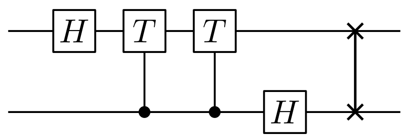
**Quantum algorithms 1** **April 2023**

# Circuits, QFT, Grover: exercises

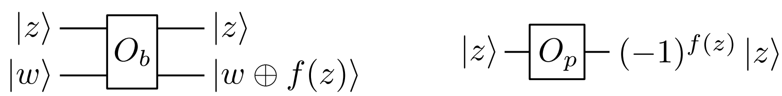
*Lecturer: Simon Apers (apers@irif.fr)*

**Exercise 1** (QFT)**.** What does $F_2$, the QFT on 1 qubit, correspond to? Consider the following circuit, where the last operation denotes swapping of the two qubits.



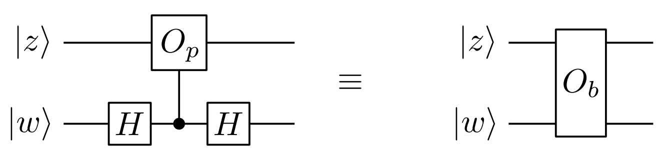

Show that this circuit corresponds to $F_4$, the QFT on 2 qubits.

**Exercise 2** (Oracles)**.** We described a bit oracle $O_b$ and a phase oracle $O_p$ for accessing a function $f : \{0,1\}^n \to \{0,1\}$. They are defined as follows, with $z \in \{0,1\}^n$ and $w \in \{0,1\}$:

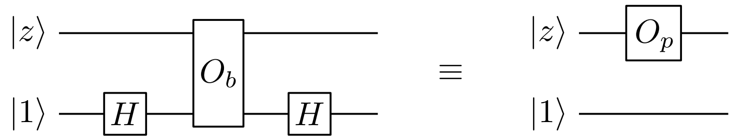



We can show that both oracles are equivalent in a sense.

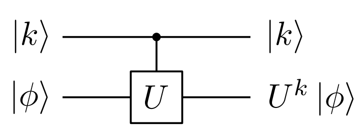
- Show that the phase oracle can simulate the bit oracle:



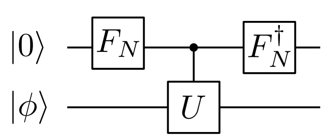

- Show that the bit oracle can simulate the phase oracle:




**Exercise 3** (Quantum phase estimation)**.** Assume access to a unitary $U$ and eigenvector $|\phi\rangle$ such that $U|\phi\rangle = e^{2\pi i\theta}|\phi\rangle$ for some $\theta \in [0,1)$. To avoid approximation issues, we assume that $N\theta$ is an integer for some $N = 2^n$. Consider the controlled version of $U$, represented by the following circuit:




where now $k \in \{0,1,\ldots,N-1\}$. The circuit for quantum phase estimation is the following:



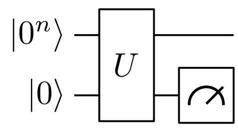

Show that we can learn $\theta$ from the output of this circuit.

**Exercise 4** (Amplitude amplification)**.** A useful variation on Grover's algorithm is called *amplitude amplification*. Assume that we have access to a unitary $U$ such that

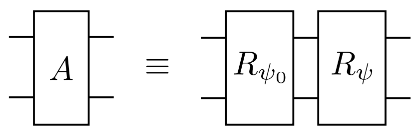
$$U\,|0^n\rangle\,|0\rangle = |\psi\rangle = \sqrt{p}\,|\psi_1\rangle\,|1\rangle + \sqrt{1-p}\,|\psi_0\rangle\,|0\rangle\,,$$

and we would like to prepare the "marked" state $|\psi_1\rangle$.

- The following circuit presents a simple solution. What is its success probability?

