Example solution - written exam May 2024
10385 Quantum Information Technology

July 9, 2024

Problem 1: Fock states in a beam-splitter network

1.1

Let $\hat{a}_A$, $\hat{a}_B$, and $\hat{a}_{A'}$, $\hat{a}_{B'}$ denote the input and output mode operators, respectively. We take the following convention for the beam-splitter transformation

$$\hat{a}_{A'} = \frac{1}{\sqrt{2}}(\hat{a}_A + \hat{a}_B), \tag{1}$$

$$\hat{a}_{B'} = \frac{1}{\sqrt{2}}(\hat{a}_A - \hat{a}_B), \tag{2}$$

and hence $\hat{a}_A = \frac{1}{\sqrt{2}}(\hat{a}_{A'} + \hat{a}_{B'})$ and $\hat{a}_B = \frac{1}{\sqrt{2}}(\hat{a}_{A'} - \hat{a}_{B'})$. Recall that the Fock states are given by $|n\rangle = \frac{1}{\sqrt{n!}}(\hat{a}^\dagger)^n|vac\rangle$. The input state is

$$|\psi_{in}\rangle_{AB} = |13\rangle = \frac{1}{\sqrt{3!}}\hat{a}_A^\dagger(\hat{a}_B^\dagger)^3|vac\rangle. \tag{3}$$

Since operators on different modes commute, we have

$$\begin{aligned} \hat{a}_A\hat{a}_B^3 &= \frac{1}{4}(\hat{a}_{A'} + \hat{a}_{B'})(\hat{a}_{A'} - \hat{a}_{B'})^3 && (4)\\ &= \frac{1}{4}(\hat{a}_{A'}^2 - \hat{a}_{B'}^2)(\hat{a}_{A'} - \hat{a}_{B'})^2 && (5)\\ &= \frac{1}{4}(\hat{a}_{A'}^4 - \hat{a}_{B'}^4 - 2\hat{a}_{A'}^3\hat{a}_{B'} + 2\hat{a}_{A'}\hat{a}_{B'}^3). && (6) \end{aligned}$$

The output state is therefore

$$\begin{aligned} |\psi_{out}\rangle_{A'B'} &= \frac{1}{4\sqrt{3!}}((\hat{a}_{A'}^\dagger)^4 - (\hat{a}_{B'}^\dagger)^4 - 2(\hat{a}_{A'}^\dagger)^3\hat{a}_{B'}^\dagger + 2\hat{a}_{A'}^\dagger(\hat{a}_{B'}^\dagger)^3)|vac\rangle && (7)\\ &= \frac{\sqrt{4!}}{4\sqrt{3!}}(|40\rangle - |04\rangle) - \frac{\sqrt{3!}}{2\sqrt{3!}}(|30\rangle - |03\rangle) && (8)\\ &= \frac{1}{2}(|40\rangle - |04\rangle - |31\rangle + |13\rangle). && (9) \end{aligned}$$

1.2

From the state (9) above, we see that the possible numbers of photons in mode A' are $n = 0, 1, 3, 4$. Each occur with probability $\left(\frac{1}{2}\right)^2 = \frac{1}{4}$. Since the beam splitter preserves the total number of photons, and the initial state has 4 photons, the conditional state of mode B' upon detecting n photons in A' is $|4-n\rangle_{B'}$. This can also be seen directly from the output state (9).

1.3

In the previous problem 1.2, we found that the possible numbers of photons in mode A' are $n = 0, 1, 3, 4$. Inserting a beam splitter in this mode cannot change the number of photons. Thus, after the additional beam splitter, the total photon number must still be 0, 1, 3, or 4. Detecting a single photon in each detector is therefore impossible. The probability for this event to occur is zero, and the conditional state in mode B' is undefined.

1.4

An equal superposition of a single photon in three modes (also known as a tripartite W-state) can be obtained as illustrated in Fig.1.

