In this exercise sheet we will prove two things: Grover's search algorithm for the unstructured search is quadratically better than any classical algorithm; and no quantum algorithm can perform the search significantly faster than Grover's algorithm, i.e. Grover is optimal.

Exercise 1. *Warm-up: classical query complexity for unstructured search*

As for the 'quantum data base search' discussed in the lecture we consider the problem of the 'classical data base search' in the following form:

> Given an oracle O_f for some function $f : \{0,1\}^n \to \{0,1\}$ and assuming we are promised that exactly one input $x = w$ is such that $f(w) = 1$, find w, i.e.
>
> $$f(x) = \begin{cases} 1, & \text{if } x = w, \\ 0, & \text{otherwise.} \end{cases} \tag{1}$$

The name 'unstructured search' says that there is no inherent structure in the data one could make use of to accelerate the algorithm. In complexity theory it is often asked what is the minimal number of queries to an oracle necessary to achieve a certain task – this is called the query complexity.

(a) If we are interested in a deterministic classical algorithm determining w, how often does this algorithm have to query the oracle in the worst case? Be precise in the argumentation.

(b) Assume we consider algorithms whose output is w only with success probability p. What is the worst case number of queries?

(c) Conclude that a classical algorithm solving the search problem has to consult the oracle at least $\Omega(N)$ times[1].

Exercise 2. *Optimality of Grover's search algorithm in quantum computation*

We have seen in the lecture that Grover's search algorithm consults the oracle only $O(\sqrt{N})$ times[2] ($N = 2^n$). In this exercise we show that no quantum algorithm can perform this task using fewer than $\Omega(\sqrt{N})$ queries, hence Grover's algorithm is optimal. For simplicity we assume that there is a unique solution. The oracle is then described by the unitary operation $\tilde{U}_w = \mathbb{1} - 2|w\rangle\langle w|$, as encountered in the lecture[3].

Suppose the algorithm starts in a state $|\psi_0\rangle$ and applies the oracle $\tilde{U}_w$ exactly k times, interleaved with unitary operations[4] $U_1, \ldots, U_k$. Define

$$|\psi_k^w\rangle = U_k \tilde{U}_w U_{k-1} \tilde{U}_w \cdots U_1 \tilde{U}_w |\psi_0\rangle, \qquad \text{(state } \textit{with} \text{ oracle operations)} \tag{2}$$

$$|\psi_k\rangle = U_k U_{k-1} \cdots U_1 |\psi_0\rangle, \qquad \text{(state } \textit{without} \text{ oracle operations)} \tag{3}$$

[1] For two functions h, g one says $h = \Omega(g)$, 'h is Big Omega of g', if $\exists c > 0, \exists N_0$ s.t. $\forall N > N_0$: $h(N) \geq c \cdot g(N)$.

[2] As a reminder: $h = O(g)$, 'h is Big O of g', if $\exists c > 0, \exists N_0$ s.t. $\forall N > N_0$: $h(N) \leq c \cdot g(N)$.

[3] The subscript of the oracle is chosen to be w instead of f (as it was done in the lecture) because this simplifies the notation later and because f is completely defined by w.

[4] In the Grover algorithm the U_k are all equal to $H^{\otimes n} \tilde{U}_0 H^{\otimes n}$, where $\tilde{U}_0$ is the new notation for $\tilde{U}_{f_0}$.

and define the deviation after k steps caused by the oracle as

$$D_k = \sum_w \left\| |\psi_k^w\rangle - |\psi_k\rangle \right\|^2. \tag{4}$$

If D_k is small there is only a small difference between $|\psi_k^w\rangle$ and $|\psi_k\rangle$ and it is not possible to correctly identify w with high probability.

(a) Using Eqs. (5.1) and (6), show that $D_k \leq 4k^2$ by induction.

(b) Assume that for all possible functions f, i.e. all possible w, an observation yields a solution to the search with probability at least $1/2$. This is, $|\langle w|\psi_k^w\rangle|^2 \geq \frac{1}{2}$ for all w. Furthermore, assume[5] $\langle w|\psi_k^w\rangle = |\langle w|\psi_k^w\rangle|$. Using Eqs. (5.2) and (7), show that in this case $D_k \geq cN$ for some c and sufficiently large N.

Together these two points prove that $k = \Omega(\sqrt{N})$ if the algorithm is to succeed, hence any quantum algorithm solving the search problem has to query the oracle at least $\Omega(\sqrt{N})$ times.

Hints:

(i) The Cauchy-Schwarz inequality is helpful in various steps of this exercise.

(ii) For any two vectors a, b in a Hilbert space $\mathcal{H}$, show that

$$\|a+b\|^2 \leq \|a\|^2 + \|b\|^2 + 2\|a\|\|b\| \quad \text{and} \quad \|a+b\|^2 \geq \|a\|^2 + \|b\|^2 - 2\|a\|\|b\|. \tag{5}$$

(iii) Let $\{a_i\}_{i=0}^{N-1}$ be an orthonormal basis of an N-dimensional Hilbert space $\mathcal{H}$ with inner product $(\cdot\,,\cdot)$ and $b \in \mathcal{H}$ normalized. Then

$$\sum_i |(a_i, b)|^2 = 1. \tag{6}$$

(iv) Same setting as in (iii) with $N = \dim(\mathcal{H})$, show that

$$\sum_i \|b - a_i\|^2 \geq 2N - 2\sqrt{N}. \tag{7}$$

[5] Replacing $|w\rangle$ with $e^{i\theta}|w\rangle$ does not change the probability of success, so w.l.o.g. we may assume that $\langle w|\psi_k^w\rangle = |\langle w|\psi_k^w\rangle|$.