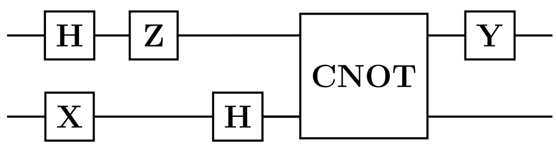
Introduction to Quantum Computer Science and Applications

Exercise Sheet 4

Exercise 1 (Inverting quantum circuits)**.** *Given a quantum circuit implementing a unitary $\mathbf{U}$, how is the quantum circuit implementing the inverse of $\mathbf{U}$, namely $\mathbf{U}^{-1}$?*

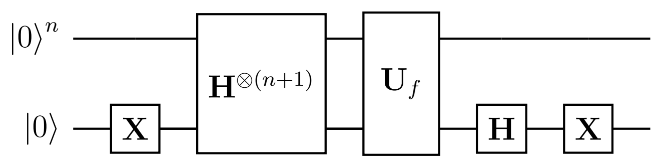
Give the circuit implementing the inverse of the unitary represented by the following circuit



Exercise 2. *Let $f : \{0,1\}^n \to \{0,1\}$. Recall that $\mathbf{U}_f$ is the following unitary,*

$$\mathbf{U}_f : |\mathbf{x}\rangle |y\rangle = |\mathbf{x}\rangle |y \oplus f(\mathbf{x})\rangle$$

Show that the output of the following circuit



is

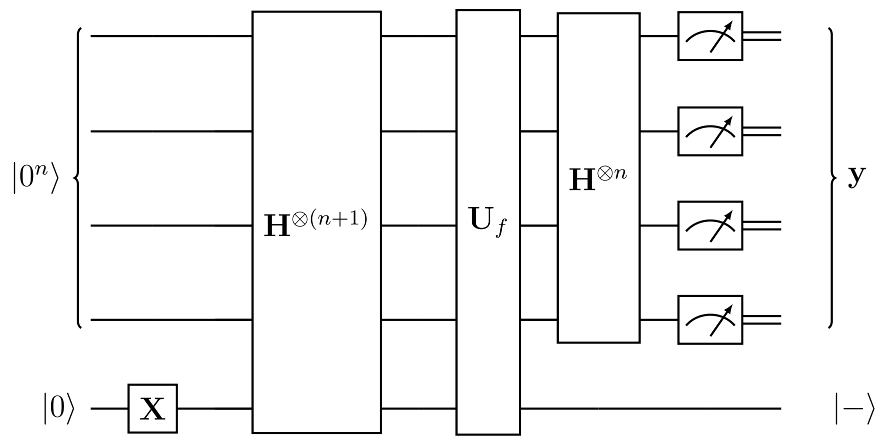
$$\frac{1}{\sqrt{2^n}} \sum_{\mathbf{x}\in\{0,1\}^n} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle |0\rangle$$

Exercise 3 (Deutsch-Jozsa and Bernstein-Vazirani algorithms)**.**

1. *In Deutsch-Jozsa's problem we are given as input a function which is either constant or balanced*[1]*. The goal is to determine if f is either constant or balanced. How many classical queries to f do we need to make the right decision with probability one?*

2. *Deutsch-Josza's quantum algorithm solves Deutsch-Josza's problem. The associated quantum circuit is given by:*

[1] It is equal to 0 for half of the possible inputs.



Show that this quantum circuit indeed solves Deutsch-Josza's problem. How many queries to f does this circuit perform? What do you conclude?

Hint: *you can use the fact that* $\sum_{\mathbf{x}\in\{0,1\}^n}(-1)^{\mathbf{x}\cdot\mathbf{z}} = \begin{cases} 0 & \textit{if } \mathbf{z}\neq 0 \\ 2^n & \textit{otherwise} \end{cases}$

3. *Let $|\psi\rangle$ the quantum state just before the final measurements. Prove that*

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

where recall that $\mathbf{x}\cdot\mathbf{y} = \sum_{i=1}^n x_i y_i \mod 2$ *for* $\mathbf{x} = x_1\ldots x_n$ *and* $\mathbf{y} = y_1\ldots y_n$.

