Quantum Computing HW2

Nir Stiassnie and Shay Kricheli

May 2020

Question 1 - Multiple qubits and quantum circuits

In this question, for each state $|x_0, x_1\rangle$, for $x_i \in \{0, 1\}$, we are to apply the circuit given. Let us apply each operation individually.

- Let $x_0 = 0, x_1 = 0$. Let us apply the circuit on $|0, 0\rangle$. Let us first apply the Hadamard gate:

$$H \otimes H|0, 0\rangle = |+, +\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) = \frac{1}{2}\Big(|0, 0\rangle + |0, 1\rangle + |1, 0\rangle + |1, 1\rangle\Big)$$

  Now let us apply the CNOT gate:

$$\begin{aligned} &CNOT|+, +\rangle = CNOT\frac{1}{2}\Big(|0, 0\rangle + |0, 1\rangle + |1, 0\rangle + |1, 1\rangle\Big) = \\ &\frac{1}{2}\Big(CNOT|0, 0\rangle + CNOT|0, 1\rangle + CNOT|1, 0\rangle + CNOT|1, 1\rangle\Big) = \\ &\frac{1}{2}\Big(|0, 0\rangle + |0, 1\rangle + |1, 0\rangle + |1, 1\rangle\Big) = |+, +\rangle \end{aligned}$$

  Finally let us apply the Hadamard gate again:

$$H \otimes H|+, +\rangle = |0, 0\rangle$$

- Let $x_0 = 0, x_1 = 1$. Let us apply the circuit on $|0, 1\rangle$. Let us first apply the Hadamard gate:

$$H \otimes H|0, 1\rangle = |+, -\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) = \frac{1}{2}\Big(|0, 0\rangle - |0, 1\rangle + |1, 0\rangle - |1, 1\rangle\Big)$$

  Now let us apply the CNOT gate:

$$\begin{aligned} &CNOT|+, -\rangle = CNOT\frac{1}{2}\Big(|0, 0\rangle - |0, 1\rangle + |1, 0\rangle - |1, 1\rangle\Big) = \\ &\frac{1}{2}\Big(CNOT|0, 0\rangle - CNOT|0, 1\rangle + CNOT|1, 0\rangle - CNOT|1, 1\rangle\Big) = \\ &\frac{1}{2}\Big(|0, 0\rangle - |0, 1\rangle + |1, 1\rangle - |1, 0\rangle\Big) = \frac{1}{2}\Big(|0\rangle \otimes \big(|0\rangle - |1\rangle\big) - |1\rangle \otimes \big(|0\rangle - |1\rangle\big)\Big) = \\ &\frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) = |-\rangle \otimes |-\rangle = |-, -\rangle \end{aligned}$$

  Finally let us apply the Hadamard gate again:

$$H \otimes H|-, -\rangle = |1, 1\rangle$$

- Let $x_0 = 1, x_1 = 0$. Let us apply the circuit on $|1,0\rangle$. Let us first apply the Hadamard gate:

$$H \otimes H|1,0\rangle = |-,+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) = \frac{1}{2}\Big(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle\Big)$$

  Now let us apply the CNOT gate:

$$\begin{aligned} &CNOT|-,+\rangle = CNOT\frac{1}{2}\Big(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle\Big) = \\ &\frac{1}{2}\Big(CNOT|0,0\rangle + CNOT|0,1\rangle - CNOT|1,0\rangle - CNOT|1,1\rangle\Big) = \\ &\frac{1}{2}\Big(|0,0\rangle + |0,1\rangle - |1,0\rangle - |1,1\rangle\Big) = |-,+\rangle \end{aligned}$$

  Finally let us apply the Hadamard gate again:

$$H \otimes H|-,+\rangle = |1,0\rangle$$

- Let $x_0 = 1, x_1 = 1$. Let us apply the circuit on $|1,1\rangle$. Let us first apply the Hadamard gate:

$$H \otimes H|1,1\rangle = |-,-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \otimes \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) = \frac{1}{2}\Big(|0,0\rangle - |0,1\rangle - |1,0\rangle + |1,1\rangle\Big)$$

