Basic quantum algorithms: BB84, dense coding, teleportation

Yipeng Huang

Rutgers University

September 26, 2022

Table of contents

Quantum postulate 3: Measurement

When a closed quantum system with state $|\psi\rangle$ interacts with the environment, measurement takes place:

- The probability of the post-measurement state being in state $|a_n\rangle$ is: $p(|a_n\rangle) = \langle\psi| |a_n\rangle \langle a_n| |\psi\rangle = |\langle a_n| |\psi\rangle|^2$
- The state of the quantum system is then renormalized to $\frac{|a_n\rangle\langle a_n||\psi\rangle}{\sqrt{p(|a_n\rangle)}}$

Let's practice this with measuring a single-qubit state.

No-cloning theorem

There is no way to duplicate an arbitrary quantum state

Suppose a cloning operation U_c exists. Then:

- $$U_c(|\phi\rangle \otimes |\omega\rangle) = |\phi\rangle \otimes |\phi\rangle\,,$$
  $$U_c(|\psi\rangle \otimes |\omega\rangle) = |\psi\rangle \otimes |\psi\rangle\,,$$
  for arbitrary states $|\phi\rangle\,, |\psi\rangle$ we wish to copy.
- The overlap of the initial states is:

$$\langle\phi| \otimes \langle\omega| \, |\psi\rangle \otimes |\omega\rangle = \langle\phi| \, |\psi\rangle \cdot \langle\omega| \, |\omega\rangle = \langle\phi| \, |\psi\rangle$$

No-cloning theorem

There is no way to duplicate an arbitrary quantum state

Suppose a cloning operation U_c exists. Then:

- $$U_c(|\phi\rangle \otimes |\omega\rangle) = |\phi\rangle \otimes |\phi\rangle\,,$$
  $$U_c(|\psi\rangle \otimes |\omega\rangle) = |\psi\rangle \otimes |\psi\rangle\,,$$
  for arbitrary states $|\phi\rangle\,, |\psi\rangle$ we wish to copy.
- The overlap of the final states is:
  $$\langle\phi| \otimes \langle\phi| \, |\psi\rangle \otimes |\psi\rangle = \langle\phi| \, |\psi\rangle \cdot \langle\phi| \, |\psi\rangle = (\langle\phi| \, |\psi\rangle)^2$$
- The overlap of the final states is also:
  $$\langle\phi| \otimes \langle\phi| \, |\psi\rangle \otimes |\psi\rangle = \langle\phi| \otimes \langle\omega| \, U^\dagger U \, |\psi\rangle \otimes |\omega\rangle = \langle\phi| \otimes \langle\omega| \, |\psi\rangle \otimes |\omega\rangle = \langle\phi| \, |\psi\rangle$$
- $(\langle\phi| \, |\psi\rangle)^2 = \langle\phi| \, |\psi\rangle$, so $\langle\phi| \, |\psi\rangle = 0$, or $\langle\phi| \, |\psi\rangle = 1$, $|\phi\rangle$ and $|\psi\rangle$ cannot be arbitrary states as claimed.

Table of contents

Entangled states: Bell state circuit

Bell state circuit

$$|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle + |10\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = |\Phi^+\rangle$$

Can $|\Phi^+\rangle$ be treated as the tensor product (composition) of two individual qubits?

Prove that the Bell state cannot be factored into two single-qubit states

Bell state circuit

$$|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle + |10\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = |\Phi^+\rangle$$

Can $|\Phi^+\rangle$ be treated as the tensor product (composition) of two individual qubits?
No.

Bell states form an orthogonal basis set

1. $|00\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle + |10\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle\Big) = |\Phi^+\rangle$
2. $|01\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|01\rangle + |11\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle\Big) = |\Psi^+\rangle$
3. $|10\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle - |10\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle\Big) = |\Phi^-\rangle$
4. $|11\rangle \xrightarrow{H\otimes I} \frac{1}{\sqrt{2}}\Big(|01\rangle - |11\rangle\Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big) = |\Psi^-\rangle$

Superdense coding

Transmit 2 bits of classical information by sending 1 qubit

1. Alice wishes to tell Bob two bits of information: 00, 01, 10, or 11.
2. Alice and Bob each have one qubit of a Bell pair in state $|P\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)$.
3. Alice performs I, X, Z, or ZX on her qubit; she then sends her qubit to Bob.
4. Bob measures in the Bell basis to receive 00, 01, 10, or 11.

Superdense coding circuit

`https://github.com/quantumlib/Cirq/blob/master/examples/superdense_coding.py`

Superdense coding

Transmit 2 bits of classical information by sending 1 qubit

1. Alice wishes to tell Bob two bits of information: 00, 01, 10, or 11.
2. Alice and Bob each have one qubit of a Bell pair in state $|P\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big)$.
3. Alice performs I, X, Z, or ZX on her qubit; she then sends her qubit to Bob.
4. Bob measures in the Bell basis to receive 00, 01, 10, or 11.