4. *Assume our function f satisfies the following property: $\exists\mathbf{s}\in\{0,1\}^n, f(\mathbf{x}) = \mathbf{x}\cdot\mathbf{s}$. Show that the above algorithm always outputs $\mathbf{y}=\mathbf{s}$. This algorithm is known as the Bernstein-Vazirani algorithm, if we have the promise that the function f satisfies the property above, then this algorithm finds $\mathbf{s}$ with a single query to $\mathbf{U}_f$.*

Exercise 4 (Clean your workspace!)**.**

Let $\mathbf{x} = (x_0, x_1)$. Suppose that we can implement the following 1-qubit unitary

$$\mathbf{O}_{\mathbf{x},\pm} : |b\rangle \longmapsto (-1)^{x_b}\,|b\rangle$$

1. *Suppose that we run the 1-qubit circuit $\mathbf{HO}_{\mathbf{x},\pm}\mathbf{H}$ on initial state $|0\rangle$ and then measure. What is the probability distribution on the output bit, as a function of $\mathbf{x}$?*

2. *Now suppose the query leaves some workspace in a second qubit, which is initially* $|0\rangle$*:*

$$\mathbf{O}'_{\mathbf{x},\pm} : |b\rangle\,|0\rangle \longmapsto (-1)^{x_b}\,|b\rangle\,|b\rangle$$

   Suppose we just ignore the workspace and run the algorithm of Question 1. *on the first qubit with* $\mathbf{O}'_{\mathbf{x},\pm}$*, instead of* $\mathbf{O}_{\mathbf{x},\pm}$ *(and* $\mathbf{H}\otimes\mathbf{I}$ *instead of* $\mathbf{H}$*, and initial state* $|00\rangle$*). What is now the probability distribution on the output bit (*i.e.*, if we measure the first of the two bits)?*

Comment: this exercise illustrates why it's important to "clean up" (*i.e.*, set back to $|0\rangle$) workspace qubits of some subroutine before running it on a superposition of inputs: the unintended entanglement between the address and workspace registers can thwart the intended interference effects.

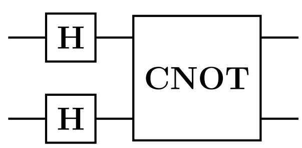
Exercise 5 (Quantum unitary that mimics a permutation)**.** *Consider a permutation* π *acting on* $\{0,1\}^n$ *such that* π *and* π^{-1} *are efficiently computable, which means that we can efficiently construct the quantum unitaries*

$$\mathbf{U}_\pi\,|\mathbf{x}\rangle\,|\mathbf{y}\rangle = |\mathbf{x}\rangle\,|\mathbf{y}\oplus\pi(\mathbf{x})\rangle \quad \text{and} \quad \mathbf{U}_{\pi^{-1}}\,|\mathbf{x}\rangle\,|\mathbf{y}\rangle = |\mathbf{x}\rangle\,\left|\mathbf{y}\oplus\pi^{-1}(\mathbf{x})\right\rangle.$$

Show how to construct the unitary $\mathbf{U}\,|\mathbf{x}\rangle = |\pi(\mathbf{x})\rangle$*, using auxiliary qubits. You can use the above unitaries as well as any elementary operations.*

Hint: *here is a construction that builds* $\mathbf{U}$ *with a single call to* $\mathbf{U}_\pi$*, a single call to* $\mathbf{U}_{\pi^{-1}}$ *and two swap gates - not necessarily in this order*

Exercise 6. *Write the unitary acting on* 2 *qubits corresponding to the following circuit in matrix form (in the* $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ *basis):*



