Revision class TT: Quantum Information

Please do not hand in answers to the following problems. The quantum cryptography and revision problems will be discussed in the revision class in detail. The additional worked examples will not be discussed in class unless you have queries about them. They share similarities with previous exam questions and can be used for revision.

6 Quantum cryptography

1. We assume that a communication channel used by Alice and Bob for a BB84 key distribution is capable of transmitting 1000qubits per second (assuming that δ may be set to zero in this case). What is the average key generation rate that Alice and Bob can achieve if they a) assume that no eavesdropper can be present and thus do not publicly compare parts of their key; b) an eavesdropper using intercept/resend strategy on each second qubit should be detected with 99.9% probability after two seconds. How much mutual information can be established between Alice's bit string A and the eavesdropper during these two seconds?

2. For the phase encoding systems in Fig. 1 determine the probability for a photon to be incident on D_0 and D_1 as a function of the two phases induced by the two independent phase modulators (PM) with phases ϕ_A and ϕ_B. Note that for the setup shown in Fig. 1b the photons going along paths SS and LL do not contribute to the signal. Explain how these setups can be used to realize the BB84 protocol. Show how a difference in the optical path length of the two fibres connecting Alice and Bob in Fig. 1a leads to errors.

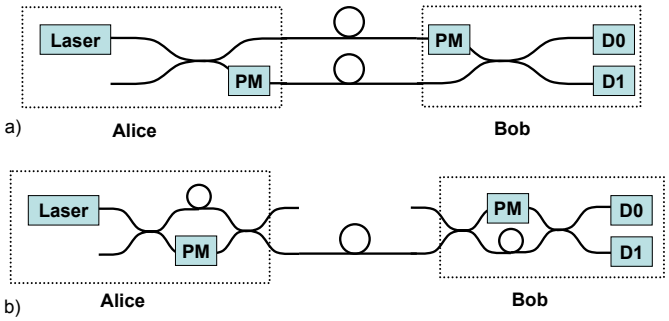


Figure 1: Phase encoding in the BB84 protocol

3. In quantum key distribution with EPR pairs calculate the probabilities $P_{\pm\pm}(\phi^a, \phi^b)$ for the Bell state

$$|\Psi\rangle \quad = \quad \frac{1}{\sqrt{2}}\left[|V\rangle_1|H\rangle_2 - |H\rangle_1|V\rangle_2\right]$$

created by the EPR source. Use these results to calculate the expectation value $E(\phi^a, \phi^b)$ and check that $S = -2\sqrt{2}$.

Revision class problems

The revision class problems are taken from the C2 paper of 2008.

4. The result of a quantum mechanical measurement can be described by a Hermitian operator M. If the system is in an eigenstate $|m\rangle$ of M, then the outcome of the measurement is the corresponding eigenvalue m (you may assume that all eigenvalues are non-degenerate), and the state is unchanged. Describe what happens if the system is not in an eigenstate. Show that the eigenvalues m are real, and that eigenstates corresponding to distinct eigenvalues are orthogonal.

Consider a single qubit which is known to be in one of two states, $|0\rangle$ or $|+\rangle$, with equal probability. Explain why these states cannot be distinguished by a single measurement, and why repeated measurements do not help. Describe what happens to each of the two states if a measurement is made in the Z-basis. Show that only one of the possible outcomes can provide certain knowledge of the initial state of the qubit, while the other outcome is ambiguous. Calculate the overall probability of each outcome occurring, and determine what probabilistic conclusions can be drawn about the initial state in each case. What would happen if the measurement was made in the X-basis instead?

An alternative approach, due to Helstrom, is to design a measurement which allows both states to be detected as well as possible, although neither can be detected unambiguously. In this case it is simpler to consider distinguishing between the two states

$$\begin{aligned} |a\rangle &= \cos(\pi/8)\ |0\rangle + \sin(\pi/8)\ |1\rangle\ , \quad \text{and} \\ |b\rangle &= \cos(3\pi/8)\ |0\rangle + \sin(3\pi/8)\ |1\rangle\ , \end{aligned}$$

which are again assumed to occur with equal probability. What probabilistic conclusions can be drawn about the initial state for each outcome of a measurement made in the Z-basis? What would happen if the measurement was made in the X-basis instead?