  Now let us apply the CNOT gate:

$$\begin{aligned} &CNOT|-,-\rangle = CNOT\frac{1}{2}\Big(|0,0\rangle - |0,1\rangle - |1,0\rangle + |1,1\rangle\Big) = \\ &\frac{1}{2}\Big(CNOT|0,0\rangle - CNOT|0,1\rangle - CNOT|1,0\rangle + CNOT|1,1\rangle\Big) = \\ &\frac{1}{2}\Big(|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle\Big) = |+,-\rangle \end{aligned}$$

  Finally let us apply the Hadamard gate again:

$$H \otimes H|+,-\rangle = |0,1\rangle$$

Now let us repeat the calculation with the second circuit. Let us define:

$$CNOT^T|a,b\rangle := |a \oplus b, b\rangle$$

Now:

- Let $x_0 = 0, x_1 = 0$. Let us apply the circuit on $|0,0\rangle$.

$$CNOT^T|0,0\rangle = |0 \oplus 0, 0\rangle = |0,0\rangle$$

- Let $x_0 = 0, x_1 = 1$. Let us apply the circuit on $|0,1\rangle$.

$$CNOT^T|0,1\rangle = |0 \oplus 1, 1\rangle = |1,1\rangle$$

- Let $x_0 = 1, x_1 = 0$. Let us apply the circuit on $|1,0\rangle$.

$$CNOT^T|1,0\rangle = |1 \oplus 0, 0\rangle = |1,0\rangle$$

- Let $x_0 = 1, x_1 = 1$. Let us apply the circuit on $|1,1\rangle$.

$$CNOT^T|1,1\rangle = |1 \oplus 1, 1\rangle = |0,1\rangle$$

Let us compare the results of applying the first circuit with the regular $CNOT$ and the second one with $CNOT^T$:

	First Circuit	Second Circuit
$\|0,0\rangle$	$\|0,0\rangle$	$\|0,0\rangle$
$\|0,1\rangle$	$\|1,1\rangle$	$\|1,1\rangle$
$\|1,0\rangle$	$\|1,0\rangle$	$\|1,0\rangle$
$\|1,1\rangle$	$\|0,1\rangle$	$\|0,1\rangle$

Table 1: Circuits Results Comparison

We can see that both unitary transformations produce the same results and thus they are equal. Moreover, we can see that the $CNOT$ operation does not necessarily retain the control qubit - as it changes for the states $|+,+\rangle$ and $|-,-\rangle$.

Question 2 - Do We Really Need Complex Numbers?

We are asked to prove that all amplitudes in a quantum computation are real numbers. In order to do so, we will show that any quantum circuit on n qubits that uses T two-qubit gates can be simulated exactly by a quantum circuit on $n+1$ qubits, that uses at most T three-qubit gates. Let us provide an appropriate construction.

Remark: The question is about an operation of two-qubit gates on states that are composed of n qubits. In order to do so, in each step - two qubits on which the apply the gate are chosen and the rest remain the same. Mathematically - this operation is done by using tensor product of $n-2$ identity matrices and the appropriate gate respective to the desired indices. We will discuss the general case in which the gates acts upon n qubits each time for simplification.

Let $1 \leq t \leq T$ and let us denote the state of circuit C at step t as:

$$|\psi_t\rangle = \sum_{x \in \{0,1\}^n} (a_{x_t} + ib_{x_t})|x\rangle$$

In order to represent $|\psi_t\rangle$ with no complex amplitudes, we will use an extra qubit as an indicator to indicate whether we use the real or imaginary part of each qubit, as follows:

$$|\psi'_t\rangle = \sum_{x \in \{0,1\}^n} (a_{x_t}|0x\rangle + b_{x_t}|1x\rangle)$$

Claim 1. *Let C be a quantum circuit on n qubits that uses T two-qubit gates. Let us define C' to be a quantum circuit on $n+1$ qubits that uses T three-qubit gates. Then C can be simulated exactly by C' - as in for each step $1 \leq t \leq T$ - there exists a gate V_{U_t} at step t of circuit C' works in an equivalent way to the gate U_t at step t of circuit C **and** the probabilities for all base states $|x\rangle$ where $x \in \{0,1\}^n$ are the same for the complex state $|\psi_t\rangle$ and the real state $|\psi'_t\rangle$.*

