Trial exam

Course: FYS3415/FYS4415
Quantum Computing and Quantum Information

This examination paper consists of 9 pages.

Appendices: Formula sheet

Permitted aids: Approved calculator

Problem 1 (weight 35%)

(a) Let

$$\rho = |0\rangle\langle 0|, \qquad \sigma = |\psi\rangle\langle\psi|, \qquad |\psi\rangle = \frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle.$$

Compute the fidelity $F(\rho, \sigma)$ and the trace distance $D(\rho, \sigma)$.

(b) For each of the following two-qubit states, decide whether it is pure or mixed, and whether it is a product state, separable but not product, or entangled:

$$\rho_1 = |0+\rangle\langle 0+|,$$
$$\rho_2 = |\Phi^+\rangle\langle\Phi^+|,$$
$$\rho_3 = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|,$$

where $|\Phi^+\rangle$ is the Bell state. Justify your answers mathematically.

(c) Consider the two measurement operators

$$M_0 = |0\rangle\langle 0| + \frac{1}{\sqrt{2}}|1\rangle\langle 1|, \qquad M_1 = \frac{1}{\sqrt{2}}|1\rangle\langle 1|.$$

Show that these define a valid measurement. Find the POVM elements corresponding to this measurement and compute the outcome probabilities for the input state $|+\rangle$. Find the post-measurement state corresponding to each outcome.

(d) Consider the three-qubit bit-flip code

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

The error syndrome is measured using the two observables

$$Z_1Z_2, \qquad Z_2Z_3.$$

Consider an arbitrary qubit state

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

Write down the corresponding encoded qubit state $|\psi_{\mathrm{L}}\rangle$. List the syndrome outcomes for the no-error case and the three possible single bit-flip errors, and state the corresponding correction in each case. Briefly explain why the syndrome measurement identifies the error without measuring the logical information α and β.

(e) Consider the Bell state $|\Phi^+\rangle$, and define observables

$$A_\theta = \cos\theta\, Z + \sin\theta\, X.$$

First show that

$$\langle\Phi^+|A_\theta \otimes A_\phi\,|\Phi^+\rangle = \cos(\theta-\phi).$$

You may use that

$$\cos\theta\cos\phi + \sin\theta\sin\phi = \cos(\theta-\phi).$$

Then compute the CHSH quantity

$$S = E(a,b) + E(a,b') + E(a',b) - E(a',b'),$$

for

$$a = 0, \qquad a' = \frac{\pi}{2}, \qquad b = \frac{\pi}{4}, \qquad b' = -\frac{\pi}{4},$$

where

$$E(\theta,\phi) = \langle\Phi^+|A_\theta \otimes A_\phi\,|\Phi^+\rangle.$$

Does this violate the local-hidden-variable bound for S?

(f) Alice chooses a classical bit $X \in \{0,1\}$ uniformly at random. If $X = 0$, she prepares $|0\rangle$. If $X = 1$, she prepares $|+\rangle$. Let Bob receive the state. Compute the classical entropy $H(X)$, as well as the Holevo quantity χ for Bob's received ensemble. Compare χ with $H(X)$, and briefly explain the result.

Problem 2 (weight 30%)

Alice sends one of the four BB84 states

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

with probability 1/4 each. The basis $\{|0\rangle,|1\rangle\}$ is called the Z-basis, and the basis $\{|+\rangle,|-\rangle\}$ is called the X-basis. Let S denote the sent qubit. An environment qubit E starts in $|0\rangle_E$, and the joint system undergoes the unitary

$$U = |0\rangle\langle 0|_S \otimes I_E + |1\rangle\langle 1|_S \otimes R_E, \tag{1}$$

where

$$R_E = \begin{pmatrix} \frac{4}{5} & -\frac{3}{5} \\ \frac{3}{5} & \frac{4}{5} \end{pmatrix}.$$

Bob receives only qubit S, meaning that from Bob's perspective, the environment E is discarded, defining a quantum channel $\mathcal{E}$ from Alice to Bob. When Alice and Bob use the same basis, we count it as an error if Bob obtains the opposite outcome from the state Alice sent.

(a) Find Kraus operators for the channel $\mathcal{E}$. Use this to show that the channel can be written as

$$\mathcal{E}(\rho) = \frac{9}{10}\rho + \frac{1}{10}Z\rho Z.$$

(b) Show that if Alice sends a Z-basis state and Bob measures in the Z-basis, the error probability is

$$p_{\text{err},Z} = 0.$$

(c) If Alice sends an X-basis state and Bob measures in the X-basis, what is the error probability $p_{\text{err},X}$?

(d) Suppose Alice and Bob run a BB84 protocol through this channel. However, suppose they keep only the rounds where Alice sent a Z-basis state and Bob measured in the Z-basis as their sifted raw key. They test a subset of these rounds and observe no errors. Assuming that a possible eavesdropper has access to the environment E, can they conclude that Eve has no information about the remaining sifted raw key (the part not used for error testing)? Explain.

