Trial exam

Course: FYS3415/FYS4415
Quantum Computing and Quantum Information

This examination paper consists of 13 pages.

Appendices: Formula sheet

Permitted aids: Approved calculator

Solutions

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 $D(\rho,\sigma)$.

Solution:
For pure states, the fidelity is the absolute value of the inner product:

$$F(\rho,\sigma) = |\langle 0|\psi\rangle| = \frac{3}{5}.$$

The trace distance between pure states is

$$D(\rho,\sigma) = \sqrt{1 - F(\rho,\sigma)^2} = \sqrt{1 - \left(\frac{3}{5}\right)^2} = \sqrt{\frac{16}{25}} = \frac{4}{5}.$$

(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.

Solution:
First, we see that ρ_1 is a pure state because it is a rank-one projector:

$$\rho_1^2 = \rho_1, \qquad \mathrm{tr}\left(\rho_1^2\right) = 1.$$

It is also a product state, since

$$|0+\rangle = |0\rangle \otimes |+\rangle.$$

Hence ρ_1 is pure, product, separable, and not entangled.

Next, we see that ρ_2 is also pure, since

$$\rho_2^2 = \rho_2, \qquad \mathrm{tr}\left(\rho_2^2\right) = 1.$$

To check whether it is entangled, trace out the second qubit:

$$\mathrm{tr}_B(\rho_2) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}I.$$

The reduced state is mixed. A pure bipartite state is a product state if and only if its reduced states are pure. Therefore ρ_2 is entangled. This means that it is not a product state and not separable.

Finally consider ρ_3. We have

$$\begin{aligned} \rho_3^2 &= \frac{1}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11| \\ \implies \mathrm{tr}\left(\rho_3^2\right) &= \frac{1}{2} < 1. \end{aligned}$$

Thus ρ_3 is mixed. It is separable, since it is explicitly a convex combination of product states:

$$\rho_3 = \frac{1}{2}\left(|0\rangle\langle 0| \otimes |0\rangle\langle 0|\right) + \frac{1}{2}\left(|1\rangle\langle 1| \otimes |1\rangle\langle 1|\right).$$

It is not a product state. Indeed,

$$\mathrm{tr}_B(\rho_3) = \frac{1}{2}I, \qquad \mathrm{tr}_A(\rho_3) = \frac{1}{2}I,$$

so if ρ_3 were a product state, it would have to be

$$\mathrm{tr}_B(\rho_3) \otimes \mathrm{tr}_A(\rho_3) = \frac{1}{2}I \otimes \frac{1}{2}I = \frac{1}{4}I \otimes I,$$

which is not equal to ρ_3. Hence ρ_3 is mixed, separable, not product, and not entangled.

(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.

Solution:
We first check completeness:

$$M_0^\dagger M_0 + M_1^\dagger M_1 = |0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|1\rangle\langle 1| = I.$$

Thus M_0 and M_1 define a valid measurement. The corresponding POVM elements are

$$E_0 = M_0^\dagger M_0 = |0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|,$$
$$E_1 = M_1^\dagger M_1 = \frac{1}{2}|1\rangle\langle 1|.$$

For the input state $|+\rangle$, the outcome probabilities are

$$p_0 = \langle +|E_0|+\rangle = \frac{1}{2} + \frac{1}{4} = \frac{3}{4},$$
$$p_1 = \langle +|E_1|+\rangle = \frac{1}{4}.$$

The post-measurement state after outcome 0 is

$$\frac{M_0|+\rangle}{\sqrt{p_0}} = \frac{\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{2}|1\rangle}{\sqrt{3/4}} = \frac{\sqrt{2}|0\rangle + |1\rangle}{\sqrt{3}}.$$

The post-measurement state after outcome 1 is

$$\frac{M_1|+\rangle}{\sqrt{p_1}} = \frac{\frac{1}{2}|1\rangle}{\frac{1}{2}} = |1\rangle.$$

(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.

