Problem Set: TT Quantum Information

2 Basics of Information Theory

1. Alice can send four messages A, B, C, and D over a classical channel. She chooses A with probability 1/2, B with probability 1/4 and C and D with probability 1/8. How much information is contained in one of her messages? Find an optimal bit-code for encoding these messages and show that in this code each bit has equal probability of having values 0 or 1.

   Now imagine that Alice uses trits (with values 0,1,2) instead of bits to encode her messages and chooses to send A, B, C, D, and E with probabilities 1/3, 1/3, 1/9, 1/9, 1/9, respectively. What is an optimal code in this case? Show that in this code each trit has equal probability of having values 0, 1, and 2.

2. Show that the reduced density operator of each qubit of a Bell pair is the maximally mixed state. This result is independent of which Bell state is used. Why? Use this result to calculate the von Neumann entropy of a two qubit system in a Bell state as well as the reduced entropies of each of the qubits separately.

3. The density operator of two qubits A and B is given by $\rho_{AB} = (|\Psi^-\rangle\langle\Psi^-| + |\Phi^+\rangle\langle\Phi^+| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|)/4$. Calculate the von Neumann entropy $S(\rho_{AB})$ and the entropies of the reduced systems $S(\rho_A)$ and $S(\rho_B)$. Is the state ρ_{AB} entangled? If it is not entangled find the density operator ρ_{AB} in the form

$$\rho_{AB} = \sum_j p_j \rho_A^{(j)} \otimes \rho_B^{(j)}. \tag{1}$$

   Repeat the above calculations for the state $\tilde{\rho}_{AB} = (|\Psi^-\rangle\langle\Psi^-| + |\Phi^+\rangle\langle\Phi^+|)/2$.

3 Photon techniques

4. Consider the optical setup shown in Fig. 1. Find the state of the output qubit as a function of ϕ and γ for two 50/50 beam splitters. What changes if the beam splitters reflect a photon with 75% probability?

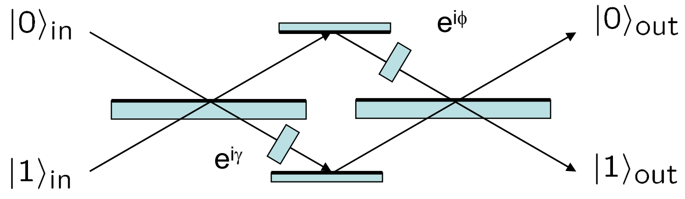

Figure 1: Interferometer setup

5. A laser with an intensity of $I = 5\mu\text{W/cm}^2$, wavelength $\lambda = 500\text{nm}$, and a bandwidth of 1GHz is attenuated by sending it through a small pinhole of area A. For which area A does the attenuated laser beam contain 1 photon per 10ns on average? What is the

probability that the attenuated laser beam contains a second photon within the coherence length of one photon?

6. Consider a momentum entanglement interferometer experiment as shown in the lecture notes. Calculate the dependence of coincident detections given the state

$$|\Psi\rangle \;=\; \frac{1}{\sqrt{2}}\left[e^{i\phi_b}|a\rangle_1|b\rangle_2 + e^{i\phi_a}|a\rangle_2|b\rangle_1\right]$$

before the beam splitters.

4 Testing EPR

7. Work out the quantum mechanical expectation values for the combination of observables Q, R at Alice's site and S, T at Bob's site (as defined in the lecute notes) which lead to a violation of the CHSH inequality for the Bell state $|\Psi^-\rangle$. Which observables should Alice and Bob measure if a CHSH type inequality should be violated for the state $|\phi^-\rangle$.

8. Consider the rare events where the UV pulse in Fig. 2 creates two indistinguishable Bell pairs each in the state

$$|\Psi\rangle \;=\; \frac{1}{\sqrt{2}}\left[|H\rangle_a|V\rangle_b + e^{i\phi}|V\rangle_a|H\rangle_b\right].$$

and determine all possible paths for one and only one photon to arrive at the detectors D1, D2 and D3 given that one photon triggers the detector T. Deduce that (up to the relative phase between the two terms) the conditional state of these photons at detectors D1, D2, and D3 given a click occurred at detector T is given by

$$|\mathrm{GHZ}'\rangle \;=\; \frac{1}{\sqrt{2}}(|HHV\rangle + |VVH\rangle).$$

How can this state $|\mathrm{GHZ}'\rangle$ be transformed into the state $|\mathrm{GHZ}\rangle$?

