EXAM QUANTUM INFORMATION, 14 DECEMBER 2023, 14–17 HOURS.

1. • *a)* Given a quantum state $|\psi\rangle = 2^{-1/2}(|0\rangle + |1\rangle)$, what will be the state after applying first the Pauli-X gate and then the Pauli-Z gate? Does it matter if you reverse the order (first the Z-gate and then the X-gate)?

   • *b)* Qubits A and B are entangled in the state

   $$|\Psi\rangle = 2^{-1/2}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B). \tag{1}$$

   Apply the CNOT gate with qubit A as the control and qubit B as the target. Compute the partial density matrix ρ_A of qubit A *before* and *after* the CNOT operation.

   • *c)* The CNOT gate has changed the partial density matrix of qubit A. Alice asks you: "I thought that the CNOT gate has no effect on the control qubit, so how can ρ_A change?" What is your explanation?

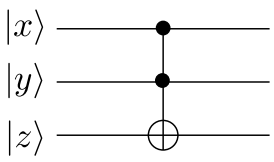
2. Alice and Bob share an entangled pair of qubits in the state $|\Psi\rangle$ given by equation (1). If Alice measures her qubit the state of Bob's qubit collapses into either $|0\rangle$ or $|1\rangle$. Call this case 1.

   • *a)* Suppose that Alice first performs a Hadamard operation on her qubit and then measures it. Into which two states does Bob's qubit collapse? Call this case 2.

   • *b)* Calculate the partial density matrix of Bob's qubit in case 1 and in case 2.

   • *c)* Explain why the no-cloning theorem prevents Bob from obtaining any information on whether or not Alice performed the Hadamard operation before measuring her qubit.

3. The Toffoli gate T is a gate that acts on three qubits, mapping the state $|x\rangle|y\rangle|z\rangle$ onto $|x\rangle|y\rangle|z \oplus xy\rangle$. Here $x, y, z \in \{0, 1\}$ and $\oplus$ is addition modulo 2. The Toffoli gate acting on the state $|x\rangle|y\rangle|0\rangle$ gives the logical AND of x and y in the third qubit. The circuit for the Toffoli gate is shown in the figure.



   • *a)* Show that T is unitary.

   • *b)* Is it possible to implement the AND operation as $|x\rangle|y\rangle \mapsto |x \oplus y\rangle|xy\rangle$ using a *two-qubit* gate (instead of a three-qubit gate)? If "yes", show the circuit, if "no", explain why not.

   • *c)* Show the circuit for a gate that implements a double AND operation: given x, y, z it outputs x AND y AND $z = xyz$.
   Hint: You need to act on 5 qubits with two Toffoli gates.

continued on second page

4. The BB84 protocol for quantum key distribution provides for a method to securely share a secret code between two parties (Alice and Bob). Alice encodes a random bit string in a set of qubits, in the following way. For each qubit she tosses a coin. If the outcome is "heads", Alice prepares the qubit in the state $|\uparrow\rangle$ to encode 0 and in the state $|\downarrow\rangle$ to encode 1; if the output is "tails", she instead prepares the qubit in the state $2^{-1/2}(|\uparrow\rangle + |\downarrow\rangle)$ to encode 0 and in the state $2^{-1/2}(|\uparrow\rangle - |\downarrow\rangle)$ to encode 1. Alice then sends the qubits to Bob, who measures each of them after tossing a coin. If the outcome is "heads" he measures the qubit directly, if the outcome is "tails", he first passes it through a Hadamard gate and then measures it. Once Bob is done with the measurements, he calls Alice on the phone.

- *a)* What conversation should Bob have with Alice to obtain the secret code? Keep in mind that the phone line is not secure, someone might be listening in.
- *b)* Suppose that an adversary, Eve, is able to intercept all of the qubits on their way from Alice to Bob. Eve carries out the same steps as Bob (tossing a coin and measuring), and then forwards each qubit to Bob. How can Alice and Bob find out that the qubits have been intercepted?
- *c)* There is a probability that the interception is not detected. How large is that probability for a code of 10 qubits?