Introduction to Quantum Computation
Master's Programme in Mathematics and Statistics
Fall 2018
Exercise set 5

Grover's search algorithm. Below n is the number of qubits and $N = 2^n$. In Exercises 5–6 you may assume N is not too small - why?

Exercise 1. The n-qubit *Walsh-Hadamard matrix* is defined as $W = H^{\otimes n}$. Show that $W_{ij} = 2^{-n/2}(-1)^{\bar{i}\cdot\bar{j}}$, where $\bar{i}\cdot\bar{j}$ is the bitwise dot product of the representations of i and j as n-bit strings (binary sequences).

Exercise 2. Let R be an n-qubit operator such that

$$R\,|x\rangle = \begin{cases} |x\rangle\,, & \text{if } x = 0, \\ -\,|x\rangle\,, & \text{if } x \neq 0. \end{cases}$$

Show that

(a) $R = 2\,|0\rangle\,\langle 0| - I$,
(b) $WRW = 2\,|\psi\rangle\,\langle\psi| - I$, where $|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$.

Exercise 3. Let $D = WRW$. Show that $D\sum_k \alpha_k\,|k\rangle = \sum_k(-\alpha_k + 2\alpha)\,|k\rangle$, where $\alpha = \sum_k \alpha_k/N$. Why does this justify the description 'inversion about average'?

Exercise 4. Let a state be a linear combination of n-qubit basic states, where one coefficient is k and all the others are l, where $k, l \in \mathbb{R}$. Show that after applying D to this state, the new coefficients are

$$k' = (\frac{2}{N} - 1)k + \frac{2(N-1)}{N}l$$
$$l' = \frac{2}{N}k + \frac{N-2}{N}l,$$

where $N = 2^n$ and n the number of qubits.

Exercise 5. Show that if $k < 0$, $l > 0$ and $|\frac{k}{l}| < \sqrt{N}$ then after applying D to the starting state of Exercise 4 the new amplitudes are all positive.

Exercise 6. Consider Grover's algorithm, where O is the oracle operator $O\,|x\rangle = (-1)^{f(x)}\,|x\rangle$ and $D = WRW$. The algorithm starts out in the n-qubit state $|0\rangle$ (i.e. corresponding to the n-bit zero string; here the oracle workspace has been left out), and applies W to it. After that the algorithm iterates the operators O and D until measurement. One can show that this will improve the possibility of measuring $|a\rangle$ (where $f(a) = 1$) as long as the coefficient of $|a\rangle$ is $0 < k < \frac{1}{\sqrt{2}}$. What happens if $k = \frac{1}{\sqrt{2}}$?