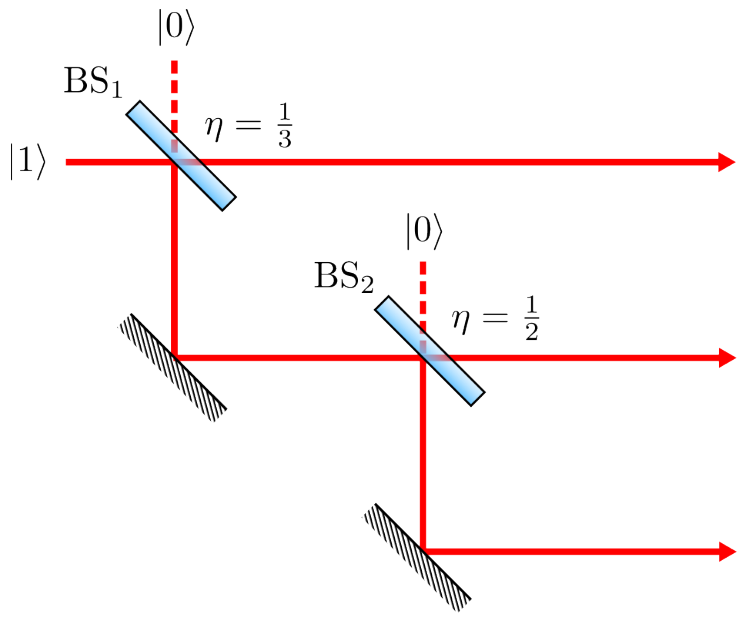

Figure 1: Beam-splitter network for creating an equal superposition of a single photon in three modes. The first beam splitter (BS_1) has transmittivity $\eta = 1/3$ while the second (BS_2) is balanced.

Starting from a single photon in one input mode and vacuum in the other two, the state transforms as

$$|100\rangle \xrightarrow[\mathrm{BS}_1]{} \sqrt{\frac{1}{3}}|100\rangle + \sqrt{\frac{2}{3}}|010\rangle \xrightarrow[\mathrm{BS}_2]{} \sqrt{\frac{1}{3}}|100\rangle + \sqrt{\frac{1}{3}}|010\rangle + \sqrt{\frac{1}{3}}|001\rangle. \tag{10}$$

Problem 2: Sensing a two-qubit interaction

2.1

This can be solved in several ways. Using a computer with e.g. *Python* or a CAS system such as *Mathematica*, it is simple to diagonalise the Hamiltonian (given the definitions of the Pauli operators). Here, we give a bit more detail.

We start by rewriting the Hamiltonian

$$\begin{aligned}
\hat{H} &= \hat{J}_x\hat{J}_z + \hat{J}_z\hat{J}_x &(11)\\
&= \frac{1}{4}(\hat{\sigma}_x\hat{\sigma}_z \otimes \mathbb{1}_2 + \hat{\sigma}_x \otimes \hat{\sigma}_z + \hat{\sigma}_z \otimes \hat{\sigma}_x + \mathbb{1}_2 \otimes \hat{\sigma}_x\hat{\sigma}_z)\\
&\quad + \frac{1}{4}(\hat{\sigma}_z\hat{\sigma}_x \otimes \mathbb{1}_2 + \hat{\sigma}_z \otimes \hat{\sigma}_x + \hat{\sigma}_x \otimes \hat{\sigma}_z + \mathbb{1}_2 \otimes \hat{\sigma}_z\hat{\sigma}_x) &(12)\\
&= \frac{1}{4}(\{\hat{\sigma}_x, \hat{\sigma}_z\} \otimes \mathbb{1}_2 + 2\hat{\sigma}_x \otimes \hat{\sigma}_z + 2\hat{\sigma}_z \otimes \hat{\sigma}_x + \mathbb{1}_2 \otimes \{\hat{\sigma}_x, \hat{\sigma}_z\}) &(13)\\
&= \frac{1}{2}(\hat{\sigma}_x \otimes \hat{\sigma}_z + \hat{\sigma}_z \otimes \hat{\sigma}_x), &(14)
\end{aligned}$$

where we used that the Paulis anti-commute $\{\hat{\sigma}_x, \hat{\sigma}_z\} = \hat{\sigma}_x\hat{\sigma}_z + \hat{\sigma}_z\hat{\sigma}_x = 0$.