Solution:
The encoded state is

$$|\psi_{\mathrm{L}}\rangle = \alpha\,|0_{\mathrm{L}}\rangle + \beta\,|1_{\mathrm{L}}\rangle = \alpha\,|000\rangle + \beta\,|111\rangle.$$

No error corresponds to the action I, while the possible single bit-flip errors correspond to the actions X_1, X_2, and X_3. For example, after an X_1 error, the state becomes

$$X_1\,|\psi_{\mathrm{L}}\rangle = \alpha\,|100\rangle + \beta\,|011\rangle.$$

Both $|100\rangle$ and $|011\rangle$ have eigenvalue -1 under Z_1Z_2 and eigenvalue $+1$ under Z_2Z_3, giving syndrome $(-1,+1)$. The other cases are computed similarly.

Thus the syndrome outcomes and corrections are:

Case	$(Z_1Z_2,\ Z_2Z_3)$	Correction
I	$(+1,+1)$	I
X_1	$(-1,+1)$	X_1
X_2	$(-1,-1)$	X_2
X_3	$(+1,-1)$	X_3

The syndrome measurement identifies which error subspace the state lies in. It does not distinguish between the logical basis states inside that subspace. For example, in the X_1-error subspace, both

$$|100\rangle \qquad \text{and} \qquad |011\rangle$$

give the same syndrome $(-1,+1)$. Thus the measurement reveals which physical qubit flipped, but it does not reveal the coefficients α and β. The logical information is therefore preserved.

(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?

Solution:
We have

$$\begin{aligned} A_\theta \otimes A_\phi = &\cos\theta\cos\phi\, Z\otimes Z + \cos\theta\sin\phi\, Z\otimes X \\ &+ \sin\theta\cos\phi\, X\otimes Z + \sin\theta\sin\phi\, X\otimes X. \end{aligned}$$

For the Bell state $|\Phi^+\rangle$, we have

$$\begin{aligned} \langle\Phi^+|(Z\otimes Z)\,|\Phi^+\rangle &= 1, & \langle\Phi^+|(X\otimes X)\,|\Phi^+\rangle &= 1, \\ \langle\Phi^+|(Z\otimes X)\,|\Phi^+\rangle &= 0, & \langle\Phi^+|(X\otimes Z)\,|\Phi^+\rangle &= 0. \end{aligned}$$

Therefore

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

For the given angles:

$$\begin{aligned} E(a,b) &= \cos\left(0-\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}}, & E(a,b') &= \cos\left(0+\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}}, \\ E(a',b) &= \cos\left(\frac{\pi}{2}-\frac{\pi}{4}\right) = \frac{1}{\sqrt{2}}, & E(a',b') &= \cos\left(\frac{\pi}{2}+\frac{\pi}{4}\right) = -\frac{1}{\sqrt{2}}. \end{aligned}$$

Therefore

$$\begin{aligned} S &= E(a,b) + E(a,b') + E(a',b) - E(a',b') \\ &= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - \left(-\frac{1}{\sqrt{2}}\right) \\ &= 2\sqrt{2}. \end{aligned}$$

The local-hidden-variable bound is $|S| \leq 2$, meaning that the bound is violated.

(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.

Solution:
Since X is uniformly distributed on two values:

$$H(X) = 1.$$

The average state received by Bob is

$$\bar{\rho} = \frac{1}{2}\,|0\rangle\langle 0| + \frac{1}{2}\,|+\rangle\langle +|.$$

Using

$$|+\rangle\langle+| = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix},$$

we get

$$\bar{\rho} = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{2}\cdot\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} = \begin{pmatrix}3/4 & 1/4\\ 1/4 & 1/4\end{pmatrix}.$$

To compute the entropy $S(\bar{\rho})$, we need to find the eigenvalues of $\bar{\rho}$, which we can do by solving the characteristic equation

$$\begin{aligned}\det(\bar{\rho} - \lambda I) &= \det\begin{pmatrix}3/4-\lambda & 1/4\\ 1/4 & 1/4-\lambda\end{pmatrix} = 0\\ \implies \lambda^2 - \lambda + \frac{1}{8} &= 0\\ \implies \lambda_\pm &= \frac{1 \pm \frac{1}{\sqrt{2}}}{2}.\end{aligned}$$

