UNIVERSITY OF OSLO

Faculty of mathematics and natural sciences

Exam in:	FYS3415/FYS4415 Quantum Computing and Quantum Information
Day of examination:	27 May 2026
Examination hours:	09:00 – 13:00

This examination paper consists of 9 pages.

Appendices:	Formula sheet
Permitted aids:	Approved calculator

Please make sure that your copy of the examination paper is complete before you attempt to answer anything.

Problem 1 (weight 35%)

(a) Let

$$|\phi_1\rangle = |0\rangle, \qquad |\phi_2\rangle = |+\rangle. \tag{1}$$

Compute the fidelity $F(|\phi_1\rangle, |\phi_2\rangle)$. Now send both states through the following circuit:

$$|\phi_i\rangle \text{ ——} \boxed{H} \text{—— } |\phi_i'\rangle \tag{2}$$

Here $i = 1, 2$. Find the fidelity $F(|\phi_1'\rangle, |\phi_2'\rangle)$ after the circuit.

(b) What is a qubit physically? Briefly list the main things that must be implemented in hardware to do quantum computing.

(c) Let $f : \{0,1\}^n \to \{0,1\}$ be a Boolean function, and let

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle \tag{3}$$

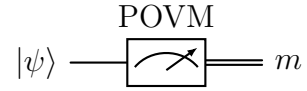
be a corresponding quantum oracle. Here $x \in \{0,1\}^n$, $y \in \{0,1\}$, and $\oplus$ denotes XOR (addition mod 2). Show that

$$U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle, \tag{4}$$

by considering the two cases $f(x) = 0$ and $f(x) = 1$. Name one quantum algorithm where oracle information is encoded into phases in this way.

(d) Explain in 2–3 sentences what it means to violate a Bell inequality and the basic idea of how such a violation can be used to certify security in device-independent quantum key distribution. Mention one assumption that is still needed in device-independent quantum key distribution.

(e) Consider a POVM measurement with two outcomes $m \in \{0, 1\}$ on a single qubit $|\psi\rangle$:



(5)

Assume that the measurement is described by two POVM operators $\{E_0, E_1\}$ such that $E_0 + E_1 = I$. You are given the measurement statistics:

$$\begin{aligned} \langle 0|E_0|0\rangle &= \frac{3}{4}, & \langle 1|E_0|1\rangle &= \frac{1}{4}, \\ \langle \phi_0|E_0|\phi_0\rangle &= \frac{3}{4}, & \langle \phi_1|E_0|\phi_1\rangle &= \frac{1}{2}, \end{aligned} \tag{6}$$

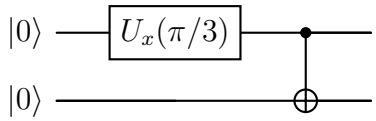
where

$$|\phi_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |\phi_1\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}}. \tag{7}$$

Determine the POVM operators E_0 and E_1.

Problem 2 (weight 35%)

Consider the following circuit:



(8)

(a) Show that the output state of the circuit is

$$|\psi_1\rangle = \frac{\sqrt{3}}{2}\,|00\rangle - \frac{i}{2}\,|11\rangle, \tag{9}$$

where the first qubit corresponds to the upper wire.

(b) Suppose both qubits in the state $|\psi_1\rangle$ are measured in the computational basis. What are the possible outcomes of the two-qubit measurement, and what is the probability of each outcome?

(c) Is $|\psi_1\rangle$ a product state or an entangled state? If it is a product state, give a decomposition. If it is entangled, explicitly show why.

(d) Calculate the reduced density matrix of the first qubit for the state $|\psi_1\rangle$. Briefly explain what measurement statistics this reduced density matrix can predict, and what kind of measurement statistics it cannot predict.