Proof. To prove the main claim, let us state several lemmas:

Lemma 1. *$|\psi_t\rangle$ and $|\psi'_t\rangle$ are equivalent representations i.e the probability of measuring $|x\rangle$ for all $x \in \{0,1\}^n$ in both of them is equal*

Proof. We know that the probability to measure $|x\rangle$ in $|\psi_t\rangle$ is the squared absolute value of the coefficient of $|x\rangle$, so:

$$P(|x\rangle) = |a_x + ib_x|^2 = a^2 + b^2$$

In order to compute the probability to measure $|x\rangle$ in $|\psi'_t\rangle$ let us observe the coefficients of $|0x\rangle$ and $|1x\rangle$, and since they are independent events:

$$P'(|x\rangle) = P'(|0x\rangle) + P'(|1x\rangle) = a^2 + b^2 = P(|x\rangle)$$

□

Let us now show the construction of the gates of C' based on the gates of C. Let us denote $U = (A + iB)$ as a two-qubit gate as in circuit C (where for two qubits $U \in \mathbb{C}^{4\times4}$, $A, B \in \mathbb{R}^{4\times4}$ and for the general case of n qubits - $U \in \mathbb{C}^{2^n \times 2^n}$, $A, B \in \mathbb{R}^{2^n \times 2^n}$) and define a new three-qubit gate V_U:

$$V_U = \begin{bmatrix} A & -B \\ B & A \end{bmatrix} \in \mathbb{R}^{8\times8}$$

Lemma 2. *If $U \in \mathbb{C}^{4\times4}$ is a unitary matrix, than $V_U \in \mathbb{R}^{8\times8}$ is an orthonormal matrix and therefore - a quantum gate.*

Proof. In order to show that V_U is an orthonormal matrix, we will show that $V_U V_U^\top = I$. Let us observe:

$$V_U^\top = \begin{bmatrix} A^\top & B^\top \\ -B^\top & A^\top \end{bmatrix}$$

$$V_U V_U^\top = \begin{bmatrix} AA^\top + BB^\top & AB^\top - BA^\top \\ BA^\top - AB^\top & AA^\top + BB^\top \end{bmatrix}$$

Since U is a unitary matrix, $UU^\dagger = I_{4\times 4}$ and thus:

$$UU^\dagger = (A+iB)(A+iB)^\dagger = (A+iB)(A^\top - iB^\top) = AA^\top + i(BA^\top - AB^\top) + BB^\top = I_{4\times 4}$$

Since, I, A and B are real matrices, the coefficient of i in the equation above must be 0:

$$BA^\top - AB^\top = 0_{4\times 4}$$

Than also:

$$(BA^\top - AB^\top)^\top = AB^\top - BA^\top = 0_{4\times 4}$$

So,

$$AA^\top + BB^\top = I_{4\times 4}$$

And we have that:

$$V_U V_U^\top = \begin{bmatrix} AA^\top + BB^\top & AB^\top - BA^\top \\ BA^\top - AB^\top & AA^\top + BB^\top \end{bmatrix} = \begin{bmatrix} I_{4\times 4} & 0_{4\times 4} \\ 0_{4\times 4} & I_{4\times 4} \end{bmatrix} = I_{8\times 8}$$

□

From both lemmas we have that V_U is a valid quantum gate and the probabilities are the same between the original state and our construction. Let us go on with the proof of the main claim, which we will do using induction on the steps t.

