University of Oslo

FYS3415/FYS4415 — Quantum computing and quantum information

Problem set 13

This problem set will be discussed on **May 13**.

Problem 1: The CHSH inequality

A singlet state can be used to violate a Bell-type inequality, exhibiting correlations stronger than any local hidden-variable (LHV) model can produce. As discussed in the lectures, for ± 1-valued observables A_0, A_1 on Alice's qubit and B_0, B_1 on Bob's qubit, the *CHSH parameter*

$$S_\rho \;\equiv\; \langle A_0 \otimes B_0 \rangle_\rho + \langle A_1 \otimes B_0 \rangle_\rho + \langle A_1 \otimes B_1 \rangle_\rho - \langle A_0 \otimes B_1 \rangle_\rho$$

satisfies the LHV bound

$$|S_{\text{LHV}}| \leq 2.$$

The singlet achieves $S_{\psi^-} = 2\sqrt{2}$ for a suitable choice of the observables.

In this problem you will investigate how much depolarizing noise a singlet can tolerate before this CHSH test no longer witnesses Bell nonlocality.

a) CHSH violation under noise.

Real quantum channels are noisy. Suppose the singlet $|\psi^-\rangle$ is sent through a global depolarizing channel, resulting in the *Werner state*

$$\rho_p \;=\; (1-p)\,|\psi^-\rangle\langle\psi^-| + p\frac{I}{4},$$

where $p \in [0,1]$ parametrises the depolarizing noise fraction ($p = 0$ is noiseless). Suppose Alice and Bob measure observables A_0, A_1, B_0, B_1 that maximise the CHSH parameter violation for the singlet, and suppose these observables are traceless. With the notation from above,

$$S_{\psi^-} = 2\sqrt{2}.$$

Calculate the CHSH parameter S_{ρ_p} for the Werner state. For which values of p does the state violate the classical CHSH bound?

Solution: Let the CHSH operator for the chosen measurement settings be

$$\mathcal{B} \;=\; A_0 \otimes B_0 + A_1 \otimes B_0 + A_1 \otimes B_1 - A_0 \otimes B_1,$$

so that

$$S_\rho = \text{Tr}(\rho\,\mathcal{B}).$$

Since the chosen observables are traceless qubit observables, we have

$$\text{Tr}(A_i \otimes B_j) = \text{Tr}(A_i)\,\text{Tr}(B_j) = 0$$

for all i, j. Hence each tensor-product term in $\mathcal{B}$ is traceless, and therefore

$$\text{Tr}(\mathcal{B}) = 0.$$

The maximally mixed part of the Werner state therefore contributes nothing:

$$S_{I/4} = \text{Tr}\left(\frac{I}{4}\mathcal{B}\right) = \frac{1}{4}\,\text{Tr}(\mathcal{B}) = 0.$$

By linearity of the trace,

$$\begin{aligned} S_{\rho_p} &= \mathrm{Tr}(\rho_p \mathcal{B}) \\ &= (1-p)\ \mathrm{Tr}\big(|\psi^-\rangle\langle\psi^-|\mathcal{B}\big) + p\ \mathrm{Tr}\left(\frac{I}{4}\mathcal{B}\right) \\ &= (1-p)S_{\psi^-} + pS_{I/4} \\ &= 2\sqrt{2}\,(1-p). \end{aligned}$$

To violate the classical CHSH bound, we require

$$|S_{\rho_p}| > 2.$$

For the chosen sign convention $S_{\rho_p} = 2\sqrt{2}\,(1-p) \geq 0$, so this becomes

$$2\sqrt{2}\,(1-p) > 2 \quad \Longleftrightarrow \quad 1-p > \frac{1}{\sqrt{2}} \quad \Longleftrightarrow \quad p < 1 - \frac{1}{\sqrt{2}} \approx 0.293.$$

Thus, this CHSH test witnesses Bell nonlocality exactly when

$$p < 1 - \frac{1}{\sqrt{2}}.$$

Problem 2: The BB84 protocol

The Bennett–Brassard 1984 (BB84) protocol is the original quantum key distribution scheme. Alice and Bob wish to share a secret bit string in the presence of an eavesdropper Eve who controls the quantum channel between them. They also have an authenticated public classical channel: Eve may listen to the public discussion, but cannot undetectably modify it. The protocol exploits the fact that non-orthogonal quantum states cannot be perfectly distinguished, so any attempt by Eve to read the transmitted states without additional side information necessarily disturbs them and is revealed by an increased error rate.

The protocol runs as follows.