Measuring in the Z-basis is the Helstrom optimised measurement for distinguishing between $|a\rangle$ and $|b\rangle$. Use the Bloch sphere picture to describe the states $|a\rangle$ and $|b\rangle$, and hence, or otherwise, determine the Helstrom measurement for distinguishing between $|0\rangle$ and $|+\rangle$.

5. The full Hamiltonian for a two spin NMR system has the Heisenberg form

$$\mathcal{H}_{\rm H} = \frac{\omega_1}{2}\,\sigma_z \otimes \mathbf{1} + \frac{\omega_2}{2}\,\mathbf{1} \otimes \sigma_z + \frac{\omega_{12}}{2}\,\sigma \cdot \sigma,$$

where the Heisenberg coupling is given by

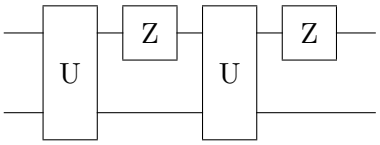
$$\sigma \cdot \sigma = \sigma_x \otimes \sigma_x + \sigma_y \otimes \sigma_y + \sigma_z \otimes \sigma_z,$$

and factors of $\hbar$ have been dropped as usual in NMR. Write down explicit matrix forms in the computational basis for the Heisenberg coupling and for $\mathcal{H}_{\rm H}$, and use perturbation theory to determine the conditions under which $\mathcal{H}_{\rm H}$ can be approximated by the Ising form

$$\mathcal{H}_{\rm I} = \frac{\omega_1}{2}\,\sigma_z \otimes \mathbf{1} + \frac{\omega_2}{2}\,\mathbf{1} \otimes \sigma_z + \frac{\omega_{12}}{2}\,\sigma_z \otimes \sigma_z.$$

Explain why this approximation is better when larger magnetic field strengths are used.

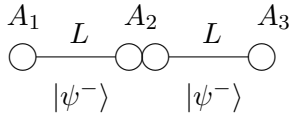
Consider the case $\omega_1 = \omega_2$ and use a rotating frame transformation to remove the Zeeman terms from the full Hamiltonian. Find an explicit matrix expression for the propagator U corresponding to evolution under the Hamiltonian in this frame for a time t and evaluate the total propagator for the network



(a modified spin-echo sequence). Explain why this network could not in fact be implemented in an NMR spin system with $\omega_1 = \omega_2$.

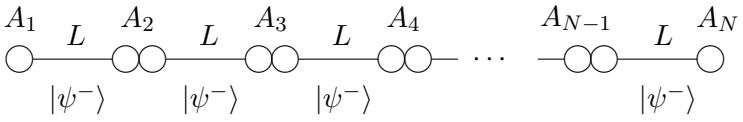
Explain briefly the difference between quantum error correction and decoherence free subspaces. Describe a simple decoherence free subspace encoding one logical qubit in two physical spins and show that a general state of the logical qubit is protected against simultaneous Z gates.

6. Three parties A_1, A_2 and A_3 separated by a distance L initially possess two pairs of entangled qubits in state $|\psi^-\rangle$ as shown in the figure.



Explain the entanglement swapping protocol which turns this initial setup into an entangled pair of qubits in state $|\psi^-\rangle$ shared between parties A_1 and A_3.

Calculate the reduced density operator of the qubits possessed by A_1 and A_3 initially and after each step of this protocol and work out their mutual information. Why does the protocol not violate causality? Calculate the amount of classical information gained by A_2 in the measurement which is part of the above protocol. Compare this with the entropy of the reduced density operator of A_2's qubits before the measurement and discuss the relation between this entropy and the information obtained by the measurement.



Consider an extension of the entanglement swapping protocol to N parties $A_1 \cdots A_N$ separated by a distance L as shown in the figure. Devise a sequence of elementary entanglement swapping steps which creates an entangled pair of qubits in state $|\psi^-\rangle$ between A_1 and A_N. Assuming that only 50% of all elementary entanglement swapping steps are successful, calculate the probability of success for the overall protocol as a function of N. Discuss possible implications of the scaling of this probability with N for long distance quantum communication via glass fibres.