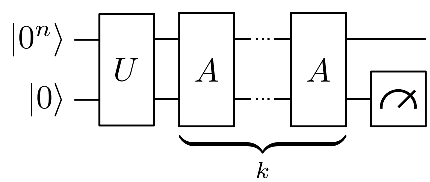



Amplitude amplification improves on this. Consider the amplitude amplification operator:




with reflections $R_\psi = 2\,|\psi\rangle\,\langle\psi| - I$ and $R_{\psi_0} = 2\,|\psi_0, 0\rangle\,\langle\psi_0, 0| - I$.

- What is the success probability of the following circuit?




**Exercise 5** (Quantum approximate counting)**.** Check that the amplitude amplification operator $A$ has eigenvectors and corresponding eigenvalues

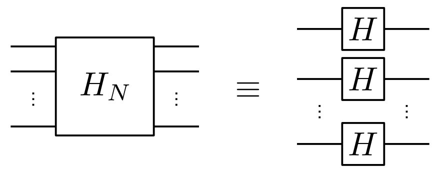
$$|\psi_\pm\rangle = \frac{|\psi_1, 1\rangle \pm i\,|\psi_0, 0\rangle}{\sqrt{2}}, \qquad \lambda_\pm = e^{\pm 2i\theta},$$

with $\theta$ such that $\sin(\theta) = \sqrt{p}$. Use quantum phase estimation on the initial state

$$|\psi\rangle = \frac{-i}{\sqrt{2}}(e^{i\theta}\,|\psi_+\rangle - e^{-i\theta}\,|\psi_-\rangle).$$

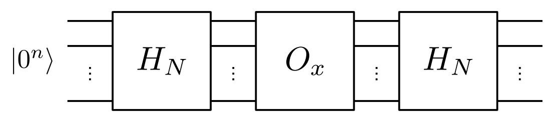
to estimate $\theta$ (and hence $p$).

**Exercise 6** (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?
- What is $H_N \left|k\right\rangle = H_N \left|k_1 \ldots k_n\right\rangle$ equal to? Use the inner product $j \cdot k = \sum_\ell j_\ell k_\ell$.[1]

**Exercise 7** (Bernstein-Vazirani algorithm)**.** Consider a string $x \in \{0,1\}^N$, for $N = 2^n$, that is determined by some unknown $a \in \{0,1\}^n$ such that $x_i = (i \cdot a) \pmod 2$. We can access the string through a "phase oracle" $O_x \left|i\right\rangle = (-1)^{x_i} \left|i\right\rangle$. What is the output of the following circuit?




**Exercise 8** (Factoring reduction (optional))**.** Here we walk through Shor's reduction from factoring to period finding. Recall that we are given an $n$-bit integer $N$ such that $2^{n-1} \leq N < 2^n$, and we wish to find a (nontrivial) factor of $N$. Without loss of generality, we can assume that $N$ is odd and not a prime power. Why?[2]

Now pick $x \in \{2, \ldots, N-1\}$ uniformly at random. If $\gcd(N, x) > 1$ then we can run Euclid's algorithm to find a factor. Hence, assume that $N$ and $x$ are coprime, and consider the series

$$x^0 = 1 \pmod N, \qquad x \pmod N, \qquad x^2 \pmod N, \qquad \ldots$$

Since $N$ and $x$ are coprime, there does not exist $s$ such that $x^s = 0 \pmod N$. Show that this implies that the series must have a period $r \leq N$ for which $x^r = 1 \pmod N$. It is precisely this factor that is calculated using quantum period finding.

One can show (not in this exercise!) that, with probability at least $1/2$ over the choice of $x$, the period $r$ will be even and both $x^{r/2} + 1$ and $x^{r/2} - 1$ are not multiples of $N$. Use $x^r = 1 \pmod N$ to show that this implies that both $x^{r/2} + 1$ and $x^{r/2} - 1$ must share a (nontrivial) factor with $N$. Once we computed $r$, we can then find these factors by computing $\gcd(x^{r/2} \pm 1, N)$.

[1] Hint: show that $H \left|k_\ell\right\rangle = \frac{1}{\sqrt{2}} \sum_{j_\ell=0}^{1} (-1)^{j_\ell k_\ell} \left|j_\ell\right\rangle$.

[2] Hint: if $N = p^k$ for some prime $p \geq 2$ then necessarily $k \leq n$.