UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Thursday, 4 June, 2009 9:00 am to 11:00 am

PAPER 53

QUANTUM INFORMATION, ENTANGLEMENT AND NONLOCALITY

*Attempt no more than **THREE** questions.*

*There are **FOUR** questions in total.*

The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

SPECIAL REQUIREMENTS
None

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1

(a) Consider a system whose Hilbert space $\mathcal{H}$ is finite-dimensional. A mixed state of the system is defined by the ensemble of vectors $\{|\psi_i\rangle\}_{i=i}^n$ with probabilities $\{p_i\}_{i=1}^n$. Write down the corresponding density matrix ρ. Show that ρ is self-adjoint and positive semi-definite and that $\mathrm{Tr}(\rho) = 1$. Show, conversely, that if a matrix ρ is self-adjoint and positive semi-definite, and obeys $\mathrm{Tr}(\rho) = 1$, then there exists an ensemble of vectors for which ρ is the density matrix.

(b) Let $D_{\mathcal{H}}$ be the set of density matrices defining mixed states of the system above. Define a *convex decomposition* of a density matrix ρ in $D_{\mathcal{H}}$ to be an expression $\rho = \sum_i a_i \rho_i$, where each ρ_i is in $D_{\mathcal{H}}$ and each $a_i > 0$, and where $\sum_i a_i = 1$. Define a density matrix ρ in $D_{\mathcal{H}}$ to be *pure* if, given any convex decomposition of ρ, we have that $\rho_i = \rho$ for all i. Show that ρ is pure (by this definition) if and only if $\rho = |\psi\rangle\langle\psi|$ for some state vector $|\psi\rangle$ in $\mathcal{H}$.

(c) Let $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ define the Hilbert space of a combined system $S = S_1 + S_2$, and let $|\psi\rangle$ be a pure state of the combined system. Define the *reduced density matrix* of $|\psi\rangle$ on S_1, explaining your notation clearly.

Now consider a general quantum measurement $\{A_i\}$ made on S_2 when the combined system is in state $|\psi\rangle$. Give expressions for the probability p_i of obtaining outcome i, and for the state $|\psi_i\rangle$ of the combined system after a measurement with this outcome. Hence show that the reduced density matrix on S_1 is unaltered by the measurement. Comment briefly on what this says about the relationship between quantum theory and special relativity.

2 State EPR's proposed criterion for identifying an element of physical reality.

A physical system of N separated particles is described by N qubits in the quantum state

$$|\psi\rangle_N = \frac{1}{\sqrt{2}}\big(|\uparrow_1 \ldots \uparrow_N\rangle - |\downarrow_1 \ldots \downarrow_N\rangle\big)\,,$$

where

$$\sigma_z|\uparrow\rangle = |\uparrow\rangle\,, \qquad \sigma_z|\downarrow\rangle = -|\downarrow\rangle\,.$$

Consider the case $N = 3$ and the operators $\sigma_x \otimes \sigma_y \otimes \sigma_y$, $\sigma_y \otimes \sigma_x \otimes \sigma_y$, $\sigma_y \otimes \sigma_y \otimes \sigma_x$ and $\sigma_x \otimes \sigma_x \otimes \sigma_x$.

Show that the predictions of quantum theory for the outcomes of measurements of these operators on $|\psi\rangle_3$ conflict with those implied by the EPR criterion.

Now consider the case of general positive integer $N \geqslant 4$ and the operators $\sigma_x \otimes \sigma_y \otimes \sigma_y \ldots \otimes \sigma_y$, $\sigma_y \otimes \sigma_x \otimes \sigma_y \ldots \otimes \sigma_y$, $\ldots$, $\sigma_y \otimes \sigma_y \otimes \sigma_y \ldots \otimes \sigma_x$ and $\sigma_x \otimes \sigma_x \otimes \sigma_x \ldots \otimes \sigma_x$.

For which integer values of N is the state $|\psi\rangle_N$ an eigenstate of all the given operators, and what are the corresponding eigenvalues?

Show that the predictions of quantum theory for the outcomes of measurements of these operators on $|\psi\rangle_N$ conflict with those implied by the EPR criterion for an infinite set of positive integer values of N.

3 Alice and Bob share four identical copies of an entangled state known to be of the form $\alpha|00\rangle + \beta|11\rangle$, with $1/\sqrt{2} < |\alpha| < 1$. They wish to try to generate some maximally entangled states, using only local operations and classical communication. One strategy is for Alice to measure the total value of the computational basis count of her four qubits (i.e. for Alice to measure $P^A = \sum_{i=1}^4 P_i^A$, where $P_i^A = |0\rangle_i^A\langle 0|_i^A$ projects on her i-th qubit) and to send the result to Bob, and then for Alice and Bob to carry out further operations. Develop this strategy, describing all the measurements involved and giving the probabilities of their outcomes. Show explicitly what Alice and Bob have to do in order to extract copies of maximally entangled pairs of qubits, in the cases where this is possible.

4 Part A

Consider the Bell states

$$|\Phi^{\pm}\rangle_{AB} = 1/\sqrt{2}(|00\rangle_{AB} \pm |11\rangle_{AB})$$

and the corresponding density matrices $\rho^{\pm}_{AB} = |\Phi^{\pm}\rangle_{AB}\langle\Phi^{\pm}|_{AB}$.

