1. Shannon entropy

(a) Relative entropy (2 P)

Use the definition of the relative entropy,

\[ H(p(x)||q(x)) := \sum_x p(x)(\log p(x) - \log q(x)), \]  

show that this quantity is always non-negative,

\[ H(p(x)||q(x)) \geq 0, \]  

and that equality holds iff \( p(x) = q(x) \forall x \).

Hint: Use that \( \ln x < x - 1 \) for \( x > 0, x \neq 1 \) and \( \ln x = x - 1 \) for \( x = 1 \).

(b) Sub-additivity of the entropy (2 P)

Show that the Shannon entropy is sub-additive (Hint: use the definition of the relative entropy for \( H(p(x,y)||p(x)p(y)) \)),

\[ H(X,Y) \leq H(X) + H(Y). \]  

(c) Mutual information (2 P)

Recall the definition of the mutual information,

\[ I(X : Y) := H(X) - H(X|Y). \]  

It measures the amount of information that is learnt about \( X \) when one gets to know \( Y \). Show that this quantity is also non-negative and that it vanishes iff \( X \) and \( Y \) are independent (use hint of [1a] and the sub-additivity theorem).
2. Turing machine

(a) Turing Machine I: (2 P)
Consider the following Turing machine: \( \Sigma = \{0, 1\} \), \( Q = \{q_S, q_h, q_1\} \), together with the program
\[
(q_S, \triangleright, q_1, \triangleright, +1) \\
(q_1, 0, q_1, 0, +1) \\
(q_1, 1, q_1, 1, +1) \\
(q_1, \#, q_h, 0, 0).
\]
Assume that the initial state of the tape is
\[
[\ldots, \#, \triangleright, 1, 0, 0, 1, 0, \ldots, \#, \ldots].
\]
What does this algorithm compute?

(b) Turing Machine II: (3 P)
Construct a Turing machine that realizes the function
\[
f(x) = x + 1, \quad \text{for } x \in \mathbb{N}.
\]
3. Complexity classes \( P \) and \( NP \)

![Figure 1: Example of an undirected graph](image)

(a) Does the upper graph contain an Euler cycle? 
   In case one exists, specify the way. \( (1 \ P) \)

(b) Does the upper graph contain a Hamilton cycle? 
   In case one exists, specify the way. \( (1 \ P) \)

(c) Develop a schematic algorithm to check whether a graph contains an Euler cycle or not (Use Euler’s theorem). Also include the approximate number of operations required for each step and give a scaling of your algorithm. (Remember to check first whether the graph is connected.) \( (3 \ P) \)

(d) Like (3c) but for a Hamilton cycle. \( (3 \ P^*) \)

Note: Exercises with an * are voluntary and lead to "bonus" points.
Quantum Information (Exercises II)
due date: 24.11.04

1. Single qubit systems
   (a) Bloch vector of pure states (2 P)
   Show that all pure states of the single qubit density operator \( \rho_{\text{pure}} \) are represented by a Bloch vector \( \vec{s} \) with length one.

   (b) Bloch vectors of orthogonal states (2 P)
   Which relation do the Bloch vectors \( \vec{s}_1 \) and \( \vec{s}_2 \) of two orthogonal single qubit density operators (i.e. \( \text{tr}(\rho_1 \rho_2) = 0 \)) have? (Hint: use \( \sigma_i \sigma_j = \delta_{ij} + i\epsilon_{ijk} \sigma_k \) and \( \text{tr}(\sigma_i = 0) \))
   Can orthogonal density operators be mixed?

   (c) Mixed states (2 P)
   Prove that the decomposition of a mixed state density matrix into a weighted sum of projectors is not unique. (Give an example of two different weighted sums of projectors onto pure states, leading to the same mixed density operator.)

2. Composite qubit systems
   (a) Tensor product I (1 P)
   Construct the state vector of the combined system \( |ab \rangle \) using the single qubit state vectors \( |a \rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \) and \( |b \rangle = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \).

   (b) Tensor product II (1 P)
   Construct the density matrices \( \rho_a \) and \( \rho_b \), using the state \( |a \rangle \) and \( |b \rangle \), respectively. Calculate the density matrix of the combined system \( \rho_{ab} \) by building the tensor product \( \rho_{ab} = \rho_a \otimes \rho_b \). Verify the result by comparing it with \( |ab \rangle \langle ab | \) from (2a).