In the computation basis (eigenbasis of $\hat{\sigma}_z$) then

$$\hat{H} = \frac{1}{2}\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & -1 & 0 \end{pmatrix}. \tag{15}$$

Using standard linear algebra (or a computer), one finds that the four eigenvalues are $\lambda_{\max} = 1$, $\lambda_{\min} = -1$, and $\lambda_0 = \lambda_0' = 0$ (doubly degenerate). The corresponding normalised eigenstates (in the computational basis) are

$$|\lambda_{\max}\rangle = \frac{1}{2}\begin{pmatrix}1\\1\\1\\-1\end{pmatrix} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle), \tag{16}$$

$$|\lambda_{\min}\rangle = \frac{1}{2}\begin{pmatrix}1\\-1\\-1\\-1\end{pmatrix} = \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle), \tag{17}$$

$$|\lambda_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{18}$$

$$|\lambda_0'\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\-1\\-1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{19}$$

Alternatively, notice that because $\hat{\sigma}_x\hat{\sigma}_z = -\hat{\sigma}_z\hat{\sigma}_x$ it follows that the two terms in (14) commute $[\hat{\sigma}_x \otimes \hat{\sigma}_z, \hat{\sigma}_z \otimes \hat{\sigma}_x] = 0$. They are both Hermitian and hence they can simultaneously diagonalised. The eigenvalues of the sum of the terms are then sums of eigenvalues of each term. $\hat{\sigma}_x \otimes \hat{\sigma}_z$ has two eigenstates with eigenvalue 1, namely $|+,0\rangle$ and $|-,1\rangle$ and two with eigenvalue -1, namely $|-,0\rangle$ and $|+,1\rangle$ (where $|\pm\rangle$ are the eigenstates of $\hat{\sigma}_x$). Similarly, $\hat{\sigma}_z \otimes \hat{\sigma}_x$ has $|0,+\rangle$ and $|1,-\rangle$ with eigenvalue 1 and $|0,-\rangle$ and $|1,+\rangle$ with eigenvalue -1.

Note that $\hat{\sigma}_z \otimes \hat{\sigma}_x|+,0\rangle = |-,1\rangle$ and $\hat{\sigma}_z \otimes \hat{\sigma}_x|-,1\rangle = |+,0\rangle$, and similarly $\hat{\sigma}_x \otimes \hat{\sigma}_z|0,+\rangle = |1,-\rangle$ and $\hat{\sigma}_x \otimes \hat{\sigma}_z|1,-\rangle = |0,+\rangle$. That is, the action of one term swaps between the eigenvalue-1 eigenstates of the other term, and vice versa. It follows that

$$|0,+\rangle + |1,-\rangle = |00\rangle + |01\rangle + |10\rangle - |11\rangle \tag{20}$$

is an eigenstate of $\hat{H}$ with eigenvalue 1. Similarly, it can be seen that

$$|0,-\rangle - |1,+\rangle = |00\rangle - |01\rangle - |10\rangle - |11\rangle \tag{21}$$

is an eigenstate of $\hat{H}$ with eigenvalue -1. It can also be seen that

$$|0,+\rangle + |0,-\rangle + |1,+\rangle - |1,-\rangle = 2(|00\rangle + |11\rangle), \tag{22}$$

$$|0,+\rangle - |0,-\rangle - |1,+\rangle - |1,-\rangle = 2(|01\rangle - |10\rangle) \tag{23}$$

are eigenstates with eigenvalue 0.

2.2

For any pure input state $|\psi\rangle$ and unitary encoding of the parameter, the quantum Fisher information (QFI) at the output is given by

$$\mathcal{Q}_\varphi = 4\,\mathrm{Var}_{|\psi\rangle}(\hat{H}) = 4\,[\langle\psi|\hat{H}^2|\psi\rangle - \langle\psi|\hat{H}|\psi\rangle^2]. \tag{24}$$

For input $|\psi\rangle = |00\rangle$ we have

$$\hat{H}|00\rangle = \frac{1}{2}(\hat{\sigma}_x \otimes \hat{\sigma}_z + \hat{\sigma}_z \otimes \hat{\sigma}_x)|00\rangle = \frac{1}{2}(|10\rangle + |01\rangle). \tag{25}$$

Hence $\langle 00|\hat{H}|00\rangle = 0$ and $\langle 00|\hat{H}^2|00\rangle = 2$ and

$$\mathcal{Q}_\varphi = 4\,\mathrm{Var}_{|\psi\rangle}(\hat{H}) = 4(\frac{1}{2} - 0) = 2, \tag{26}$$

as desired.