Here and below, the AB subscript indicates that the state is shared between Alice and Bob, while an A subscript indicates that the state is with Alice only.

Recall that a *purification* of a state ρ of a system S is a pure state $|\psi\rangle$ of a combined system $S+E$, where E is an ancillary system and where $\mathrm{Tr}_E(|\psi\rangle\langle\psi|) = \rho$.

Alice and Bob share many copies of a quantum state and can implement local operations and communicate publicly over a classical channel. Assume that the ancillary system of some purification of Alice and Bob's state is held by an eavesdropper (Eve). Which of the states below can be used to produce a secure key and which cannot? Justify your answers. (Security proofs are not needed.)

(1) $|\Phi^{+}\rangle_{AB}$

(2) $\frac{2\sqrt{2}}{3}|00\rangle_{AB} + \frac{1}{9}|11\rangle_{AB}$

(3) $\frac{1}{3}|00\rangle_{AB} + \frac{1}{3}|01\rangle_{AB} + \sqrt{\frac{7}{18}}|10\rangle_{AB} + \sqrt{\frac{7}{18}}|11\rangle_{AB}$

(4) $\frac{1}{2}(\rho^{+}_{AB} + \rho^{-}_{AB})$

(5) $\frac{1}{2}(\rho^{+}_{AB} \otimes |0\rangle_A\langle 0|_A + \rho^{-}_{AB} \otimes |1\rangle_A\langle 1|_A)$

Part B

Below are three protocols which are intended to be secure Quantum Key Distribution (QKD) schemes. However, some or all of them may be insecure or may be impossible to implement. For each protocol, state whether it is secure, insecure or impossible to implement. Justify your answers. (Security proofs are not needed.)

Recall that a Hadamard transform in the computational basis is given by the unitary map $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Protocol 1

1: Alice creates the state $|\Phi^{+}\rangle^{\otimes 2n}$, i.e. $2n$ EPR pairs.
2: Alice selects a random $2n$ bit string b, and performs a Hadamard transform on the second half of each EPR pair for which b is 1.
3: Alice sends the second half of each EPR pair to Bob.
4: Alice selects n of the $2n$ encoded EPR pairs to serve as check bits to test for Eve's interference.
5: Alice announces the bit string b, and which n EPR pairs are to be check bits.
6: Bob receives the qubits and publicly announces this fact.
7: Bob performs Hadamard transforms on the qubits where b is 1.
8: Alice and Bob each measure their halves of the n check EPR pairs in the $|0\rangle$, $|1\rangle$ basis and share the results. If too many of these measurements disagree, they abort the protocol.

9: Alice and Bob perform an entanglement purification protocol (EPP) to transform their state so as to obtain m nearly perfect EPR pairs.
10: Alice and Bob measure the remaining EPR pairs in the $|0\rangle$, $|1\rangle$ basis to obtain a shared secret key.

Protocol 2

1: Alice creates the state $|\Phi^+\rangle^{\otimes 2n}$, i.e. $2n$ EPR pairs.
2: Alice selects a random $2n$ bit string b, and performs a Hadamard transform H on the second half of each EPR pair for which b is 1.
3: Alice sends the second half of each EPR pair to Bob.
4: Bob receives the qubits and publicly announces this fact.
5: Alice selects n of the $2n$ encoded EPR pairs to serve as check bits to test for Eve's interference.
6: Alice announces which n EPR pairs are to be check bits.
7: Bob performs inverse Hadamard transforms H^{-1} on the qubits where a Hadamard transform H had been performed.
8: Alice and Bob each measure their halves of the n check EPR pairs in the $|0\rangle$, $|1\rangle$ basis and share the results. If too many of these measurements disagree, they abort the protocol.
9: Alice and Bob perform an entanglement purification protocol (EPP) to transform their state so as to obtain m nearly perfect EPR pairs.
10 Alice and Bob measure the remaining EPR pairs in the $|0\rangle$, $|1\rangle$ basis to obtain a shared secret key.

Protocol 3

1: Alice creates the state $|\Phi^+\rangle^{\otimes 2n}$, i.e. $2n$ EPR pairs.
2: Alice selects a random $2n$ bit string b, and performs a Hadamard transform H on the second half of each EPR pair for which b is 1.
3: Alice sends the second half of each EPR pair to Bob.
4: Bob receives the qubits and publicly announces this fact.
5: Alice selects n of the $2n$ encoded EPR pairs to serve as check bits to test for Eve's interference.
6: Alice announces the bit string b, and which n EPR pairs are to be check bits.
7: Bob performs Hadamards on the qubits where b is 1.
8: Alice and Bob each measure their halves of the n check EPR pairs in the $|0\rangle$, $|1\rangle$ basis and share the results. If too many of these measurements disagree, they abort the protocol.
9: Alice and Bob perform an entanglement purification protocol (EPP) to transform their state so as to obtain m nearly perfect EPR pairs.
10: Alice and Bob measure the EPR pairs in the $|0\rangle$, $|1\rangle$ basis to obtain a shared secret key.

END OF PAPER