   (c) Partial trace (1 P)
   Verify that \( \rho_b = \text{tr}_a(\rho_{ab}) \) by using the expressions from (2b).
(d) **Unitary Transformation (1 P)**

Calculate $\rho'_a = U_a \rho_a U_a^\dagger$ and $\rho'_b = U_b \rho_b U_b^\dagger$ for

$$U_a = \begin{pmatrix} \cos \phi & -\sin \phi \\ \sin \phi & \cos \phi \end{pmatrix}, \quad U_b = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$ 

(e) **Unitary Local Transformation and Partial Traces (2 P)**

Verify that $\\rho_{ab}' = U_{ab} \rho_{ab} U_{ab}^\dagger$ where $\rho_{ab}' = \rho'_a \otimes \rho'_b$ and $U_{ab} = U_a \otimes U_b$. Check whether $\text{tr}_b(\rho_{ab}') = \rho'_a$.

3. **Entanglement**

(a) **Schmidt Decomposition (2 P)**

Find the Schmidt ranks of the two states

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} (i |00\rangle + |01\rangle - |10\rangle + i |11\rangle),$$

$$|\Psi_2\rangle = \frac{1}{\sqrt{2}} (i |00\rangle + |01\rangle + |10\rangle + i |11\rangle).$$

Are the states separable or entangled?

(b) **Partial Trace and Entanglement (3 P)**

Apply the unitary transformation

$$U_{\text{cNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

to the product state

$$\rho_{ab} = |\Psi\rangle\langle\Psi| = \frac{1}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

with $|\Psi\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) |0\rangle$, to get $\rho_{ab}' = U_{\text{cNOT}} \rho_{ab} U_{\text{cNOT}}^\dagger$ (*Note: The unitary transformation represented by $U_{\text{cNOT}}$ cannot be written as product of local rotations, i.e. $U_{\text{cNOT}} \neq U_a \otimes U_b$*).

Calculate $\rho'_a = \text{tr}_b(\rho_{ab}')$ and describe the properties of that state. Is $\rho_{ab}'$ separable or entangled?
Quantum Information (Exercises III)
due date: 08.12.04

1. von Neumann entropy

(a) von Neumann entropy of pure states (2 P)

Calculate the von Neumann entropy of the reduced density operator 
\( S(\rho_a) \) of qubit \( a \) (\( \rho_a = \text{tr}_b(\rho) = \text{tr}_b(|\Psi\rangle\langle \Psi|) \)) of the two-qubit states, 
(i) \( |\Psi_i\rangle = \alpha |00\rangle + \beta |11\rangle \) with \( |\alpha|^2 + |\beta|^2 = 1 \) and (ii) \( |\Psi_{ii}\rangle = \frac{1}{\sqrt{2}} (|00\rangle + \cos \phi |10\rangle + \sin \phi |11\rangle) \). Draw a graph showing the von Neumann entropy depending on (i) \( |\alpha|^2 \) and (ii) \( \cos \phi \). What are the properties of \( |\Psi_i\rangle \) and \( |\Psi_{ii}\rangle \)?

2. Measurements

(a) Projectors (1 P)

Let \( |u\rangle \) and \( |v\rangle \) be normalized vectors. Show that \( |u\rangle \langle u| \) and \( |v\rangle \langle v| \) are projectors. Moreover, show that \( |u\rangle \langle u| + |v\rangle \langle v| \) is a projector iff \( \langle u | v \rangle = 0 \). Generalize this result to an arbitrary number of vectors.

(b) von Neumann measurements (1 P)

The measurement performed by a Stern-Gerlach apparatus oriented in \( z \)-direction is a set of orthogonal projectors, \( P_1 = |0\rangle\langle 0| \) and \( P_2 = |1\rangle\langle 1| \).

Show that this apparatus cannot distinguish between \( |\psi_1\rangle := \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \) and \( \rho_2 := \frac{1}{2} |0\rangle \langle 0| + \frac{1}{2} |1\rangle \langle 1| \). Devise an measurement achieving that.