(e) Define

$$\sigma_1 = |\psi_1\rangle\langle\psi_1|, \qquad \sigma_2 = \frac{3}{4}\,|00\rangle\langle 00| + \frac{1}{4}\,|11\rangle\langle 11|. \tag{10}$$

For each of the two density operators σ_1 and σ_2, determine whether it is pure or mixed, and whether it is entangled or not entangled. Justify your answers mathematically.

(f) Does there exist a unitary circuit such that, after applying the circuit and measuring in the computational basis, there is an outcome whose probability is different for input σ_1 than for input σ_2? If so, draw such a circuit. If not, show why.

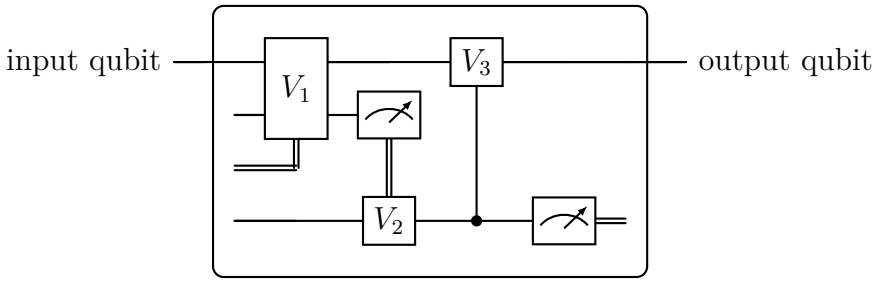
Problem 3 (weight 30%)

Alice wants to communicate with Bob by sending quantum states through some unknown black box:



(11)

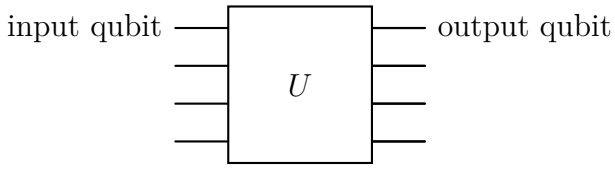
(a) Let the black box be implemented by the following quantum-classical circuit:



black box

(12)

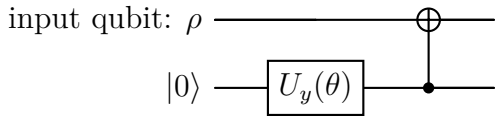
All wires other than the top input–output wire are internal to the black box and are not accessible to Alice or Bob. The internal registers are initialized in fixed states independently of the input qubit. The internal classical wire entering V_1 represents classical control of whether V_1 is applied. Explain why, as far as Alice and Bob are concerned, this circuit can be equivalently described by a single unitary operator U acting on the input qubit together with internal registers in the following way:



(13)

You may explain steps in your argument using circuit diagrams. Draw a circuit for U in terms of the quantum gates V_1, V_2, and V_3.

(b) We now consider a concrete example. Take the ancilla to be just one qubit initialized to $|0\rangle$, and take the unitary operator U to be the following two-qubit circuit:



(14)

Here $0 \leq \theta \leq \pi$. Find Kraus operators representing the induced channel from an input qubit ρ to the output qubit. Use this to show that the channel can be written as

$$\mathcal{E}(\rho) = (1-p)\rho + pX\rho X, \tag{15}$$

and determine p in terms of θ.

(c) Alice wants to communicate a uniformly random classical bit $M \in \{0, 1\}$ to Bob by sending a qubit ρ through the black box, represented by the channel $\mathcal{E}$. Suppose Alice uses the encoding $0 \mapsto |0\rangle$ and $1 \mapsto |1\rangle$. Find the state Bob receives for each sent bit M, as well as Bob's average received density operator. Use this to compute the Holevo quantity $\chi(p)$ for Bob's received states in terms of the channel parameter p. Briefly explain what the Holevo quantity says about Bob's ability to learn Alice's bit M from the transmitted quantum states.