- **Transmission.** For each of N rounds, Alice picks a uniformly random key bit $k \in \{0,1\}$ and a uniformly random basis $a \in \{Z, X\}$. She prepares and transmits the qubit

$$|\psi_{k,a}\rangle = \begin{cases} |k\rangle & \text{if } a = Z, \\ H\,|k\rangle & \text{if } a = X, \end{cases}$$

  i.e. one of the four BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Bob picks his own uniformly random basis $b \in \{Z, X\}$ and measures the received qubit in that basis, obtaining outcome $r \in \{0,1\}$. In the X basis we label the outcomes by $r = 0$ for $|+\rangle$ and $r = 1$ for $|-\rangle$.

- **Sifting.** Alice and Bob publicly compare a and b, keeping only rounds where $a = b$.

- **Parameter estimation.** They publicly compare a random sample of the surviving bits to estimate the bit error rate (QBER). If it exceeds a protocol-specific threshold, they abort.

- **Information reconciliation and privacy amplification.** The remaining unrevealed sifted bits are corrected for residual errors and then compressed to a final shared key about which Eve's information is negligible.

This problem analyses the protocol in four steps: (a) the noiseless, no-eavesdropper case; (b) an explicit attack on the channel and the resulting QBER; (c) a side-channel attack that exposes the trust assumptions on Alice's and Bob's hardware; and (d) the device-independent viewpoint.

a) Sifting and basis matching.

Assume the channel is noiseless and there is no eavesdropper. Alice transmits a single qubit prepared in $|\psi_{k,a}\rangle$ and Bob measures in basis b.

i) Show that $P(a = b) = 1/2$, so on average half of the rounds survive sifting.

ii) Show that conditional on $a = b$ (matched bases), Bob's outcome equals Alice's key bit deterministically:

$$P(r = k \mid a = b) = 1.$$

iii) Show that conditional on $a \neq b$ (mismatched bases), Bob's outcome is uniformly random and uncorrelated with Alice's key bit:

$$P(r = k \mid a \neq b) = 1/2.$$

This justifies discarding the mismatched-basis rounds.

Solution: i) The four basis pairs $(a, b) \in \{Z, X\}^2$ are equally likely, and exactly two of them, (Z, Z) and (X, X), match. Hence

$$P(a = b) = \frac{2}{4} = \frac{1}{2}.$$

ii) Take $a = b = Z$. Alice sends $|k\rangle \in \{|0\rangle, |1\rangle\}$ and Bob measures in the computational basis. The Born rule gives

$$P(r = k) = |\langle k|k\rangle|^2 = 1.$$

The case $a = b = X$ is identical with $|0\rangle, |1\rangle$ replaced by $|+\rangle, |-\rangle$, which are orthonormal in the X basis.

iii) Take $a = Z$, $b = X$. Alice sends $|k\rangle \in \{|0\rangle, |1\rangle\}$ and Bob projects onto $\{|+\rangle, |-\rangle\}$. All four overlaps are equal in magnitude:

$$|\langle +|0\rangle|^2 = |\langle -|0\rangle|^2 = |\langle +|1\rangle|^2 = |\langle -|1\rangle|^2 = \frac{1}{2}.$$

Thus Bob's outcome is uniformly random and independent of k. The case $a = X$, $b = Z$ is symmetric. The mismatched-basis rounds therefore contain no usable Alice–Bob correlation about the key bit, and discarding them costs nothing in usable correlation.

b) The entangling probe attack.

Instead of directly measuring the qubit, Eve can perform a more sophisticated attack by interacting the transmitted qubit with her own ancilla system E. Suppose she initializes her ancilla in $|0\rangle_E$ and applies a unitary U whose action on the relevant input states is

$$U|0\rangle|0\rangle_E = |0\rangle \otimes \big(\cos\theta\,|0\rangle_E + \sin\theta\,|1\rangle_E\big),$$
$$U|1\rangle|0\rangle_E = |1\rangle \otimes \big(\cos\theta\,|0\rangle_E - \sin\theta\,|1\rangle_E\big),$$

for some parameter $\theta \in [0, \pi/4]$ controlling the attack strength. Eve then forwards the qubit to Bob and keeps her ancilla to measure later.

i) Show that if Alice sends states in the Z basis, the qubit is not disturbed, so Bob observes a bit error rate $\mathrm{QBER}_Z = 0$ in the Z-basis sifted rounds.

ii) Now consider an X-basis sifted round. Suppose Alice sends the state

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Calculate the joint state of the qubit and Eve's ancilla after U. If Bob also measures in the X basis, what is the probability he obtains the wrong outcome $|-\rangle$? This probability is the contribution to the X-basis error rate QBER_X. By symmetry, the same error probability is obtained when Alice sends $|-\rangle$.

