[P7] [*The Deutsch-Josza Algorithm*]

The Deutsch-Josza Algorithm is designed to exactly reveal the nature of a Boolean function f with a single query. The function $f : \{0,1\}^n \to \{0,1\}$ is assumed to be unknown (a "black box") that is either

- constant, i.e. $f(x) = f(y)$ for all $x, y \in \{0,1\}^n$, or
- balanced, i.e. $|\{x : f(x) = 0\}| = |\{x : f(x) = 1\}| = 2^{n-1}$.

Classically, determining with certainty whether f is constant or balanced may require 2^{n-1} queries (i.e. evaluations of the function f on a given input). So it may come as a surprise that a quantum circuit that requires only a single query is able to answer this question with certainty. This circuit is depicted in Figure 1 and implements the Boolean function f as a reversible gate acting on $(n+1)$ qubits via

$$B_f|x\rangle \otimes |y\rangle = |x\rangle \otimes |y \oplus f(x)\rangle, \quad \forall x \in \{0,1\}^n, \forall y \in \{0,1\}. \tag{1}$$

Here $\oplus$ denotes addition modulo 2 and for $x = (x_1, \ldots, x_n) \in \{0,1\}^n \in \{0,1\}^n$, $|x\rangle$ is a short-hand notation of $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$. In addition to that, the circuit makes heavy use of Hadamard gates which amount to

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2}$$

in the computational basis $\{|0\rangle, |1\rangle\}$ of $\mathbb{C}^2$. The aim of this exercise is to show that this circuit is indeed capable of deciding the nature of f in a single query (run).

(1) Suppose that the algorithm depicted in Figure 1 receives the n-qubit input

$$|\Psi_{\text{input}}\rangle = \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle}_{n \text{ times}} \otimes |1\rangle.$$

Determine the state $|\Psi_{t_1}\rangle$ that is obtained after applying $(n+1)$ Hadamard gates in parallel.

(2) Show that the state $|\Psi_{t_2}\rangle = B_f|\Psi_{t_1}\rangle$ then amounts to

$$|\Psi_{t_2}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \right). \tag{3}$$

Hint: Start by showing that $|0 \oplus z\rangle - |1 \oplus z\rangle = (-1)^z (|0\rangle - |1\rangle)$ is true for any $z \in \{0,1\}$ and generalize this behavior to obtain (3).

(3) Determine the circuit's final n-qubit state $|\Psi_{t_3}\rangle$ that is obtained after discarding (omitting) the final qubit and applying Hadamard transformations to the remaining n qubits.

(4) The quantum circuit is concluded by performing n single qubit measurements in the computational basis $\{|0\rangle, |1\rangle\}$. Show that the probability for obtaining only zero-outcomes equals one, if the hidden Boolean function was constant, and is zero, if the f

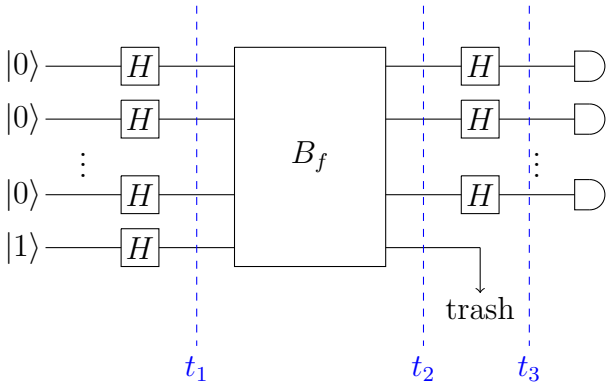

Figure 1: Circuit diagram of the Deutsch Josza Algorithm: $(n+1)$ parallel Hadamard matrices are applied to the the $(n+1)$-qubit product state $|\Psi_{\text{input}}\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$. The resulting state $|\Psi_{t_1}\rangle$ then serves as an input for the "black box circuit" B_f that encodes the action of the unknown Boolean function in a reversible way – see Eq. (1). Afterwards, the final qubit is discarded, while the other ones once more undergo a Hadamard transformation. Finally the remaining n qubits are measured in the computational basis $\{|0\rangle, |1\rangle\}$.

was balanced. Note that this result assures, that such an experiment allows to reveal the nature of f with certainty.
Hint: According to Born's rule, the probability of measuring only zeros is given by

$$\Pr(m_1 = 0, \ldots, m_n = 0) = \Big|\underbrace{\langle 0| \otimes \cdots \otimes \langle 0|}_{n \text{ times}} |\Psi_{t_3}\rangle\Big|^2.$$

(5 P.)

[P8] (Approximating circuits). The definition of the quantum Fourier transform involves the gates

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi \mathrm{i} 2^{-k}} \end{bmatrix}$$

which differ from the trivial time evolution (given by the identity matrix) only by an *exponentially small* quantity $1 - e^{2\pi \mathrm{i} 2^{-k}}$. This might be a source of concern: does a quantum algorithm require exponentially precise control? Here, we will show that this is not the case: small errors in the gates will lead only to small differences in the success probability of the algorithm. (And hence *leaving out* the R_k's for large k does not significantly alter the QFT circuit).

(1) Recall the *operator norm* of a matrix A is

$$\|A\|_\infty = \max_\phi \|A|\phi\rangle\| = \max_{\phi,\psi} \langle\psi|A|\phi\rangle,$$

where the respective maximizations are over *normalized* vectors $\|\phi\| = \|\psi\| = 1$. Show that the operator norm satisfies the *triangle inequlaity* $\|A+B\|_\infty \leq \|A\|_\infty + \|B\|_\infty$. Show that the operator norm is *unitarily invariant*: if U is a unitary, then $\|AU\|_\infty = \|UA\|_\infty = \|A\|_\infty$.

(2) Let U_1, U_2 be two ideal quantum gates. Suppose we manage to engineer V_1, V_2, which are close to the U's in the sense that $\|U_i - V_i\|_\infty \leq \epsilon$. Using the two properties established above, show that

$$\|U_2 U_1 - V_2 V_1\|_\infty \leq 2\epsilon.$$

(Of course, by induction, this implies that if a circuit consists of n gates U_i realized to within precision ϵ each, then the total error of the circuit will not exceed $n\epsilon$.)

(3) Lastly, let A be the observable used to read out the result of the computation. We assume that $\|A\|_\infty = 1$ (optional problem: convince yourself that that's true for all examples we have looked at so far). If $|\psi\rangle$ is the initial state of the computation, U the ideal unitary of the circuit, V our approximation to it, then the read-out error is

$$\left|\mathrm{tr}AU|\psi\rangle\langle\psi|U^\dagger - \mathrm{tr}AV|\psi\rangle\langle\psi|V^\dagger\right|.$$

Prove that this error is no larger than $2\|U - V\|_\infty$. (5 P.)