EXAM QUANTUM INFORMATION, 19 NOVEMBER 2021, 14.15–17.15 HOURS.

1. Consider the N-qubit density matrix

$$\rho = \frac{1}{N}(1-\eta)I + \eta|\psi\rangle\langle\psi|,$$

where I is the $N \times N$ unit matrix and $\eta \in [0, 1]$ is a real parameter.

- *a)* Why is this a valid density matrix?
- *b)* Calculate the purity $P \equiv \mathrm{tr}\,\rho^2$ of the state ρ. For which η is the state pure?
- *c)* The state ρ evolves in time with Hamiltonian H, according to $i\hbar d\rho/dt = [H, \rho]$. Derive that the purity P is time independent. How about the parameter η, can it depend on time?

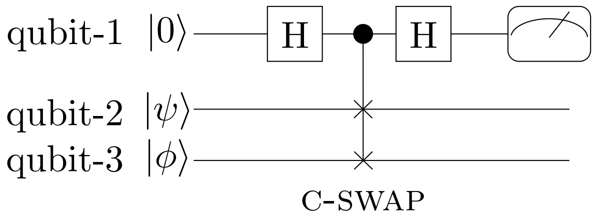
2. *In this question brief answers are sufficient, no detailed calculations are required.*

- *a)* Alice has two qubits in an entangled state $|\psi\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$. Would it be possible to use quantum teleportation as a means to transmit the state $|\psi\rangle$ to Bob? If the answer is "No", explain why not; if the answer is "Yes", specify what Alice would need for that purpose.
- *b)* Alice has two qubits, one is entangled with a qubit of Charlie, the other is entangled with a qubit of Bob. Bob and Charlie have never interacted and do *not* share any entangled qubits. Can Alice use quantum teleportation to entangle the qubits of Bob and Charlie? If the answer is "No", explain why not; if the answer is "Yes", specify between which of the three parties Alice, Bob, and Charlie there needs to be a classical communication channel.
- *c)* Alice and Bob share the Bell pair $2^{-1/2}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)$. When Alice measures her qubit the qubit of Bob *instaneously* (without any delay) collapses onto either $|\uparrow\rangle$ or $|\downarrow\rangle$. Explain why this cannot be used to instaneously transmit information from Alice to Bob. The no-cloning theorem plays a key role here: if cloning would be allowed, then such instantaneous communication would be possible, can you explain how?

continued on second page

3. The SWAP gate S operates on a two-qubit state. It leaves $|0\rangle|0\rangle$ and $|1\rangle|1\rangle$ unchanged, while $|0\rangle|1\rangle \mapsto |1\rangle|0\rangle$ and $|1\rangle|0\rangle \mapsto |0\rangle|1\rangle$.

- *a)* One qubit is in the state $|\psi\rangle$, the other qubit is in the state $|\phi\rangle$. Show that $S|\psi\rangle|\phi\rangle = |\phi\rangle|\psi\rangle$.
- *b)* Show that S is both Hermitian and unitary.



The circuit shown above operates on three qubits.
The H is a Hadamard gate: $|0\rangle \mapsto 2^{-1/2}(|0\rangle + |1\rangle)$, $|1\rangle \mapsto 2^{-1/2}(|0\rangle - |1\rangle)$;
the crosses and black dot indicate the C-SWAP (controlled swap) gate:
$|1\rangle|\psi\rangle|\phi\rangle \mapsto |1\rangle|\phi\rangle|\psi\rangle$ and $|0\rangle|\psi\rangle|\phi\rangle \mapsto |0\rangle|\psi\rangle|\phi\rangle$.
At the end of the process the first qubit is measured.

- *c)* What is the probability that the measurement outcome is 1 if $|\psi\rangle = |0\rangle$, $|\phi\rangle = |1\rangle$? Same question if $|\psi\rangle = |\phi\rangle = 2^{-1/2}(|0\rangle + |1\rangle)$.

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)* The code that is shared is random, it contains no information. How can it be used to to securely transmit information from Alice to Bob?
- *c)* Suppose that an adversary, Eve, is able to intercept the qubits on their way from Alice the Bob. Eve carries out the same steps as Bob (tossing a coin and measuring), and then forwards the qubits to Bob. How can Alice and Bob find out that the qubits have been intercepted?