AQAlg: Advanced Quantum Algorithms **2023 - 2024**

Exercise 2: Grover's algorithm and lower bounds

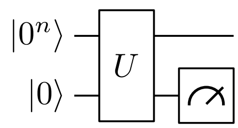
Lecturer: Simon Apers (apers@irif.fr)

Exercise 1 (Amplitude amplification)**.** A useful variation on Grover's algorithm is called *amplitude amplification*. Assume that we have access to a unitary U (and its inverse $U^\dagger$) such that

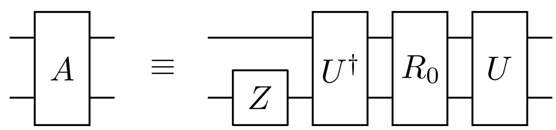
$$U|0^n\rangle|0\rangle = |\psi\rangle = \sqrt{p}\,|\psi_1\rangle|1\rangle + \sqrt{1-p}\,|\psi_0\rangle|0\rangle\,,$$

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

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

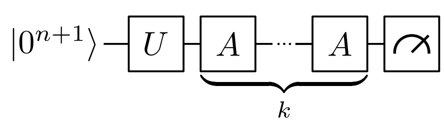


Amplitude amplification improves on this. Consider the amplitude amplification operator:



- When applied to the initial state $|\psi\rangle$, show that this circuit corresponds to a product of a reflection around $|\psi_0\rangle|0\rangle$ and a reflection around $|\psi\rangle$.

- What is the success probability of the following circuit?



Exercise 2 (Quantum approximate counting)**.** Check that the Grover operator G has eigenvectors and corresponding eigenvalues

$$|\psi_\pm\rangle = \frac{|u_1\rangle \pm i\,|u_0\rangle}{\sqrt{2}}, \qquad \lambda_\pm = e^{\pm 2i\theta}.$$

Use quantum phase estimation on the initial state

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

to estimate θ (and hence t/N).

Exercise 3 (Multilinear polynomials)**.** Show that any function $f : \{0,1\}^N \to \mathbb{C}$ has a unique representation as a multilinear polynomial of degree at most N.

Exercise 4 (Symmetric functions)**.** A function $\{0,1\}^N \to \mathbb{C}$ is called a *symmetric* function if $f(x)$ only depends on the Hamming weight $|x|$ (i.e., there exists a function $\bar{f}$ such that $f(x) = \bar{f}(|x|)$). Examples are the OR-function and the PARITY-function. Through a symmetrization argument, one can show that $\deg(f) = \deg(\bar{f})$ and $\widetilde{\deg}(f) = \widetilde{\deg}(\bar{f})$.

- If f is the PARITY-function on N bits, show that $\deg(\bar{f}) \geq N$. This implies that any zero-error quantum algorithm for PARITY must make $N/2$ quantum queries.

- If f is the PARITY-function on N bits, show that $\widetilde{\deg}(\bar{f}) \geq N$. This implies that even a bounded-error quantum algorithm for PARITY must make $N/2$ quantum queries.

Exercise 5 (Soufflé problem (optional))**.** A caveat of Grover's algorithm is the so-called "soufflé problem": doing too many iterations will again decrease the success probability $\sin^2((2k+1)\theta)$. This suggests that we need careful knowledge of t/N before running the algorithm. However, a simple variation on Grover's algorithm avoids this problem:

1. Let $c = 6/5$ and $k = 0$.
2. Pick $\ell \in \{0, 1, 2, \ldots, \lceil c^k - 1 \rceil\}$ uniformly at random. Run ℓ Grover iterations on the initial state $\frac{1}{\sqrt{N}} \sum_{i=1}^N |i\rangle$.
3. Measure the state. If this does not return a marked element, let $k = k + 1$ and go to step 2.

Show that, if there are $t > 0$ solutions, this algorithm has an expected runtime $O(\sqrt{N/t})$.[1]

[1]Hint: you can use that $\frac{1}{c^k} \sum_{\ell=0}^{c^k-1} \sin^2((2\ell+1)\theta) \geq \frac{1}{4}$ when $c^k \geq \frac{1}{|\sin(2\theta)|}$.