EXAM QUANTUM INFORMATION, 18 JANUARY 2023, 13.15–16.15 HOURS.

1. Consider the two-qubit operator

$$\rho = \tfrac{1}{4}(\sigma_z \otimes \sigma_z + I \otimes I).$$

The operator I is the single-qubit identity operator and σ_z is a Pauli matrix.

- *a)* Write ρ as a 4×4 matrix. What are its eigenvalues?
- *b)* Why is ρ a valid density matrix?
- *c)* Does ρ describe a pure state or a mixed state? Motivate your answer.

2. A single qubit with density matrix ρ may experience decoherence if it is coupled to an environment. The decoherence operation can be described by the mapping

$$\rho \mapsto (1-p)\rho + p\sigma_z\rho\sigma_z,$$

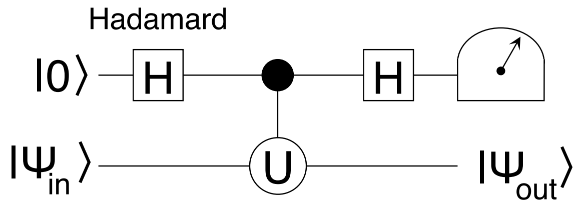
for some constant $p \in (0,1)$.

- *a)* A qubit is initially in the pure state $2^{-1/2}(|0\rangle + |1\rangle)$. What is the density matrix of the qubit in the final state, after the decoherence operation?
- *b)* The purity P of a state with density matrix ρ is defined by $P = \operatorname{Tr}\rho^2$. Calculate the purity of the final state of the qubit.
- *c)* Is the decoherence operation a unitary transformation of the density matrix? Motivate your answer.

3. Consider a single-qubit operator U that is both Hermitian and unitary. You may assume U is not proportional to the identity operator I.

- *a)* Prove that $U^2 = I$.
- *b)* Take an arbitrary single-qubit state $|\Psi\rangle$. Show that $|\Psi_+\rangle = (I+U)|\Psi\rangle$ and $|\Psi_-\rangle = (I-U)|\Psi\rangle$ are both eigenstates of U.

continued on second page



The above two-qubit circuit contains a pair of Hadamard gates (H) acting on the first qubit and a controlled-U operation, meaning that the operator U acts on the second qubit if and only if the first qubit is in the state $|1\rangle$. At the end of the circuit the first qubit is measured.

- *c)* Explain that the final state of the second qubit is an eigenstate of U. How do you find the corresponding eigenvalue?

4. The E91 protocol for quantum key distribution (developed by A. Ekert) uses quantum entanglement of photon pairs (each in a maximally entangled state) shared by two distant users (Alice and Bob) to allow them to exchange information securely — protected from eavesdropping by a third party (Eve). Alice measures each of her photons using some basis chosen randomly from the set $Z_0, Z_{\pi/8}, Z_{\pi/4}$, and Bob does the same for the set $Z_0, Z_{\pi/8}, Z_{-\pi/8}$. Here Z_θ is the polarization basis rotated by an angle θ. Alice and Bob keep their series of basis choices private until their measurements are completed. Then they use a classical communication channel to inform each other of the basis choices, without disclosing the measurement result.

- *a)* How can Alice and Bob use this information to establish a shared private key?
- *b)* How can Alice and Bob find out if some of their photons have been intercepted by Eve, and then retransmitted to Bob?
- *c)* Why is it important that the information on the basis choices is only exchanged *after* the measurements?