# University of Oslo

FYS3415/FYS4415 — Quantum computing and quantum information

Problem set 7

This problem set will be discussed on **Mar. 11**.

## Problem 1: The Deutsch-Jozsa and Bernstein-Vazirani Algorithms

**a) The Deutsch-Jozsa Interference.** Let $f : \{0,1\}^n \to \{0,1\}$ be promised to be either *constant* (same value on all inputs) or *balanced* (outputs 0 on exactly half the inputs and 1 on the other half).

Prior to the final step of the algorithm, the query register is in the state

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle. \qquad \text{(You may take this expression as given.)}$$

The final step of the algorithm then applies $H^{\otimes n}$ to the query register and then measures it in the computational basis.

**i)** Write down the final state of the algorithm.

**ii)** Isolate the amplitude of the all-zero state $|0^n\rangle = |00\ldots0\rangle$.

**iii)** Use this amplitude to prove that the algorithm measures $|0^n\rangle$ with 100% probability if $f$ is constant, and with 0% probability if $f$ is balanced.

**iv)** Briefly compare with a classical algorithm. How many queries to $f(x)$ are needed (a) in the worst case for a *deterministic* classical algorithm to always decide constant vs. balanced, and (b) for a *randomized* classical algorithm allowed error probability at most 1/3?

**Solution:**

**i)** We apply $H^{\otimes n}$ to the state $|\psi\rangle$. Since the operator is linear, we can bring it inside the sum to act directly on the basis states $|x\rangle$:

$$\begin{aligned} H^{\otimes n}|\psi\rangle &= H^{\otimes n}\left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle\right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \Big(H^{\otimes n}|x\rangle\Big). \end{aligned}$$

Now we substitute the provided formula for $H^{\otimes n}|x\rangle$:

$$H^{\otimes n}|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \left(\frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} (-1)^{x\cdot z} |z\rangle\right).$$

By combining the scalar factors and swapping the order of the sums to group all terms attached

to a specific basis state $|z\rangle$, we get:

$$H^{\otimes n}|\psi\rangle = \frac{1}{2^n}\sum_{z\in\{0,1\}^n}\left(\sum_{x\in\{0,1\}^n}(-1)^{f(x)+x\cdot z}\right)|z\rangle.$$

**ii)** We want the amplitude of the state where $z = 0^n$. For this string, $x \cdot z = 0$ for all $x$, so $(-1)^{x\cdot z} = 1$. The amplitude $A_{0^n}$ is:

$$A_{0^n} = \frac{1}{2^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}.$$

**iii)** We evaluate $A_{0^n}$ for the two promised cases:

- **Constant:** $f(x)$ is always 0 or always 1, so $(-1)^{f(x)}$ is always $+1$ or always $-1$.

$$A_{0^n} = \frac{1}{2^n}(\pm 2^n) = \pm 1 \quad \Rightarrow \quad \Pr(0^n) = |A_{0^n}|^2 = 1.$$

- **Balanced:** half the terms are $+1$ and half are $-1$, so they cancel:

$$A_{0^n} = \frac{1}{2^n}\big(2^{n-1}(+1) + 2^{n-1}(-1)\big) = 0 \quad \Rightarrow \quad \Pr(0^n) = 0.$$

Thus one quantum query suffices to distinguish the two cases with certainty.

**iv)**

- **Deterministic classical:** In the worst case you need $2^{n-1}+1$ queries. Indeed, after seeing $2^{n-1}$ identical outputs you still cannot rule out a balanced function (you might have queried only inputs from the "0 half"); the $(2^{n-1}+1)$st query forces a different output if $f$ is balanced, and if it is still the same then $f$ must be constant (by the promise).
- **Randomized classical (bounded error):** Query $m$ uniformly random inputs; if you ever see both outputs declare "balanced", otherwise declare "constant". If $f$ is balanced, the probability all $m$ answers are equal is $2\cdot(1/2)^m = 2^{1-m}$, so taking $m = 3$ gives error $\leq 1/4 < 1/3$. (More generally, error $\leq \delta$ needs $m \geq 1 + \log_2(1/\delta)$ queries.)