iii) For the rest of this subproblem, use the following convention: the raw key is extracted from the Z-basis sifted rounds, while the X-basis sifted rounds are test rounds used to estimate the disturbance. We want to compute the Holevo quantity $\chi(K:E)$, since it upper bounds the classical information Eve can obtain about a Z-basis key bit by measuring her ancilla. In this case, we can calculate it by considering the following classical–quantum state

$$\rho_{KE} = \frac{1}{2}\big(|0\rangle\langle 0|_K \otimes |e_0\rangle\langle e_0|_E + |1\rangle\langle 1|_K \otimes |e_1\rangle\langle e_1|_E\big),$$

where

$$|e_0\rangle = \cos\theta\,|0\rangle_E + \sin\theta\,|1\rangle_E, \qquad |e_1\rangle = \cos\theta\,|0\rangle_E - \sin\theta\,|1\rangle_E.$$

Find Eve's reduced state ρ_E, determine its eigenvalues, and calculate the Holevo quantity using the following formula:

$$\chi(K:E) = I_{\mathrm{q}}(K:E) = S(\rho_K) + S(\rho_E) - S(\rho_{KE}).$$

Express your answer in terms of the binary entropy

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

iv) Using the basis-dependent error rates QBER_Z from part i) and QBER_X from part ii), compute the overall average QBER over the sifted rounds when Z and X bases are chosen with equal probability. How does this attack allow Eve to tune her eavesdropping strategy compared to the simple random-basis intercept-resend attack?

Solution: i) If Alice prepares $|k\rangle$ for $k \in \{0,1\}$, Eve's unitary maps the joint state to

$$|k\rangle\,|e_k\rangle,$$

where $|e_k\rangle$ is a normalized state of Eve's ancilla. Tracing out Eve's system, the reduced state of the transmitted qubit is perfectly unchanged:

$$\rho_{\mathrm{qubit}} = |k\rangle\langle k|.$$

Thus, when Bob measures in the Z basis, he recovers $r = k$ with probability 1, resulting in

$$\mathrm{QBER}_Z = 0.$$

ii) If Alice sends $|+\rangle$, the initial state is

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle_E.$$

Applying U gives

$$\begin{aligned}|\Psi\rangle &= \frac{1}{\sqrt{2}}\Big(|0\rangle\big(\cos\theta\,|0\rangle_E + \sin\theta\,|1\rangle_E\big) + |1\rangle\big(\cos\theta\,|0\rangle_E - \sin\theta\,|1\rangle_E\big)\Big)\\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\cos\theta\,|0\rangle_E + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\sin\theta\,|1\rangle_E\\ &= \cos\theta\,|+\rangle\,|0\rangle_E + \sin\theta\,|-\rangle\,|1\rangle_E.\end{aligned}$$

When Bob measures in the X basis, the probability he obtains $|-\rangle$ is the weight of the $|-\rangle$ component, namely

$$\sin^2\theta.$$

Since the correct outcome is $|+\rangle$, this is the error probability for this X-basis sifted round.

By symmetry, if Alice sends $|-\rangle$, the wrong X-basis outcome is $|+\rangle$, again with probability $\sin^2\theta$. Therefore

$$\mathrm{QBER}_X = \sin^2\theta.$$

iii) For the classical-quantum state ρ_{KE}, the reduced state of Alice's key register is the completely mixed state $I/2$, so

$$S(\rho_K) = 1.$$

Because the states $|0\rangle_K$ and $|1\rangle_K$ are orthogonal and the conditional states $|e_0\rangle_E$ and $|e_1\rangle_E$ are pure, the joint entropy is

$$S(\rho_{KE}) = H(1/2, 1/2) = 1.$$

Thus the mutual information simplifies to

$$I(K:E) = S(\rho_E).$$

Eve's reduced state is

$$\begin{aligned}\rho_E &= \frac{1}{2}\big(|e_0\rangle\langle e_0|_E + |e_1\rangle\langle e_1|_E\big)\\ &= \frac{1}{2}\begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}\begin{pmatrix}\cos\theta & \sin\theta\end{pmatrix} + \frac{1}{2}\begin{pmatrix}\cos\theta\\ -\sin\theta\end{pmatrix}\begin{pmatrix}\cos\theta & -\sin\theta\end{pmatrix}\\ &= \begin{pmatrix}\cos^2\theta & 0\\ 0 & \sin^2\theta\end{pmatrix}.\end{aligned}$$

The eigenvalues are $\cos^2\theta$ and $\sin^2\theta$, so

$$I(K:E) = \chi(K:E) = h_{\mathrm{b}}(\sin^2\theta).$$

This quantity is the Holevo information about a Z-basis key bit, and upper bounds Eve's accessible classical information about that bit. On the chosen interval $\theta \in [0, \pi/4]$, it increases from 0 to 1. At $\theta = \pi/4$, the states $|e_0\rangle$ and $|e_1\rangle$ are orthogonal, so Eve can in principle distinguish them perfectly.

iv) From parts i) and ii), the basis-dependent error rates are

$$\mathrm{QBER}_Z = 0, \qquad \mathrm{QBER}_X = \sin^2\theta.$$

Thus the Z-basis key rounds have no bit errors, while the X-basis test rounds reveal the disturbance caused by Eve's attack.