Exercise 7 ($\star$ **Constructing reflexions over a quantum state** $\star$)**.** *Consider a* n *qubit state* $|\psi\rangle$ *and assume we have an efficiently computable unitary* $\mathbf{U}$ *such that*

$$\mathbf{U}\,|0^n\rangle = |\psi\rangle\,.$$

Our goal is to show that we can compute the reflexion $\mathbf{R}_{|\psi\rangle}$ i.e., *the unitary satisfying*

$$\mathbf{R}_{|\psi\rangle}(|\psi\rangle) = |\psi\rangle\,, \qquad \textit{and } \forall\,|\varphi\rangle \textit{ such that } |\psi\rangle \perp |\varphi\rangle\,,\ \mathbf{R}_{|\psi\rangle}(|\varphi\rangle) = -\,|\varphi\rangle$$

with one call to $\mathbf{U}$*, one call to* $\mathbf{U}^\dagger$ *and* $O(n)$*-calls to some* 2*-qubits unitaries.*

1. *Show that for all* $|\varphi\rangle$ *such that* $|\varphi\rangle \perp |\psi\rangle$*, we can write*

$$\mathbf{U}^\dagger(|\varphi\rangle) = \sum_{\substack{\mathbf{i}\in\{0,1\}^n \\ \mathbf{i}\neq 0^n}} \alpha_{\mathbf{i}}\,|\mathbf{i}\rangle\,.$$

2. *Argue, without writing the circuit, that one can efficiently compute the unitary* $\mathbf{V}$ *on* $n+1$ *qubits that satisfies*

$$\mathbf{V}(|\mathbf{x}\rangle\,|y\rangle) \rightarrow |\mathbf{x}\rangle\,|y \oplus g(\mathbf{x})\rangle$$

   where $g(\mathbf{x}) = 0$ *if and only if* $\mathbf{x} = 0^n$ *and* $g(\mathbf{x}) = 1$ *otherwise.*

3. *Construct using the previous unitaries and elementary gates the unitary* $\mathbf{W}$ *on* n *qubits with an extra auxiliary qubit such that*

$$\mathbf{W}\,|\mathbf{x}\rangle\,|0\rangle = (-1)^{g(\mathbf{x})}\,|\mathbf{x}\rangle\,|0\rangle\,.$$

   There is a construction that uses only 2 *calls to* $\mathbf{V}$ *or* $\mathbf{V}^\dagger$ *and a phase flip gate* $\mathbf{Z}$*. There is another construction that uses a single call to* $\mathbf{V}$ *and* 2 *calls to* $\mathbf{H}$ *or* $\mathbf{H}^\dagger$ *and* 2 *calls to the bit flip* $\mathbf{X}$*. Find at least one construction, can you find both?*

4. *Show how to build* $\mathbf{R}_{|\psi\rangle}$ *(with an auxiliary qubit) with* 2 *calls to* $\mathbf{U}$ *or* $\mathbf{U}^\dagger$ *and* 1 *call to* $\mathbf{W}$*.*

Exercise 8 (One-time pad)**.** *For* $\mathbf{k} \in \{0,1\}^n$*, consider the* one-time pad function*,*

$$E_{\mathbf{k}} : \mathbf{x} \in \{0,1\}^n \longrightarrow \mathbf{k} \oplus \mathbf{x} \in \{0,1\}^n$$

1. *Show that there is a quantum polynomial time algorithm querying* $\mathbf{U}_{E_{\mathbf{k}}}$ *just once that distinguishes* $\mathbf{E}_k$ *from a random function* P *of* $\{0,1\}^n$*.*

   You can admit that for a random function P *of* $\{0,1\}^n$ *we have for any* $\mathbf{y} \in \{0,1\}^n$*,*

$$\frac{1}{2^{2n}} \sharp \left\{\mathbf{x} \in \{0,1\}^n \,:\, P(\mathbf{x}) \oplus \mathbf{x} = \mathbf{y}\right\}^2 \approx \frac{1}{2^{n-1}}$$

   where the $\approx$ *stands for the expectation.*

2. *What property did you crucially use?*