Exercise 9 – Grover's algorithm

Suppose we whish to search through a search space of N elements. Rather than to search the elements directly, we concentrate on the *index* to those elements, which is just a number in the range 0 to $N-1$. We assume that N is a power of 2, $N = 2^n$, and that the search problem has exactly one solution.

The Grover's algorithm is summarized as follows:

1. Prepare the initial state $|0\rangle^{\otimes n}$.
2. Apply the Hadamard transform to all qubits:
$$|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} \tag{1}$$
3. Apply the Grover iteration $\mathcal{G}$ approximately $R \approx \frac{\pi}{4}\sqrt{N}$ times, where
$$\mathcal{G} = (2|\psi\rangle\langle\psi| - \mathbb{1})\,\mathcal{O}, \tag{2}$$
and $\mathcal{O}$ is a quantum oracle as described in problem 1.
4. Measure the register x_0.

Problem 1 – Quantum oracle

Suppose we are supplied with a quantum oracle. More precisely, the oracle is a unitary operator $\mathcal{O}$, defined by its action on the computational basis:

$$|x\rangle |q\rangle \stackrel{\mathcal{O}}{\to} |x\rangle |q \oplus f(x)\rangle\,, \tag{3}$$

where $|x\rangle$ is the index register, $|q\rangle$ is the oracle qubit, $\oplus$ denotes addition modulo 2, and $f(x) = 1$ if x is a solution to the search problem, and $f(x) = 0$ if x is not a solution to the search problem.

a) Calculate the action of the oracle on an element of the search space if the oracle qubit was originally in the state $(|0\rangle - |1\rangle)/\sqrt{2}$.

b) Show that the state of the oracle qubit is not changed.

c) Show that the oracle marks the solution to the search problem by shifting the phase of the solution.

Problem 2 – Grover's algorithm

a) Consider the normalized states

$$|\alpha\rangle \equiv \frac{1}{\sqrt{N-1}} \sum_{x, x\neq\beta} |x\rangle\,, \qquad |\beta\rangle\,, \tag{4}$$

where β is the solution to the search problem, and

$$|\psi\rangle = \sqrt{\frac{N-1}{N}}\,|\alpha\rangle + \frac{1}{\sqrt{N}}\,|\beta\rangle\,. \tag{5}$$

Show that in the $|\alpha\rangle$, $|\beta\rangle$ basis, we may write the Grover iteration as

$$\mathcal{G} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}. \tag{6}$$

b) Calculate $\mathcal{G}^k\,|\psi\rangle$.

c) Show that the Grover iteration has to be repeated approximately $R \approx \frac{\pi}{4}\sqrt{N}$ times for $N \gg 1$.

d) What is the probability that the algorithm succeeds for $N = 8$, $N = 128$, and $N = 1024$?

e) What is the minimum, maximum and average number of comparisons needed by a classical linear search? What is the complexity of this algorithm?

f) What is the complexity to search a sorted list?