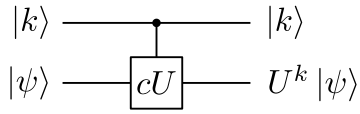
AQAlg: Advanced Quantum Algorithms **2022 - 2023**

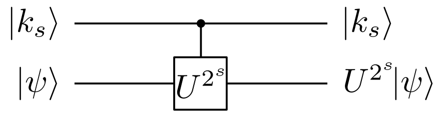
Exercises 1: QFT, phase estimation and Shor's algorithm

Lecturer: Simon Apers

Exercise 1 (Controlled unitary)**.** Recall the controlled unitary gate:

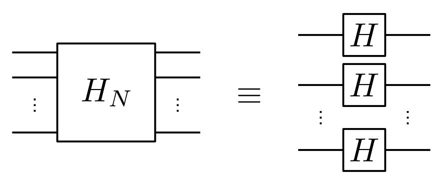


where $k = k_1 \dots k_n$ is an n-bit integer. Expand this gate into more elementary gates of the form



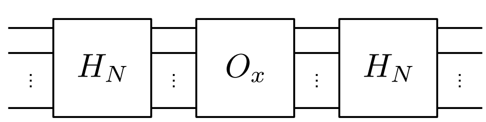
for $k_s \in \{0, 1\}$ and $s \in \{0, 1, \dots, n-1\}$.

Exercise 2 (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 $H_N\,|0\rangle^n$ equal to?
- What is $H_N\,|k\rangle = H_N\,|k_1 \dots k_n\rangle$ equal to? Use the inner product $j \cdot k = \sum_\ell j_\ell k_\ell$.[1]

Exercise 3 (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" $O_x\,|i\rangle = (-1)^{x_i}\,|i\rangle$. Turn usual oracle into phase oracle? What is the output of the following circuit?



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

Exercise 4 (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 $\gcd(x^{r/2} \pm 1, N)$.

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