Written Exam, Friday May 17th 2024

Course name:	Quantum Information Technology.
Course number:	10385.
Aids:	All aids are allowed (no internet).
Duration:	4 hours.
Weighting:	All sub-problems have equal weight in the evaluation.

Problem 1: Fock states in a beam-splitter network

In this problem, we consider the photonic Fock states $|n\rangle$ ($n = 0, 1, 2...$) - which are eigenstates of the harmonic oscillator - and their interference in beam splitters.

Consider an optical setup with two modes, A and B, that are combined on a symmetric beam splitter. The two input modes to the beam splitter are in the Fock states $|1\rangle$ and $|3\rangle$, respectively.

1.1 Find the joint output state of the two modes in the Fock basis.

The two modes after the beam splitter are called A' and B'.

1.2 The number of photons in mode A' is counted with a photon number resolving detector. What are the possible projective states of mode B' after the measurement and with what probability do they occur?

1.3 Assume now that a symmetric beam splitter is inserted in mode A' and the resulting two outputs are measured using two photon number resulting detectors. What is the output state of mode B' conditioned on the measurement of a single photon in each of the two detectors?

1.4 Suggest an optical setup of input Fock states and beam splitters that generates the three-mode state $|\psi\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ (where e.g. $|100\rangle$ corresponds to one photon in the first mode and zero photons in the two other modes).

Problem 2: Sensing a two-qubit interaction

Consider a system of two qubits. Let $\hat{\sigma}_x$, $\hat{\sigma}_y$, $\hat{\sigma}_z$ be the Pauli operators and $|0\rangle$, $|1\rangle$ the +1 and -1 eigenstates of $\hat{\sigma}_z$. Define the following collective operators for the total spin along x and z, respectively

$$\hat{J}_x = \frac{1}{2}(\hat{\sigma}_x \otimes \mathbb{1}_2 + \mathbb{1}_2 \otimes \hat{\sigma}_x), \tag{1}$$

$$\hat{J}_z = \frac{1}{2}(\hat{\sigma}_z \otimes \mathbb{1}_2 + \mathbb{1}_2 \otimes \hat{\sigma}_z), \tag{2}$$

where $\mathbb{1}_2$ denotes the identity on a single qubit. Furthermore, define the two-qubit interaction operator

$$\hat{H} = \hat{J}_x \hat{J}_z + \hat{J}_z \hat{J}_x. \tag{3}$$

We consider the problem of sensing the strength of an interaction of the form $\hat{H}$. The two qubits are first prepared in some (pure) initial state, then undergo the unitary $\hat{U}_\varphi = \exp(-i\varphi\hat{H})$, and are then measured. The goal is to estimate φ.

2.1 Find the eigenvalues of $\hat{H}$ and the eigenstates expressed in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

2.2 Show that, when the input state is $|00\rangle$, the quantum Fisher information (QFI) at the output is $\mathcal{Q}_\varphi = 2$.

2.3 Show that an optimal input state is $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ and find the corresponding value of $\mathcal{Q}_\varphi$.

2.4 Suggest an optimal measurement and show that it achieves the optimal Fisher information.

Problem 3: QRNG by homodyning

Consider a scheme for quantum random-number generation (QRNG) consisting of a source emitting a quantum state of light and a homodyne detector implementing a quadrature measurement. The output of the measurement is discretised by dividing the real line into a given number of bins.

In the simplest case, the source prepares a vacuum state $|0\rangle$ and the detector measures the $\hat{X}$ quadrature. The outcome x is discretised to a single bit by sign binning. That is, we define an output y by

$$y = \begin{cases} 0, & \text{if } x \leq 0 \\ 1, & \text{if } x > 0. \end{cases} \tag{4}$$

3.1 Determine the probability distribution $p(x)$ of the measurement outcome and argue that, for perfect source and detector, y given by the sign binning above defines a uniformly random bit.

The procedure can be generalised to more bins. Instead of a binary output, we can define a four-valued output as follows (where $\Delta > 0$)

$$y = \begin{cases} 0, & \text{if } x \in]-\infty, -\Delta] \\ 1, & \text{if } x \in]-\Delta, 0] \\ 2, & \text{if } x \in]0, \Delta] \\ 3, & \text{if } x \in]\Delta, \infty[\end{cases} \tag{5}$$

3.2 Draw a plot of $p(x)$ as a function of x and illustrate the four-valued binning above.

3.3 Let Y be a random variable associated with the four-valued output. Show that the min-entropy of Y is

$$H_{\min}(Y) = -\log_2 \max\{\frac{1}{2}\operatorname{erf}(\Delta), \frac{1}{2}[1 - \operatorname{erf}(\Delta)]\}, \tag{6}$$

where $\operatorname{erf}(\cdot)$ is the error function. Argue that up to 2 uniformly random bits per round can be extracted using this scheme, for the right choice of Δ.

3.4 Suggest a general binning strategy allowing the extraction of an integer number N of uniform bits per round. For perfect sources and detectors, how large can N be? What effects might limit N in practice?

Suppose now that the source is not well characterised and is under the control of an adversary Eve, while the user controls the homodyne detector (which is perfect) and applies a binning strategy which is know to Eve.

3.5 Suggest a strategy of Eve for preparing source states such that, from the user's perspective (averaged over many rounds), the outcome distribution $p(x)$ is identical to that of a vacuum source, while in any given round, Eve can predict the value of y with certainty.

End of set