1.) SEARCHING A SMALL QUANTUM PHONEBOOK

Imagine you live in a pre-computer world, you meet someone in a bar, and hit it off. You get their phone number (in writing). But the next morning you realize that you have completely forgotten their name. What to do? Brute force approach would be to check their phone number one-by-one against the phone numbers listed in a phonebook (which is alphabetized by name). What a drag! If there are $N \sim 10^6$ names in the phonebook (guess you live in a pretty big city) this would (typically) take you a time of order $N$ and you’d be out of luck. Indeed, if you could look up one name per second this would take you several months! But if you had a quantum phonebook at home (which implements Grover’s algorithm) it would be possible to find the name of your friend in time of order $\sqrt{N}$, which, for a “look-up time” of one second (more correctly the time it takes the quantum computer to implement a single Grover iteration, see below) would take roughly 3 hours. Perhaps even worth it. [You might think it a strange world in which quantum computers would be available before classical computers. So I guess this is a pretty silly scenario...].

Surely just for illustrative purposes, let’s see how the Grover’s algorithm running on some quantum hardware fares against classical hardware (a phonebook) which contains just $N = 4$ names (maybe your friend lives in a really small town, somewhere in the boondocks).

(A) Comparing your friends phone number against the phone numbers in the phonebook, you would need at most 3 look-ups to find your friends name (since if you got unlucky the first three times you would know that the remaining name is your friend). What is the average number of look-ups that would be needed to find your friends name?

And now for the quantum computer. Let $x = 0, 1, ..., N - 1$ label the locations of the alphabetized names in the book, and $F(x)$ store the corresponding phone numbers. Denoting your friends number as $F_0$, you are looking for the location of your friends name, call it $x_0$, that satisfies $F(x_0) = F_0$. In essence, you are trying to invert the function $F(x)$.

Your quantum computer (which is a black-box to you, sometimes called an “oracle” by computer types) can do the look-ups for you. Specifically, if you provide the computer with your friends number, $F_0$, and a guess for the location of your friends name, $x$, the computer will return a function $f_{F_0}(x)$ which is given by $f_{F_0}(x = x_0) = 1$ and $f_{F_0}(x \neq x_0) = 0$.

In quantum terms, the black-box implements a unitary transformation, $U_{F_0}$, defined by its operation on the ket $|x\rangle$, a 2 qbit input for $N = 4$, and on the ket $|y\rangle$ a single “register” qbit;

$$U_{F_0}|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f_{F_0}(x)\rangle,$$

where $\oplus$ denotes a binary addition.

(B) It is convenient to set the qbit register $|y\rangle$ to the state $(|0\rangle - |1\rangle)/\sqrt{2}$. Show that,

$$U_{F_0}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2} \rightarrow (\tilde{U}_{F_0}|x\rangle(|0\rangle - |1\rangle)/\sqrt{2},$$

where $\tilde{U}_{F_0}$, which acts only in the computational subspace, is given by,

$$\tilde{U}_{F_0} = 1 - 2|x_0\rangle\langle x_0|.$$

Notice that the quantum oracle changes the sign of the ket labeling the location of your friends name, $|x_0\rangle \rightarrow -|x_0\rangle$, leaving all of the other computational states, $|x \neq x_0\rangle$, unchanged.

Now the quantum computer has been engineered to prepare an initial state of the form,

$$|s\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{N-1} |x\rangle,$$

an equal weight linear superposition of all the states in the computational basis. Notice that the overlap probability with the searched for ket $|x_0\rangle$ is $\langle x_0|s\rangle|^2 = 1/N$, equal to the probability that you will find your friend on the
very first (classical) look-up in the phonebook. The idea behind the Grover’s algorithm is to “rotate” the ket $|s\rangle$ to (progressively) increases its overlap with $|x_0\rangle$.

Now your quantum computer has also been programmed to be capable of implementing the general unitary transformation,

$$U_s = 2|s\rangle\langle s| - 1,$$

(5)

(which is independent of your friends phone number, $F_0$, and the location of his/her name $|x_0\rangle$). The Grover operation is defined as the unitary transformation,

$$\mathcal{G}_{F_0} = U_s \tilde{U}_{F_0},$$

(6)

which is implemented successively. And the quantum algorithm (“program”) consists of iterating this procedure some integer number of times, $T$,

$$\mathcal{G}_{F_0} \mathcal{G}_{F_0} \ldots \mathcal{G}_{F_0} |\psi_0\rangle \rightarrow |\psi_T\rangle,$$

(7)

where the output state $|\psi_T\rangle$ is some other (normalized) state in the operational Hilbert space spanned by $|x\rangle$ with $x = 0, 1, \ldots, N - 1$. In the Grover algorithm the “input” state is chosen as $|\psi_0\rangle = |s\rangle$ which is a linear superposition of all the basis states in the computational basis. The amazing feature of a quantum computer is its “quantum parallelism”. In this case, the computer can perform a “look-up” (ie a computation) simultaneously on all of the computational basis states $|x\rangle$ in the Hilbert space - effectively “looking” at every location in the phonebook at the same “time”.

The output of the quantum computation consists of measuring the value of $\{x\}$ (ie projecting into the computational basis) which gives the correct location of your friends name with probability, $|\langle x_0|\psi_T\rangle|^2$. The trick is in the choice of the optimal value of $T$, call it $T_N$, which maximizes the overlap of $|\psi_T\rangle$ with $|x_0\rangle$. This optimal value depends on the size of the Hilbert space, $N$, (number of names in the phonebook) and for large $N$ is given by $T_N = (\pi/4)\sqrt{N}[1 + O(N^{-1/2})]$. Moreover, with this choice for the “time” $T_N$ the “targeted” name will be measured (ie located) with unit probability, up to $1/N$ corrections. Remarkably, this corresponds to a qualitative squareroot speed-up relative to the linear $N$ scaling for (the best possible) classical search algorithm.

(C) For the special case $N = 4$, by explicit calculation, show that the Grover algorithm with a single iteration, $T = 1$, will give an output $|\psi_1\rangle$ which enables the location of your friends name with (exactly) unit probability. Notice the “speed-up” relative to the (average) number of classical look-ups which were required to locate your friends name (in part (A)).

(D) Also for $N = 4$, compute the probability of finding your friends name if the Grover’s iteration is implemented twice, $T = 2$, a sub-optimal value of times. Remarkably, in contrast to the classical phonebook where increasing the number of look-up’s can only increase your chance of success, running your quantum computer for twice as long has made matters worse.