OPTI 646 **Homework Set #3** **Jessen**

Distributed 11/7, Due 11/14 2022

I
Quantum Key Distribution

Alice and Bob want to execute a quantum key distribution protocol. Alice is equipped to prepare either one of the two states $|u\rangle$ or $|v\rangle$. These two states, in the chosen basis, can be expressed as

$$|u\rangle = \begin{pmatrix}\cos\alpha \\ \sin\alpha\end{pmatrix},\ |v\rangle = \begin{pmatrix}\sin\alpha \\ \cos\alpha\end{pmatrix},$$

where $0 < \alpha < \pi/4$. Alice decides at random to send either $|u\rangle$ or $|v\rangle$ to Bob, and Bob is to make a measurement to determine what she sent. As we know, when the two states are not orthogonal Bob cannot distinguish the states perfectly.

(a) Bob realizes that he cannot expect to be able to identify Alice's qubit every time, so he settles for a procedure that is successful only some of the time. He performs a POVM with three possible outcomes: $\neg u$, $\neg v$, or DON'T KNOW. If he obtains the result $\neg u$, he is certain that $|v\rangle$ was sent, and if he obtains $\neg v$, he is certain that $|u\rangle$ was sent. If the result is DON'T KNOW, then his measurement is inconclusive. This POVM is defined by the operators

$$F_{\neg u} = A(\mathbf{1} - |u\rangle\langle u|),\quad F_{\neg v} = A(\mathbf{1} - |v\rangle\langle v|),\quad F_{DK} = (1-2A)\mathbf{1} + A(|u\rangle\langle u| + |v\rangle\langle v|),\quad \text{(i)}$$

where A is a positive real number. For a given α, how should Bob choose A to minimize the probability of the outcome DK, and what is this minimal DK probability (assuming that Alice chooses from $\{|u\rangle,|v\rangle\}$ equiprobably)?

Hint: if A is too large, F_{DK} will have negative eigenvalues, and (i) is not a POVM. To solve the eigenvalue problem, for use F_{DK}, use

$$|u\rangle\langle u| = \begin{pmatrix}\cos\alpha \\ \sin\alpha\end{pmatrix}(\cos\alpha, \sin\alpha) = \begin{pmatrix}\cos^2\alpha & \frac{1}{2}\sin 2\alpha \\ \frac{1}{2}\sin 2\alpha & \sin^2\alpha\end{pmatrix}$$ and analogously for $|v\rangle\langle v|$ to find

the matrix representation of F_{DK}, then find the eigenvalues and optimize w.r.t. alpha

(b) Design a quantum key distribution protocol using Alice's source and Bobs POVM**.**

(c) **(Bonus problem)** Of course Eve also wants to know what Alice is sending to Bob. Hoping that Alice and Bob won't notice, she intercepts each qubit that Alice sends, by performing an orthogonal measurement that projects onto the basis $\left\{\begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}0\\1\end{pmatrix}\right\}$. If she obtains the outcome $\begin{pmatrix}1\\0\end{pmatrix}$ she sends the state $|u\rangle$ on to Bob, and if she obtains the outcome $\begin{pmatrix}0\\1\end{pmatrix}$, she sends $|v\rangle$ on to Bob. Therefore, each time Bob's POVM has a conclusive outcome, Eve knows with certainty what that outcome is. But Eve's tampering causes detectable errors; sometimes Bob obtains a "conclusive" outcome that differs from what Alice sent. What is the probability of such an error?