Quantum Information Processing

Homework 10

Exercise 1 *Product states and CSHS inequality*

We take the usual setting of the CSHS (Bell) inequality as seen in class, except that we replace the EPR pairs by pairs in product states of the form $|\Psi\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle$. Alice makes measurements in the (linear polarization) basis $|\alpha\rangle$, $|\alpha_\perp\rangle$ and records $a = \pm 1$. Similarly Bob makes measurements in the basis $|\beta\rangle$, $|\beta_\perp\rangle$ and records $b = \pm 1$.

a) Compute the conditional probabilities $p(a, b|\alpha, \beta)$ and show that the locality assumption is here satisfied (because we have a product state) i.e., we have $p(a, b|\alpha, \beta) = p_A(a|\alpha)p_B(b|\beta)$. So we ask that you compute all three terms in this equation for values $(a, b) = (1, 1), (1, -1), (-1, 1), (-1, -1)$ and check the identity.

Remarks: we recall the notation here. Alice makes measurements in the (linear polarization) basis $|\alpha\rangle$, $|\alpha_\perp\rangle$ and records $a = \pm 1$. Similarly Bob makes measurements in the basis $|\beta\rangle$, $|\beta_\perp\rangle$ and records $b = \pm 1$. Moreover here there are no "hidden variables" and the locality assumption is therefore simpler.

b) Consider the usual correlation coefficient

$$X = \langle \Psi| A \otimes B + A \otimes B' - A' \otimes B + A' \otimes B' |\Psi\rangle$$

where A, B, A', B' are the observables of polarization in the linear polarization basis defined by angles α, β, α', β'. So for example $A = (+1)|\alpha\rangle\langle\alpha| + (-1)|\alpha_\perp\rangle\langle\alpha_\perp|$. Prove that $-2 \leq X \leq 2$.

Exercise 2 *The difference between a Bell state and a statistical mixture of* $|00\rangle$ *and* $|11\rangle$

We consider a source that distributes to A and B either an EPR pair in the perfect Bell state $|B_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, or distributes a pair of qubits in a statistical mixture of states $|00\rangle$, $|11\rangle$ with uniform probabilities 1/2. This exercise illustrates in many ways that the two kind of situations are completely different.

a) Write down the density matrix ρ_{Bell} associated to the Bell state in Dirac notation as well as in matrix array form (in the computational basis).

b) Write down the density matrix ρ_{stat} associated to the statistical mixture above in Dirac notation as well as in matrix array form (in the computational basis).

c) In a Bell/CSHS experiment one measures the observable

$$\mathcal{B} = A \otimes B + A \otimes B' - A' \otimes B + A' \otimes B'$$

What is the theoretical average if the state when the state is ρ_{Bell} ? (Use results proven in class and no need to reproduce calculations). And now compute the theoretical average if the state is ρ_{stat}. What are the values of the of these two averages for the optimal CSHS-angles $\alpha = 0$, $\alpha' = -\frac{\pi}{4}$, $\beta = \frac{\pi}{8}$, $\beta' = -\frac{\pi}{8}$?

Exercise 3 *Optional exercise - not graded - Ekert 1991 QKD protocol*

In this exercise we guide you through the general principle of a QKD protocol invented by Arthur Ekert in 1991. Alice and Bob are situated at remote locations and want to generate a one-time pad.

They share a set of N Bell pairs in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ distributed by a source. Alice does measurements of her qubits by choosing at random among the three (linear polarization) basis with angles $\alpha = 0$, $\alpha' = -\frac{\pi}{4}$, $\alpha'' = -\frac{\pi}{8}$. Similarly Bob does measurements of his qubits by choosing at random among the three (linear polarization) basis with angles $\beta = \frac{\pi}{8}$, $\beta' = -\frac{\pi}{8}$, $\beta'' = 0$.

Note that the angles α, α', β, β' are a set that yield the maximal violation of the Bell/CSHS inequality, namely $X = 2\sqrt{2}$ (usual definition of X). In the Ekert protocol we have two extra basis choices with angles $\alpha'' = -\frac{\pi}{8}$ and $\beta'' = 0$.

a) When Alice and Bob choose the same angles what can you say about the classical bits they record in their measurements ? If N Bell pairs are shared how many times on average will Alice and Bob choose the same angles ?

b) Based on the observations in the previous question, propose a scheme to generate a common string of bits between Alice and Bob, i.e., a one-time pad. What is the length of this one-time pad ?

c) Alice and Bob need to devise a security test. However unlike in BB84 here they do not want to sacrifice any small fraction of the one-time pad. Propose one such test based on the Bell/CSHS inequality.

d) Imagine now the following attack from an eavesdropper: the Bell pairs are intercepted during their distribution and each qubit measured in the basis $\alpha = 0$, $\alpha' = -\frac{\pi}{4}$, $\alpha'' = -\frac{\pi}{8}$ and $\beta = \frac{\pi}{8}$, $\beta' = -\frac{\pi}{8}$, $\beta'' = 0$. The state of the pair is thus left in a product state of the type $|\gamma\rangle \otimes |\delta\rangle$ and the eavesdropper distributes $|\gamma\rangle$ to Alice and $|\delta\rangle$ to Bob.

What are the possible values that γ and δ can take ? If your security test proposed in the previous question is "good" then Alice and Bob should be able to detect the presence of the eavesdropper: explain why!