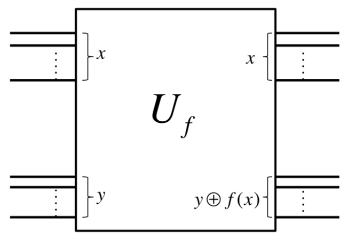
Name: ______________________________

Entry number: ________________________

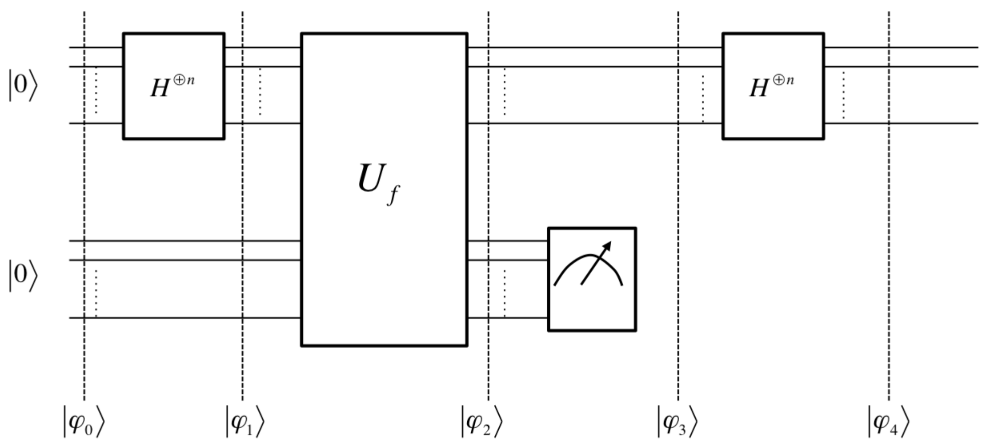
There are 2 questions for a total of 20 points.

---

1. (10 points) Given a 4-to-1 function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ such that $f(x) = f(x \oplus a) = f(x \oplus b) = f(x \oplus a \oplus b)$ for some $a, b \neq 0^n$ and $a \neq b$. Give an efficient Quantum algorithm for finding a and b. Discuss running time. You may use the following Quantum gate:



Solution: The circuit for is the same as the circuit for the Simon's problem.



The quantum states are given as below:

$$
\begin{aligned}
|\psi_0\rangle &= |0\rangle\,|0\rangle \\
|\psi_1\rangle &= \frac{1}{2^{n/2}} \sum_x |x\rangle\,|0\rangle \\
|\psi_2\rangle &= \frac{1}{2^{n/2}} \sum_x |x\rangle\,|f(x)\rangle \\
|\psi_3\rangle &= \frac{1}{2}\left(|x\rangle + |x \oplus a\rangle + |x \oplus b\rangle + |x \oplus a \oplus b\rangle\right) \quad \text{(for some } x\text{)} \\
|\psi_4\rangle &= \frac{1}{2} \cdot \frac{1}{2^{n/2}} \sum_z \left((-1)^{z \cdot x} + (-1)^{z \cdot (a \oplus x)} + (-1)^{z \cdot (b \oplus x)} + (-1)^{z \cdot (a \oplus b \oplus x)}\right) |z\rangle \\
&= \frac{1}{2} \cdot \frac{1}{2^{n/2}} \sum_z (-1)^{z \cdot x} \left[1 + (-1)^{z \cdot a} + (-1)^{z \cdot b} + (-1)^{z \cdot a}(-1)^{z \cdot b}\right] |z\rangle
\end{aligned}
$$

So, a measurement performed on state $|\psi_4\rangle$ uniformly samples an element from the set