**b) The Bernstein-Vazirani algorithm.** Now consider a different promise: $f(x) = s \cdot x \pmod 2$ for some unknown *secret string* $s \in \{0,1\}^n$. Using the same oracle $U_f$ and the same algorithm as Deutsch-Jozsa, the query register is in the state

$$|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{s\cdot x}|x\rangle$$

after a single oracle call. The goal is to determine the string $s$.

**i)** Substitute $f(x) = s \cdot x$ into $|\psi\rangle$. Show that this state can be neatly factored into a tensor product of $n$ independent qubits.

**ii)** By applying a Hadamard gate to each qubit individually in this factored form, prove that the final measurement yields the string $s$ exactly.

**iii)** How many classical queries to $f(x)$ would be needed to determine $s$? Justify your answer and contrast it with the quantum case.

**Solution:**

**i)** We can rewrite the sum over all $n$-bit strings as independent sums over each bit $x_i \in \{0,1\}$:

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x_1,\ldots,x_n} (-1)^{s_1 x_1} \cdots (-1)^{s_n x_n} |x_1\rangle \otimes \cdots \otimes |x_n\rangle$$
$$= \left( \frac{1}{\sqrt{2}} \sum_{x_1 \in \{0,1\}} (-1)^{s_1 x_1} |x_1\rangle \right) \otimes \cdots \otimes \left( \frac{1}{\sqrt{2}} \sum_{x_n \in \{0,1\}} (-1)^{s_n x_n} |x_n\rangle \right).$$

Writing out the sums for each qubit explicitly ($x_i = 0$ and $x_i = 1$), the state completely factors into:

$$|\psi\rangle = \left( \frac{|0\rangle + (-1)^{s_1} |1\rangle}{\sqrt{2}} \right) \otimes \left( \frac{|0\rangle + (-1)^{s_2} |1\rangle}{\sqrt{2}} \right) \otimes \cdots \otimes \left( \frac{|0\rangle + (-1)^{s_n} |1\rangle}{\sqrt{2}} \right).$$

**ii)** The final step is to apply $H^{\otimes n}$, which means applying a single Hadamard gate to each of the factored qubits. Recall how the Hadamard gate acts on the basis states: $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$ and $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle$. Because $H$ is its own inverse, the reverse is also true:

- If $s_i = 0$, the qubit is $\frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle$. Applying $H$ yields $|0\rangle$.
- If $s_i = 1$, the qubit is $\frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle$. Applying $H$ yields $|1\rangle$.

This can be summarized compactly as $H\left(\frac{|0\rangle+(-1)^{s_i}|1\rangle}{\sqrt{2}}\right) = |s_i\rangle$. Applying this to the entire register:

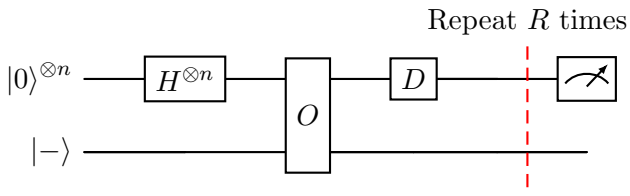
$$H^{\otimes n}|\psi\rangle = |s_1\rangle \otimes |s_2\rangle \otimes \cdots \otimes |s_n\rangle = |s_1 s_2 \ldots s_n\rangle = |s\rangle.$$

Thus, measuring the register yields the secret string $s$ with 100% certainty.

**iii)** Classically, querying $f(x)$ returns a single bit of information. To find $s$, we would need to query the function with basis inputs where only one bit is 1. For example: $f(100\ldots0) = s_1$, $f(010\ldots0) = s_2$, etc. Therefore, it takes exactly $n$ classical queries to uncover the $n$-bit string $s$. The quantum algorithm achieves this in exactly 1 query, demonstrating a linear speedup.

## Problem 2: Grover's Search Algorithm

Suppose you are searching an unsorted database of $N = 2^n$ items for one (or more) "marked" items that satisfy some criterion. Classically, there is no shortcut: you must check items one at a time, requiring $O(N)$ queries in the worst case. Grover's algorithm achieves this with only $O(\sqrt{N})$ queries — a quadratic speedup.




