm{A}}\,|\Psi\rangle_{\mathrm{B}}\,. \tag{1}$$

No-Cloning Algorithm

$$\begin{aligned}\mathcal{L}(|\Psi\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}}) &= |\Psi\rangle_{\mathrm{A}}|\Psi\rangle_{\mathrm{B}} \\ &= (\alpha|0\rangle_{\mathrm{A}} + \beta|1\rangle_{\mathrm{A}}) \otimes (\alpha|0\rangle_{\mathrm{B}} + \beta|1\rangle_{\mathrm{B}}) \\ &= \alpha^2|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + \alpha\beta|0\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}} + \beta\alpha|1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + \beta^2|1\rangle_{\mathrm{A}}|1\rangle_{\mathrm{B}} \\ &= \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle\end{aligned}$$

while on the other hand

$$\begin{aligned}|\Psi\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} &= (\alpha|0\rangle_{\mathrm{A}} + \beta|1\rangle_{\mathrm{A}})|0\rangle_{\mathrm{B}} \\ &= \alpha|0\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} + \beta|1\rangle_{\mathrm{A}}|0\rangle_{\mathrm{B}} \\ &= \alpha|00\rangle + \beta|10\rangle\,.\end{aligned}$$

Now,

$$\begin{aligned}\mathcal{L}(\alpha|00\rangle + \beta|10\rangle) &= \mathcal{L}\alpha|00\rangle + \mathcal{L}\beta|10\rangle \\ &= \alpha|00\rangle + \beta|11\rangle + 0|01\rangle + 0|10\rangle\,.\end{aligned}$$

- This means $\alpha = 0$ or $\beta = 0$.
- It is possible to clone the basis states but not other superposition states.

Quantum Teleportation Algorithm

- Purpose: transfer the state of Alice's with state $|\psi\rangle_{\mathrm{A}} = \alpha\,|0\rangle_{\mathrm{A}} + \beta\,|1\rangle_{\mathrm{A}}$ electron to Bob's electron with a possible state $|0\rangle_{\mathrm{B}}$, in no time, regardless of their distance.
- The algorithm is in three steps:
  1. create an en entanglement between $|\psi\rangle_{\mathrm{A}}$ and $|0\rangle_{\mathrm{B}}$,
  2. measure Alice qubits $|+\rangle\,/|-\rangle$ basis,
  3. complete the teleportation using a classical channel.

Quantum Teleportation Algorithm

create an entanglement between $|\psi\rangle_{\mathrm{A}}$ and $|0\rangle_{\mathrm{B}}$

- Entanglement can be created using a hypothetical CNOT Gate ($\mathrm{U}_{\mathrm{XOR}}$).
- $|\psi\rangle_{\mathrm{A}}$ and $|0\rangle_{\mathrm{B}}$ form a $\mathbb{C}^4$ space of

$$\begin{aligned} |\psi\rangle_{\mathrm{A}} \otimes |0\rangle_{\mathrm{B}} &= (\alpha\,|0\rangle + \beta\,|1\rangle)_{\mathrm{A}} \otimes |0\rangle_{\mathrm{B}} \\ &= \alpha\,|0\rangle_{\mathrm{A}}\,|0\rangle_{\mathrm{B}} + \beta\,|1\rangle_{\mathrm{A}}\,|0\rangle_{\mathrm{B}} \\ &= \alpha\,|00\rangle + \beta\,|10\rangle\,. \end{aligned}$$

- Applying a CNOT gate the state of the 2-qubits system becomes

$$\alpha\,|00\rangle + \beta\,|11\rangle\,.$$

- Which is an entangled state.

- Now, Alice measures her qubit in the $|+\rangle / |-\rangle$ basis using

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \,\text{and}\,,$$
$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle).$$

- Which leads to

$$\begin{aligned}\alpha |00\rangle + \beta |11\rangle &= \alpha |0\rangle_{\mathrm{A}} |0\rangle_{\mathrm{B}} + \beta |1\rangle_{\mathrm{A}} |1\rangle_{\mathrm{B}} \\ &= |+\rangle \frac{1}{\sqrt{2}}(\alpha |0\rangle_{\mathrm{B}} + \beta |1\rangle_{\mathrm{B}}) \\ &\quad + |-\rangle \frac{1}{\sqrt{2}}(\alpha |0\rangle_{\mathrm{B}} - \beta |1\rangle_{\mathrm{B}}).\end{aligned}$$

- Bob's qubit gets some information related to Alice's qubit's original state, i.e. it has α and β as the coefficients