If Alice and Bob choose the two bases with equal probability and combine all sifted rounds into a single average error rate, then

$$\mathrm{QBER}_{\mathrm{avg}} = \frac{1}{2}\mathrm{QBER}_Z + \frac{1}{2}\mathrm{QBER}_X = \frac{1}{2}\sin^2\theta.$$

This average is only a single-number summary of the basis-dependent disturbance; in this subproblem, the raw key itself comes from the Z-basis rounds.

This attack lets Eve continuously tune the trade-off between the Holevo upper bound on her information about Z-basis raw key bits,

$$\chi(K:E) = h_{\mathrm{b}}(\sin^2\theta),$$

and the disturbance she induces in the X-basis test rounds,

$$\mathrm{QBER}_X = \sin^2\theta.$$

Equivalently, if one reports a single average over equally likely sifted Z- and X-basis rounds, the average disturbance is

$$\mathrm{QBER}_{\mathrm{avg}} = \frac{1}{2}\sin^2\theta.$$

This is more flexible than the canonical full random-basis intercept-resend attack, which produces a characteristic average QBER of 25% when applied to all signals, although intercept-resend can also be weakened by applying it only to a subset of signals. The present attack is basis-asymmetric:

$$\mathrm{QBER}_Z = 0, \qquad \mathrm{QBER}_X = \sin^2\theta.$$

Thus, if Alice and Bob only checked one averaged QBER without analyzing the bases separately, they might underestimate the basis-dependent nature of the attack. A careful BB84 implementation estimates the relevant error rates well enough to bound Eve's information before privacy amplification.

c) The trust assumption.

The argument in part b) silently *trusted* Alice's and Bob's devices. Alice's source must actually emit the four BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and Bob's measurement device must implement true projective measurements in the Z and X bases. In real implementations these are non-trivial assumptions: physical sources can produce preparation-dependent fingerprints, such as timing, wavelength, or mean photon number, that a sufficiently clever Eve can exploit.

Suppose Alice's source is faulty and, on each round, leaks a copy of the basis label a to Eve through a hidden side channel before Eve has to choose how to interact with the travelling qubit. Eve still controls the quantum channel between Alice and Bob, and uses this leaked side-channel information to choose her attack on each round. What QBER do Alice and Bob now estimate from their sample, and how much information does Eve hold about the final key? Explain in 3–5 sentences why the analysis of part b) does not detect this attack.

Solution: If Eve learns the basis a before choosing her measurement, then the two possible signals in that basis are orthogonal. She can intercept the travelling qubit, measure it in basis a, learn the key bit k perfectly, and resend the same BB84 state $|\psi_{k,a}\rangle$ to Bob. Because Bob receives exactly the state Alice intended, all sifted rounds satisfy $r = k$, so the estimated QBER

is

$$\mathrm{QBER} = 0.$$

Nevertheless, Eve knows every sifted raw key bit; if Alice and Bob fail to account for this side channel and still extract a nonzero key, Eve can compute the final key as well, since the reconciliation and privacy-amplification procedures are public. A correct security analysis would treat Eve as knowing the entire sifted raw key and would therefore extract no secret key from these data. The analysis of part b) assumes that Eve's only information comes from her interaction with the intended quantum signal; once the source leaks a, the four BB84 states split into two known orthogonal pairs, which Eve can measure without causing the usual wrong-basis disturbance.

d) Device independence.

(i) Explain briefly why standard BB84 is not device-independent.

(ii) Explain what device-independent QKD is, and how a Bell inequality violation can be used to certify security.

(iii) Mention assumptions that are still needed in device-independent QKD.

Solution:

(i) Standard BB84 is not device-independent because its security proof assumes that Alice's source really prepares the intended BB84 states, and that Bob's measurement device really performs the intended measurements, such as the Z- and X-basis measurements. Thus, the security relies partly on a model of the devices and not only on the observed data.

(ii) Device-independent QKD aims to certify security from the observed input-output statistics of Alice's and Bob's devices, without needing to know the internal workings of the signal source or measurement devices. A Bell inequality violation, for example observing a CHSH parameter with $|S| > 2$, means that the observed correlations cannot be explained by any local hidden-variable model. Such a violation certifies that Alice and Bob share nonclassical correlations, which can be used to bound how much information Eve can have about their measurement outcomes.

(iii) Some assumptions are still needed. For example, Alice's and Bob's labs must be secure, so that the devices do not leak the key to Eve, and the devices must not be able to communicate during the measurement rounds, for instance because the labs are spacelike separated. Alice's and Bob's measurement choices must also be random and unknown to Eve and to the devices before the measurements, the public classical communication channel must be authenticated, and the Bell violation must be obtained without loopholes such as postselection or undetected events that could fake nonlocal correlations.