The search criterion is encoded in an *oracle*: a function $f : \{0,1\}^n \to \{0,1\}$ with $f(x) = 1$ if

and only if $x$ is a solution. There are $M \geq 1$ solutions among the $N$ items. In this problem you will build Grover's algorithm from scratch.

**a) The phase oracle.** In circuit form, the standard boolean oracle is a unitary $U_f$ acting as $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. However, for Grover's algorithm we need a *phase oracle* $O$ that marks solutions by flipping their quantum phase (sign) instead of flipping an ancilla bit:

$$O |x\rangle = (-1)^{f(x)} |x\rangle.$$

Show how to implement this phase oracle $O$ using a single application of $U_f$ and a suitable ancilla qubit. What state should the ancilla be initialised in, and why does it safely factorise out at the end of the operation?

**Solution:** We prepare the ancilla in the state $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and apply the standard oracle $U_f$:

$$U_f |x\rangle |-\rangle = U_f \left( |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle \frac{|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle}{\sqrt{2}}$$

If $f(x) = 0$, the ancilla remains $\frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle$.
If $f(x) = 1$, the ancilla becomes $\frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|-\rangle$.
This can be written compactly as:

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

Since the ancilla remains in the $|-\rangle$ state regardless of the input $x$, it is unentangled from the query register and factorises out completely. The net effect on the $n$-qubit query register is exactly the phase oracle $|x\rangle \to (-1)^{f(x)} |x\rangle$.

**b) The Grover iteration.** Grover's algorithm starts by preparing the uniform superposition of all possible items, $|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_x |x\rangle$. It then repeatedly applies a two-part sequence called the *Grover iteration* ($G$):

- **Step 1. The Oracle ($O$):** Flips the sign of every solution state.
- **Step 2. The Diffusion Operator ($D$):** Defined mathematically as $D = H^{\otimes n}(2 |0\rangle^{\otimes n} \langle 0|^{\otimes n} - \mathbb{1}) H^{\otimes n}$.

  **i)** Using the definition of $|\psi\rangle$, prove that the diffusion operator can be rewritten as $D = 2 |\psi\rangle\langle\psi| - \mathbb{1}$.

  **ii)** The operator $2 |\psi\rangle\langle\psi| - \mathbb{1}$ is famous for performing *inversion about the mean*. Prove this by applying it to an arbitrary state $|\Phi\rangle = \sum_k \alpha_k |k\rangle$. Show that the new amplitude for each state $|k\rangle$ becomes $2\bar{\alpha} - \alpha_k$, where $\bar{\alpha} = \frac{1}{N} \sum_k \alpha_k$ is the average amplitude.

**Solution: i)** We substitute $|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n}$. Because the Hadamard transform is its own inverse ($H^{\otimes n} H^{\otimes n} = \mathbb{1}$), we can expand $D$:

$$\begin{aligned} D &= H^{\otimes n}(2 |0\rangle^{\otimes n} \langle 0|^{\otimes n} - \mathbb{1}) H^{\otimes n} \\ &= 2(H^{\otimes n} |0\rangle^{\otimes n})(\langle 0|^{\otimes n} H^{\otimes n}) - H^{\otimes n} \mathbb{1} H^{\otimes n} \\ &= 2 |\psi\rangle\langle\psi| - \mathbb{1} \end{aligned}$$

**ii)** We apply this operator to the arbitrary state $|\Phi\rangle$:

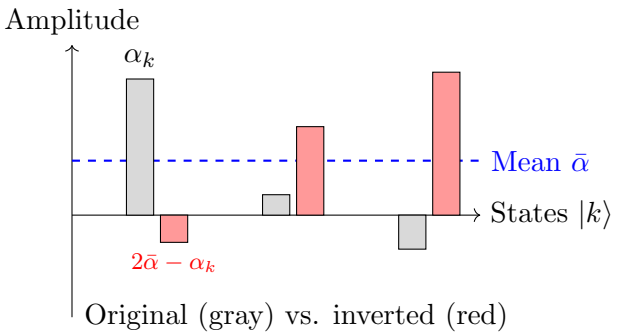
$$(2\,|\psi\rangle\langle\psi| - \mathbb{1})\,|\Phi\rangle = 2\,|\psi\rangle\langle\psi|\Phi\rangle - |\Phi\rangle$$

