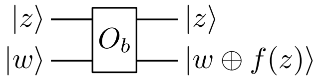
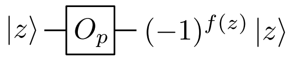
Exercises 1: QFT, phase estimation and Shor's algorithm

Lecturer: Simon Apers (apers@irif.fr)

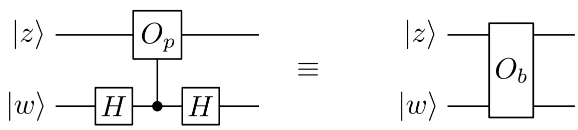
Exercise 1 (Oracles)**.** For accessing a function $f : \{0,1\}^n \to \{0,1\}$ with a quantum circuit, we use a *bit oracle* O_b or a *phase oracle* O_p. For $z \in \{0,1\}^n$ and $w \in \{0,1\}$, these are defined as follows:



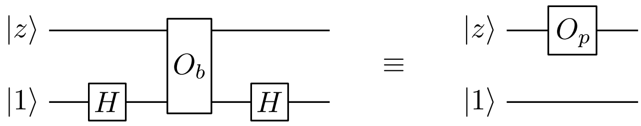


We can show that both oracles are equivalent in a sense.

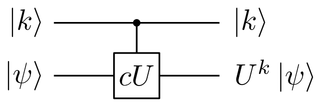
- Show that the phase oracle can simulate the bit oracle:



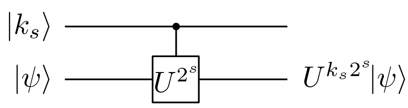
- Show that the bit oracle can simulate the phase oracle:



Exercise 2 (Controlled unitary)**.** Recall the controlled unitary gate:

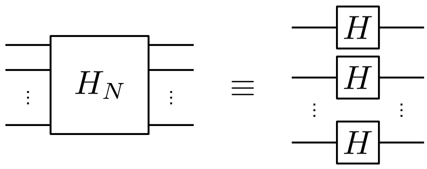


where $k = \sum_{j=0}^{n-1} k_j 2^j$ is an n-bit integer. Expand this gate into more elementary gates of the form



for $k_s \in \{0,1\}$ and $s \in \{0,1,\ldots,n-1\}$.

Exercise 3 (Hadamard transform)**.** A variation on the quantum Fourier transform is the Hadamard transform H_N for $N = 2^n$. It is defined by $H_N = H^{\otimes n}$, which corresponds to the circuit

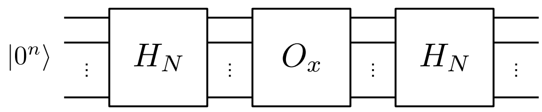


- What is $H_N \left|0^n\right\rangle$ equal to?
- Let $k = \sum_{j=0}^{n-1} k_j 2^j$. What is $H_N \left|k\right\rangle = H_N \left|k_0 \dots k_{n-1}\right\rangle$ equal to?
  (Hint: Use the inner product $x \cdot k = \sum_\ell x_\ell k_\ell$, and use that $H \left|k_\ell\right\rangle = \frac{1}{\sqrt{2}} \sum_{x_\ell=0}^{1} (-1)^{x_\ell k_\ell} \left|x_\ell\right\rangle$.)

Exercise 4 (Bernstein-Vazirani algorithm)**.** Let $N = 2^n$. Consider a function $f : \{0,1\}^n \to \{0,1\}$ that is determined by some hidden string $a \in \{0,1\}^n$ in the following way:

$$f(x) = (x \cdot a) \pmod 2.$$

We can access the function through the phase oracle $O_x \left|x\right\rangle = (-1)^{f(x)} \left|x\right\rangle$. What is the output of the following circuit?



Exercise 5 (Fourier analysis)**.** Consider natural numbers q, m, r, s such that $q = mr$ and $s < r$. Prove the following critical identity in Shor's algorithm for period finding:

$$\frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} \left|s + jr\right\rangle \quad \overset{F_q^\dagger}{\mapsto} \quad \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} \omega_q^{-s\ell m} \left|\ell m\right\rangle,$$