Alice applies different operators on her qubit so Bob measures the message

1. $|P\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \xrightarrow{I\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle + |10\rangle \Big) \xrightarrow{H\otimes I} |00\rangle$
2. $|P\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \xrightarrow{X\otimes I} \frac{1}{\sqrt{2}}\Big(|10\rangle + |01\rangle \Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|11\rangle + |01\rangle \Big) \xrightarrow{H\otimes I} |01\rangle$
3. $|P\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \xrightarrow{Z\otimes I} \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle \Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(|00\rangle - |10\rangle \Big) \xrightarrow{H\otimes I} |10\rangle$
4. $|P\rangle = \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big) \xrightarrow{ZX\otimes I} \frac{1}{\sqrt{2}}\Big(-|10\rangle + |01\rangle \Big) \xrightarrow{CNOT} \frac{1}{\sqrt{2}}\Big(-|11\rangle + |01\rangle \Big) \xrightarrow{H\otimes I} |11\rangle$

Table of contents

Quantum teleportation

"Teleport" a qubit state by transmitting classical information

1. Alice wishes to give Bob a qubit state $|Q\rangle$.
2. Alice and Bob each have one qubit of a Bell pair in state $|P\rangle$.
3. Alice first entangles $|Q\rangle$ and $|P\rangle$; then, she measures her local two qubits.
4. Alice tells Bob (via classical means) her two-bit measurement result.
5. Bob uses Alice's two bits to perform I, X, Z, or ZX on his qubit to obtain $|Q\rangle$.

Step-by-step qubit state calculation up to Alice's measurement

$$
\begin{aligned}
|Q\rangle \otimes |P\rangle &= \big(\alpha\,|0\rangle + \beta\,|1\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \\
&= \frac{\alpha}{\sqrt{2}}\,|0\rangle\,\big(\,|00\rangle + |11\rangle\,\big) + \frac{\beta}{\sqrt{2}}\,|1\rangle\,\big(\,|00\rangle + |11\rangle\,\big) \\
&\xrightarrow{CNOT_{0,1}} \frac{\alpha}{\sqrt{2}}\,|0\rangle\,\big(\,|00\rangle + |11\rangle\,\big) + \frac{\beta}{\sqrt{2}}\,|1\rangle\,\big(\,|10\rangle + |01\rangle\,\big) \\
&\xrightarrow{H\otimes I\otimes I} \frac{\alpha}{2}\big(\,|0\rangle + |1\rangle\,\big)\big(\,|00\rangle + |11\rangle\,\big) + \frac{\beta}{2}\big(\,|0\rangle - |1\rangle\,\big)\big(\,|10\rangle + |01\rangle\,\big) \\
&= \frac{1}{2}\,|00\rangle\,\big(\alpha\,|0\rangle + \beta\,|1\rangle\,\big) \\
&\quad + \frac{1}{2}\,|01\rangle\,\big(\alpha\,|1\rangle + \beta\,|0\rangle\,\big) \\
&\quad + \frac{1}{2}\,|10\rangle\,\big(\alpha\,|0\rangle - \beta\,|1\rangle\,\big) \\
&\quad + \frac{1}{2}\,|11\rangle\,\big(\alpha\,|1\rangle - \beta\,|0\rangle\,\big)
\end{aligned}
$$

Quantum teleportation

"Teleport" a qubit state by transmitting classical information

1. Alice wishes to give Bob a qubit state $|Q\rangle$.
2. Alice and Bob each have one qubit of a Bell pair in state $|P\rangle$.
3. Alice first entangles $|Q\rangle$ and $|P\rangle$; then, she measures her local two qubits.
4. Alice tells Bob (via classical means) her two-bit measurement result.
5. Bob uses Alice's two bits to perform I, X, Z, or ZX on his qubit to obtain $|Q\rangle$.

Depending on if Alice measures 00, 01, 10, or 11, Bob applies I, X, Z, or ZX to recover $|Q\rangle$

$$
\begin{aligned}
|Q\rangle \otimes |P\rangle &= \big(\alpha\,|0\rangle + \beta\,|1\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big) \\
&= \frac{\alpha}{\sqrt{2}}\,|0\rangle\big(|00\rangle + |11\rangle\big) + \frac{\beta}{\sqrt{2}}\,|1\rangle\big(|00\rangle + |11\rangle\big) \\
&\xrightarrow{CNOT_{0,1}} \frac{\alpha}{\sqrt{2}}\,|0\rangle\big(|00\rangle + |11\rangle\big) + \frac{\beta}{\sqrt{2}}\,|1\rangle\big(|10\rangle + |01\rangle\big) \\
&\xrightarrow{H\otimes I\otimes I} \frac{\alpha}{2}\big(|0\rangle + |1\rangle\big)\big(|00\rangle + |11\rangle\big) + \frac{\beta}{2}\big(|0\rangle - |1\rangle\big)\big(|10\rangle + |01\rangle\big) \\
&= \frac{1}{2}\,|00\rangle\big(\alpha\,|0\rangle + \beta\,|1\rangle\big) \quad \text{Alice measures 00 so Bob applies I} \\
&+ \frac{1}{2}\,|01\rangle\big(\alpha\,|1\rangle + \beta\,|0\rangle\big) \quad \text{Alice measures 01 so Bob applies X} \\
&+ \frac{1}{2}\,|10\rangle\big(\alpha\,|0\rangle - \beta\,|1\rangle\big) \quad \text{Alice measures 10 so Bob applies Z} \\
&+ \frac{1}{2}\,|11\rangle\big(\alpha\,|1\rangle - \beta\,|0\rangle\big) \quad \text{Alice measures 11 so Bob applies ZX}
\end{aligned}
$$