First, let us calculate the inner product $\langle\psi|\Phi\rangle$. Since $\langle\psi| = \frac{1}{\sqrt{N}}\sum_j \langle j|$:

$$\langle\psi|\Phi\rangle = \left(\frac{1}{\sqrt{N}}\sum_j \langle j|\right)\left(\sum_k \alpha_k\,|k\rangle\right) = \frac{1}{\sqrt{N}}\sum_k \alpha_k$$

Recognizing that $\sum_k \alpha_k = N\bar{\alpha}$, we get $\langle\psi|\Phi\rangle = \frac{N\bar{\alpha}}{\sqrt{N}} = \sqrt{N}\,\bar{\alpha}$. Substituting this back into the main equation:

$$\begin{aligned} 2\,|\psi\rangle(\sqrt{N}\,\bar{\alpha}) - |\Phi\rangle &= 2(\sqrt{N}\,\bar{\alpha})\left(\frac{1}{\sqrt{N}}\sum_k |k\rangle\right) - \sum_k \alpha_k\,|k\rangle \\ &= \sum_k 2\bar{\alpha}\,|k\rangle - \sum_k \alpha_k\,|k\rangle \\ &= \sum_k (2\bar{\alpha} - \alpha_k)\,|k\rangle \end{aligned}$$

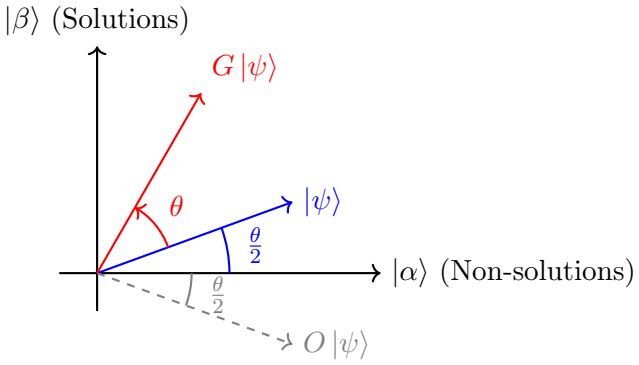



Thus, every individual amplitude $\alpha_k$ is mapped to $2\bar{\alpha} - \alpha_k$, which is the geometric formula for reflecting a point about the mean value $\bar{\alpha}$.

**c) Geometric picture and performance.** The power of Grover's algorithm is beautifully visualized geometrically. We can group the massive $N$-dimensional space into just two normalised basis states:

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_{x:\,f(x)=0} |x\rangle \quad (\text{“non-solutions”}), \qquad |\beta\rangle = \frac{1}{\sqrt{M}}\sum_{x:\,f(x)=1} |x\rangle \quad (\text{“solutions”}).$$

These are orthogonal, meaning the entire algorithm takes place in a simple two-dimensional plane.




**i)** Show that the initial uniform superposition can be written as $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle$, and define the value of $\sin\left(\frac{\theta}{2}\right)$.

**ii)** Argue that the oracle $O$ acts as a *reflection about* $|\alpha\rangle$ in this plane, and that the diffusion operator $D$ acts as a *reflection about* $|\psi\rangle$.

**iii)** A standard geometric theorem states that the composition of two reflections whose axes are separated by an angle $\phi$ results in a pure rotation by $2\phi$. Using this fact, write down the state of the system $G^k|\psi\rangle$ after $k$ full Grover iterations.

**iv)** We want to measure the system when the state vector is rotated as close to the "solution" axis $|\beta\rangle$ as possible. For the standard case of $M = 1$ solution among a massive database ($N \gg 1$), prove that the optimal number of iterations is $R \approx \frac{\pi}{4}\sqrt{N}$.