The two states in the ensemble, $|0\rangle$ and $|+\rangle$, are pure, so

$$S(|0\rangle\langle 0|) = 0, \qquad S(|+\rangle\langle+|) = 0.$$

Therefore the Holevo quantity is

$$\begin{aligned}\chi &= S(\bar{\rho}) - \frac{1}{2}S(|0\rangle\langle 0|) - \frac{1}{2}S(|+\rangle\langle+|)\\ &= S(\bar{\rho})\\ &= -\lambda_+ \log_2 \lambda_+ - \lambda_- \log_2 \lambda_-\\ &= h_{\mathrm{b}}\left(\frac{1+\frac{1}{\sqrt{2}}}{2}\right)\\ &\approx 0.601.\end{aligned}$$

Thus

$$\chi < H(X) = 1.$$

Since $\chi < 1 = H(X)$, no measurement Bob can do can extract the full one bit of classical information on average. This is consistent with the fact that $|0\rangle$ and $|+\rangle$ are nonorthogonal and therefore cannot be perfectly distinguished by any measurement.

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

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

Solution:
Label the computational basis for the environment $|k\rangle_E$, $k \in \{0, 1\}$. Since

$$R_E |0\rangle_E = \frac{4}{5} |0\rangle_E + \frac{3}{5} |1\rangle_E,$$

we get

$$M_0 = {}_E\langle 0|U|0\rangle_E = |0\rangle\langle 0| + \frac{4}{5}|1\rangle\langle 1|,$$
$$M_1 = {}_E\langle 1|U|0\rangle_E = \frac{3}{5}|1\rangle\langle 1|.$$

They satisfy completeness since

$$M_0^\dagger M_0 + M_1^\dagger M_1 = |0\rangle\langle 0| + \left(\frac{16}{25} + \frac{9}{25}\right)|1\rangle\langle 1| = I.$$

Now

$$\begin{aligned}\mathcal{E}(\rho) &= M_0\rho M_0^\dagger + M_1\rho M_1^\dagger \\ &= \left(|0\rangle\langle 0| + \frac{4}{5}|1\rangle\langle 1|\right)\rho\left(|0\rangle\langle 0| + \frac{4}{5}|1\rangle\langle 1|\right) + \frac{9}{25}|1\rangle\langle 1|\rho|1\rangle\langle 1| \\ &= |0\rangle\langle 0|\rho|0\rangle\langle 0| + \frac{4}{5}|0\rangle\langle 0|\rho|1\rangle\langle 1| + \frac{4}{5}|1\rangle\langle 1|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1|.\end{aligned}$$

On the other hand, using

$$I = |0\rangle\langle 0| + |1\rangle\langle 1|, \qquad Z = |0\rangle\langle 0| - |1\rangle\langle 1|,$$

we get

$$\frac{9}{10}\rho + \frac{1}{10}Z\rho Z = |0\rangle\langle 0|\rho\,|0\rangle\langle 0| + \frac{4}{5}\,|0\rangle\langle 0|\rho\,|1\rangle\langle 1| + \frac{4}{5}\,|1\rangle\langle 1|\rho\,|0\rangle\langle 0| + |1\rangle\langle 1|\rho\,|1\rangle\langle 1|.$$

This is the same expression as above. Hence

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

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

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

Solution:
Since

$$Z\,|0\rangle\langle 0|Z = |0\rangle\langle 0|, \qquad Z\,|1\rangle\langle 1|Z = |1\rangle\langle 1|,$$

using the channel form from part **(a)** gives

$$\mathcal{E}(|0\rangle\langle 0|) = |0\rangle\langle 0|, \qquad \mathcal{E}(|1\rangle\langle 1|) = |1\rangle\langle 1|.$$

Thus, if Alice sends $|0\rangle$, Bob obtains outcome 0 with probability 1. If Alice sends $|1\rangle$, Bob obtains outcome 1 with probability 1. Hence