(d) Alice now decides to transmit her classical bit M through the black box using quantum error correction. She first uses the same encoding as in part **(c)** to prepare a qubit state ρ. Then, instead of sending ρ directly, she encodes it into 3 physical qubits using the bit-flip code:

$$|0_{\mathrm{L}}\rangle = |000\rangle, \qquad |1_{\mathrm{L}}\rangle = |111\rangle. \tag{16}$$

She then sends the three physical qubits independently through the channel $\mathcal{E}$. Bob then performs the standard bit-flip-code recovery and decoding. This defines an effective logical channel $\mathcal{E}_{\mathrm{L}}(\rho)$ from Alice's qubit state ρ to Bob's decoded output state.

The probability of a single bit-flip error occurring for a physical qubit transmitted through the channel $\mathcal{E}$ is p. Therefore, the probability for getting n physical bit-flip errors for a transmitted encoded qubit is:

n	probability
0	$(1-p)^3$
1	$3p(1-p)^2$
2	$3p^2(1-p)$
3	p^3

(17)

Determine an expression for the logical channel $\mathcal{E}_{\mathrm{L}}$. Write down the Holevo quantity χ_{L} for this logical channel expressed in terms of the function $\chi(\cdot)$ from part **(c)** and the channel parameter p. Assume that the Holevo bound is tight in this case. How much obtainable classical information does this give per use of the physical channel $\mathcal{E}$?

Formula sheet

Linear algebra

Cauchy–Schwarz:

$$|\langle\phi|\psi\rangle|^2 \leq \| \, |\phi\rangle\|^2 \, \| \, |\psi\rangle\|^2$$

Triangle inequality:

$$\| \, |\psi\rangle + |\phi\rangle\| \leq \| \, |\psi\rangle\| + \| \, |\phi\rangle\|$$

Completeness:

$$I = \sum_i |i\rangle\langle i|$$

Trace:

$$\mathrm{tr}(A) = \sum_i \langle i| A \, |i\rangle$$

Partial trace:

$$\mathrm{tr}_B(\rho_{AB}) = \sum_i {}_B\langle i| \, \rho_{AB} \, |i\rangle_B$$

Spectral decomposition:

$$A = \sum_k \lambda_k \, |v_k\rangle\langle v_k|$$

Operator functions:

$$f(A) = \sum_k f(\lambda_k) \, |v_k\rangle\langle v_k|$$

Absolute value:

$$|A| = \sqrt{A^\dagger A}$$

Normal operator:

$$A^\dagger A = A A^\dagger$$

Hermitian operator:

$$H = H^\dagger$$

Unitary operator:

$$U^\dagger U = U U^\dagger = I$$

Positive operator:

$$E \geq 0 \iff \langle\psi| E \, |\psi\rangle \geq 0 \quad \forall \, |\psi\rangle$$

Projector (orthogonal):

$$P^2 = P, \quad P^\dagger = P$$

States

Z-basis (computational basis) states:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

X-basis states:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Y-basis states:

$$|+i\rangle = \frac{|0\rangle + i \, |1\rangle}{\sqrt{2}}, \quad |-i\rangle = \frac{|0\rangle - i \, |1\rangle}{\sqrt{2}}$$

Qubit pure state:

$$|\psi\rangle = \alpha \, |0\rangle + \beta \, |1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$

Bloch vector:

$$\begin{aligned} \vec{r} &= (\sin\theta\cos\phi, \, \sin\theta\sin\phi, \, \cos\theta) \\ &= \langle\psi| \, \vec{\sigma} \, |\psi\rangle, \quad \vec{\sigma} = (X, Y, Z) \end{aligned}$$

Bell states:

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$
$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

Schmidt decomposition:

$$|\psi\rangle_{AB} = \sum_k \sqrt{\lambda_k} \, |u_k\rangle_A \, |v_k\rangle_B,$$
$$\lambda_k \geq 0, \quad \sum_k \lambda_k = 1$$