**Solution: i)** The initial state $|\psi\rangle$ contains all $N$ basis states with an equal amplitude of $1/\sqrt{N}$. We can group these into the $N - M$ non-solutions and the $M$ solutions:

$$|\psi\rangle = \sum_{x:\, f(x)=0} \frac{1}{\sqrt{N}}|x\rangle + \sum_{x:\, f(x)=1} \frac{1}{\sqrt{N}}|x\rangle$$

By factoring out the normalisation constants for $|\alpha\rangle$ and $|\beta\rangle$, we get:

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$$

Comparing this to the trigonometric identity $\cos^2(\phi) + \sin^2(\phi) = 1$, we define $\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}$ and $\cos\left(\frac{\theta}{2}\right) = \sqrt{\frac{N-M}{N}}$.

**ii)** The oracle $O$ flips the sign of solutions but leaves non-solutions alone. Thus $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$. Geometrically, flipping the vertical component while keeping the horizontal component identical is exactly a reflection across the horizontal $|\alpha\rangle$ axis. Similarly, the operator $2|\psi\rangle\langle\psi| - \mathbb{1}$ explicitly preserves the component parallel to $|\psi\rangle$ and flips the sign of any component orthogonal to $|\psi\rangle$. This is the definition of a reflection across the $|\psi\rangle$ axis.

**iii)** The initial state $|\psi\rangle$ sits at an angle of $\theta/2$ from the $|\alpha\rangle$ axis. Since $G$ consists of a reflection about $|\alpha\rangle$ followed by a reflection about $|\psi\rangle$ (which are separated by an angle of $\theta/2$), the composition theorem tells us that $G$ rotates the state by exactly $2 \times (\theta/2) = \theta$ towards $|\beta\rangle$. After $k$ iterations, the state has rotated by $k\theta$ from its starting position. The total angle from the horizontal axis is therefore $\frac{\theta}{2} + k\theta = \frac{(2k+1)\theta}{2}$. The state is:

$$G^k|\psi\rangle = \cos\left(\frac{(2k+1)\theta}{2}\right)|\alpha\rangle + \sin\left(\frac{(2k+1)\theta}{2}\right)|\beta\rangle$$

**iv)** To maximize our chance of measuring a solution, we want the state to be parallel to $|\beta\rangle$. This means we want the sine term to equal 1, which occurs when the angle is $\pi/2$:

$$\frac{(2R+1)\theta}{2} \approx \frac{\pi}{2} \implies 2R+1 \approx \frac{\pi}{\theta} \implies R \approx \frac{\pi}{2\theta}$$

For $M = 1$ and $N \gg 1$, the angle $\theta$ is incredibly small. We can use the small-angle approximation $\sin(x) \approx x$. Therefore, $\sin\left(\frac{\theta}{2}\right) = \frac{1}{\sqrt{N}} \implies \frac{\theta}{2} \approx \frac{1}{\sqrt{N}} \implies \theta \approx \frac{2}{\sqrt{N}}$. Substituting this into our equation for $R$:

$$R \approx \frac{\pi}{2(2/\sqrt{N})} = \frac{\pi}{4}\sqrt{N}$$

**d) Worked example:** Set $N = 4$, $M = 1$. Let us see the "magic" of the amplitudes firsthand. Consider a 2-qubit search space ($N = 4$) with exactly one marked item $x_0$.

**i)** Using the exact geometric formulas from part (c), compute $\theta$ and show that exactly $R = 1$ Grover iteration is required.

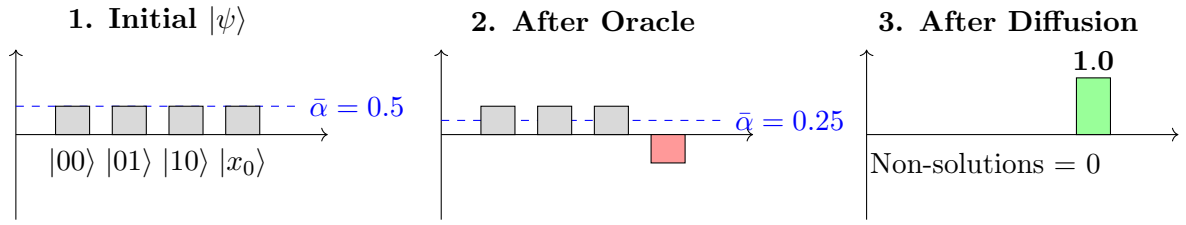
**ii)** Starting from the uniform superposition $|\psi\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$, manually apply one full Grover iteration: first apply $O$ (flip the sign of $|x_0\rangle$), then apply the inversion about the mean formula. Show that the non-solution amplitudes cancel perfectly to zero, leaving the state as $|x_0\rangle$ with 100% certainty!