3. Entanglement and decoherence

(a) Density operator of the singlet (2 P)

Given the singlet state 
\[
|\psi^-\rangle = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle).
\] (23)

i) Write \( |\psi^-\rangle \) in another basis \( \{ |\overline{0}\rangle, |\overline{1}\rangle \} \), defined by \( |\overline{0}\rangle = \alpha |0\rangle + \beta |1\rangle \) and 
\( |\overline{1}\rangle = -\beta^* |0\rangle + \alpha^* |1\rangle \), with \( |\alpha|^2 + |\beta|^2 = 1 \).
ii) Show that $|\psi^-\rangle \langle \psi^-|$ can be written as

$$\rho = \frac{1}{4} \left( 1 \otimes 1 - \sum_i \sigma_i \otimes \sigma_i \right).$$

(24)

(b) The depolarizing channel (2 P)

This channel can be used to describe a qubit subjected to the following error model: With probability $1 - p$, nothing happens to the qubit, and with probability $p$ one of the following errors occurs with equal probability:

- Bit flip: $|0\rangle \rightarrow |1\rangle$, $|1\rangle \rightarrow |0\rangle$, i.e. $|\psi\rangle \rightarrow \sigma_x |\psi\rangle$.
- Phase flip: $|0\rangle \rightarrow |0\rangle$, $|1\rangle \rightarrow -|1\rangle$, i.e. $|\psi\rangle \rightarrow \sigma_z |\psi\rangle$.
- Bit and phase flip: $|0\rangle \rightarrow i|1\rangle$, $|1\rangle \rightarrow -i|0\rangle$, i.e. $|\psi\rangle \rightarrow \sigma_y |\psi\rangle$.

We can describe this channel by the following unitary evolution in the Hilbert space of the qubit plus environment:

$$|\psi\rangle_A \otimes |0\rangle_E \rightarrow \sqrt{1-p} |\psi\rangle_A \otimes |0\rangle_E + \sqrt{\frac{p}{3}} \sum_i \sigma_i |\psi\rangle_A \otimes |i\rangle_E$$

(25)

Compute the Bloch vector representation of a general pure state after the evolution.

4. Quantum teleportation

(a) Entanglement swapping (2 P)

In the lecture the entanglement swapping protocol was presented. Show that a Bell measurement on particles $Z$ and $A$ in the state

$$|\psi^{\text{total}}\rangle = |\psi\rangle_{YZ} \otimes |\psi^-\rangle_{AB}$$

$$= [\alpha |01\rangle + \beta |10\rangle]_{YZ} \otimes \frac{1}{\sqrt{2}} [ |01\rangle - |10\rangle]_{AB},$$

followed by an appropriate rotation of the particles $B$, results in the desired state $|\psi\rangle_{BY}$, up to a global phase. Which rotation of $B$ is needed for which outcome of the Bell measurement?
Quantum Information (Exercises IV)
due date: 22.12.04

1. Quantum cloning

(a) **Copying a set of quantum states** (3 P)

Is it possible to perfectly (with probability one) clone a quantum state \( |\Psi_i\rangle \in \{ |\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_K\rangle \} \) using an ancilla \( |A_0\rangle \), i.e. \( U |\psi_i\rangle |i\rangle |A_0\rangle = |\psi_i\rangle |\psi_i\rangle |A_i\rangle \)? If this is possible, which sets of states can be used for such a procedure and which role plays the ancilla?

(b) **Superluminal information transfer** (3 P)

Show that it would be possible to send information faster than light, if one could perfectly copy any quantum state. Consider the case where Alice and Bob share a singlet \( |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \) and Alice does a measurement in the basis \( z \) if she wants to send a 0 and in the basis \( x \) if she wants to send a 1 to Bob. Assume that Bob uses a perfect cloning machine. Show that Bob could distinguish between Alice’s measurement bases by measuring his perfect copies.

(c) **Signalling with probabilistic cloning** (1 P*)

If one uses probabilistic cloning, it is possible to clone certain sets of quantum states perfectly with a probability \( p_i > 0 \). Consider the same scenario as in (1b). Which property of the occurring states forbids superluminal information transfer with this procedure?
2. Quantum cryptography

(a) The six state protocol (4 P)

Generalize the BB84 protocol presented in the lecture to the so-called “six state protocol” (use the same structure for the protocol as in the script), using the eigenstates of $\sigma_x$, $\sigma_y$, and $\sigma_z$ as measurement bases for Alice and Bob.

i) How long is the sifted key after the basis reconciliation process\(^1\) as a fraction of the number of qubits sent from Alice to Bob?

ii) How big is the fraction of errors introduced by Eve, who uses a simple intercept-resend strategy?

