Example solution - written exam May 2025 10385 Quantum Information Technology

July 15, 2025

Problem 1: Qubit thermometry

1.1

Normalisation requires that

$$1 = \mathrm{Tr}[\hat{\rho}_T] = \frac{1}{Z_T}(1 + e^{-\Delta/T}). \tag{1}$$

So we must have $Z_T = 1 + e^{-\Delta/T}$.

1.2

The probabilities are just the diagonal elements of $\hat{\rho}_T$ in the energy eigenbasis.

$$p_0 = \langle 0|\hat{\rho}_T|0\rangle = \frac{1}{Z_T} = \frac{1}{1 + e^{-\Delta/T}}, \tag{2}$$

$$p_1 = \langle 1|\hat{\rho}_T|1\rangle = \frac{e^{-\Delta/T}}{Z_T} = \frac{e^{-\Delta/T}}{1 + e^{-\Delta/T}} = \frac{1}{1 + e^{\Delta/T}}, \tag{3}$$

as desired.

Since the measurement only has two outcomes, $p_1 = 1 - p_0$. The classical Fisher information is given by

$$\mathcal{F}_T = \frac{\dot{p}_0^2}{p_0} + \frac{\dot{p}_1^2}{p_1} = \frac{\dot{p}_0^2}{p_0} + \frac{\dot{p}_0^2}{1 - p_0} = \frac{\dot{p}_0^2}{p_0(1 - p_0)}, \tag{4}$$

where the dot denotes derivative with respect to T. We have

$$\dot{p}_0 = \frac{\partial}{\partial T}\frac{1}{Z_T} = -\frac{1}{Z_T^2}\frac{\partial Z_T}{\partial T} = -\frac{\dot{Z}_T}{Z_T^2} = -\frac{\Delta e^{-\Delta/T}}{(1 + e^{-\Delta/T})^2 T^2}, \tag{5}$$

and thus

$$\mathcal{F}_T = \frac{(\dot{Z}_T/Z_T^2)^2}{(1/Z_T)(1 - 1/Z_T)} = \frac{\dot{Z}_T^2}{Z_T^2(Z_T - 1)} \tag{6}$$

$$= \frac{(\Delta e^{-\Delta/T}/T^2)^2}{(1 + e^{-\Delta/T})^2 e^{-\Delta/T}} = \frac{e^{-\Delta/T}}{(1 + e^{-\Delta/T})^2}\frac{\Delta^2}{T^4} = \mathrm{sech}^2(\frac{\Delta}{2T})\frac{\Delta^2}{4T^4}. \tag{7}$$

1.3

Since $\hat{\rho}_T$ is diagonal in the energy eigenbasis, to compute $\dot{\hat{\rho}}_T = \frac{\partial}{\partial T}\hat{\rho}_T$ we just need to derive the diagonal entries. For the first entry

$$\frac{\partial}{\partial T}\langle 0|\hat{\rho}_T|0\rangle = \dot{p}_0 = -\frac{\dot{Z}_T}{Z_T^2}, \tag{8}$$

as shown above. Since $\hat{\rho}_T$ is normalised, the second entry is $p_1 = \langle 1|\hat{\rho}_T|1\rangle = 1 - \langle 0|\hat{\rho}_T|0\rangle = 1 - p_0$. Hence

$$\frac{\partial}{\partial T}\langle 1|\hat{\rho}_T|1\rangle = -\dot{p}_0 = \frac{\dot{Z}_T}{Z_T^2}, \tag{9}$$

as claimed.

1.4

Let $\hat{M}$ denote the expression given in the problem

$$\hat{M} = \frac{\dot{Z}_T}{Z_T}\begin{pmatrix} -1 & 0 \\ 0 & e^{\Delta/T} \end{pmatrix}. \tag{10}$$

In general, the symmetric logarithmic derivative is uniquely defined by the equation $\dot{\hat{\rho}}_T = \frac{1}{2}\left[\hat{\rho}_T\hat{L}_T(\hat{\rho}_T) + \hat{L}_T(\hat{\rho}_T)\hat{\rho}_T\right]$. It is thus sufficient to show that $\hat{M}$ fulfills this. Furthermore, $\hat{M}$ is diagonal in the same basis as $\hat{\rho}_T$, so they commute. It is therefore enough to show that $\dot{\hat{\rho}}_T = \hat{\rho}_T\hat{M}$. We have

$$\begin{aligned} \hat{\rho}_T\hat{M} &= \frac{1}{Z_T}\exp(-\hat{H}/T)\hat{M} = \frac{1}{Z_T}\begin{pmatrix} 1 & 0 \\ 0 & e^{-\Delta/T} \end{pmatrix}\frac{\dot{Z}_T}{Z_T}\begin{pmatrix} -1 & 0 \\ 0 & e^{\Delta/T} \end{pmatrix} & (11) \\ &= \frac{\dot{Z}_T}{Z_T^2}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \dot{\hat{\rho}}_T, & (12) \end{aligned}$$

where the last equality follows from Problem 1.3.

