EXAM QUANTUM INFORMATION, 4 NOVEMBER 2024, 9–12 HOURS.

1. The basis of the Hilbert space of N qubits is formed by the states

$$|s_1\rangle|s_2\rangle\cdots|s_N\rangle \equiv |s_1 s_2 \cdots s_N\rangle,$$

where $s_n \in \{0,1\}$. The bit string $s_1 s_2 \cdots s_N$ represents in binary notation an integer x in the interval $[0, 2^N - 1]$. For example, the 5-qubit state $|1\rangle|1\rangle|0\rangle|1\rangle|0\rangle$ is written as $|x\rangle$ with $x = 11010$ equal to $2^1 + 2^3 + 2^4 = 26$ in binary notation.

- *a)* Consider a register of N qubits, all in the state $|0\rangle$. We wish to transform this state into the superposition $\sum_{x=0}^{2^N-1} |x\rangle$. Can this be done using *only* single-qubit operations? How does the number of single-qubit operations needed for the transformation scale with N?
- *b)* A certain function $f(x)$ gives as output a binary number in the interval $[0, 2^N - 1]$ for any given x in that interval. Why is it not possible in general to construct a unitary transformation that maps $|x\rangle$ onto $|f(x)\rangle$?
- *c)* Bob claims that by including a second register of N qubits, initialized in the state $|0\rangle$, the function $f(x)$ can be implemented as the unitary transformation $|x\rangle|0\rangle \mapsto |x\rangle|f(x)\rangle$. Alice argues this is not possible in general: if $f(x) = x$ for all x this transformation becomes $|x\rangle|0\rangle \mapsto |x\rangle|x\rangle$, which would violate the no-cloning theorem.
Is Alice right? Please explain.

2. The von Neumann entropy S_ρ of a density matrix ρ is defined by

$$S_\rho = -\operatorname{tr} \rho \log_2 \rho.$$

- *a)* Alice and Bob each have one qubit. The two qubits are in the *pure state* $|\psi\rangle = 2^{-1/2}\,|\uparrow\uparrow\rangle + 2^{-1/2}\,|\downarrow\downarrow\rangle$. Calculate the partial density matrix ρ_A of Alice's qubit and find the corresponding von Neumann entropy S_{ρ_A}.
- *b)* Next consider the case that the two qubits are in a *mixed state*, with density matrix $\rho = 2^{-1}\,|\uparrow\uparrow\rangle\langle\uparrow\uparrow| + 2^{-1}\,|\downarrow\downarrow\rangle\langle\downarrow\downarrow|$. What is now the partial density matrix ρ_A and the von Neumann entropy S_{ρ_A}?
- *c)* Compare the pure state and the mixed state considered in a) and b). Is the pure state entangled? Is the mixed state entangled? Explain your answer.

continued on second page

3. • *a)* The CNOT gate is a unitary operation acting on two qubits. What is the corresponding unitary matrix? As basis states you can use $|\uparrow\uparrow\rangle$, $|\uparrow\downarrow\rangle$, $|\downarrow\uparrow\rangle$, $|\downarrow\downarrow\rangle$.

- *b)* Alice and Bob have two non-entangled qubits, Alice's qubit is in the state $|\psi\rangle = 2^{-1/2}\,|\uparrow\rangle + 2^{-1/2}\,|\downarrow\rangle$, while Bob's qubit is in the state $|\uparrow\rangle$. They entangle the two qubits by applying a CNOT gate with Alice's qubit as the control and Bob's qubit as the target. Compute the partial density matrix of Alice's qubit before and after the CNOT operation.

- *c)* The CNOT gate is sometimes described in words as follows: "The control qubit is unchanged, the target qubit is flipped if the control is up". Bob does not understand this description, because the CNOT operation in b) has changed the partial density matrix of Alice's control qubit.
  How do you clarify this to Bob?

4. Alice and Bob wish to securely share a secret code. 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. Once Bob has received the qubits, 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 can measure the qubits in any way she likes, and then pass them on to Bob. Eve is also able to listen in on the phone conversation Bob will have with Alice.
  Why can't Eve obtain the code without Alice and Bob noticing? Why must Alice and Bob wait with their phone call until *after* Bob has received the qubits?