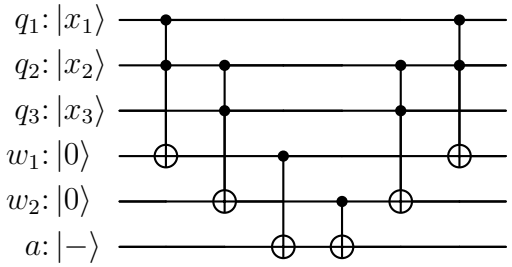
(e) Suppose now that Alice and Bob run the usual BB84 protocol, keeping all rounds where they both picked the same basis, either Z or X, as their sifted raw key. After sifting, they estimate the relevant error rates from test rounds and then apply error correction and privacy amplification. Assume that the parameter-estimation test accepts. Is this a device-independent security argument? Explain.

Problem 3 (weight 35%)

Grover's algorithm searches for certain bit strings using a phase oracle

$$O_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle, \tag{2}$$

where $f(x)$ is a Boolean function with $f(x) = 1$ for solution strings and $f(x) = 0$ for all other bit strings. Here we let $x = x_1\,x_2\,x_3$ be a three-bit string. Consider the following implementation of a Grover phase oracle on three query qubits, two work qubits, and one ancilla qubit:

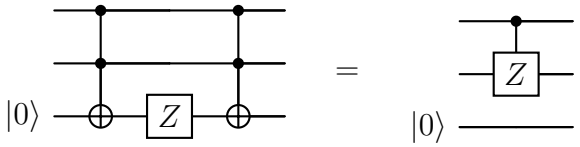


(3)

(a) Determine the Boolean function $f(x_1, x_2, x_3)$ implemented by this oracle, and list the computational-basis states that are solutions. Why is the ancilla qubit initialized in $|-\rangle$ rather than in $|0\rangle$ when this circuit is used as a Grover oracle?

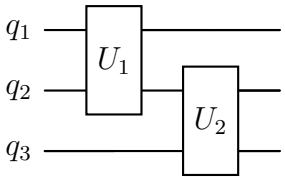
(b) Grover's algorithm proceeds iteratively, where one Grover iteration consists of applying the oracle and a diffusion operator. Describe qualitatively how the probability of measuring a solution state behaves as the number of Grover iterations increases, and explain what this implies for choosing the number of iterations before measuring.

(c) Show that the following circuit identity holds when the bottom qubit is initialized to $|0\rangle$ and the first two qubits are arbitrary:



(4)

(d) Simplify the oracle circuit (3) to a circuit of the form:



(5)

Determine U_1 and U_2. To do this, first analyze how a CNOT acts when its target is $|-\rangle$, and replace each such CNOT by a one-qubit gate on its control. Then use (4) and gate commuting.

(e) Why is the final oracle circuit (5) preferable for real hardware compared with the original circuit (3)? Give at least two reasons.

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:

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

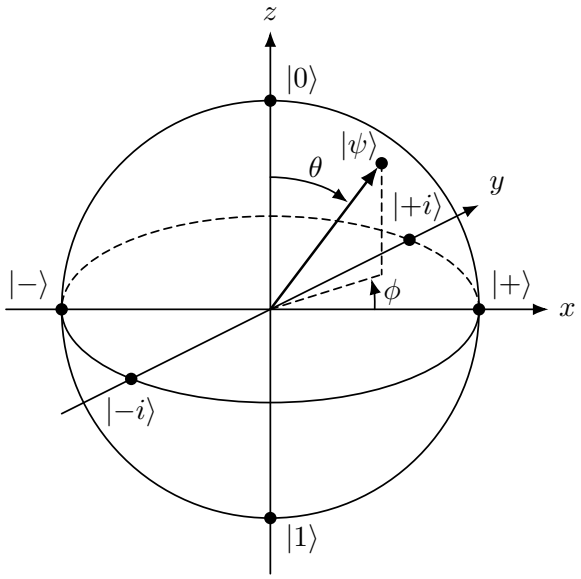
Bloch vector:

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

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.

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

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

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

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

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

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

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

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

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

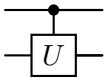
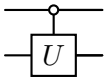
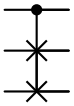
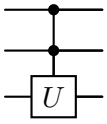
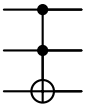
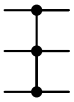
$$U_x(\varphi) = e^{-i\frac{\varphi}{2}X} = \cos\frac{\varphi}{2}\, I - i\sin\frac{\varphi}{2}\, X$$
$$= \begin{pmatrix} \cos\frac{\varphi}{2} & -i\sin\frac{\varphi}{2} \\ -i\sin\frac{\varphi}{2} & \cos\frac{\varphi}{2} \end{pmatrix}$$

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

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

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:

$$|S| \leq 2$$