To see whether the measurement is optimal, we compute the quantum Fisher information (QFI), which is given by the expectation value of $\hat{L}_T^2(\hat{\rho}_T)$,

$$\begin{aligned} \mathcal{Q}_T(\hat{\rho}_T) &= \mathrm{Tr}[\hat{\rho}_T\hat{L}_T^2(\hat{\rho}_T)] \\ &= \mathrm{Tr}\left[\frac{1}{Z_T}\begin{pmatrix} 1 & 0 \\ 0 & e^{-\Delta/T} \end{pmatrix}\left[\frac{\dot{Z}_T}{Z_T}\begin{pmatrix} -1 & 0 \\ 0 & e^{\Delta/T} \end{pmatrix}\right]^2\right] \\ &= \frac{\dot{Z}_T^2}{Z_T^3}(1 + e^{\Delta/T}) = \frac{\dot{Z}_T^2}{Z_T^3}Z_T e^{\Delta/T} = \frac{\dot{Z}_T^2}{Z_T^2(Z_T - 1)} = \mathcal{F}_T, \end{aligned} \tag{13}$$

where we have used the result for $\mathcal{F}_T$ from Problem 1.2. Since the classical Fisher information equals the QFI, the energy measurement is optimal.

Problem 2: Beam splitting and randomness

2.1

The beam splitter transformation preserves the total photon number. Since there is exactly one photon at the inputs, if one photon is detected in A there must be zero photons in E and vice versa. So the conditional states for $x = 0$ and $x = 0$ are $|1\rangle_E$ and $|0\rangle_E$, respectively.

These states are orthogonal and can hence be perfectly discriminated (e.g. by a measurement of the photon number). Therefore Eve can deduce x exactly from observation of mode E, so her guessing probability is $p_g = 1$ and no randomness can be extracted.

2.2

The joint input state is $\sqrt{\lambda}|0,0\rangle + \sqrt{1-\lambda}|1,0\rangle$. Taking the phase convention of the beam splitter such that that a photon in the first input port transforms to $\sqrt{\eta}|1,0\rangle_{AE} + \sqrt{1-\eta}|0,1\rangle_{AE}$, the input state transforms to

$$\sqrt{\lambda}\,|0,0\rangle_{AE} + \sqrt{(1-\lambda)\eta}\,|1,0\rangle_{AE} + \sqrt{(1-\lambda)(1-\eta)}\,|0,1\rangle_{AE}. \tag{14}$$

When both modes A and E are measured in the Fock basis, the outcome probabilities are simply the squared amplitudes of the corresponding terms

$$\begin{aligned} P_{AE}(0,0) &= \lambda, & P_{AE}(0,1) &= (1-\lambda)(1-\eta), \\ P_{AE}(1,0) &= (1-\lambda)\eta, & P_{AE}(1,1) &= 0. \end{aligned} \tag{15}$$

2.3

Eve has access to y and is trying to infer x. Her average guessing probability is given by

$$p_g = \sum_{y=0}^{1} P_E(y) \max_x P_{A|E}(x|y), \tag{16}$$

where $P_E(y)$ is the distribution of Eve's outcome and $P_{A|E}(x|y)$ the conditional probability of x knowing y. Both can be determined from the joint distribution. $P_E(y)$ is the marginal

$$P_E(y) = \sum_{x=0}^{1} P_{AE}(x,y), \tag{17}$$

so

$$P_E(0) = \lambda + (1-\lambda)\eta, \quad \text{and} \quad P_E(1) = (1-\lambda)(1-\eta). \tag{18}$$

From the definition of conditional probabilities we have

$$P_{A|E}(x|y) = \frac{P_{AE}(x,y)}{P_E(y)}, \tag{19}$$

We get

$$\begin{aligned} P_{A|E}(0|0) &= \frac{\lambda}{\lambda + (1-\lambda)\eta}, \qquad P_{A|E}(0|1) = 1, \\ P_{A|E}(1|0) &= \frac{(1-\lambda)\eta}{\lambda + (1-\lambda)\eta}, \qquad P_{A|E}(1|1) = 0. \end{aligned} \tag{20}$$

Inserting in (16) we find

$$\begin{aligned} p_g &= (1-\lambda)(1-\eta) + [\lambda + (1-\lambda)\eta] \max\{\frac{\lambda}{\lambda + (1-\lambda)\eta}, \frac{(1-\lambda)\eta}{\lambda + (1-\lambda)\eta}\} \\ &= (1-\lambda)(1-\eta) + \max\{\lambda, (1-\lambda)\eta\}, \end{aligned} \tag{21}$$

as desired.