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

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

Solution:
We use that

$$Z\,|+\rangle = |-\rangle, \qquad Z\,|-\rangle = |+\rangle.$$

Thus

$$\mathcal{E}(|+\rangle\langle +|) = \frac{9}{10}\,|+\rangle\langle +| + \frac{1}{10}Z\,|+\rangle\langle +|Z = \frac{9}{10}\,|+\rangle\langle +| + \frac{1}{10}\,|-\rangle\langle -|,$$

and similarly

$$\mathcal{E}(|-\rangle\langle -|) = \frac{9}{10}\,|-\rangle\langle -| + \frac{1}{10}\,|+\rangle\langle +|.$$

In the X basis, Alice sends $|+\rangle$ half of the time, in which case Bob obtains the wrong outcome $|-\rangle$ with probability 1/10. The other half of the time, Alice sends $|-\rangle$, in which case Bob obtains the wrong outcome $|+\rangle$ with probability 1/10. Therefore

$$p_{\text{err},X} = \frac{1}{2}\frac{1}{10} + \frac{1}{2}\frac{1}{10} = \frac{1}{10}.$$

(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.

Solution:
No. Observing no errors in these Z-basis test rounds does not imply that Eve has no information about the remaining sifted raw key. To see this, consider what happens to the environment for the two possible Z-basis states. If Alice sends $|0\rangle$, then

$$U|0\rangle_S|0\rangle_E = |0\rangle_S|0\rangle_E.$$

If Alice sends $|1\rangle$, then

$$\begin{aligned} U|1\rangle_S|0\rangle_E &= |1\rangle_S R_E|0\rangle_E \\ &= |1\rangle_S\left(\frac{4}{5}|0\rangle_E + \frac{3}{5}|1\rangle_E\right). \end{aligned}$$

In both cases Bob receives the correct Z-basis state, so Alice and Bob see no Z-basis errors. However, the environment states are different:

$$|e_0\rangle = |0\rangle, \qquad |e_1\rangle = \frac{4}{5}|0\rangle + \frac{3}{5}|1\rangle.$$

Since these states are not equal, the environment contains some information about Alice's Z-basis bit. For example, if Eve measures E in the computational basis and obtains outcome 1, then she knows that Alice sent $|1\rangle$. Thus Eve can have partial information about the sifted raw key even though the tested Z-basis rounds show no errors.

(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.

Solution:
No. This is not a device-independent security argument. The security argument here assumes a model of Alice's and Bob's devices. For example, one assumes that Alice's device really prepares the states $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, and that Bob's device really measures in the Z- or X-basis.

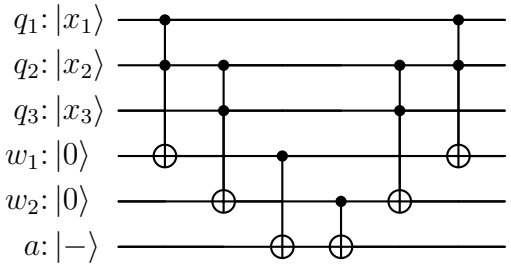
A device-independent security argument would not rely on trusting the internal implementation of the preparation and measurement devices. Instead, it would try to certify security from observed input-output statistics alone, using stronger tests such as Bell-type correlations.

Problem 3 (weight 35%)

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

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

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?

Solution:
The first two Toffoli gates compute

$$w_1 \mapsto 0 \oplus x_1 x_2 = x_1 x_2, \qquad w_2 \mapsto 0 \oplus x_2 x_3 = x_2 x_3.$$

Consider a CNOT gate with the control qubit in the computational-basis state $|c\rangle$, $c \in \{0, 1\}$ and $|-\rangle$ as the target:

$$\begin{aligned} |c\rangle\,|-\rangle &= \begin{cases} c = 0 : \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle - |0\rangle\,|1\rangle) \mapsto \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle - |0\rangle\,|1\rangle) = |c\rangle\,|-\rangle \\ c = 1 : \frac{1}{\sqrt{2}}(|1\rangle\,|0\rangle - |1\rangle\,|1\rangle) \mapsto \frac{1}{\sqrt{2}}(|1\rangle\,|1\rangle - |1\rangle\,|0\rangle) = -\,|c\rangle\,|-\rangle \end{cases} \\ &= (-1)^c\,|c\rangle\,|-\rangle. \end{aligned}$$