The setup shown in the figure can be used to transmit two classical bits of information from A_1 to A_N. Devise a scheme to achieve this where the intermediate parties A_n

with $1 < n < N$ are allowed to know the classical information transmitted from A_1 to A_N. Show that, neglecting the time needed for local operations, the transmission can be completed in a time $t = (N-1)L/c$ with c the speed of light. Explain how, by using entanglement swapping prior to transmitting the classical bits, a scheme which does not give the intermediate parties access to the classical information can be realized. Discuss practical disadvantages of this scheme.

7. Some internal states of an atom are suitable for representing basis states of a qubit. Which properties should internal atomic states have to make a 'good' qubit? Identify two atomic states of the alkali atom ^{87}Rb (nuclear spin $I = 3/2$) which possess these properties and can be used to realize a qubit. Explain how single qubit gates can be performed in this atomic qubit.

A laser setup is switched on for a time 2τ and induces the two qubit SWAP gate with truth table

$$\begin{aligned} |0\rangle \otimes |0\rangle &\rightarrow |0\rangle \otimes |0\rangle \\ |0\rangle \otimes |1\rangle &\rightarrow |1\rangle \otimes |0\rangle \\ |1\rangle \otimes |0\rangle &\rightarrow |0\rangle \otimes |1\rangle \\ |1\rangle \otimes |1\rangle &\rightarrow |1\rangle \otimes |1\rangle \end{aligned}$$

on two adjacent atomic qubits. Write down the state resulting from the application of this gate to an arbitrary two qubit product state $|\psi\rangle \otimes |\phi\rangle$. Hence, or otherwise, discuss whether the SWAP gate in combination with single qubit gates constitute a universal set of quantum gates.

By turning the lasers on for a time τ, the operation $\sqrt{\text{SWAP}}$ is realized. The states $|0\rangle \otimes |0\rangle$ and $|1\rangle \otimes |1\rangle$ are unaffected by the dynamics. Calculate a matrix representation of this $\sqrt{\text{SWAP}}$ gate in the computational basis. Apply the network

$$U = H_2 \sqrt{\text{SWAP}}\, Z_1 \sqrt{\text{SWAP}}\, \sqrt{Z_2}\, H_2$$

to the four computational basis states. Here Z_i denotes the Z-gate applied to the i-th qubit and H_2 is the Hadamard gate on the second qubit. Extend this network using single qubit gates to realize a CNOT gate. Discuss whether the $\sqrt{\text{SWAP}}$ gate together with single qubit gates constitute a universal set of quantum gates.

Additional worked examples

8. For quantum dense coding Bob needs a Bell state analyzer. What is the channel capacity (number of classical bits transmitted in one use of the channel) if Bob has an ideal Bell state analyzer? How is this channel capacity reduced if the Bell state analyzer is only able to identify the two Bell states $|\Psi^{\pm}\rangle$ but cannot differentiate between the two Bell states $|\Phi^{\pm}\rangle$?

Solution: Per use of the channel 2 bits are transmitted $\rightarrow$ channel capacity of 2 bits. Possible encoding $|\psi^+\rangle = |00\rangle$, $|\psi^-\rangle = |01\rangle$, $|\phi^-\rangle = |10\rangle$, $|\phi^+\rangle = |11\rangle$

If the states $|10\rangle$ and $|11\rangle$ are not distinguished three distinct messages can be sent over the channel per use.

$\rightarrow C(N) = \log_2(3) = 1.53$bits

9. In the ZZZ basis a GHZ state is given by

$$|\text{GHZ}\rangle \;=\; \frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle).$$

By rewriting this GHZ state in the bases XYY, YXY and YYX show that measuring two of the photons in circular polarization determines the polarization of the third photon in the X basis with certainty. Rewrite the GHZ state in the XXX basis and show that measuring in this XXX basis violates the expectations of local realism.