2.4

The max will select the first term when $\lambda \geq (1-\lambda)\eta \Leftrightarrow \lambda \geq \frac{\eta}{1+\eta}$ and the second term otherwise. For $\lambda \geq \frac{\eta}{1+\eta}$ therefore

$$p_g = (1-\lambda)(1-\eta) + \lambda = \eta\lambda + 1 - \eta, \tag{22}$$

which is an increasing function of λ (since $\eta \geq 0$). For $\lambda < \frac{\eta}{1+\eta}$ instead

$$p_g = (1-\lambda)(1-\eta) + (1-\lambda)\eta = 1 - \lambda, \tag{23}$$

which is a decreasing function of λ. The optimal λ minimising p_g is therefore $\lambda = \frac{\eta}{1+\eta}$ and the minimal p_g is

$$p_g = 1 - \frac{\eta}{1+\eta} = \frac{1}{1+\eta}. \tag{24}$$

We see that perfect transmission ($\eta = 1$, no light to Eve) gives $p_g = \frac{1}{2}$, a perfect random bit, while zero transmission ($\eta = 1$, all light reflected to Eve) gives $p_g = 1$, no randomness, as might be expected.

Problem 3: Dual-rail photonic qubits

3.1

Up to a global phase, any single-qubit unitary $\hat{U}$ can be decomposed in terms of Pauli rotations on the Bloch sphere as $\hat{U} = \hat{R}_z(\varphi)\hat{R}_y(\phi)\hat{R}_z(\theta)$, for some angles θ, ϕ, φ. It is therefore sufficient to be able to implement y- and z-rotations. Using linear optical components, for dual-rail qubits, rotations around z can be implemented by a phase shift of one mode with respect to the other, and rotations around y can be implemented by a beam splitter with variable transmittivity between the modes. See Fig. 1.

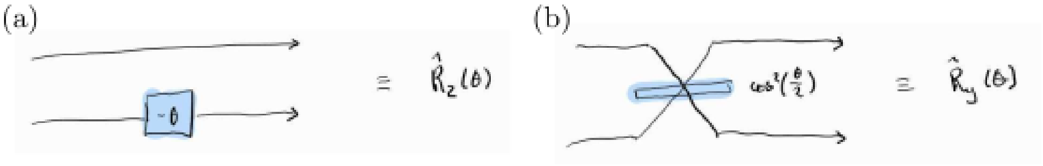
(a)
$-\theta$
$\equiv \hat{R}_z(\theta)$
(b)
$\cos^2(\frac{\theta}{2})$
$\equiv \hat{R}_y(\theta)$

Figure 1: (a) $\hat{R}_z(\theta)$ on a dual-rail qubit can be implemented by a $-\theta$ phase shift on the second mode. **(b)** $\hat{R}_y(\theta)$ on a dual-rail qubit can be implemented by a beam splitter with transmittivity $\cos^2(\theta/2)$ (up to local phases / mode relabelling depending on the beam splitter convention used).

3.2

The two modes of dual-rail qubits could be realised, for instance, by *i)* separate spatial modes, *ii)* orthogonal polarisations, *iii)* different time bins. Some advantages and disadvantages of such implementations are

i) Spatial.
Physical realisation: Two free-space modes, waveguides, or fibres.
Advantages: Easy to separate and manipulate.
Disadvantages: Sensitive to path-length fluctuations and alignment.

ii) Polarisation.
Physical realisation: Orthogonal polarisations in shared spatial mode.
Advantages: Same spatial mode; less sensitive to mechanical drift.
Disadvantages: Polarization control can be difficult over long distances.

iii) Time-bin.
Physical realisation: Early/late pulses.
Advantages: Robust in optical fibers
Disadvantages: Requires fast detectors and modulators.

3.3

In the KLM scheme, the controlled-phase (CZ) gate can be implemented probabilistically by using two probabilistic nonlinear sign-shift (NS) gates.

Each NS gate acts on one dual-rail qubit and uses two ancilliary modes with a single photon in one of them, as illustrated in Fig. 2. The NS gate succeeds when a single photon is detected in one of the ancilliary modes, which happens with probability 1/4.