**Solution: i)** Using the definition $\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}} = \sqrt{\frac{1}{4}} = \frac{1}{2}$. The angle whose sine is $1/2$ is $\pi/6$. Therefore $\frac{\theta}{2} = \frac{\pi}{6}$, which means $\theta = \frac{\pi}{3}$. We want the final angle to be exactly $\pi/2$. Using our formula:

$$\frac{(2R+1)\theta}{2} = \frac{\pi}{2} \implies (2R+1)\left(\frac{\pi}{6}\right) = \frac{\pi}{2} \implies 2R+1 = 3 \implies R = 1$$

Exactly 1 iteration will align the vector perfectly with the solution axis.

**ii)** Let's trace the amplitudes. Initially, all four states have an amplitude of $1/2$.




- **After Oracle ($O$):** The amplitude of the solution $|x_0\rangle$ flips to $-1/2$. The three non-solutions remain at $+1/2$.
- **Calculate the Mean:** The new average amplitude $\bar{\alpha}$ across all four states is:

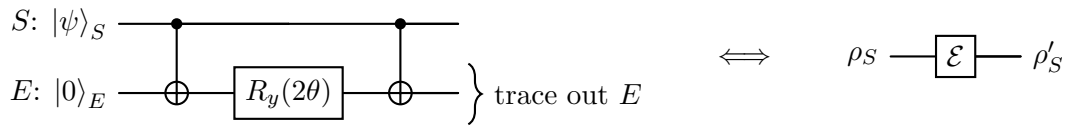
$$\bar{\alpha} = \frac{3 \times (1/2) + 1 \times (-1/2)}{4} = \frac{1.5 - 0.5}{4} = \frac{1}{4}$$

- **Inversion about the Mean ($2\bar{\alpha} - \alpha_k$):** For the three non-solutions, the new amplitude is $2(1/4) - 1/2 = 1/2 - 1/2 = \mathbf{0}$.
  For the one solution $|x_0\rangle$, the new amplitude is $2(1/4) - (-1/2) = 1/2 + 1/2 = \mathbf{1}$.

The destructive interference on the non-solutions is perfect. After just one query, the state of the quantum computer is exactly $|x_0\rangle$, and measuring it yields the correct answer with 100% certainty.

## Problem 3: Quantum channels and Kraus operators

Consider the following two-qubit circuit, where $S$ is a system qubit in some initial state $|\psi\rangle_S$ and $E$ is an environment qubit initially prepared in $|0\rangle_E$:




Let $U$ be the two-qubit unitary implemented by the circuit.

**i)** Show that

$$U(|\psi\rangle_S \otimes |0\rangle_E) = \cos\theta\ |\psi\rangle_S |0\rangle_E + \sin\theta\, Z\, |\psi\rangle_S |1\rangle_E.$$

**ii)** Using the computational basis $\{|0\rangle_E, |1\rangle_E\}$ for the environment, define

$$M_k = {}_E\langle k|\, U\, |0\rangle_E, \qquad k \in \{0, 1\}.$$

Determine $M_0$ and $M_1$, and verify that

$$\sum_k M_k^\dagger M_k = I_S.$$

**iii)** Show that for any single-qubit state $\rho_S$,

$$\mathrm{Tr}_E\big(U(\rho_S \otimes |0\rangle\langle 0|_E)U^\dagger\big) = \sum_k M_k\, \rho_S\, M_k^\dagger.$$

Hence find an explicit expression for $\mathcal{E}(\rho_S)$. If

$$\rho_S = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix},$$

what happens to the diagonal and off-diagonal entries under $\mathcal{E}$?