Solution: We identify $|H\rangle$ and $|V\rangle$ with $|0\rangle$ and $|1\rangle$ in the Z basis and then denote the corresponding basis states in the X basis by $|H'\rangle$ and $|V'\rangle$ and in the Y basis by $|R\rangle$ and $|L\rangle$. Using $\sqrt{2}|H'\rangle = |H\rangle + |V\rangle$, $\sqrt{2}|V'\rangle = |H\rangle - |V\rangle$ and $\sqrt{2}|R'\rangle = |H\rangle + i|V\rangle$, $\sqrt{2}|L\rangle = |H\rangle - i|V\rangle$ we find

$$\begin{aligned}
\frac{1}{\sqrt{2}}\left(|HHH\rangle + |VVV\rangle\right) &= \frac{1}{4}(|(H'+V')(R+L)(R+L)\rangle - |(H'-V')(L-R)(L-R)\rangle) \\
&= \frac{1}{4}(|H'RR\rangle + |H'RL\rangle + |H'LR\rangle + |H'LL\rangle \\
&\quad +|V'RR\rangle + |V'RL\rangle + |V'LR\rangle + |V'LL\rangle \\
&\quad -|H'RR\rangle + |H'RL\rangle + |H'LR\rangle - |H'LL\rangle \\
&\quad +|V'RR\rangle - |V'RL\rangle - |V'LR\rangle + |V'LL\rangle) \\
&= \frac{1}{2}(|H'RL\rangle + |H'LR\rangle + |V'LL\rangle + |V'RR\rangle),
\end{aligned}$$

and by symmetry we find in the other bases

$$\frac{1}{\sqrt{2}}\left(|HHH\rangle + |VVV\rangle\right) \;=\; \frac{1}{2}(|RH'L\rangle + |LH'R\rangle + |LV'L\rangle + |RV'R\rangle),$$

$$\frac{1}{\sqrt{2}}\left(|HHH\rangle + |VVV\rangle\right) \;=\; \frac{1}{2}(|RLH'\rangle + |LRH'\rangle + |LLV'\rangle + |RRV'\rangle),$$

Therefore, measuring two photons in circular R, L polarization the state of the third photon is fixed; if the two results are identical RR or LL then the third photon is in state V' and for opposite plarizations LR or RL the polarization of the third photon is H'. Let us consider a measurement in the XXX basis. Quantum mechanically we find

$$\begin{aligned}
\frac{1}{\sqrt{2}}\left(|HHH\rangle + |VVV\rangle\right) &= \frac{1}{4}(|(H'+V')(H'+V')(H'+V')\rangle + \\
&\quad |(H'-V')(H'-V')(H'-V')\rangle) \\
&= \frac{1}{2}(|H'H'H'\rangle + |H'V'V'\rangle + |V'H'V'\rangle + |V'V'H'\rangle),
\end{aligned}$$

Which outcomes are possible if the polarizations are elements of reality? The permutations of $|\text{GHZ}\rangle$ above imply that if H (V) is obtained for one photon the other two have to have opposite(identical) circular polarization. Imagine we find V and V for photons 2 and 3. Since 3 is V, 1 and 2 have to have identical circular polarization. Also, since 2 is V, 1 and 3 have to have identical circular polarization. If all of these are elements of reality then all photons have identical circular polarization. Thus photon 1 needs to

carry polarization V. We conclude that $|VVV\rangle$ is a possible outcome. Similarly one can verify that the only four possible outcomes

$$|V'V'V'\rangle, \qquad |H'H'V'\rangle, \qquad |H'V'H'\rangle, \qquad |V'H'H'\rangle.$$

Local realism and quantum mechanics predict opposite results in all cases!

10. Alice and Bob share an entangled pair of qubits in the state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ and Alice wants to use this EPR pair, a perfect Bell state analyzer and a classical communication channel to transmit an unknown state $|\psi\rangle$ of a third qubit to Bob. Bob is able to apply any single-qubit operation to his qubit. Describe and explain a protocol for achieving this, giving the three-qubit state after each step in the protocol. How much classical information needs to be transmitted over the classical channel to transmit one qubit?

Now assume that Alice has an imperfect Bell state analyzer which cannot distinguish the states $|\phi^+\rangle$ and $|\phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$. She does not tell Bob about this imperfection but randomly assumes one of the two states whenever the Bell state analyzer gives an ambiguous result. Calculate the fidelity with which an arbitrary state $|\psi\rangle$ is teleported in this case. Which states are teleported with maximum fidelity and which states are teleported with minimum fidelity?

Solution: Teleportation protocol with entangled pair $|\phi^+\rangle_{12} = (|00\rangle + |11\rangle)/\sqrt{2}$ and particle to be teleported $|\psi\rangle_3 = \alpha|0\rangle + \beta|1\rangle$.

