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?

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

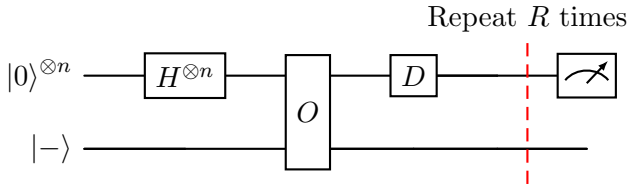
$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} (-1)^{s\cdot x} |x\rangle$$

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.

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?

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 $D = H^{\otimes n}(2 |0\rangle^{\otimes n}\langle 0|^{\otimes n} - \mathbb{1})H^{\otimes n}$.

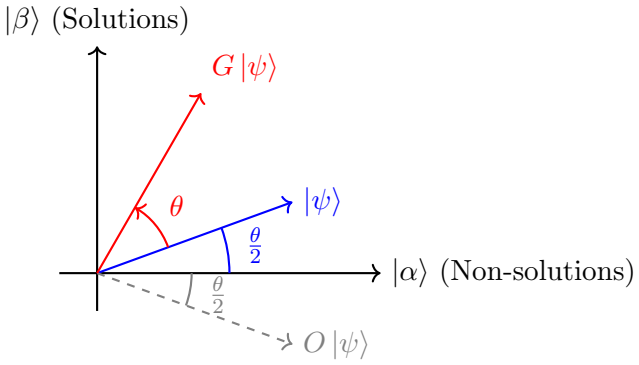
  i) Using the definition of $|\psi\rangle$, prove that the diffusion operator can be rewritten as $D = 2 |\psi\rangle\langle\psi| - \mathbb{1}$.

  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.

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 ϕ results in a pure rotation by 2ϕ. 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 $R \approx \frac{\pi}{4}\sqrt{N}$.

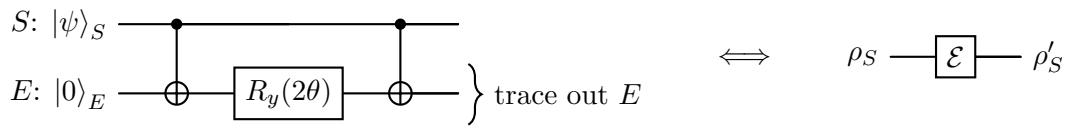
d) Worked example: Set $N = 4$, $M = 1$. Let us see the "magic" of the amplitudes firsthand. Consider a 2-qubit search space ($N = 4$) with exactly one marked item x_0.

i) Using the exact geometric formulas from part (c), compute θ 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!

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 ρ_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.