**iv)** Now use the Hadamard basis $\{|+\rangle_E, |-\rangle_E\}$ for the environment, and define

$$M_\pm = {}_E\langle \pm|\, U\ |0\rangle_E.$$

Determine $M_+$ and $M_-$, show that

$$M_\pm = \frac{M_0 \pm M_1}{\sqrt{2}},$$

and verify that

$$\mathcal{E}(\rho_S) = M_+ \rho_S M_+^\dagger + M_- \rho_S M_-^\dagger.$$

Thus, two different sets of Kraus operators describe the same quantum channel.

**Solution: i)** Let

$$|\psi\rangle_S = \alpha\,|0\rangle + \beta\,|1\rangle.$$

Using the standard convention

$$R_y(2\theta)\,|0\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle, \qquad R_y(2\theta)\,|1\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle,$$

we follow the circuit gate by gate:

$$\begin{aligned}
&|\psi\rangle_S\,|0\rangle_E = \alpha\,|00\rangle + \beta\,|10\rangle \\
&\xrightarrow{\text{CNOT}_{S\to E}} \alpha\,|00\rangle + \beta\,|11\rangle \\
&\xrightarrow{R_y(2\theta)\text{ on }E} \alpha\big(\cos\theta\,|00\rangle + \sin\theta\,|01\rangle\big) + \beta\big(-\sin\theta\,|10\rangle + \cos\theta\,|11\rangle\big) \\
&\xrightarrow{\text{CNOT}_{S\to E}} \alpha\big(\cos\theta\,|00\rangle + \sin\theta\,|01\rangle\big) + \beta\big(\cos\theta\,|10\rangle - \sin\theta\,|11\rangle\big).
\end{aligned}$$

Collecting terms,

$$\begin{aligned}
U(|\psi\rangle_S\,|0\rangle_E) &= \cos\theta\,(\alpha\,|0\rangle + \beta\,|1\rangle)\,|0\rangle + \sin\theta\,(\alpha\,|0\rangle - \beta\,|1\rangle)\,|1\rangle \\
&= \cos\theta\;|\psi\rangle_S\,|0\rangle_E + \sin\theta\,Z\,|\psi\rangle_S\,|1\rangle_E,
\end{aligned}$$

since

$$Z\,|\psi\rangle_S = \alpha\,|0\rangle - \beta\,|1\rangle.$$

**ii)** By definition,

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

Using the result from part **i)**, for an arbitrary state $|\psi\rangle_S$ we find

$$\begin{aligned}
M_0\,|\psi\rangle_S &= {}_E\langle 0|\,U(|\psi\rangle_S\,|0\rangle_E) = {}_E\langle 0|\big(\cos\theta\;|\psi\rangle_S\,|0\rangle_E + \sin\theta\,Z\,|\psi\rangle_S\,|1\rangle_E\big) \\
&= \cos\theta\;|\psi\rangle_S,
\end{aligned}$$

and similarly

$$\begin{aligned}
M_1\,|\psi\rangle_S &= {}_E\langle 1|\,U(|\psi\rangle_S\,|0\rangle_E) = {}_E\langle 1|\big(\cos\theta\;|\psi\rangle_S\,|0\rangle_E + \sin\theta\,Z\,|\psi\rangle_S\,|1\rangle_E\big) \\
&= \sin\theta\,Z\,|\psi\rangle_S.
\end{aligned}$$

Since this holds for every $|\psi\rangle_S$, the Kraus operators are

$$M_0 = \cos\theta\,I_S, \qquad M_1 = \sin\theta\,Z.$$

To verify the completeness relation,

$$\begin{aligned}
M_0^\dagger M_0 + M_1^\dagger M_1 &= \cos^2\theta\,I_S + \sin^2\theta\,Z^\dagger Z \\
&= \cos^2\theta\,I_S + \sin^2\theta\,I_S \\
&= (\cos^2\theta + \sin^2\theta)I_S = I_S.
\end{aligned}$$

**iii)** Using the definition of the partial trace in the computational basis of $E$,

$$\begin{aligned}\mathrm{Tr}_E\big(U(\rho_S\otimes|0\rangle\langle 0|_E)U^\dagger\big) &= \sum_{k=0}^{1} {}_E\langle k|\, U(\rho_S\otimes|0\rangle\langle 0|_E)U^\dagger\, |k\rangle_E \\ &= \sum_{k=0}^{1} \big({}_E\langle k|U\,|0\rangle_E\big)\,\rho_S\,\big({}_E\langle k|U\,|0\rangle_E\big)^\dagger \\ &= \sum_{k=0}^{1} M_k\,\rho_S\,M_k^\dagger.\end{aligned}$$

Thus the reduced dynamics are indeed given by the operator-sum representation.