2.3

For a unitary encoding generated by Hamiltonian $|H\rangle$, an optimal input is given by evenly weighted superposition of the eigenstates of $|H\rangle$ with minimal and maximal eigenvalues (as seen e.g. in an exercise in the course). Using the eigenstates found above, we see that

$$|\psi_{\mathrm{opt}}\rangle = \frac{1}{\sqrt{2}}(|\lambda_{\min}\rangle + |\lambda_{\max}\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle). \tag{27}$$

Therefore, the given input state is optimal. The corresponding value of the QFI is (as can be seen e.g. from Eq. (24))

$$\mathcal{Q}_\varphi = (\lambda_{\max} - \lambda_{\min})^2 = (1 - (-1))^2 = 4. \tag{28}$$

2.4

The optimal state $|\psi_{\mathrm{opt}}\rangle$ is optimal because it rotates quickly towards an orthogonal state when the parameter changes (the QFI measures the rate of change in state space). One optimal measurement is a binary projective measurement onto the optimal state, since the probabilities will also change quickly.

The state at the output is

$$|\psi_\varphi\rangle = \hat{U}_\varphi|\psi_{\mathrm{opt}}\rangle = \frac{1}{\sqrt{2}}(e^{i\varphi}|\lambda_{\min}\rangle + e^{-i\varphi}|\lambda_{\max}\rangle). \tag{29}$$

The outcome probabilities corresponding to projecting on $|\psi_{\mathrm{opt}}\rangle$ are

$$p_0 = |\langle\psi_{\mathrm{opt}}|\psi_\varphi\rangle|^2 = \left(\frac{e^{i\varphi}+e^{-i\varphi}}{2}\right)^2 = \cos^2(\varphi), \tag{30}$$

$$p_1 = 1 - p_0 = \sin^2(\varphi). \tag{31}$$

The Fisher information of this binary distribution is (here the dot denotes derivative with respect to φ)

$$\mathcal{F}_\varphi = \frac{\dot{p_0}^2}{p_0} + \frac{\dot{p_1}^2}{p_1} = \frac{\dot{p_0}^2}{p_0(1-p_0)} = \frac{4\cos^2(\varphi)\sin^2(\varphi)}{\cos^2(\varphi)\sin^2(\varphi)} = 4, \tag{32}$$

which equals the optimal QFI found above.

Alternatively, in this case it is also optimal to perform a measurement in the computational basis (which has four outcomes). To see this, note that

$$\begin{aligned}|\psi_\varphi\rangle &= \frac{1}{\sqrt{2}}(e^{i\varphi}|\lambda_{\min}\rangle + e^{-i\varphi}|\lambda_{\max}\rangle) \qquad (33)\\ &= \frac{e^{i\varphi}}{2\sqrt{2}}(|00\rangle - |01\rangle - |10\rangle - |11\rangle) + \frac{e^{-i\varphi}}{2\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)\\ &= \frac{1}{\sqrt{2}}(\cos(\varphi)|00\rangle - i\sin(\varphi)|01\rangle - i\sin(\varphi)|10\rangle - \cos(\varphi)|11\rangle). \qquad (34)\end{aligned}$$

The outcome probabilities in the computational basis are therefore

$$p_{00} = p_{11} = \frac{1}{2}\cos^2(\varphi), \tag{35}$$

$$p_{01} = p_{10} = \frac{1}{2}\sin^2(\varphi). \tag{36}$$

The Fisher information is

$$\mathcal{F}_\varphi = \frac{\dot{p_{00}}^2}{p_{00}} + \frac{\dot{p_{01}}^2}{p_{01}} + \frac{\dot{p_{10}}^2}{p_{10}} + \frac{\dot{p_{11}}^2}{p_{11}} = 2\left(\frac{\dot{p_{00}}^2}{p_{00}} + \frac{\dot{p_{11}}^2}{p_{11}}\right) = 4, \tag{37}$$

as before.

