exercises

king adversarially

outcomes bound ex:matching-min

Recall that if Alice measures her qubit in the standard basis, and the resulting post-measurement state on her qubit and Eve's system E is a classical-quantum (cq) state

$$\rho_{XE} = 1200 \otimes \rho_E^{Z,0} + 1211 \otimes \rho_E^{Z,1},$$

then the optimal guessing probability $P_{guess}(X|E)$ such that

$$(X|E) = -\log P_{guess}(X|E)$$

is given by the Helström measurement, for which $P_{guess}(X|E) = 12 + 14\|\rho_E^{Z,0} - \rho_E^{Z,1}\|_1$.

The same reasoning holds for any other choice of Alice's basis, notably the Hadamard basis $\{|+\rangle, |-\rangle\}$. In the BB'84 protocol Alice chooses with probability $1/2$ one of the two bases in which to measure her qubit. If we denote by $P_{guess}(X|E, \Theta = X)$ and $P_{guess}(X|E, \Theta = 1)$ the optimal guessing probabilities for Alice measuring in the standard ($\Theta = 0$) and Hadamard ($\Theta = 1$) bases respectively, the desired lower bound is given by

$$(X|E\Theta) = -\log\left[12P_{guess}(X|E, \Theta = 0) + 12P_{guess}(X|E, \Theta = 1)\right].$$

enumerate

S uppose Alice and Bob share a pure EPR pair , uncorrelated with Eve's system: $\rho_{ABE} = {}_{AB} \otimes \rho_E$. What is $(X|E)$?

N ow consider the general case, where Ψ_{ABE} is an arbitrary state prepared by Eve. Let p be the probability that this state succeeds in the matching outcomes test, when Alice and Bob both measure in the same basis Θ chosen at random. Give coefficients a, b, c such that

$$p = a\Psi_{ABE}X_A \otimes X_B \otimes_E \Psi_{ABE} + b\Psi_{ABE}Z_A \otimes Z_B \otimes_E \Psi_{ABE} + c,$$

where X, Z are the Pauli observables $X = 01 + 10$ and $Z = +- + -+$.

L et p_X (resp. p_Z) be the probability that the state Ψ_{ABE} passes the matching outcomes test in the Hadamard (resp. computational) basis, so that $p = 12(p_X + p_Z)$. By expanding the qubit A in the computational basis, the state Ψ_{ABE} can be expressed as $\Psi_{ABE} = 0 \otimes u_{0BE} + 1 \otimes u_{1BE}$, with $\|u_{0BE}\|^2 + \|u_{1BE}\|^2 = 1$. Give coefficients a', b' such that $\Psi_{ABE}X_A \otimes X_B \otimes_E \Psi_{ABE} = a'\,\Re(u_0 X_B \otimes_E u_1) + b'$.