Hence the total phase after the two CNOTs targeting the $|-\rangle$ ancilla qubit is

$$(-1)^{w_1}(-1)^{w_2} = (-1)^{w_1 \oplus w_2} = (-1)^{x_1 x_2 \oplus x_2 x_3},$$

where $\oplus$ is XOR (addition modulo 2). The final Toffoli gates uncompute the work qubits:

$$w_1 \mapsto 0, \qquad w_2 \mapsto 0.$$

Thus the whole circuit maps

$$|x_1\, x_2\, x_3\, 0\, 0\, -\rangle \mapsto (-1)^{x_1 x_2 \oplus x_2 x_3}\,|x_1\, x_2\, x_3\, 0\, 0\, -\rangle,$$

meaning that the Boolean function implemented by the oracle is

$$f(x_1, x_2, x_3) = x_1 x_2 \oplus x_2 x_3 = x_2(x_1 \oplus x_3).$$

Therefore $f(x) = 1$ precisely when $x_2 = 1$ and $x_1 \neq x_3$. The solution states are

$$|011\rangle \qquad \text{and} \qquad |110\rangle.$$

If the ancilla were initialized in $|0\rangle$, the CNOT gates would store information in the ancilla instead of producing a phase:

$$|x\rangle\,|0\rangle \mapsto |x\rangle\,|f(x)\rangle.$$

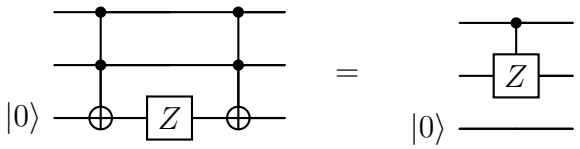
An algorithm that only maps basis states to basis states without phases is essentially just reversible classical computation, while phases allow quantum algorithms to use interference to make the correct answers more likely.

(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.

Solution:
Grover's algorithm can be understood geometrically. The state evolves in the two-dimensional subspace spanned by the uniform superposition of solution states and the uniform superposition of non-solution states. One Grover iteration, consisting of the oracle followed by the diffusion operator, rotates the state towards the solution subspace.

At first, each Grover iteration increases the amplitudes of the solution states, and therefore the probability of measuring a solution state increases. However, the probability does not increase forever. If too many Grover iterations are applied, the state rotates past the solution subspace, and the success probability begins to decrease again. Thus one should stop near the first maximum of the success probability.

(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)

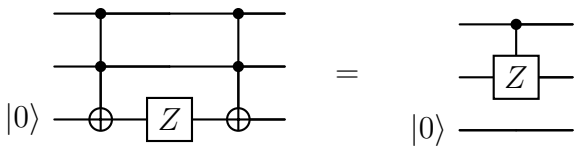
Solution:
Let the first two qubits be in a computational-basis state

$$|i\rangle\,|j\rangle, \qquad i, j \in \{0, 1\}.$$

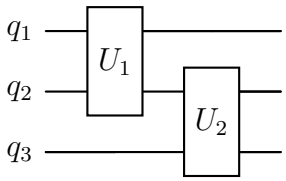
The first circuit maps

$$|i\rangle\,|j\rangle\,|0\rangle \mapsto |i\rangle\,|j\rangle\,|ij\rangle \mapsto (-1)^{ij}\,|i\rangle\,|j\rangle\,|ij\rangle \mapsto (-1)^{ij}\,|i\rangle\,|j\rangle\,|0\rangle.$$

This applies a phase -1 exactly when $i = j = 1$. That is precisely the action of a controlled-Z gate on the first two qubits, with the bottom qubit left unchanged. By linearity the identity also holds when the first two qubits are arbitrary. Therefore



(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.

