

Assignment4

22D10126 Yuya Okada

♠Q22

- (1) When the input state to the quantum circuit represented by (110) is $|11\rangle$, the results for a step-by-step calculation are as follows.

$$|\Psi_{\text{in}}\rangle = |11\rangle \quad (1)$$

$$|\Psi_{\text{mid}}\rangle = (\hat{H}|1\rangle) \otimes |1\rangle \quad (2)$$

$$|\Psi_{\text{out}}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \quad (3)$$

- (2) Applying the CNOT gate to a single state $|S\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ changes it to

$$\frac{|01\rangle - |11\rangle}{\sqrt{2}}. \quad (4)$$

This can be rewritten as a separable state

$$\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes |1\rangle \quad (5)$$

and proved to be not entangled.

- (3) For example, consider the superposition of $|\Phi_+\rangle$ and $|\Psi_+\rangle$. If c_0 and c_1 are complex, the superposition of $|\Phi_+\rangle$ and $|\Psi_+\rangle$ can be written as

$$c_0|\Phi_+\rangle + c_1|\Psi_+\rangle. \quad (6)$$

If $c_0 = c_1$, then the above equation becomes

$$\begin{aligned} c_0(|\Phi_+\rangle + |\Psi_+\rangle) &= c_0 \left(\frac{|00\rangle + |11\rangle + |01\rangle + |10\rangle}{\sqrt{2}} \right) \\ &= c_0 \left(\frac{|00\rangle + |10\rangle + |01\rangle + |11\rangle}{\sqrt{2}} \right) \\ &= c_0 \left(\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \otimes |0\rangle + \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \otimes |1\rangle \right) \\ &= c_0 \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \otimes (|0\rangle + |1\rangle), \end{aligned} \quad (7)$$

which is the not entangled state. Thus, it is shown that even superposition of entangled states may not result in an entangled state.

♠Q23

- (1) When the initial state of qubit A is $|\psi\rangle + c_0|0\rangle + c_1|1\rangle$, the three-qubit state before the process denoted by E is

$$c_0|001\rangle + c_1|110\rangle. \quad (8)$$

- (2) When the three-qubit state is preserved by the process E , the final state of qubit A is $c_0|0\rangle + c_1|1\rangle$.

- (3) the final three-qubit state : $c_0|110\rangle + c_1|010\rangle$
the final qubit A state : $c_0|1\rangle + c_1|0\rangle$
- (4) the final three-qubit state : $c_0|011\rangle + c_1|011\rangle$
the final qubit A state : $c_0|0\rangle + c_1|0\rangle$
- (5) the final three-qubit state : $c_0|000\rangle + c_1|100\rangle$
the final qubit A state : $c_0|0\rangle + c_1|1\rangle$
- (6) the final three-qubit state : $c_0|010\rangle + c_1|110\rangle$
the final qubit A state : $c_0|0\rangle + c_1|1\rangle$

♠Q24

Quantum bits(qubit)

Quantum bit is the smallest unit of a quantum and is represented by a superposition of zero and one states. A qubit represents quantum state transitions using probabilities. Classical bits can only take either 0 or 1 state, and the number of bits increases exponentially with the number of bits to represent all combinations of states, but a qubit can treat each combination as a single probabilistic state. A quantum computer that uses this property is expected to significantly shorten computation time.

Quantum Cryptography

Quantum cryptography is a method of splitting the key for decryption apart from the encrypted information and sending it on a photon. Current cryptography is secured by increasing the computational complexity of prime factorization when solving it, but this could be solved by a quantum computer. Quantum cryptography uses the property of photons to change states when they are observed to detect information theft and to create a new key with the information that has not been stolen.

Quantum Computation

Quantum computation is a method of computing using quantum superpositions. In classical computation, the computational complexity increases exponentially with the number of bits, whereas in quantum computation, the superposition of multiple states can be represented as a single state vector, so the computational complexity increases only polynomial as the number of digits increases. On the other hand, measurements must be repeated to obtain the desired answer, and algorithms such as the quantum Fourier transform are used to select only the states necessary for the answer from the states of the computation results.