5 Quantum communication

9. Explain the quantum dense coding protocol and determine the states which are received by Bob if Alice and Bob start from the joint Bell state $|\phi^+\rangle$ and Alice uses the operations $\mathbf{1}$, σ_x^1, σ_z^1, and $\sigma_z^1\sigma_x^1$ for encoding 00, 01, 10, and 11, respectively. Show that if Bob could only carry out measurements on one of the two particles he would not gain any information about the message sent by Alice.

10. Work out the quantum teleportation protocol if the qubits 2 and 3 are created in the Bell state $|\Phi^+\rangle_{23}$. Show that without classical communication no information about the state of qubit 1 is transferred to qubit 3. Explain why it is impossible to transmit the quantum state of a qubit from Alice to Bob by classical communication only.

11. Entanglement swapping: The state of qubit 1 which is entangled with a system 4 can be written as $|\Psi\rangle = (|0\rangle_1|\Phi_0\rangle_4 + |1\rangle_1|\Phi_1\rangle_4)/\sqrt{2}$. Show that if the teleportation protocol is applied to qubit 1 the entanglement with system 4 is swapped to qubit 3.

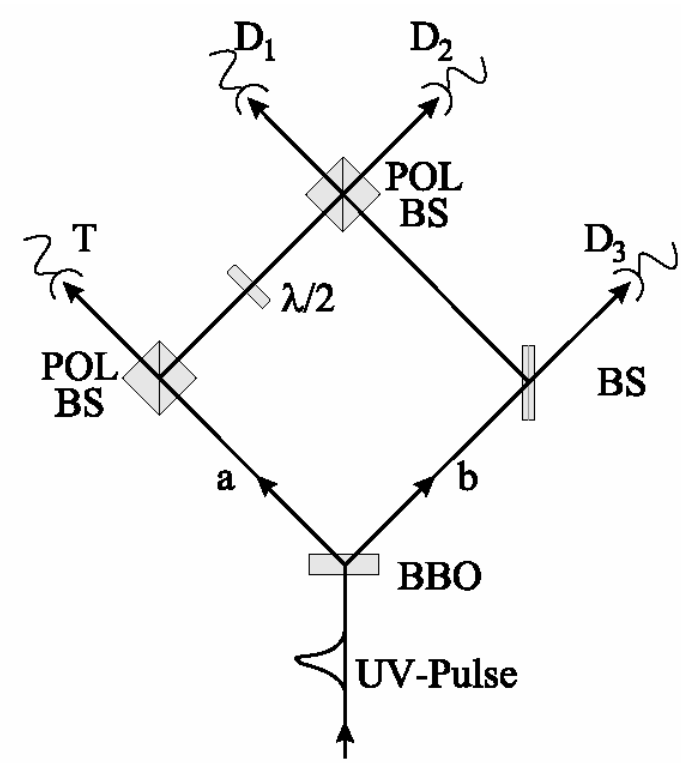

Figure 2: GHZ state creation

Additional worked examples

Please do not hand in answers to the following problems. These examples will not be discussed in class unless you have queries about them. Some of these examples contain detailed calculations which may be of interest to you, others are on topics which go slightly beyond the core syllabus of C2.

12. The 26 letters of the alphabet appear with percentages given below in common English texts. What is the average information content of an English text with 100 letters? What is the maximum information that a text with 100 letters could contain? Which percentage of letters in an English text can be transmitted wrongly without (on average) destroying the information contained in the text?

E 11.1607%	A 8.4966%	R 7.5809%	I 7.5448%
O 7.1635%	T 6.9509%	N 6.6544%	S 5.7351%
L 5.4893%	C 4.5388%	U 3.6308%	D 3.3844%
P 3.1671%	M 3.0129%	H 3.0034%	G 2.4705%
B 2.0720%	F 1.8121%	Y 1.7779%	W 1.2899%
K 1.1016%	V 1.0074%	X 0.2902%	Z 0.2722%
J 0.1965%	Q 0.1962%		

Solution: The average Shannon entropy of one letter in the English language is $S_{\text{English}} = \sum_{j=A\cdots Z} -p_j \log_2(p_j) = 4.2468$ while the maximum Shannon entropy of one out of 26 letters is $S_{\text{max}} = \log_2(26) = 4.7004$. Therefore an English text with 100 letters contains

425 bits of information while the maximum is 470 bits. The 425 bits of information could in principle be transmitted with 91 letters. About 9% of the sent letters are redundant (ignoring the frequency of words) and can be transmitted wrongly without affecting the message.