Quantum Teleportation Algorithm

complete the teleportation using a classical channel

- The results of Alice is $|+\rangle$ or $|-\rangle$ and Bob's qubit becomes either $\alpha\,|0\rangle_{\mathrm{B}} + \beta\,|1\rangle_{\mathrm{B}}$ or $\alpha\,|0\rangle_{\mathrm{B}} - \beta\,|1\rangle_{\mathrm{B}}$
- This is because the collapse of the wavefunction and it is instantaneous.
- Alice 's state is teleported to Bob faster than the speed of light.
- No transfer of useful information as Bob does not know Alice has performed the measurement
- Bob doesn't know if his qubit has a state $\alpha\,|0\rangle_{\mathrm{B}} + \beta\,|1\rangle_{\mathrm{B}}$ or $\alpha\,|0\rangle_{\mathrm{B}} - \beta\,|1\rangle_{\mathrm{B}}$

Quantum Teleportation Algorithm

complete the teleportation using a classical channel

- Alice will then call Bob and let him know her outcome through a classical channel, which is slower than or the same as the speed of the light.
- Case Alice measured $|+\rangle$, Bob knows that his electron is in the state of $|\psi\rangle$, and the quantum teleportation process is completed. Or equivalently, he will apply an identity gate to his qubit.
- Case Alice measured $|-\rangle$, Bob knows that his electron is in the state of $\alpha\,|0\rangle_{\mathrm{B}} - \beta\,|1\rangle_{\mathrm{B}}$ and not $|\psi\rangle$.
- bob applies a Z-gate which is a phase shift gate with angle being π to convert it his measurement to $|\psi\rangle$ and the quantum teleportation process is completed.

Quantum Teleportation Algorithm

large distance quantum gate?

- An ideal CNOT gate that needs to operate on two qubits separated by a large distance is hypothetical.
- A possible solution is to use one additional qubit called the ancillary qubit.
- The ancillary qubit is transported from Bob's lab to Alice's lab before performing any quantum teleportation.

Quantum Teleportation Algorithm

large distance quantum gate?

- Bob will entangle his qubit, $|0\rangle_{\mathrm{B}}$ with the ancillary qubit initialized as $|0\rangle_{\mathrm{BB}}$.
- Bob's qubit is the LSB.
- The state of Bob's qubits is $|0\rangle_{\mathrm{BB}} \otimes |0\rangle_{\mathrm{B}}$.
- Bob applies the Hadamard gate to create a superposition of the basis states as $\frac{1}{\sqrt{2}}(|0\rangle_{\mathrm{BB}} + |1\rangle_{\mathrm{BB}}) \otimes |0\rangle_{\mathrm{B}} = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$
- A CNOT gate applied, which results in $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, which is an entangled state ($|\phi^{+}\rangle$ Bell state).

Quantum Teleportation Algorithm

large distance quantum gate?

- Bob sends the extra qubit to Alice (still entangled) with his original qubit.
- Alice decides to quantum teleport her qubit information to Bob. $|\psi\rangle_{\mathrm{A}} = \alpha\,|0\rangle_{\mathrm{A}} + \beta\,|1\rangle_{\mathrm{A}}$.
- She performs a CNOT operation, by using her qubit A as the control qubit, on qubit BB which was sent by Bob earlier and is still entangled with Bob's qubit B. Before the CNOT gate,

$$|\psi_{\mathrm{A}}\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha\,|000\rangle + \beta\,|100\rangle + \alpha\,|011\rangle + \beta\,|111\rangle)$$

- After the CNOT gate

$$\frac{1}{\sqrt{2}}(\alpha\,|000\rangle + \beta\,|110\rangle + \alpha\,|011\rangle + \beta\,|101\rangle)$$

$$\frac{1}{\sqrt{2}}(\alpha\,|000\rangle + \beta\,|101\rangle + \alpha\,|011\rangle + \beta\,|110\rangle)$$

- Alice performs a measurement on the second qubit (BB) on the $|0\rangle / |1\rangle$ basis.
- Case $|0\rangle$, the whole system has collapsed to a state having only $|000\rangle$ and $|101\rangle$.
- Considering only the MSB and the LSB, they are entangled!
- Alice calls Bob telling him that she got $|0\rangle$ and their qubits have been entangled and they can continue to perform Step 2 and Step 3 to complete the quantum teleportation.

