Exercise Set 6: Solution
Quantum Computation

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

(a) First observe that $\{0,1\}^n$ is divided into two sets: H and $H \oplus b$, where b is any vector in $\{0,1\}^n$ such that $b \notin H$ (this is because H is a $(n-1)$-dimensional linear subspace of H). Before the final measurement of the first n qubits, the output of the algorithm is

$$|\psi_4\rangle = \frac{1}{2^n} \sum_{x\in\{0,1\}^n} \sum_{y\in\{0,1\}^n} (-1)^{f(x)+x\cdot y} |y\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$$
$$= \sum_{y\in\{0,1\}^n} \left(\frac{1}{2^n} \sum_{x\in H} (-1)^{x\cdot y} - \sum_{x\in H\oplus b} (-1)^{x\cdot y} \right) |y\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$$
$$= \sum_{y\in\{0,1\}^n} \left(\frac{1}{2^n} \sum_{x\in H} (-1)^{x\cdot y}(1-(-1)^{b\cdot y}) \right) |y\rangle \otimes \frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big)$$

So the output probability of a given state $|y\rangle$ is

$$|\alpha_y|^2 = \left| \frac{1}{2^n} \sum_{x\in H} (-1)^{x\cdot y} \cdot (1-(-1)^{b\cdot y}) \right|^2 = \left| \frac{1}{2^{n-1}} \sum_{x\in H} (-1)^{x\cdot y} \right|^2 \cdot \left| \frac{(1-(-1)^{b\cdot y})}{2} \right|^2$$

Because of the first factor in this final expression, the probability is non-zero *if and only if* $y \in H^\perp$. Indeed, if $y \in H^\perp$, then $x \cdot y = 0$ for every $x \in$H, so $\sum_{x\in H} (-1)^{x\cdot y} = |H|$. If on the other hand, $y \notin H^\perp$, then there exist $x_0 \in H$ such that $x_0 \cdot y = 1$. So in this case, by the fact that H is a subgroup,

$$\sum_{x\in H} (-1)^{x\cdot y} = \sum_{x\in H} (-1)^{(x+x_0)\cdot y} = \sum_{x\in H} (-1)^{x\cdot y} \cdot (-1)^{x_0\cdot y} = -\sum_{x\in H} (-1)^{x\cdot y}$$

so the sum is equal to 0 in this case, which proves the above claim.

Finally, $H^\perp$ is one-dimensional and contains therefore only two elements, the vector $y = 0$ and another non-zero vector. Therefore the output cannot be equal to $y = 0$, as this would imply $1 - (-1)^{b\cdot y} = 1 - 1 = 0$, so the only possible output is the non-zero vector of $H^\perp$, which occurs with probability 1.

Particular cases:

- $n = 3$ and $H_1 = \text{span}\{(1,0,0),(0,1,0)\}$: in this case, the output is $y = (0,0,1)$ with probability 1.

- $n = 3$ and $H_2 = \text{span}\{(1,1,0),(0,0,1)\}$: in this case, the output is $y = (1,1,0)$ with probability 1.

(b) Using Simon's algorithm with the same function f would lead to the same output as above, or the the output $y = 0$, with equal probabilities $1/2$.

Exercise 2 *Outcome probabilities of Simon's algorithm*

After one run of Simon's circuit, the success probability of the algorithm is equal to

$$\left(1-\frac{1}{2^{n-k}}\right)\left(1-\frac{1}{2^{n-k-1}}\right)\cdots\left(1-\frac{1}{2}\right)=\prod_{i=1}^{n-k}\left(1-\frac{1}{2^i}\right)$$

This probability is clearly the largest for $k=n-1$, in which case its value is equal to $1/2$ for all values of n (and therefore also asymptotically); it is on the contrary the smallest for $k=1$, in which case it converges to

$$\prod_{i=1}^{n-1}\left(1-\frac{1}{2^i}\right)\underset{n\to\infty}{\rightarrow}\prod_{i\geq 1}\left(1-\frac{1}{2^i}\right)\simeq 0.28$$

also known as Euler's function $\phi(q)=\prod_{i\geq 1}(1-q^i)$ evaluated in $q=1/2$.

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

(a) First observe that $H_\varepsilon^\dagger = H_\varepsilon$, so

$$H_\varepsilon H_\varepsilon^\dagger = H_\varepsilon^2 = \frac{1}{2}\begin{pmatrix}\sqrt{1+\varepsilon} & \sqrt{1-\varepsilon}\\ \sqrt{1-\varepsilon} & -\sqrt{1+\varepsilon}\end{pmatrix}^2=\frac{1}{2}\begin{pmatrix}1+\varepsilon+1-\varepsilon & 0\\ 0 & 1-\varepsilon+1+\varepsilon\end{pmatrix}=I$$

(b) The state of the system after the first passage of the Hadamard gates is given by

$$\begin{aligned}|\psi_1\rangle &= H_\varepsilon|0\rangle\otimes H_\varepsilon|0\rangle\otimes H|1\rangle\\ &=\frac{1}{2}\left(\sqrt{1+\varepsilon}\,|0\rangle+\sqrt{1-\varepsilon}\,|1\rangle\right)\otimes\left(\sqrt{1+\varepsilon}\,|0\rangle+\sqrt{1-\varepsilon}\,|1\rangle\right)\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}\\ &=\frac{1}{2}\left((1+\varepsilon)|00\rangle-\sqrt{1-\varepsilon^2}\,(|01\rangle+|10\rangle)+(1-\varepsilon)|11\rangle\right)\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}\end{aligned}$$

Let us write this state as

$$|\psi_1\rangle=\sum_{x\in\{0,1\}^2}\beta_x|x\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

where $\beta_{00}=\frac{1+\varepsilon}{2}$, $\beta_{01}=\beta_{10}=\frac{\sqrt{1-\varepsilon^2}}{2}$ and $\beta_{11}=\frac{1-\varepsilon}{2}$. Then the output of the circuit (before the measurement) is given by

$$|\psi_4\rangle=\frac{1}{2}\sum_{y\in\{0,1\}^2}\left(\sum_{x\in\{0,1\}^2}\beta_x(-1)^{f(x)+x\cdot y}\right)|y\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

So the probability that the output state is $|00\rangle$ when f is constant is given by

$$|\alpha_{00}|^2=\left(\frac{(1+\varepsilon)+2\sqrt{1-\varepsilon^2}+(1-\varepsilon)}{4}\right)^2=\left(\frac{1+\sqrt{1-\varepsilon^2}}{2}\right)^2$$

(c) From the above expression, using successively the approximations $\sqrt{1-x} \simeq 1 - \frac{x}{2}$ and $(1-x)^2 \simeq 1 - 2x$, both valid for x small, we obtain

$$|\alpha_{00}|^2 \simeq \left(1 - \frac{\varepsilon^2}{4}\right)^2 \simeq 1 - \frac{\varepsilon^2}{2}$$

So the error probability $\delta \simeq \frac{\varepsilon^2}{2}$. In order to ensure $\delta \leq 0.1$, ε should be taken less than 0.33; for $\delta \leq 0.01$, $\varepsilon \leq 0.14$ is needed.

Exercise 4 *Implementation of Simon's algorithm* (optional)

See the attached Jupyter Notebook