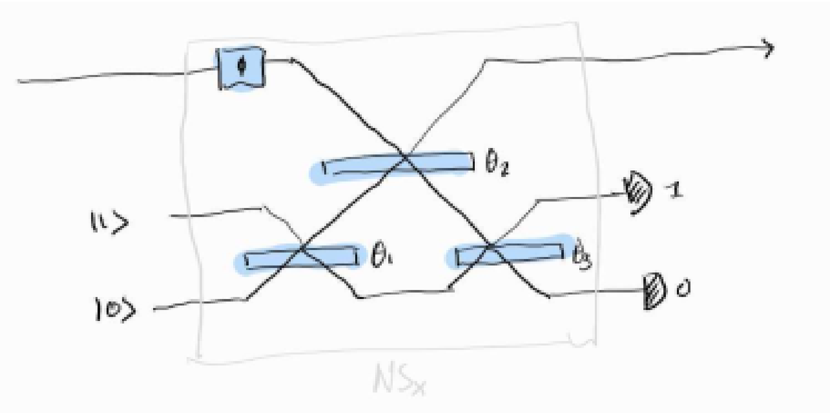

Figure 2: NS gate. The gate requires one single photon in the first ancilla mode and succeeds if one photon is detected in the first ancilla mode and zero in the second. By choosing the phase ϕ and beam-splitter angles θ_1, θ_2, θ_3 the setup can be tuned to apply a sign flip $x = -1$ to two-photon components of the state of the input mode.

A direct implementation of the two-CZ circuit is illustrated in Fig. 2. In this implementation, the circuit success probability depends on the success probability of the NS gates.

Alternatively, to improve the success probability, gate teleportation can be used to implement the CZ gates. In this case, the NS gates become part of the state preparation, and the CZ success probability instead depends on the success probability for teleportation.

3.4

In the direct implementation, we can count as follows. Each NS gate requires one ancilla photon. Thus each CZ gate requires two ancilla photons and the entire two-CZ circuit requires four ancilla photons. The success probability for each NS gate is $\frac{1}{4}$ and the successes are independent events. The overall success probability for the circuit is therefore $\left(\frac{1}{4}\right)^4 = \frac{1}{256}$.

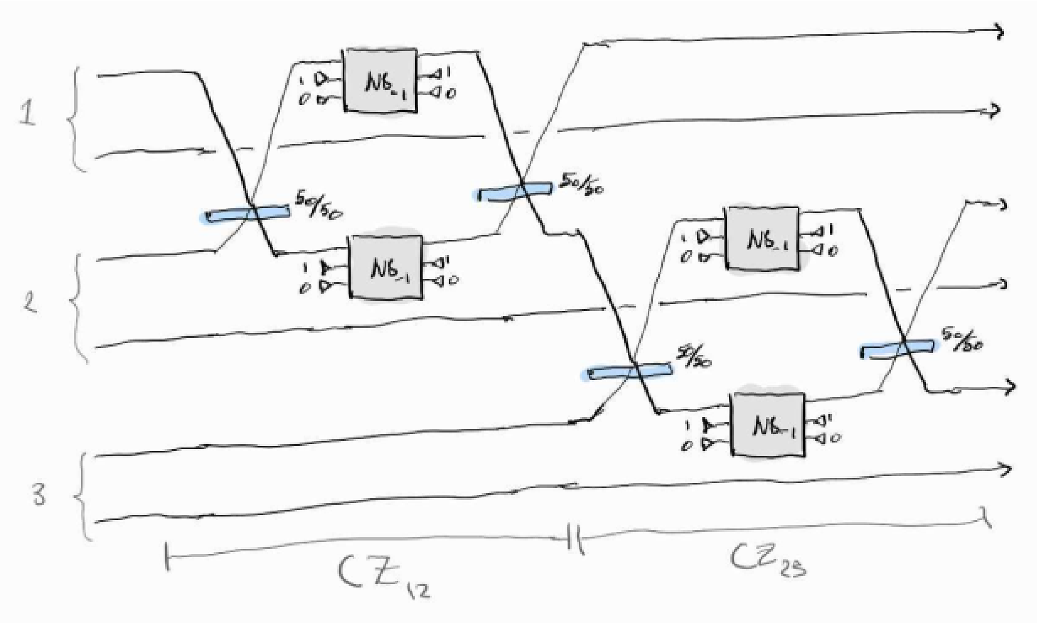

Figure 3: KLM implementation of the two-CZ circuit acting on three dual-rail qubits. The first part of the circuit applies a CZ-gate between qubits 1 and 2, and the second half a CZ-gate between qubits 2 and 3.

Using gate teleportation instead, the circuit can be made near-deterministic in principle. Specifically, for each CZ gate, using $4n$ additional ancilliary modes with $2n$ single photons in them to prepare the entangled state needed for teleportation, a CZ with success probability $\frac{n^2}{(n+1)^2}$ can be achieved. The two-CZ circuit then succeeds with probability $\frac{n^4}{(n+1)^4}$. In the simplest case, $n = 1$, we get $\frac{1}{16}$.