Quantum Teleportation Algorithm - Cont

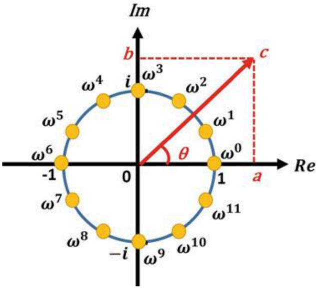
measurement of the Ancillary Qubit

- Case $|1\rangle$, the whole system has collapsed to a state having only $|011\rangle$ and $|110\rangle$.
- Considering only the MSB and the LSB, they are entangled, because when the MSB is 1 (or 0), the LSB is always 0 (or1).
- Alice calls Bob telling him that she got $|1\rangle$ and Bob just needs to apply a NOT gate to his qubit to flip the bit value in the basis states and they can continue to perform Step 2 and Step 3 to complete the quantum teleportation.

Discrete Fourier Transform DFT

Basic reminders

- The N-th root of unity: $\mathrm{z}^{\mathrm{N}} = 1$
- $\omega = \mathrm{e}^{\mathrm{i}2\pi/\mathrm{N}}$
- $\omega^{\mathrm{m+N}} = \omega^{\mathrm{m}}$
- $\sum_{\mathrm{m}=0}^{\mathrm{N}-1} \omega^{\mathrm{m}} = 0$ (destructive interference)
- For an integer $\mathrm{q} \neq 0$, $\sum_{\mathrm{m}=0}^{\mathrm{N}-1} \omega^{\mathrm{mq}} = 0$ (destructive interference)
- For an integer $\mathrm{q} = 0$, $\sum_{\mathrm{m}=0}^{\mathrm{N}-1} \omega^{\mathrm{mq}} = \mathrm{N}$ (constructive interference)
- $\omega^{\mathrm{N-m}} = \omega^{-\mathrm{m}}$



Discrete Fourier Transform DFT

Classical definition

- The DFT is defined as

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{-kj} x_j = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-i2\pi kj} x_j$$

given

$$x = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix} \text{ and, } y = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix}$$

Discrete Fourier Transform DFT

- In matrix form,

$$y = \Omega x$$

$$\begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{pmatrix} = \frac{1}{\sqrt{N}} \begin{pmatrix} \omega^{-0\cdot 0} & \omega^{-0\cdot 1} & \dots & \omega^{-0\cdot(N-1)} \\ \omega^{-1\cdot 0} & \omega^{-1\cdot 1} & \dots & \omega^{-1\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{-(N-1)\cdot 0} & \omega^{-(N-1)\cdot 1} & \dots & \omega^{-(N-1)\cdot(N-1)} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{pmatrix}$$

- Each column and row in the DFT matrix are composed of a power series of the N-th roots of unity
- DFT that it is constructed in a way to perform constructive and destructive interferences by arranging the power series of the N -th roots of unity in the rows and columns.

Quantum Fourier Transform QFT

- In simple terms, DFT is just a rotation of the vector on a given basis

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega^{-kj} x_j = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-i2\pi kj} x_j$$

- If the quantum basis states $|j\rangle$ are used as the basis vectors, DFT is called QFT.
- QFT is a quantum gate and must be unitary.

Quantum Fourier Transform QFT

- In an N-dimensional space, $N = 2^n$ with n qubits, with a matrix, U_{QFT} , is defined exactly as Ω

$$U_{QFT} = \frac{1}{\sqrt{N}} \begin{pmatrix} \omega^{-0\cdot 0} & \omega^{-0\cdot 1} & \dots & \omega^{-0\cdot(N-1)} \\ \omega^{-1\cdot 0} & \omega^{-1\cdot 1} & \dots & \omega^{-1\cdot(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega^{-(N-1)\cdot 0} & \omega^{-(N-1)\cdot 1} & \dots & \omega^{-(N-1)\cdot(N-1)} \end{pmatrix}$$

- U_{QFT} transforms the basis vectors $|j\rangle$ and $|k\rangle$ as

$$U_{QFT}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{-kj}|k\rangle$$

Quantum Fourier Transform QFT

QFT on basis vectors $|0\rangle$ and $|1\rangle$

- 1-qubit QFT

$$
\begin{aligned}
\mathrm{U_{QFT}}\,|0\rangle &= \frac{1}{\sqrt{\mathrm{N}}}\sum_{\mathrm{k}=0}^{\mathrm{N}-1}\omega^{-\mathrm{k}\cdot 0}\,|\mathrm{k}\rangle \\
&= \frac{1}{\sqrt{2}}(\omega^{-0\cdot 0}\,|0\rangle + \omega^{-1\cdot 0}\,|1\rangle) \\
&= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
&= |+\rangle
\end{aligned}
$$

- Similarly

$$\mathrm{U_{QFT}}\,|1\rangle = |-\rangle$$

- This is the same as the definition of the Hadamard gate

The End

Questions? Comments?