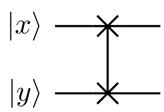
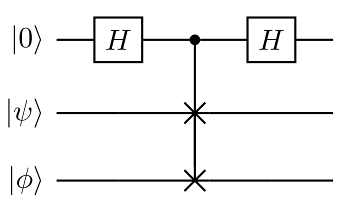
# Intro to Quantum Computing 2021

# Exercise Set III

**Exercise 1.** *Recall the SWAP transformation which, for* $x, y \in \{0, 1\}$, *performs the map* $|x\rangle|y\rangle \to |y\rangle|x\rangle$ *and is denoted in a quantum circuit by*



1. *Write down the matrix corresponding to SWAP with respect to the standard computational basis* $|0\rangle, |1\rangle$ *and show that SWAP is unitary.*
2. *Show that, for any single Qbit states* $|\psi\rangle, |\phi\rangle$ *we have that* $\mathrm{SWAP}(|\psi\rangle|\phi\rangle) = |\phi\rangle|\psi\rangle$.
3. *Consider the following quantum circuit:*



*where* $|\psi\rangle, |\phi\rangle$ *are any single Qbit states. What is the probability that the result of measuring the first Qbit is 1 in each of these two cases:*

(a) $|\psi\rangle = |0\rangle$ *and* $|\phi\rangle = |1\rangle$,

(b) $|\psi\rangle = |\phi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.

**Exercise 2.** *Construct a quantum circuit that computer the parity of three Qbits. In particular, construct a quantum circuit on* four *Qbits that maps the state* $|y_1\rangle|y_2\rangle|y_3\rangle|0\rangle$ *to the state* $|y_1\rangle|y_2\rangle|y_3\rangle|y_1 \oplus y_2 \oplus y_3\rangle$.

*You might need to consider appropriate control gates.*

**Exercise 3.** *Show that a* $CZ$ *(controlled* $Z$*) gate can be implemented using a* $CNOT$ *gate and Hadamard gates. Write down the corresponding circuit.*

**Exercise 4.** *Consider Grover's problem in the 4-element set* $\{0, 1\}^2$, *where there is a unique marked element, say* $x_0 = 10$.

1. *Write down the matrix for the oracle operation $U_f$ for this value of $x_0$ with respect to the standard computational basis $\{|0\rangle, |1\rangle\}$.*
2. *Provide the matrix for the* diffusion *(inversion about the mean) in Grover's algorithm for $N = 4$, again with respect to the standard computational basis.*
3. *Multiply out all the matrices and vectors occurring for one step of Grover's algorithm, to verify the claim that the algorithm finds the marked element with certainty.*
4. *What is the final state if one more step is made? What is the probability that the marked element is found if this state is measured?*

**Exercise 5.** *Answer the following:*

1. *Show that*
$$H^{\otimes n}\big(|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I\big)H^{\otimes n} = 2|u\rangle\langle u| - I,$$
*where*
$$u = H^{\otimes n}|0^{\otimes n}\rangle = \frac{1}{\sqrt{n}} \sum_{x\in\{0,1\}^n} |x\rangle.$$
2. *Show that the oracle in Grover's algorithm (that performs that* phase shift *for the marked element $x^*$) can be written as*
$$R = I - |x^*\rangle\langle x^*|.$$
3. *Show that the above operator $R$ is unitary. Show also that $R^2$ is also unitary.*
4. *Imagine we have 8 items, two of which, say $x_1, x_2$ are marked (i.e., $f(x_1) = f(x_2) = 1$ and $f(y) = 0$, for all $y \neq x_1, x_2$). Show that* one *oracle call to $R$ is enough to solve the problem of finding an element $x^* : f(x^*) = 1$ (i.e., just one run of Grover's iteration).* Hint: after just one iteration, what is the overlap of the state of Grover's algorithm with the state $|S\rangle$ which corresponds to the uniform superposition of all marked elements in $S$?