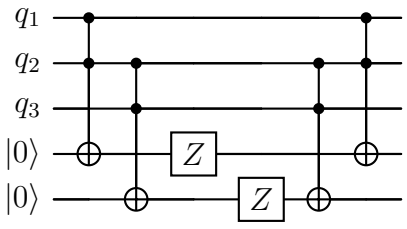
Solution:
By the same analysis as in part **(a)**, a CNOT with $|-\rangle$ at the target maps basis states

$$|c\rangle\,|-\rangle \mapsto (-1)^c\,|c\rangle\,|-\rangle.$$

We see that this is the same action as a Z gate on the control qubit. By linearity, we can therefore replace any CNOT with $|-\rangle$ as the target, with a Z gate at the CNOT's control qubit. Thus

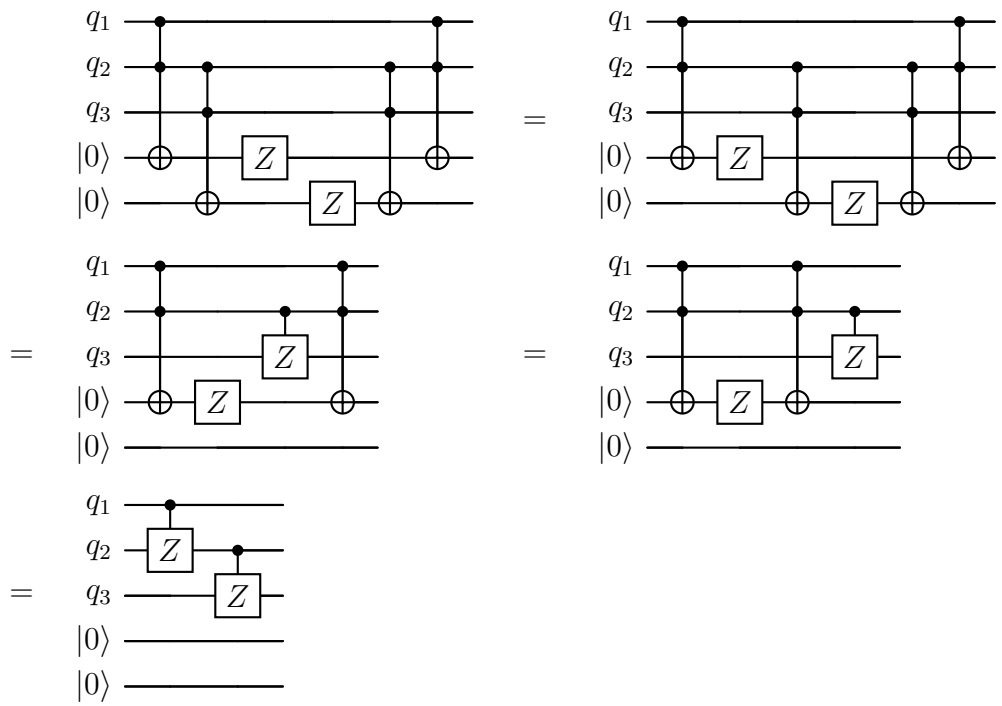


Applying this to the two CNOT gates with the ancilla at the target gives the following equivalent circuit, where the ancilla has become completely unchanged and is therefore omitted:



We can then commute gates acting on different qubits, as well as controlled gates whose only shared wires are common control wires, and use the result from part

(c). Repeating these techniques gives:



We see that the work qubits are also unchanged, remaining in $|0\rangle$, so they may also be omitted. The oracle therefore reduces to the circuit with two two-qubit gates given in the problem text, with both U_1 and U_2 being controlled-Z gates.

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

Solution:
The simplified oracle is preferable for real hardware for several reasons: First, it uses fewer qubits, involving only the 3 input qubits and no extra work or ancilla qubits. Second, the simplified circuit uses fewer gates, reducing the count from 6 to 2. Third, the simplified circuit uses gates that couple fewer qubits at a time, as the original has 3-qubit gates and the simplified only has two-qubit gates. Gates involving 3 or more qubits such as Toffoli gates are usually not native hardware gates, so each Toffoli must be decomposed into many one- and two-qubit gates.

These reductions are beneficial because every additional qubit and gate gives more opportunities for noise, gate errors, and decoherence to affect the computation. A shorter circuit with fewer qubits is therefore generally easier to implement accurately on real hardware, and is more likely to produce the correct measurement outcome.