Exercises

1 Hadamard test

Let $U \in \mathbb{C}^{2^n \times 2^n}$ be a unitary matrix and ψ be an eigenvector of U with eigenvalue $e^{i\theta}$.

We will use a Hadamard test to estimate the value of the angle θ.

For the real part, we will use this circuit

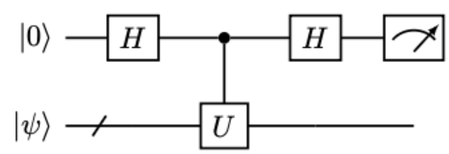

Figure 1: Real part estimation

and for the imaginary part, this circuit

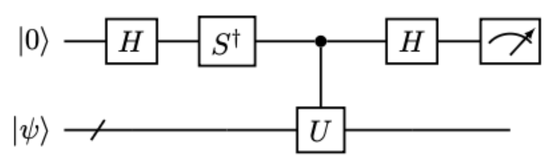

Figure 2: Imaginary part estimation

1. For the real part, check that the probability $p(q_0 = |0\rangle) = \frac{1}{2}(1 + \mathrm{Re}(\langle \psi, U\psi \rangle))$. What happens if θ is close to π?
2. For the imaginary part, check that the probability $p(q_0 = |0\rangle) = \frac{1}{2}(1 + \mathrm{Im}(\langle \psi, U\psi \rangle))$.

2 Block encoding

Let $A \in \mathbb{C}^{2^n \times 2^n}$ be a matrix such that $\|A\| \leq 1$.

If A is not unitary, then A cannot be implemented as a quantum algorithm. However, it may be a submatrix of a unitary matrix of a larger size. This technique is called *block encoding*. More precisely, we will say that $U_A \in \mathbb{C}^{2^{n+m} \times 2^{n+m}}$ is an (α, m)-block encoding of A if

$$\langle 0|^{\otimes m} \otimes I_n U_A |0\rangle^{\otimes m} \otimes I_n = \alpha A.$$

1. In matrix form, show that it is equivalent to

$$U_A = \begin{bmatrix} \alpha A & * \\ * & * \end{bmatrix}.$$

2. Using the SVD (U, Σ, V^*) of A, show that A has a $(1,1)$-block encoding.

Hint: show that $\begin{bmatrix} \Sigma & \sqrt{I-\Sigma^2} \\ \sqrt{I-\Sigma^2} & -\Sigma \end{bmatrix}$ is a unitary matrix.

Suppose that the entries of A satisfy $|a_{ij}| \leq 1$ for all $1 \leq i,j \leq 2^n$. Let $O_A \in \mathbb{C}^{2^{2n+1} \times 2^{2n+1}}$ be the matrix defined by: for any $0 \leq i,j \leq 2^n$

$$O_A|0\rangle \otimes |i\rangle \otimes |j\rangle = (a_{ij}|0\rangle + \sqrt{1-|a_{ij}|^2}|1\rangle) \otimes |i\rangle \otimes |j\rangle$$

and

$$O_A|0\rangle \otimes |i\rangle \otimes |j\rangle = (-a_{ij}|1\rangle + \sqrt{1-|a_{ij}|^2}|0\rangle) \otimes |i\rangle \otimes |j\rangle.$$

3. Verify that O_A defines a unitary matrix.
4. Let U_A be the matrix defined by

$$U_A = (I_1 \otimes H^{\otimes n} \otimes I_n)(I_1 \otimes \text{SWAP})O_A(I_1 \otimes H^{\otimes n} \otimes I_n).$$

Show that U_A is a $(\frac{1}{2^n}, n+1)$ block encoding of A.

3 Simon problem

In the Simon problem, a function $f : \{0,1\}^n \to \{0,1\}^n$ is given which has the property

$$\exists s \in \{0,1\}^n, \forall\, x,y \in \{0,1\}^n, f(x) = f(y) \Rightarrow x = y \oplus s,$$

where $\oplus$ is the component-wise addition (modulo 2) in $\{0,1\}^n$.

The goal is to determine the vector s.

3.1 Preliminary question

1. Show that if $s \neq 0$, then there is a unique pair $(x,y) \in \{0,1\}^n$ such that $f(x) = f(y)$.

In the Simon problem, we thus work only with functions f that are either 1-to-1 (if $s = 0$) or 2-to-1.

3.2 Mathematical formulation of the quantum algorithm

In this tutorial, we will demonstrate the quantum advantage for this problem.

1. Show that classically, the cost to determine s is of the order 2^{n-1}.

Let U_f be a quantum gate acting on $2n$ qubits such that for $|x\rangle, |w\rangle$ two n-qubit states, we have

$$U_f(|x,w\rangle) = U_f(|x\rangle \otimes |w\rangle) = |x\rangle \otimes |f(x) \oplus w\rangle.$$

In this setting, U_f is called an *oracle*.

2. Check that $U_f^{-1} = U_f$ and deduce that it indeed defines a quantum gate.

We consider the following circuit to determine the period s.

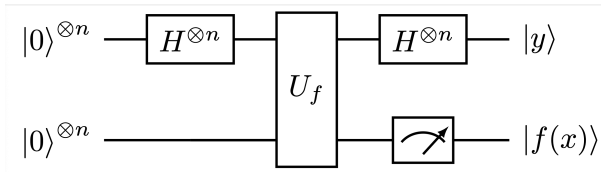

Figure 3: Simon circuit

3. We suppose that the output of the measure of the last n qubits give $|f(x)\rangle$ for some quantum state x. Show that the output $|y\rangle$ of the first n qubits is such that $y \perp s$.
4. Suppose that the circuit above is run $n+k$ times and the result of the first n qubits are stored in the vectors $(y_i)_{1 \leq i \leq n+k}$. Show that with probability at least $1 - \frac{1}{2^{k+1}}$, $\text{Span}(y_1, \dots, y_{n+k}) = s^{\perp}$.
5. Prove that the quantum algorithm exhibits a quantum advantage.