

## CO481/CS467/PHYS467 Assignment 4

Due March 17, 2025, 8:30am

**Instruction:** Please submit your solutions to Crowdmark by the due date and time. Take special care to place the answer to each question in the right place. Questions are ordered according to the sequence of topics covered in class, and not by difficulty. Also, if you do not prove an earlier part of a question, you can still use the earlier part to answer a later part.

### Question 1. Detecting eavesdropping in a preliminary version of BB84 [7 marks]

In this preliminary version of BB84, Alice wants to send a uniformly random secret key bit  $s \in \{0, 1\}$  to Bob. To protect the secret, Alice picks a second uniformly random bit  $b \in \{0, 1\}$ . She stores the secret in system  $A_1$ , and the basis information in system  $A_2$ . She prepares the state  $H^b|s\rangle$  in system  $C$  and sends  $C$  through an *insecure* quantum channel hoping that it will arrive at Bob's home safely. (In other words, Alice encodes her secret  $s$  either in the  $\{|0\rangle, |1\rangle\}$  basis or the  $\{|+\rangle, |-\rangle\}$  basis depending on whether  $b = 0$  or 1 respectively.)

(a) [2 marks] What is the density matrix for the state on  $A_1 A_2 C$ ? You can leave your answer in Dirac notation and there is no need to expand  $|\pm\rangle$  for this part.

(b) [1 mark] An eavesdropper Eve cuts the optical fibre (the quantum channel) and receives the quantum state in system  $C$  instead! Eve knows the protocol that Alice uses, but knows nothing about  $s$  or  $b$ . Let  $\rho_0$  and  $\rho_1$  be the density matrices on system  $C$  conditioned on  $s = 0$  and 1 respectively. Write down  $\rho_0$  and  $\rho_1$ . You can leave the answer in Dirac notation and in terms of  $|0\rangle, |1\rangle, |\pm\rangle$ .

(c) [2 marks] Eve wants to determine the secret  $s$ . This is a state discrimination problem, in which with probability  $\frac{1}{2}$ ,  $s = 0$  and Eve receives from Alice  $\rho_0$ , and with probability  $\frac{1}{2}$ ,  $s = 1$  and Eve receives from Alice  $\rho_1$ . Suppose Eve's measurement outcome is  $e$ , stored in system  $E$ . The Helstrom-Holevo Theorem (topic 4) can be extended to the discrimination of mixed states and you can assume without proof that the measurement that maximizes the probability for  $e = s$  is given by the projectors:

$$P_0 = \frac{1}{2} \left( I + \frac{Z+X}{\sqrt{2}} \right) \quad \text{and} \quad P_1 = \frac{1}{2} \left( I - \frac{Z+X}{\sqrt{2}} \right).$$

What is the probability for  $e = s$ ?

(d) [2 marks] Suppose Eve writes her measurement outcome on system  $E$ , and forwards the postmeasurement state (2-dim) in system  $C$  to Bob (without the measurement outcome). This is called an intercept-and-resend attack. Bob tells Alice he receives system  $C$ , and then Alice tells Bob the value of  $b$ . Bob measures in the  $\{|0\rangle, |1\rangle\}$  basis if  $b = 0$ , and  $\{|+\rangle, |-\rangle\}$  basis if  $b = 1$ . Let his outcome be  $t$ .

Conditioned on  $s = 0$ ,  $b = 0$ , and  $e = 0$ , what is  $\Pr(t \neq s)$ ?

Note that in the absence of Eve's attack, Bob's measurement outcome  $t$  should always be the secret  $s$ . As Eve learns (incomplete) information about the state in  $C$ , her measurement disturbs the state so that Bob's measurement no longer always gives  $t = s$ . If this experiment is repeated  $n$  times, and Alice and Bob cross-check "hashes" of the  $n$ -bit secret, they can detect Eve's attack with high probability. Quantum key distribution does not stop Eve from learning about the key, but to detect that she has tried to eavesdrop on the transmission as she disturbs the state.

**Question 2. Decoherence, measurement, and the diagonalization map** [8 marks]

(a) [1 marks] Consider the following function from  $2 \times 2$  matrices to  $2 \times 2$  matrices

$$\mathcal{D}_1(\rho) = \frac{1}{2} \left( e^{i\theta Z} \rho e^{-i\theta Z} + e^{-i\theta Z} \rho e^{i\theta Z} \right)$$

where  $Z$  is the Pauli- $z$  matrix, and  $\theta$  is a small positive real number. This describes a quantum operation in which the qubit system goes through a small  $Z$  rotation in a random direction. Show that:

$$\mathcal{D}_1 \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \begin{bmatrix} a & \cos 2\theta b \\ \cos 2\theta c & d \end{bmatrix}.$$

Note that the overall affect on the density matrix is the shrinking of the off-diagonal entries, which is called “decoherence”.