Density operators

Density operator:

$$\rho = \rho^\dagger, \quad \rho \geq 0, \quad \mathrm{tr}(\rho) = 1$$

Ensemble:

$$\rho = \sum_k p_k \, |\psi_k\rangle\langle\psi_k|,$$
$$p_k \geq 0, \quad \sum_k p_k = 1$$

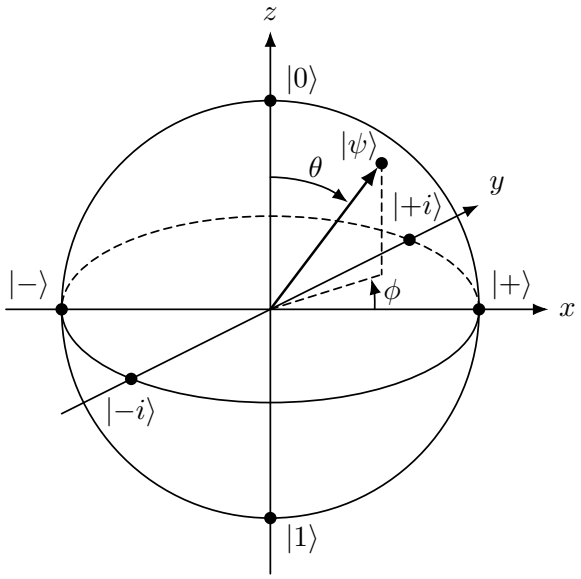
Bloch vector:

$$\vec{r} = (r\sin\theta\cos\phi,\, r\sin\theta\sin\phi,\, r\cos\theta)$$
$$= \mathrm{tr}(\rho\,\vec{\sigma}), \quad \vec{\sigma} = (X, Y, Z)$$

Purification:

$$\rho_A = \sum_k \lambda_k \, |v_k\rangle\langle v_k|$$
$$\implies |\psi\rangle_{AR} = \sum_k \sqrt{\lambda_k}\, |v_k\rangle_A \, |k\rangle_R$$

Bloch sphere



Sine and cosine values

θ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$
$\sin\theta$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\cos\theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0

Single-qubit gates

Matrix representations are in the computational basis.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathrm{NOT} = X = \sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z = \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$S = \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$T = \sqrt{S} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$P(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$$

$$U_{\hat{n}}(\varphi) = e^{-i\frac{\varphi}{2}(\hat{n}\cdot\vec{\sigma})} = \cos\frac{\varphi}{2}\, I - i\sin\frac{\varphi}{2}\hat{n}\cdot\vec{\sigma}$$

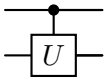
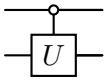
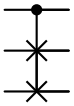
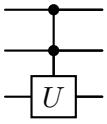
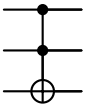
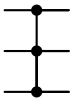
$$U_x(\varphi) = e^{-i\frac{\varphi}{2}X} = \cos\frac{\varphi}{2}\, I - i\sin\frac{\varphi}{2}\, X$$
$$= \begin{pmatrix} \cos\frac{\varphi}{2} & -i\sin\frac{\varphi}{2} \\ -i\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{pmatrix}$$

$$U_y(\varphi) = e^{-i\frac{\varphi}{2}Y} = \cos\frac{\varphi}{2}\, I - i\sin\frac{\varphi}{2}\, Y$$
$$= \begin{pmatrix} \cos\frac{\varphi}{2} & -\sin\frac{\varphi}{2} \\ \sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{pmatrix}$$

$$U_z(\varphi) = e^{-i\frac{\varphi}{2}Z} = \cos\frac{\varphi}{2}\, I - i\sin\frac{\varphi}{2}\, Z$$
$$= \begin{pmatrix} e^{-i\frac{\varphi}{2}} & 0 \\ 0 & e^{i\frac{\varphi}{2}} \end{pmatrix}$$

Multi-qubit gates

In the expressions below, tensor factors from left to right correspond to wires from top to bottom.