- Induction base:
  The input to a quantum circuit is in the standard basis and so, in the base of our induction, we know that the state has only real amplitudes. Thus, let us denote the initial state and gate (respectively) as:

  $$|\psi_1\rangle = \sum_x a_{x_1}|x\rangle \ ; \ U_1 = A_1 + iB_1$$

  where $U_1 \in \mathbb{C}^{4\times 4}$, $A_1, B_1 \in \mathbb{R}^{4\times 4}$. Let us recall that applying a gate matrix on a vector is done by: Thus after applying the gate U_1 on $|\psi_1\rangle$ we have the next state $|\psi_2\rangle$:

  $$|\psi_2\rangle = U_1|\psi_1\rangle = (A_1 + iB_1)\sum_x a_{x_1}|x\rangle = \sum_x a_{x_1}(A_1 + iB_1)|x\rangle = \sum_x \Big(a_{x_1}A_1 + ia_{x_1}B_1\Big)|x\rangle =$$

  $$\sum_x \Big(a_{x_1}A_1|x\rangle + ia_{x_1}B_1|x\rangle\Big)$$

  Let $a_{x_2}, b_{x_2} \in \mathbb{R}$ be two scalars that result by operating $a_{x_1}A_1$ and $a_{x_1}B_1$ on $|x\rangle$, respectively, so that they satisfy:

  $$\sum_x a_{x_1}A_1|x\rangle = \sum_x a_{x_2}|x\rangle$$

  $$\sum_x a_{x_1}B_1|x\rangle = \sum_x b_{x_2}|x\rangle$$

  Thus:

  $$\sum_x \Big(a_{x_1}A_1|x\rangle + ia_{x_1}B_1|x\rangle\Big) = \sum_x (a_{x_2} + ib_{x_2})|x\rangle$$

Let us observe that this pattern accommodate our construction. Let V_{U_1} be the corresponding gate to U_1 by the construction in the circuit C':

$$V_{U_1} = \begin{bmatrix} A_1 & -B_1 \\ B_1 & A_1 \end{bmatrix}$$

Since $b_{x_1} = 0$ we have by the construction that the equivalent initial state is:

$$|\psi_1'\rangle = \sum_x a_{x_1}|0x\rangle$$

By our construction, we are to prove that $|\psi_2'\rangle = V_{U_1}|\psi_1'\rangle = \sum_x (a_{x_2}|0x\rangle + b_{x_2}|1x\rangle)$. From the first lemma we'll have that Let:

$$|\psi_2'\rangle = V_{U_1}|\psi_1'\rangle = \begin{bmatrix} A_1 & -B_1 \\ B_1 & A_1 \end{bmatrix} \sum_x a_{x_1}|0x\rangle = \sum_x a_{x_1} \begin{bmatrix} A_1 & -B_1 \\ B_1 & A_1 \end{bmatrix} |0x\rangle =$$

$$\sum_x a_{x_1}\Big(|0\rangle A_1|x\rangle + |1\rangle B_1|x\rangle\Big) = \sum_x \Big(a_{x_1}|0\rangle A_1|x\rangle + a_{x_1}|1\rangle B_1|x\rangle\Big) =$$

$$\sum_x \Big(|0\rangle a_{x_1} A_1|x\rangle + |1\rangle a_{x_1} B_1|x\rangle\Big)$$

Plugging in the values a_{x_2} and b_{x_2} we get:

$$|\psi_2'\rangle = \sum_x \Big(|0\rangle a_{x_2}|x\rangle + |1\rangle b_{x_2}|x\rangle\Big) = \sum_x \Big(a_{x_2}|0x\rangle + b_{x_2}|1x\rangle\Big)$$

As required.

- Induction assumption:
  Let $t \in [1, T]$. Let us assume correctness for t. Let $|\psi_t\rangle = \sum_{x\in\{0,1\}^n}(a_{x_t} + ib_{x_t})|x\rangle$ be the state at step t in the circuit C. Let $|\psi_t'\rangle$ be the state at step t in the circuit C'. Then let us assume that $|\psi_t'\rangle = \sum_{x\in\{0,1\}^n}(a_{x_t}|0x\rangle + b_{x_t}|1x\rangle)$.