$$\{z|(z \cdot a) = 0 \text{ AND } (z \cdot b) = 0\}.$$

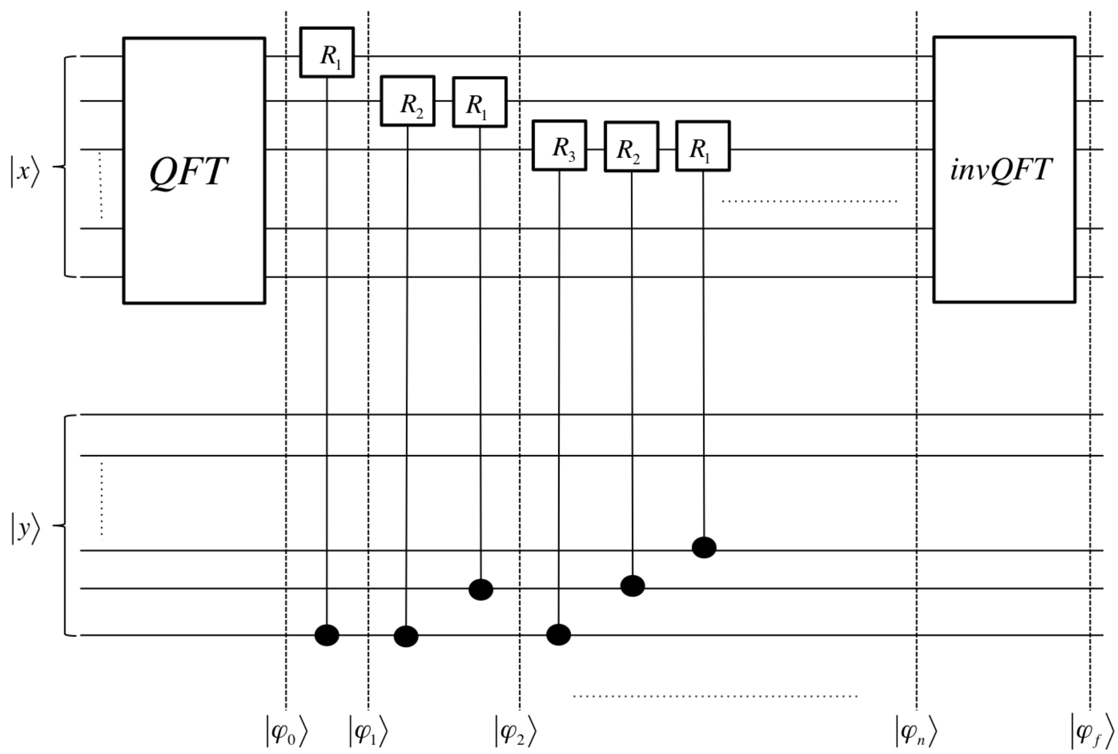
As we have seen from the discussion in the class on the Simon's problem that $O(n)$ repetitions are sufficient to find a given that each time an element from the set $\{z|(z \cdot a) = 0\}$ is uniformly sampled. The same arguments can be extended to show that $O(n)$ samples are sufficient to obtain both a and b.

2. (10 points) Suppose you are given the following quantum gates:

   1. $\texttt{QFT}_n$: n-qubit QFT
   2. $\texttt{InvQFT}_n$: n-qubit inverse QFT
   3. $R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$ for $k = 1, ..., n$.

   Given two n-qubit registers that are initialized to $|x\rangle$ and $|y\rangle$ respectively, describe how you would compute $|(x + y) \ (mod\ 2^n)\rangle$ using just the gates given above. You may also use the controlled operations.

Solution: Here is the circuit for the problem:



Let $z = (x + y)\ (mod\ 2^n)$. The intermediate states explain the procedure:

$$
\begin{aligned}
|\psi_0\rangle &= \left(\frac{|0\rangle + e^{(2\pi i)[0.x_n]}\,|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{(2\pi i)[0.x_{n-1}x_n]}\,|1\rangle}{\sqrt{2}}\right)...\left(\frac{|0\rangle + e^{(2\pi i)[0.x_1...x_n]}\,|1\rangle}{\sqrt{2}}\right)\\
|\psi_1\rangle &= \left(\frac{|0\rangle + e^{(2\pi i)[0.x_n+0.y_n]}\,|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{(2\pi i)[0.x_{n-1}x_n]}\,|1\rangle}{\sqrt{2}}\right)...\left(\frac{|0\rangle + e^{(2\pi i)[0.x_1...x_n]}\,|1\rangle}{\sqrt{2}}\right)\\
&= \left(\frac{|0\rangle + e^{(2\pi i)[0.z_n]}\,|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{(2\pi i)[0.x_{n-1}x_n]}\,|1\rangle}{\sqrt{2}}\right)...\left(\frac{|0\rangle + e^{(2\pi i)[0.x_1...x_n]}\,|1\rangle}{\sqrt{2}}\right)\\
|\psi_2\rangle &= \left(\frac{|0\rangle + e^{(2\pi i)[0.z_n]}\,|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{(2\pi i)[0.z_{n-1}z_n]}\,|1\rangle}{\sqrt{2}}\right)...\left(\frac{|0\rangle + e^{(2\pi i)[0.x_1...x_n]}\,|1\rangle}{\sqrt{2}}\right)\\
|\psi_n\rangle &= \left(\frac{|0\rangle + e^{(2\pi i)[0.z_n]}\,|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + e^{(2\pi i)[0.z_{n-1}z_n]}\,|1\rangle}{\sqrt{2}}\right)...\left(\frac{|0\rangle + e^{(2\pi i)[0.z_1...z_n]}\,|1\rangle}{\sqrt{2}}\right)\\
|\psi_f\rangle &= |z\rangle
\end{aligned}
$$