Gate	Circuit	Expression
CU		$\|0\rangle\langle 0\| \otimes I_2 + \|1\rangle\langle 1\| \otimes U$
Anti-CU		$\|0\rangle\langle 0\| \otimes U + \|1\rangle\langle 1\| \otimes I_2$
CNOT = CX		$\|0\rangle\langle 0\| \otimes I_2 + \|1\rangle\langle 1\| \otimes X$
CZ		$\|0\rangle\langle 0\| \otimes I_2 + \|1\rangle\langle 1\| \otimes Z$
SWAP		$\sum_{x,y\in\{0,1\}} \|x\,y\rangle\langle y\,x\|$
Fredkin = CSWAP		$\|0\rangle\langle 0\| \otimes I_4 + \|1\rangle\langle 1\| \otimes \mathrm{SWAP}$
CCU		$(I_4 - \|11\rangle\langle 11\|) \otimes I_2 + \|11\rangle\langle 11\| \otimes U$
Toffoli = CCNOT = CCX		$(I_4 - \|11\rangle\langle 11\|) \otimes I_2 + \|11\rangle\langle 11\| \otimes X$
CCZ		$(I_4 - \|11\rangle\langle 11\|) \otimes I_2 + \|11\rangle\langle 11\| \otimes Z$

Pauli algebra

$$\sigma_i\sigma_j = \delta_{ij}I + i\sum_{k=1}^{3}\epsilon_{ijk}\sigma_k$$

$$[\sigma_i, \sigma_j] = 2i\sum_{k=1}^{3}\epsilon_{ijk}\sigma_k$$

$$\{\sigma_i, \sigma_j\} = 2\delta_{ij}I$$

$$\delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$$

$$\epsilon_{ijk} = \begin{cases} +1, & ijk \text{ even perm. of } 123 \\ -1, & ijk \text{ odd perm. of } 123 \\ 0, & \text{otherwise} \end{cases}$$

Quantum channels

Definition:

$$\mathcal{E}(\rho) = \mathrm{tr}_E\Big[U(\rho \otimes |0\rangle\langle 0|_E)U^\dagger\Big]$$

Operator-sum form:

$$\mathcal{E}(\rho) = \sum_k M_k\rho M_k^\dagger, \quad \sum_k M_k^\dagger M_k = I$$

Kraus operators / operation elements:

$$M_k = {}_E\langle k|\,U\,|0\rangle_E$$

Projective measurements: $\{P_m\}$

Definition:

$$\sum_m P_m = I,$$
$$P_m = P_m^\dagger,$$
$$P_m P_n = \delta_{mn} P_m$$

Probability:

$$p(m) = \mathrm{tr}(P_m \rho)$$

State update:

$$\rho \mapsto \frac{P_m \rho P_m}{\mathrm{tr}(P_m \rho)}$$

Observable:

$$A = \sum_a a P_a$$

Expectation value:

$$\langle A \rangle_\rho = \mathrm{tr}(A\rho)$$

General measurements: $\{M_m\}$

Definition:

$$\sum_m M_m^\dagger M_m = I$$

Probability:

$$p(m) = \mathrm{tr}\Big(M_m \rho M_m^\dagger\Big)$$

State update:

$$\rho \mapsto \frac{M_m \rho M_m^\dagger}{\mathrm{tr}\Big(M_m \rho M_m^\dagger\Big)}$$

POVM measurements: $\{E_m\}$

Definition:

$$\sum_m E_m = I,$$
$$E_m \geq 0$$

Probability:

$$p(m) = \mathrm{tr}(E_m \rho)$$

State discrimination

Trace distance:

$$D(\rho, \sigma) = \frac{1}{2} \mathrm{tr}\,|\rho - \sigma|$$

Trace distance for pure states:

$$D(|\psi\rangle, |\phi\rangle) = \sqrt{1 - |\langle\psi|\phi\rangle|^2}$$

Trace distance operational:

$$D(\rho, \sigma) = \max_{0 \leq E \leq I} |\mathrm{tr}(E\rho) - \mathrm{tr}(E\sigma)|$$