- Induction step:
  Let us prove correctness for $t+1$. Let $U_t = A_t + iB_t$ be the gate that operates at step t in the circuit C. Then the state at step $t+1$ in the circuit C is: $|\psi_{t+1}\rangle = U_t|\psi_t\rangle = \sum_x (a_{x_{t+1}} + ib_{x_{t+1}})|x\rangle$. Let V_{U_t} be the corresponding gate to U_t by the construction in the circuit C'. We are to show that $|\psi_{t+1}'\rangle = V_{U_t}|\psi_t'\rangle = \sum_x (a_{x_{t+1}}|0x\rangle + b_{x_{t+1}}|1x\rangle)$.
  Let us consider the state $|\psi_{t+1}\rangle$:

$$|\psi_{t+1}\rangle = U_t|\psi_t\rangle = \big(A_t + iB_t\big)\sum_x (a_{x_t} + ib_{x_t})|x\rangle = \sum_x \big(A_t + iB_t\big)(a_{x_t} + ib_{x_t})|x\rangle =$$

$$\sum_x \Big[a_{x_t}A_t - b_{x_t}B_t + i\big(b_{x_t}A_t + a_{x_t}B_t\big)\Big]|x\rangle = \sum_x \Big[\big(a_{x_t}A_t - b_{x_t}B_t\big)|x\rangle + i\big(b_{x_t}A_t + a_{x_t}B_t\big)|x\rangle\Big]$$

Let $a_{x_{t+1}}, b_{x_{t+1}} \in \mathbb{R}$ be two scalars that result by operating $a_{x_t}A_t - b_{x_t}B_t$ and $b_{x_t}A_t + a_{x_t}B_t$ on $|x\rangle$, respectively, so that they satisfy:

$$\sum_x \big(a_{x_t}A_t - b_{x_t}B_t\big)|x\rangle = \sum_x a_{x_{t+1}}|x\rangle$$

$$\sum_x \big(b_{x_t}A_t + a_{x_t}B_t\big)|x\rangle = \sum_x b_{x_{t+1}}|x\rangle$$

Thus:

$$\sum_x \Big[\big(a_{x_t}A_t - b_{x_t}B_t\big)|x\rangle + i\big(b_{x_t}A_t + a_{x_t}B_t\big)|x\rangle\Big] = \sum_x (a_{x_{t+1}} + ib_{x_{t+1}})|x\rangle$$

By the construction:

$$V_{U_t} = \begin{bmatrix} A_t & -B_t \\ B_t & A_t \end{bmatrix}$$

Thus by the induction assumption:

$$|\psi'_{t+1}\rangle = V_{U_t}|\psi'_t\rangle = \begin{bmatrix} A_t & -B_t \\ B_t & A_t \end{bmatrix} \sum_x (a_{x_t}|0x\rangle + b_{x_t}|1x\rangle) = \sum_x \begin{bmatrix} A_t & -B_t \\ B_t & A_t \end{bmatrix} (a_{x_t}|0x\rangle + b_{x_t}|1x\rangle)$$

$$\sum_x \left[a_{x_t} \begin{bmatrix} A_t & -B_t \\ B_t & A_t \end{bmatrix} |0x\rangle + b_{x_t} \begin{bmatrix} A_t & -B_t \\ B_t & A_t \end{bmatrix} |1x\rangle \right] =$$

$$\sum_x \left[a_{x_t} \Big(|0\rangle A_t + |1\rangle B_t \Big) + b_{x_t} \Big(-|0\rangle B_t + |1\rangle A_t \Big) \right] |x\rangle =$$

$$\sum_x \left[a_{x_t} \Big(|0\rangle A_t|x\rangle + |1\rangle B_t|x\rangle \Big) + b_{x_t} \Big(-|0\rangle B_t|x\rangle + |1\rangle A_t|x\rangle \Big) \right] =$$

$$\sum_x \left[\Big(|0\rangle a_{x_t} A_t|x\rangle + |1\rangle a_{x_t} B_t|x\rangle \Big) + \Big(-|0\rangle b_{x_t} B_t|x\rangle + |1\rangle b_{x_t} A_t|x\rangle \Big) \right] =$$

$$\sum_x \left[|0\rangle \Big(a_{x_t} A_t - b_{x_t} B_t \Big)|x\rangle + |1\rangle \Big(a_{x_t} B_t + b_{x_t} A_t \Big)|x\rangle \right]$$

Plugging in the values $a_{x_{t+1}}$ and $b_{x_{t+1}}$ we get:

$$|\psi'_{t+1}\rangle = \sum_x \Big(|0\rangle a_{x_{t+1}}|x\rangle + |1\rangle b_{x_{t+1}}|x\rangle \Big) = \sum_x \Big(a_{x_{t+1}}|0x\rangle + b_{x_{t+1}}|1x\rangle \Big)$$

This coclude the induction.