Bell state measurement at Alice's site with initial state before measurement: $|\psi\rangle_{123} = (\alpha|000\rangle + \alpha|110\rangle + \beta|001\rangle + \beta|111\rangle)/\sqrt{2}$ has the following possible outcomes

${}_{23}\langle\phi^+|\psi\rangle_{123} = (\alpha|0\rangle_1 + \beta|1\rangle_1)/2 = |\psi^+_\phi\rangle/2,$

${}_{23}\langle\phi^-|\psi\rangle_{123} = (\alpha|0\rangle_1 - \beta|1\rangle_1)/2 = |\psi^-_\phi\rangle/2,$

${}_{23}\langle\psi^+|\psi\rangle_{123} = (\alpha|1\rangle_1 + \beta|0\rangle_1)/2 = |\psi^+_\psi\rangle/2,$

${}_{23}\langle\psi^-|\psi\rangle_{123} = (\beta|0\rangle_1 - \alpha|1\rangle_1)/2 = |\psi^-_\psi\rangle/2.$

Each measurement outcome has probability 1/4. Not knowing the outcome of the measurement the density operator is $\rho_{123} = 1/4(|\psi^+_\phi\rangle_1\langle\psi^+_\phi| \otimes |\phi^+\rangle_{23}\langle\phi^+| + ...)$. If the outcome is known the part corresponding to this outcome (renormalized) will be the actual density operator.

After telling Bob the outcome he applies to his particle:

$|\phi^+\rangle : \mathbb{I}$, $|\phi^-\rangle : \sigma^z_1$, $|\psi^+\rangle : \sigma^x_1$, $|\psi^-\rangle : \sigma^x_1\sigma^z_1$ (up to a global phase).

Thus the state of the three particles becomes $\rho_{123} = |\psi\rangle_1\langle\psi| \otimes (|\phi^+\rangle_{23}\langle\phi^+| + |\phi^-\rangle_{23}\langle\phi^-| + ...)/4$.

This state is a product state of particle 1 with particles 2,3. All information about the initial state is transferred to particle 1. The reduced state of Bob's particle is pure $\rho_1 = \mathrm{tr}_{23}\{\rho_{123}\} = |\psi\rangle_1\langle\psi|$ with $|\psi\rangle_1 = \alpha|0\rangle_1 + \beta|1\rangle_1$, i.e. the state has been teleported.

Classical information: Alice needs to send one of four messages (the measurement outcomes) with equal probability per teleported qubit. This corresponds to $H = \log_2(4) = 2$ bits of classical information.

In the case of an imperfect Bell state analyzer the knowledge about the state of particles 23 is not perfect leading to $(\alpha|0\rangle + \beta|1\rangle)|\psi^\pm\rangle \to |\psi\rangle\langle\psi| \otimes |\phi^\pm\rangle\langle\phi^\pm|/2 + |\psi_E\rangle\langle\psi_E| \otimes |\phi^\pm\rangle\langle\phi^\pm|/2,$

where $|\psi_E\rangle = \alpha|0\rangle - \beta|1\rangle$. After Bob applies his unitary operation we find $\tilde{\rho}_{123} = |\psi\rangle\langle\psi| \otimes (|\phi^+\rangle\langle\phi^+|/8 + |\phi^-\rangle\langle\phi^-|/8 + |\psi^-\rangle\langle\psi^-|/4 + |\psi^+\rangle\langle\psi^+|/4) + |\psi_E\rangle\langle\psi_E| \otimes (|\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-|)/8$. We can now again trace over particles 2, 3 yielding $\tilde{\rho}_1 = 3|\psi\rangle\langle\psi|/4 + |\psi_E\rangle\langle\psi_E|/4$. The resulting fidelity is then given by $F = \langle\psi|\tilde{\rho}_1|\psi\rangle = 3/4 + 1/4|\langle\psi_E|\psi\rangle|^2 = 3/4 + |1 - 2|\beta|^2|/4$ with a maximum value of $F_{\max} = 1$ for $|\beta|^2 = 0$ or $|\beta|^2 = 1$ and states $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$. The minimum value $F_{\min} = 3/4$ is obtained for $|\beta|^2 = 1/2$ and states $|\psi\rangle = (|0\rangle + e^{i\phi}|1\rangle)/\sqrt{2}$ with arbitrary phase $\phi \in [0, 2\pi[$.