(b) Optimal Eavesdropping (3 P)

Consider the BB84 protocol, where Alice sends qubits taken from the two basis sets $A := \{|0\rangle, |1\rangle\}$ and $\bar{A} := \{|\bar{0}\rangle, |\bar{1}\rangle\}$ to Bob. When Eve is allowed only to interact with one qubit at a time (a so-called “individual attack”), the most general unitary transformation she can devise is\(^2\)

\[
\begin{align*}
|0\rangle & \rightarrow U |0\rangle |X\rangle = \sqrt{F} |0\rangle |A\rangle + \sqrt{1-F} |1\rangle |B\rangle, \\
|1\rangle & \rightarrow U |1\rangle |X\rangle = \sqrt{F} |1\rangle |C\rangle + \sqrt{1-F} |0\rangle |D\rangle,
\end{align*}
\]

where the first ket denotes the qubit sent from Alice to Bob, the second ket an ancilla that Eve can employ, and $F$ is the fidelity ($\frac{1}{2} \leq F \leq 1$) of the state which Bob holds after Eve interacted with the state sent by Alice.

Calculate the mutual information $I(A:B)$ between Alice and Bob, given the fact that Alice randomly prepares one of the states in $A$.

---

\(^1\)At this stage Alice announces the basis in which she prepared each qubit and both discard all instances where Bob measured in a different basis.

\(^2\)The action of Eve has to be same on both basis sets $A$ and $\bar{A}$, otherwise Alice and Bob could easily detect her by comparing the error rates for the two sets. Thus it is enough to consider only the basis $A$. 
Quantum Information (Exercises V)
due date: 19.01.05

1. Classical and quantum gates

(a) Universality of the NAND gate (2 P)
Show that the NAND gate, \((a, b) \rightarrow a \land b, a, b \in \{0, 1\}\), is universal on its own, provided that one is allowed to double inputs, i.e. \(a \rightarrow (a, a)\).

(b) CNOT in a rotated basis (2 P)
Show that:

\[
\begin{array}{cc}
H & H \\
\oplus & H
\end{array}
\]

2. Quantum networks

(a) Creating GHZ states with quantum networks (2 P)
Generalize the “Bell state network”

\[
\begin{array}{c}
| x \rangle \\
| y \rangle
\end{array}
\begin{array}{cc}
H & \\
\oplus &
\end{array}
\rightarrow
\begin{array}{c}
| \text{Bell} \rangle
\end{array}
\]

presented in the lecture to a network creating (and measuring) the eight \(n = 3\) qubit GHZ states

\[
| \text{GHZ}_i \rangle_\pm = \frac{1}{\sqrt{2}} (| i \rangle \pm | 2^n - 1 - i \rangle), \quad i = 0, 1, \ldots, n,
\]

where numbers in the kets on the right hand side are in binary notation.\(^3\)

(b) Universal single qubit gates (2 P)
Show that any single qubit unitary transformation can be implemented by the Hadamard gate \(H\) and the phase shift gate \(\Phi\) using the following network:

\[
\begin{array}{ccc}
H & 2\theta & H \\
& \oplus & \frac{\pi}{2} + \phi
\end{array}
\]

\(^3\) For instance, \(| \text{GHZ}_2 \rangle = 1/\sqrt{2}(|2\rangle + |5\rangle) = 1/\sqrt{2}(|010\rangle + |101\rangle).\)
(c) **The controlled-\(U\) gate (2 P)**

Write the unitary operator \(U_c = |0\rangle\langle 0| \otimes \mathbf{1} + |1\rangle\langle 1| \otimes U\), i.e.

\[
\begin{array}{c}
|x\rangle \\
|y\rangle
\end{array}
\rightarrow
\begin{array}{c}
|x\rangle U^x |y\rangle
\end{array}

as a sequence of single qubit operations and controlled-NOT gates.

(d) **The controlled global phase operation (1 P)**

Consider the operation \(f(x) = -x\) (global phase) represented by the unitary operator \(U_f = -\mathbf{1}\). Which single qubit operation does the controlled \(U_f\) gate correspond to?

\[
\begin{array}{c}
y \\
x
\end{array}
\rightarrow
\begin{array}{c}
y
\end{array}
\]

(e) **Hamiltonian for controlled-NOT gate (2 P)**

Find a Hamiltonian \(\hat{H}\) that performs the control-NOT gate

\[
U = \begin{pmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0
\end{pmatrix}
\]

\[(44)\]

(*Hint:*) Write the Hamiltonian as a sum of direct products of Pauli matrices \(\{1, \sigma_x, \sigma_y, \sigma_z\}\) and remember that \(U = e^{i\hat{H}t}\).
3. Quantum algorithms

(a) Period finding on a quantum computer (3 P)

Find the period of the function

\[ f(x) := \frac{1}{2} (\cos(\pi x) + 1), \]  

(45)

assuming \( x \) is stored in a \( n = 3 \)-qubit register, i.e.

\[ 0 \leq x < N = 2^n = 8, x \in \mathbb{N}. \]

Recipe:

- Calculate the state

\[ |\psi_0\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle. \]  

(46)

- Compute the state of the first register (left ket) for the case that a measurement on the second register (right ket) resulted in a “0”.