Using the Kraus operators from part **ii)**,

$$\begin{aligned}\mathcal{E}(\rho_S) &= M_0\rho_S M_0^\dagger + M_1\rho_S M_1^\dagger \\ &= \cos^2\theta\,\rho_S + \sin^2\theta\, Z\rho_S Z.\end{aligned}$$

So the channel is explicitly

$$\boxed{\mathcal{E}(\rho_S) = \cos^2\theta\,\rho_S + \sin^2\theta\, Z\rho_S Z.}$$

Now let

$$\rho_S = \begin{pmatrix}\rho_{00} & \rho_{01}\\ \rho_{10} & \rho_{11}\end{pmatrix}.$$

Then

$$Z\rho_S Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}\rho_{00} & \rho_{01}\\ \rho_{10} & \rho_{11}\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} = \begin{pmatrix}\rho_{00} & -\rho_{01}\\ -\rho_{10} & \rho_{11}\end{pmatrix}.$$

Hence

$$\begin{aligned}\mathcal{E}(\rho_S) &= \cos^2\theta\begin{pmatrix}\rho_{00} & \rho_{01}\\ \rho_{10} & \rho_{11}\end{pmatrix} + \sin^2\theta\begin{pmatrix}\rho_{00} & -\rho_{01}\\ -\rho_{10} & \rho_{11}\end{pmatrix} \\ &= \begin{pmatrix}\rho_{00} & (\cos^2\theta-\sin^2\theta)\rho_{01}\\ (\cos^2\theta-\sin^2\theta)\rho_{10} & \rho_{11}\end{pmatrix} \\ &= \begin{pmatrix}\rho_{00} & \cos(2\theta)\,\rho_{01}\\ \cos(2\theta)\,\rho_{10} & \rho_{11}\end{pmatrix}.\end{aligned}$$

Therefore, the diagonal entries are unchanged, while the off-diagonal entries are multiplied by $\cos(2\theta)$.

**iv)** Using

$$|\pm\rangle_E = \frac{|0\rangle_E \pm |1\rangle_E}{\sqrt{2}},$$

we obtain

$$\begin{aligned}M_+ = {}_E\langle +|\,U\,|0\rangle_E &= \frac{1}{\sqrt{2}}\big({}_E\langle 0| + {}_E\langle 1|\big)U\,|0\rangle_E \\ &= \frac{1}{\sqrt{2}}(M_0+M_1) = \frac{1}{\sqrt{2}}(\cos\theta\, I_S + \sin\theta\, Z),\end{aligned}$$

and similarly

$$\begin{aligned} M_- &= {}_E\langle -|\, U\, |0\rangle_E = \frac{1}{\sqrt{2}}\big({}_E\langle 0| - {}_E\langle 1|\big)U\,|0\rangle_E \\ &= \frac{1}{\sqrt{2}}(M_0 - M_1) = \frac{1}{\sqrt{2}}(\cos\theta\, I_S - \sin\theta\, Z). \end{aligned}$$

Thus

$$M_\pm = \frac{M_0 \pm M_1}{\sqrt{2}}.$$

To verify that these give the same channel, compute

$$\begin{aligned} M_+\rho_S M_+^\dagger + M_-\rho_S M_-^\dagger &= \frac{1}{2}(M_0 + M_1)\rho_S(M_0^\dagger + M_1^\dagger) + \frac{1}{2}(M_0 - M_1)\rho_S(M_0^\dagger - M_1^\dagger) \\ &= M_0\rho_S M_0^\dagger + M_1\rho_S M_1^\dagger \\ &= \mathcal{E}(\rho_S). \end{aligned}$$

So the two sets

$$\{M_0, M_1\} \qquad \text{and} \qquad \{M_+, M_-\}$$

describe exactly the same quantum channel.