13. The density operator of a two qubit system is given by

$$\rho = \rho_A \otimes \rho_B.$$

Show that the von Neumann entropy of this system is given by $S(\rho_{AB}) = S(\rho_A) + S(\rho_B)$.

Solution: The density operators can be written as $\rho_A = \sum_j p_j^A |\psi_j\rangle\langle\psi_j|$ and $\rho_B = \sum_n p_n^B |\phi_n\rangle\langle\phi_n|$. The eigenvectors of the density operator are thus $|\psi_j\rangle \otimes |\phi_j\rangle$ with a probability of $p_j^A p_n^B$ where p_j^A are the eigenvalues (probabilities) of the density operator ρ_A and p_n^B are the eigenvalues of ρ_B. We can thus write $S(\rho) = -\sum_{j,n} p_j^A p_n^B \log_2(p_j^A p_n^B) = -\sum_{j,n} p_j^A p_n^B \log_2(p_n^B) - \sum_{j,n} p_j^A p_n^B \log_2(p_j^A) = -\sum_n p_n^B \log_2(p_n^B) - \sum_j p_j^A \log_2(p_j^A) = S(\rho_A) + S(\rho_B)$.

14. Show that the classical conditional Shannon entropy $H(Y|X)$ is always larger or equal zero, while the conditional von Neumann entropy $S(\rho_A|\rho_B)$ is larger or equal to zero for a pure state ρ_{AB} if and only if ρ_{AB} is not entangled, i.e. if it can be written as

$$\rho = \rho_A \otimes \rho_B$$

and is smaller than zero for entangled states.

Solution: The probability of having values x for X and y for Y is given by $p(x,y) = p(x)p(y|x)$. Furthermore

$$\begin{aligned} H(X,Y) &= -\sum_{x,y} p(x,y)\log_2(p(x)p(y|x)) = -\sum_x p(x)\log_2(p(x)) - \sum_{x,y} p(x,y)\log_2(p(y|x)) \\ &= H(x) - \sum_{x,y} p(x,y)\log_2(p(y|x)), \end{aligned}$$

and therefore

$$H(Y|X) = -\sum_{x,y} p(x,y)\log_2(p(y|x)) \geq 0,$$

since $p(x,y) \geq 0$ and $-\log_2(p(y|x)) \geq 0$. $H(Y|X)$ is only equal to zero if Y is a deterministic function of X.

If $\rho = |\Psi_A\rangle\langle\Psi_A| \otimes |\Psi_B\rangle\langle\Psi_B|$ then $S(\rho) = 0$, $S(\rho_A) = 0$ and also $S(\rho_B) = 0$. Thus $S(\rho_A|\rho_B) = 0$. If $S(\rho_A|\rho_B) \geq 0$ then

$$0 \leq S(\rho_A|\rho_B) = S(\rho) - S(\rho_B) = -S(\rho_B) \leq 0,$$

since $S(\rho) = 0$ for any pure state. Therefore $0 \leq -S(\rho_B) \leq 0$ and so $S(\rho_B) = 0$ and therefore ρ_B is a pure state. This means that $\rho = \rho_A \otimes \rho_B$ and since ρ is pure we also have a pure ρ_A.

15. Consider a two photon Franson interferometer as shown in the lecture notes. Under which condition on the coherence length of the photons created in the EPR source will there be no interference in each of the two arms? However, SS and LL detections are still coincident and can be selected by time gating. How do coincidence clicks between detections in the two arms change as a function of the sum of the two path differences α and β.