Problem 3: QRNG by homodyning

3.1

The probability distribution for the $\hat{X}$ measurement is given by the norm square of the $\hat{X}$-space wavefunction of the vacuum state

$$p(x) = |\psi_{|0\rangle}(x)|^2 = \frac{1}{\sqrt{\pi}}e^{-x^2}. \tag{38}$$

This is an even function (symmetric around zero). Therefore $P(y=0) = P(y=1) = \frac{1}{2}$, and hence the outcome of the sign binning is a uniformly random bit.

3.2

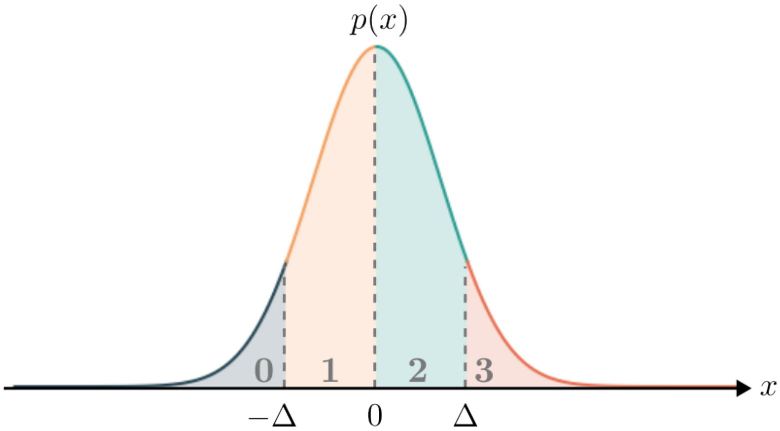

Figure 2: The gaussian distribution of the quadrature measurement outcome with four bins indicated.

3.3

We compute the probabilities for the four outcomes. Because the distribution is symmetric, we have

$$P_Y(0) = P_Y(3) = \int_{\Delta}^{\infty} p(x)dx = \frac{1}{\sqrt{\pi}} \int_{\Delta}^{\infty} e^{-x^2} dx = \frac{1}{2}(1 - \mathrm{erf}(\Delta), \tag{39}$$

$$P_Y(1) = P_Y(2) = \int_{0}^{\Delta} p(x)dx = \frac{1}{\sqrt{\pi}} \int_{0}^{\Delta} e^{-x^2} dx = \frac{1}{2}\mathrm{erf}(\Delta), \tag{40}$$

by definition of the error function $\mathrm{erf}(\cdot)$

The min-entropy is

$$H_{\min}(Y) = -\log_2 \max_y P(y) = -\log_2 \max\{\frac{1}{2}\mathrm{erf}(\Delta), \frac{1}{2}(1 - \mathrm{erf}(\Delta))\}, \tag{41}$$

as claimed. The (asymptotic) number of extractable bits per round is given by $H_{\min}(Y)$. The entropy is maximised for the uniform distribution, which is obtained by choosing Δ such that all bins have equal probability, i.e. such that $\mathrm{erf}(\Delta) = 1 - \mathrm{erf}(\Delta)$. Then $P_Y(y) = \frac{1}{4}$ for all y, and $H_{\min}(Y) = 2$.

3.4

N bits corresponds to 2^N possible outcomes. N uniform bits can thus be obtained by defining 2^N bins chosen such that they have equal probability weights (i.e. $p(x)$ integrated over each bin is the same).

As the $\hat{X}$ measurement gives a continuous outcome, in the absence of imperfections there is no a priori limit to the number of bins. However, due to electronic noise and other imperfections in the homodyne detector, there is some uncertainty in detected outcome and very small differences in x cannot be discerned. In practice, the bin widths should be significantly larger than the detection uncertainty. Fundamental limits connected to the physics of how the photodetectors function and to the finite extent in time of detection events also limit the resolution.

3.5

If Eve is capable of preparing arbitrarily squeezed states, she can get perfect knowledge of the outcomes of the user with the following strategy.

In each round, Eve picks a value x according to the distribution $p(x)$ above. She then prepares a state very strongly squeezed in $\hat{X}$ and displaced such that it is centered at x. This state is transmitted to the user. The user measures $\hat{X}$ and will obtain an outcome very tightly concentrated around x (in the limit of infinite squeezing, he obtains x with certainty). Averaged over many rounds, the user will observe the distribution $p(x)$, but in every round, Eve is able to predict the output bin as accurately as she would like.