Exercise Set 6 (graded)
Quantum Computation

Exercise 1 *Difference(s) between Deutsch-Josza's and Simon's circuits*

Let H be a linear subspace of $\{0,1\}^n$ of dimensison $n-1$ and $f : \{0,1\}^n \to \{0,1\}$ be the function defined as

$$\begin{cases} f(x) = 0 & \text{if } x \in H \\ f(x) = 1 & \text{if } x \notin H \end{cases}$$

(a) Assume we run Deutsch-Josza's circuit with the quantum oracle U_f corresponding to the above function f (starting with the same input state $|\psi_0\rangle = |0,0,\ldots,0\rangle \otimes |1\rangle$ as in D-J's algorithm). What is/are then the possible output state(s) of the circuit, and its/their associated probability(ies)?

Consider in particular the special cases $n = 3$ and $H_1 = \text{span}\{(1,0,0),(0,1,0)\}$, as well as $n = 3$ and $H_2 = \text{span}\{(1,1,0),(0,0,1)\}$ (*Hint:* You may actually start with these examples in order to figure out what happens in the general case).

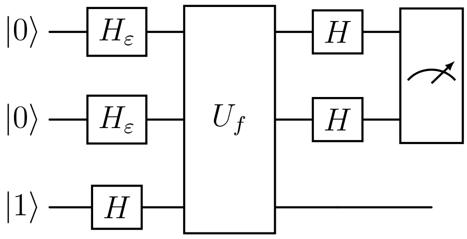
(b) What difference(s) do you observe with the output of Simon's circuit (with the same quantum oracle U_f and the input state $|\psi_0\rangle = |0,0,\ldots,0\rangle \otimes |0\rangle$)?

Exercise 2 *Outcome probabilities of Simon's algorithm*

Let H be a k-dimensional linear subspace of $\{0,1\}^n$. Compute the exact success probability of one run of Simon's algorithm. Assuming that n is fixed, for what value of $1 \leq k \leq n-1$ is this success probability the smallest / the largest? What is the asymptotic value as $n \to \infty$ of this success probability in both cases? (in one of the two cases, an approximative value suffices)

Exercise 3 *Deutsch-Josza's algorithm with noisy Hadamard gates*

Let us consider Deutsch's problem with $n = 2$. The aim of the algorithm is to decide whether $f : \{0,1\}^2 \to \{0,1\}$ is constant or balanced by using the following circuit:



where the Hadamard gates H_ε (with $0 \leq \varepsilon \leq 1$) are defined as

$$\begin{cases} H_\varepsilon |0\rangle = \sqrt{\frac{1+\varepsilon}{2}}\, |0\rangle + \sqrt{\frac{1-\varepsilon}{2}}\, |1\rangle \\ H_\varepsilon |1\rangle = \sqrt{\frac{1-\varepsilon}{2}}\, |0\rangle - \sqrt{\frac{1+\varepsilon}{2}}\, |1\rangle \end{cases}$$

(a) Verify that H_ε is unitary, for any $0 \leq \varepsilon \leq 1$.

(b) Compute the probability that the output state of the (first two qubits of the) above circuit is equal to $(0,0)$ when f is constant.

(c) In order to ensure an error probability no greater than δ, what is the (approximate) maximum value taken by the parameter ε? Check in particular the cases $\delta = 0.1$ and $\delta = 0.01$.

Exercise 4 *Implementation of Simon's algorithm* (OPTIONAL: for your interest only ;-)

In this exercise, you will implement Simon's algorithm on the IBM-Q machine (use the simulator only!) to find a hidden subspace H of codewords within the vector space $\{0,1\}^n$ of binary strings of length n.

The dimension of the hidden subspace is $k = 4$. To implement the algorithm, you are given an oracle whose function is to apply the parity check matrix P to any binary vector v of length $n = 7$, where $P \cdot v = 0$ if and only if $v \in H$, the hidden subspace. In other words, consider two vectors v_1, v_2: $P \cdot (v_1 - v_2) = 0$ iff $v_1 - v_2 \in H$.

The parity check matrix P is given by

$$P = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

(a) How many qubits does your circuit need in total?

(b) Which of those will be measured?

(c) How many shots (at least) do you need to run the circuit? In other words, how many linearly independent output vectors do you need to determine the hidden subspace? Don't forget to check that the output vectors are linearly independent!

(d) It suffices to get the basis vectors of the orthogonal subspace $H^\perp$ (you do not have to perform the Gaussian elimination to find the basis of H afterwards).

(e) To verify your results, you can check that the output binary vectors $y_1, \ldots, y_{n-k}$ after the measurement belong to the orthogonal subspace $H^\perp$. To do that, recall that P is the parity check matrix of the (7,4)-Hamming code, so all the vectors $y_1, \ldots, y_{n-k}$ you measure should be orthogonal to the matrix H which forms the basis of the hidden subspace of codewords, i.e. $\forall i : H \cdot y_i = 0$.

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$