ELEC-C9420 Introduction to Quantum Technology, Fall 22
Midterm exam 2, model solutions

Problem 1

Connect the correct concept with the correct formula. Write the letter-number pairs on the answer sheet. (+3p for a right answer, −3p for a wrong answer. Minimum 0 points for the whole problem.)

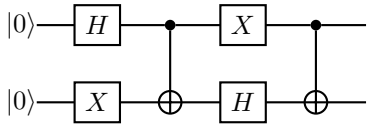
A) state vector normalization	1) $\sigma_x \sigma_p \geq \hbar/2$
B) Heisenberg uncertainty principle	2) $\lambda = h/p,\ f = E/h$
C) de Broglie hypothesis	3) $\|\psi\rangle = \cos(\theta/2)\|0\rangle + e^{i\varphi}\sin(\theta/2)\|1\rangle$
D) Bloch sphere	4) $\langle\psi\|\psi\rangle = 1$

Model solution

A4, B1, C2, D3

Problem 2

Consider the quantum circuit below.



a) Find the final state of the circuit. (3p)
b) Are the two qubits entangled in the final state? (3p)
c) Compute the expectation value for the value of the first qubit in the final state. (3p)
d) Compute the expectation value of the observable X for the second qubit in the final state. (3p)

HINT: Both the gate X and the observable X are defined by the following action on the single-qubit computational basis states: $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$.

Model solution

a)
The initial state is $|00\rangle$, applying Hadamard gate to the first qubit
$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$

And then applying the X gate to the second qubit
$\frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$

Applying the first cNOT-gate
$\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

Applying the X-gate to the first qubit and Hadamard gate to the second qubit
$\frac{1}{\sqrt{2}}(|11\rangle + |00\rangle) \longrightarrow \frac{1}{\sqrt{2}}(|1\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) + |0\rangle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{1}{2}(|10\rangle - |11\rangle + |00\rangle + |01\rangle)$

Finally applying the last cNOT-gate for the final state
$\frac{1}{2}(|11\rangle - |10\rangle + |00\rangle + |01\rangle) = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle)$

b)
The final state is entangled, if the state cannot be represented as a product of two single qubit states.
The product of two arbitrary one qubit states is
$(a_1|0\rangle + b_1|1\rangle)(a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$

Note that $b_1 a_2$ has to equal to $-\frac{1}{2}$, meaning that either b_1 or a_2 has to be negative.
If a_2 is negative, then a_1 has to be negative too in order for $a_1 a_2$ to be positive, meaning that $b_1 b_2$ wouldn't be positive as b_2 has to be negative in order to make the product $a_1 b_2$ positive.
Therefore the final state cannot be represented as a product of any two single qubit states, meaning that it is an entangled state.

c)
The expectation value for the first qubit can be calculated as the expectation value of the operator $\hat{b} \otimes I$, which can be calculated as follows

$\frac{1}{4}(\langle 00| + \langle 01| - \langle 10| + \langle 11|)\hat{b} \otimes I(|00\rangle + |01\rangle - |10\rangle + |11\rangle)$

$= \frac{1}{4}(\langle 00| + \langle 01| - \langle 10| + \langle 11|)(-|10\rangle + |11\rangle)$

$= \frac{1}{4}(1 + 1) = \frac{1}{2}$

d)
The expectation value of the observable X for the second qubit is f

$\frac{1}{4}(\langle 00| + \langle 01| - \langle 10| + \langle 11|)I \otimes X(|00\rangle + |01\rangle - |10\rangle + |11\rangle)$

$= \frac{1}{4}(\langle 00| + \langle 01| - \langle 10| + \langle 11|)(|01\rangle + |00\rangle - |11\rangle + |10\rangle)$

$= \frac{1}{4}(1 + 1 - 1 - 1) = 0$

The observable X swaps the second qubit, resulting in two states with negative signs and two states with positive signs, cancelling each other out.

Problem 3

Answer in the following questions with a couple of full sentences. Explain the reasons behind your answers, i.e., yes/no answer is not sufficient. (max. 3p per question)

a) Can quantum mechanical correlations be explained classically?
b) Does quantum state collapse allow for superluminal (i.e., faster than the speed of light) communication?
c) Why does quantum computing pose a threat to cyber safety?
d) How does the BB84 (mistakenly called BB88 in the lectures) quantum key distribution protocol take advantage of the no-cloning theorem?

Model solution

a) Can quantum mechanical correlations be explained classically?

Not all quantum mechanical correlations can be explained classically. (1p) Quantum entanglement causes correlations that violate classical logic and probability theory. For example, Bell's theorem demonstrates that the correlations in the Bell state differ from those that are classically permitted. (2p) Any theory of hidden variables must contradict locality. Quantum computing makes use of quantum correlations and the high dimensionality of the state space.

b) Does quantum state collapse allow for superluminal (i.e., faster than the speed of light) communication?

No, collapsing an entangled pair occurs instantaneously but cannot be used to transmit information faster than light. (1p) Since the measurement result cannot be selected before the measurement is performed, classic information is needed to transmit the measurement results. For instance, entanglement is used in quantum teleportation to send quantum states over long distances. But teleportation also needs a classical bit sent along with the entangled qubits. As a result, even though entanglement operates

instantly, information transfer is slowed down by the speed of classical information, which is limited to the speed of light. (2p)

c) Why does quantum computing pose a threat to cyber safety?

Some of the currently widely used cryptography, such as RSA encryption, is based on the problem of factoring large numbers. (1p) Shor's algorithm is a quantum computer algorithm for finding the prime factors of an integer. The algorithm can factor integers in polynomial time. (1p) Thus, quantum computers pose a threat to the cyber system by being able to solve the problem in a reasonably short time. (1p)

d) How does the BB84 (mistakenly called BB88 in the lectures) quantum key distribution protocol take advantage of the no-cloning theorem?

The no-cloning theorem states that there does not exist an algorithm to make a copy of a generic quantum state of a qubit. (1p) Quantum key distribution (QKD) proposes to use a quantum channel to exchange private encryption keys between the sender and the receiver. (1p) Because the eavesdropper will be detected by the sender and receiver if they perform a measurement, BB84 is unconditionally secure if the sender emits a single photon. However, if the sender emits multiple photons the eavesdropper could theoretically use a photon number splitting attack to obtain complete information on bit values without causing any bit errors. Keeping in mind that the multi-photon emission event can be viewed as the scenario in which the eavesdropper can create some copies of the single-photon that Alice emitted. Because cloning is strictly forbidden by the no-cloning theorem, the security of QKD is protected. (1p)