Solution: If the coherence length of a photon $c\tau_c$ (with c the speed of light) is much shorter than the path difference between the long and the short arm $\Delta L_j = L_j - S_j$ with $j = (1, 2)$ there will be no interference in each arm. By suitable time gating the contributions $|SS\rangle$ and $|LL\rangle$ can be selected. If the coherence length of the pump $c\tau_{\text{pump}}$ is much longer than the path differences ΔL_j the paths $|SS\rangle$ and $|LL\rangle$ can interfere. Also, it is important that the two photon coherence length $c\tau_{tpc}$ (which is usually similar to $c\tau_c$) is much longer than the difference between the two long paths $\Delta L = L_1 - L_2$. With $\alpha = \Delta L_1$ and $\beta = \Delta L_2$ the phase difference between $|SS\rangle$ and $|LL\rangle$ is given by

$$\Delta\phi = \frac{\omega_p}{2c}(\alpha + \beta),$$

where ω_p is the pump laser frequency. The part of the state selected by time gating is

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\Big(|SS\rangle + e^{i\Delta\phi}|LL\rangle\Big)$$

which yields a dependence of the rate of true coincidence clicks on the phase difference $\Delta\phi$ given by

$$\frac{1}{2}|1 + e^{i\Delta\phi}|^2 = 1 + 1\cos(\Delta\phi).$$

Typical experimental parameters are $\Delta L_j \approx 63$cm, $c\tau_{\text{pump}} \approx 6$m and $c\tau_p \approx c\tau_{tpc} \approx 36\mu$m and yield a visibility of $\approx 90\%$.

16. Using the symmetry properties of photons explain how the Bell states $|\Psi^\pm\rangle$ can be distinguished in a partial Bell state analyzer for polarization encoded photons. Why can the other two states not be distinguished? Imagine that photons were fermions (which is not true!). How would the partial Bell state analyzer work in this case?

Solution: For bosonic photons the overall wave function symmetric.

$|\Psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$ has an asymmetric polarization wave function $\Rightarrow$ the photons need to go into two different arms to preserve overall symmetry causing correlated clicks at two detectors in different arms.

$|\Psi^+\rangle = (|HV\rangle + |VH\rangle)/\sqrt{2}$ has a symmetric polarization wave function $\Rightarrow$ the photons need to go into the same arm causing correlated clicks at two detectors in the same arm.

The same symmetry arguments lead to two clicks in one detector for the states $|\Phi^\pm\rangle$ which can thus not be distinguished.

In the case of fermionic particles the arguments are based on overall asymmetry of the wave function. Again the states $|\Phi^\pm\rangle$ are not distinguishable (they cause the same type of correlated clicks in the two different arms).

17. Explain why the BB84 protocol cannot be directly used for securely transmitting a message but allows establishing a random key between Alice and Bob.

In the BB84 protocol with $n = 500$ how large do Alice and Bob have to choose the parameter δ if they want to be left with at least $2n$ key bits with a probability of $p = 99.9\%$ after Bob has performed his measurements? How likely will Alice and Bob detect an eavesdropper who is using the intercept/resend strategy on each second qubit on an otherwise perfect channel when comparing n bits of their established key?

Solution: BB84 cannot be used for sending messages directly since it is not know which qubits will result in a transmission of information from Alice to Bob. However, after the qubits have been sent Alice and Bob can find out which of their measurements are perfectly correlated without revealing the results. Thus they can use those measurement results to establish a secret key.

The probability of getting a useless measurement result is 1/2. Thus the probability of getting y useful measurements out of x is given by

$$p(x,y) = \left(\begin{array}{c} x \\ y \end{array} \right) 2^{-x}$$

and we approximate this by the normal distribution with mean value $x/2$ and variance of $x/4$. Thus the probability of $2n$ or more successes is given by the error function (using the appropriate continuity correction)

$$p = \sum_{y=2n}^{x} p(x,y) \approx \frac{1}{2}\left[1 - \operatorname{erf}\left(\frac{2n - 1/2 - x/2}{\sqrt{x/2}}\right)\right]$$

For $p = 99.9\%$ this equation has the solution $x \approx 2142$ and thus $\delta = x/n - 4 = 28\%$. This result agrees excellently with exactly summing up the probabilities according to the binomial distribution. The probability that measurements of Alice and Bob in the same basis yield disagreement is 1/4 for each qubit which Eve intercepted. Thus by comparing $n = 500$ bits of which $n/2$ have been intercepted results in a probability of not detecting the eavesdropper

$$p_{nd} = (\frac{3}{4})^{250} \approx 6 \times 10^{-32}.$$

This does not take into account that Eve could randomly choose which qubits to intercept and thus assumes that exactly 250 qubits were intercepted by Eve.