- Perform the Fourier transformation

\[ |x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i k x/N} |k\rangle. \]  

(47)

- The period \( r \) is given by

\[ \frac{c}{N} = \frac{\lambda}{r}, \]  

(48)

where \( c \) is the outcome of the final measurement of register 1 and \( \lambda \) is some constant such that \( \lambda/r \) is an irreducible fraction.
1. **Grover algorithm**

(a) **Oracle of the Grover algorithm for two qubits** (2 P)

The "oracle" marks the searched element \(x_s\) by minus one, i.e. it applies the transformation \(|\Psi\rangle = \sum_i (-1)^{f(x_i)} |x_i\rangle\) with \(f(x_s) = 1\) and \(f(x_i) = 0\ \forall\ x_i \neq x_s\). In case of two qubits the unitary matrix is

\[
U_{\text{oracle}} = \begin{pmatrix}
(-1)^{f(x_1)} & 0 & 0 & 0 \\
0 & (-1)^{f(x_2)} & 0 & 0 \\
0 & 0 & (-1)^{f(x_3)} & 0 \\
0 & 0 & 0 & (-1)^{f(x_4)}
\end{pmatrix}. \tag{50}
\]

Devise the four quantum circuits implementing the unitary transformation of the oracle for each search solution.

(b) **A two qubit example of the Grover algorithm** (3 P)

Calculate the unitary transformation represented by the circuit in the figure below, choosing \(x_s = 3\) for the oracle transformation. Calculate the state vector after applying this transformation to the initial state \(|\phi\rangle = |00\rangle\). To which step of the algorithm (lecture) does the part in the red box belong?

![Quantum Circuit](image)

2. **Error correction**

(a) **Classical error correction (Hamming bound)** (2 P)

Determine the upper number of possible code words with length \(k = 7\) in a Hamming code that corrects one error. Thus, is the \([7, 4, 3]\)- Hamming code introduced in the lecture a good (i.e. tightly packed) code? How many bit flips (\(\eta\)) in a codeword can maximally be corrected if a message of 3 bit length is encoded in 9 bits?
(b) QUANTUM ERROR CORRECTION (2 P)

Construct an encoding scheme to protect a single qubit against a qubit flip.

Hint: Find an analog to the classical repetition scheme.

(c) QUANTUM HAMMING BOUND (2 P)

What is the minimum code word length for a quantum Hamming code that corrects any error on one qubit?

3. Entanglement criteria

(a) REDUCTION CRITERION (2 P)

i. Prove the reduction criterion, which reads:

\[ \rho \text{ separable } \Rightarrow \rho_A \otimes 1 - \rho \geq 0 \text{ and } 1 \otimes \rho_B - \rho \geq 0, \tag{51} \]

where \( \rho_A := \text{tr}_B \rho \) and \( \rho_B := \text{tr}_A \rho \).

Hint: First show that the map \( \Lambda : B(\mathcal{H}) \rightarrow B(\mathcal{H}), \Lambda(\rho) := (\text{tr} \rho) 1 - \rho, \rho \in B(\mathcal{H}), \) maps positive operators to positive operators. Then use the fact that applying this map to one subsystem of a separable state has to lead to a positive matrix.

ii. Apply the reduction criterion to the Werner state

\[ \rho_w = \frac{1-p}{4} 1 + p |\phi^+\rangle \langle \phi^+|, \tag{52} \]

i.e. find the corresponding threshold for \( p \).

(b) MAJORISATION CRITERION (2 P)

Apply the majorisation criterion to the Werner state (eq. [52]) and find the corresponding threshold for \( p \).

---

4By saying “\( \rho \) is positive” we mean “positive semi-definite”, i.e. \( \langle \psi | \rho | \psi \rangle \geq 0, \forall | \psi \rangle. \)