(b) [1 mark] Consider the following function from  $2 \times 2$  matrices to  $2 \times 2$  matrices,

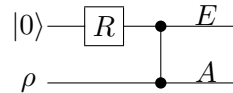
$$\mathcal{D}_2(\rho) = (1 - p)\rho + pZ\rho Z.$$

where  $0 < p < 1$  is a small positive real number. This describes a quantum operation in which the qubit system has a “phase error”  $Z$  with a small probability  $p$ . Show that:

$$\mathcal{D}_2 \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \begin{bmatrix} a & (1 - 2p)b \\ (1 - 2p)c & d \end{bmatrix}.$$

Note that  $\mathcal{D}_2 = \mathcal{D}_1$  if we match the noise parameters  $1 - 2p = \cos 2\theta$ . This is an example of the non-uniqueness of the Kraus representation.

(c) [2 marks] Consider the following circuit:



where  $R = \begin{bmatrix} \sqrt{1-p} & -\sqrt{p} \\ \sqrt{p} & \sqrt{1-p} \end{bmatrix}$ , and the gate depicted with the vertical line ending with filled circles is

the controlled- $Z$  gate (diagonal with entries  $1, 1, 1, -1$ ).

The circuit specifies a quantum operation  $\mathcal{D}_3$  via a Stinespring dilation  $U$  from the second (bottom) qubit to  $EA$ , if the partial trace is applied to  $E$ . Derive the matrix representation for  $U$  (a  $4 \times 2$  matrix) from the above circuit showing clearly the  $2 \times 2$  blocks.

Your answer should show that each block gives a Kraus operator of  $\mathcal{D}_2$  in part (b) so  $\mathcal{D}_2 = \mathcal{D}_3$  and  $U$  is a Stinespring dilation of  $\mathcal{D}_2$ . (But you should not use this information to obtain  $U$ .)

(d) [4 marks] Let  $1 - 2p = \cos 2\theta$  so  $\mathcal{D}_1 = \mathcal{D}_2 = \mathcal{D}_3$ . Find a unitary  $V$  acting only on  $E$  after the controlled- $Z$  in the circuit, such that a subsequent partial trace of  $E$  in the computational basis gives  $\mathcal{D}_1$  with the Kraus operators as given in part (a) (including the ordering which is the first/second Kraus operator).

This is a concrete example to see that the choice of basis used in the partial trace of  $E$  gives rise to the non-uniqueness of the Kraus representation.

**Question 3. When is a quantum operation reversible?** [5+1 marks]

We say that a quantum operation  $\mathcal{E}$  taking system  $A$  to system  $B$  is *reversible* if there is another quantum operation  $\mathcal{D}$  taking  $B$  to  $A$  such that the composition  $\mathcal{D} \circ \mathcal{E}$  is the identity map  $\mathcal{I}$  on  $A$ . For example, unitary operations are reversible, in that if  $\mathcal{E}(\rho) = U\rho U^\dagger$ , then, for  $\mathcal{D}(\sigma) = U^\dagger\sigma U$ ,  $\mathcal{D} \circ \mathcal{E} = \mathcal{I}$ .

Let  $\mathcal{E}$  taking system  $A$  to system  $B$  be an arbitrary quantum operation with Stinespring dilation  $U$  which takes vectors in  $A$  to  $BE$ ; and  $\mathcal{E}(M) = \text{tr}_E U M U^\dagger$ . Let  $A$  be  $d$ -dimensional. Let  $R$  be a  $d$ -dimensional system, and  $|\psi\rangle_{RBE} = (I_R \otimes U_A)|\Phi\rangle_{RA}$ , where  $I_R$  is the identity matrix on  $R$ . Note that  $|\psi\rangle$  is a tripartite state on  $RBE$ , and  $\text{tr}_{BE} |\psi\rangle\langle\psi| = \frac{1}{d}I_R$ .

Show that, if there exists a density matrix  $\eta$  on system  $E$ , such that  $\text{tr}_B |\psi\rangle\langle\psi| = \frac{1}{d}I_R \otimes \eta_E$ , then,  $\mathcal{E}$  is reversible. (This condition is also necessary, due to the information gain implies disturbance principle, but you do not need to show necessity here.)

You can use the following fact without proof: Let  $\mathcal{N}$  be any linear map taking  $d \times d$  matrices to  $d \times d$  matrices, and  $R$  be a  $d$ -dimensional system. Let  $\mathcal{I}$  be the identity map on  $R$ . Let  $|\Phi\rangle$  be the maximally entangled state on  $RA$ ,  $|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i\rangle|i\rangle$ . **Fact:** If  $(\mathcal{I} \otimes \mathcal{N})(|\Phi\rangle\langle\Phi|) = |\Phi\rangle\langle\Phi|$ , then  $\mathcal{N}$  is the identity map on  $A$ .

Hint: find two useful purifications of  $(I/d)_R \otimes \eta_E$  and relate them.