Triangle inequality:

$$D(\rho, \tau) \leq D(\rho, \sigma) + D(\sigma, \tau)$$

Joint convexity of trace distance:

$$D\left(\sum_x p_x \rho_x, \sum_x p_x \sigma_x\right) \leq \sum_x p_x D(\rho_x, \sigma_x)$$

Fidelity:

$$F(\rho, \sigma) = \mathrm{tr}\sqrt{\sqrt{\rho}\,\sigma\sqrt{\rho}}$$

Fidelity for pure states:

$$F(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|$$

Fidelity with one pure state:

$$F(|\psi\rangle, \sigma) = \sqrt{\langle\psi|\,\sigma\,|\psi\rangle}$$

Uhlmann's theorem:

$$F(\rho_A, \sigma_A) = \max_{\substack{|\psi_\rho\rangle_{AR}, |\phi_\sigma\rangle_{AR} \\ \text{purifications}}} |\langle\psi_\rho|\phi_\sigma\rangle|$$

Joint concavity of fidelity:

$$F\left(\sum_x p_x \rho_x, \sum_x p_x \sigma_x\right) \geq \sum_x p_x F(\rho_x, \sigma_x)$$

Relations:

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F(\rho, \sigma)^2}$$

$$D(|\psi\rangle, |\phi\rangle) = \sqrt{1 - F(|\psi\rangle, |\phi\rangle)^2}$$

Error correction

Probability of getting exactly n errors among N independent trials with error probability p:

$$\Pr(n) = \binom{N}{n} p^n (1-p)^{N-n},$$
$$\binom{N}{n} = \frac{N!}{n!\,(N-n)!}$$

Bit-flip code encoding:

$$|0_\mathrm{L}\rangle = |000\rangle, \quad |1_\mathrm{L}\rangle = |111\rangle$$

Phase-flip code encoding:

$$|0_\mathrm{L}\rangle = |+++\rangle, \quad |1_\mathrm{L}\rangle = |---\rangle$$

Shor code encoding:

$$|0_\mathrm{L}\rangle = \frac{(|000\rangle + |111\rangle)^{\otimes 3}}{2\sqrt{2}},$$
$$|1_\mathrm{L}\rangle = \frac{(|000\rangle - |111\rangle)^{\otimes 3}}{2\sqrt{2}}$$

Classical entropy

Convention: $0 \log 0 = 0$.

Binary entropy:

$$h_\mathrm{b}(p) = -p \log_2 p - (1-p) \log_2 (1-p)$$

Shannon entropy:

$$H(X) = -\sum_x p(x) \log_2 p(x)$$

Joint entropy:

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

Conditional entropy:

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

Mutual information:

$$I(X:Y) = H(X) + H(Y) - H(X,Y)$$

Relative entropy:

$$H(p\|q) = \sum_x p(x) \log_2 \frac{p(x)}{q(x)}$$

Quantum entropy

Von Neumann entropy:

$$S(\rho) = -\operatorname{tr}(\rho \log_2 \rho)$$

Joint entropy:

$$S(A,B) = S(\rho_{AB})$$

Conditional entropy:

$$S(A|B) = S(A,B) - S(B)$$

Mutual information:

$$I(A:B) = S(A) + S(B) - S(A,B)$$

Relative entropy:

$$S(\rho\|\sigma) = \operatorname{tr}(\rho \log_2 \rho) - \operatorname{tr}(\rho \log_2 \sigma)$$

Holevo quantity:

$$\chi = S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S(\rho_x)$$

Holevo bound:

$$I(X:Y) \leq \chi$$

Bell tests

Correlator:

$$E(x,y) = \sum_{a,b=\pm 1} ab\, p(a,b|x,y)$$

CHSH parameter:

$$S = E(0,0) + E(0,1) + E(1,0) - E(1,1)$$

Local hidden-variable theory:

$$|S| \leq 2$$