□

Question 3 - Grover's Algorithm with an unknown number of marked items

We are given an oracle with K marked items, and K is unknown. We are to design an algorithm that finds a marked item using $O\left(\sqrt{\frac{N}{K}}\right)$ queries, with probability of more than $\frac{1}{2}$.

(1)

We are to show that when K is known, there is an algorithm that finds the marked element with probability close to 1, with a running time of $O\left(\sqrt{\frac{N}{K}}\right)$. To answer this question - we can use Grover's algorithm for the multiple marked items case as we saw in class: The algorithm receives an oracle to a string of length N which we will denote as $x = (x_1, ..., x_N)$ where there are K characters that are 1 - which are called marked items and the rest are zeros. Let use define the set of all marked indices:

$$J = \{i \mid x_i = 1\}$$

Moreover, let us define the following states:

$$|\alpha\rangle \frac{1}{\sqrt{N-K}} \sum_{i \in \{0,1\}^n \setminus J} |i\rangle \ ; \ |\beta\rangle = \frac{1}{\sqrt{K}} \sum_{i \in J} |i\rangle \ ;$$

Let us recall the oracle phase shift as seen in class:

$$V_x|i\rangle = (-1)^{x_i}|i\rangle$$

Given N and K, let us define the algorithm which we will denote $\mathcal{A}_{K_T}$ that receives a parameter T :

1. Let us define:
   (a) The state $|\psi_0\rangle = H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}} \sum_{i \in \{0,1\}^n} |i\rangle$
   (b) The operator that performs a reflection about $|\psi_0\rangle$ as: $U_{\psi_0} = 2|\psi_0\rangle\langle\psi_0| - I$
2. Repeat for T iterations:
   (a) Apply V_x
   (b) Apply U_{ψ_0}
3. Perform a measurement of the qubits in the standard basis and return the result

Let us define the algorithm $\mathcal{A}_K$ by running $\mathcal{A}_{K_T}$ with $T = \left\lfloor \frac{\pi\sqrt{\frac{N}{K}}}{4} - \frac{1}{2} \right\rfloor$.

Claim 2. *Given N and K, the algorithm $\mathcal{A}_K$ returns an index of a marked item and runs in a running time of $O\left(\sqrt{\frac{N}{K}}\right)$ with a probability close to 1.*

Proof. First of all, since T is finite, then $\mathcal{A}_K$ halts. Let us show that for the value mentioned for T - the algorithm will return an index of a marked item. As mentioned, the algorithm $\mathcal{A}_K$ is exactly Grover's algorithm for K marked items (when K is known) as seen in class. Let us consider the two-dimensional space S spanned by $|\alpha\rangle$ and $|\beta\rangle$ and observe that $|\psi_0\rangle$ lies somewhere between them as mentioned. Let us assume that the state $|\psi_0\rangle$ is with angle θ about the $|\alpha\rangle$ axis. Let us observe that: $|\psi_0\rangle = \sqrt{\frac{N-K}{N}}|\alpha\rangle + \sqrt{\frac{K}{N}}|\beta\rangle$. Thus $|\psi_0\rangle = \sqrt{\frac{N-K}{N}}|\alpha\rangle + \sqrt{\frac{K}{N}}|\beta\rangle = \cos(\theta)|\alpha\rangle + \sin(\theta)|\beta\rangle$ and we have that $\sin(\theta) = \sqrt{\frac{K}{N}}$. Using small angles approximation and assuming $K \ll N$, we can assume

that $\sin(\theta) \approx \theta$ and thus $\theta \approx \sqrt{\frac{K}{N}}$. We saw in class that in each iteration, the operations performed result in a total rotation of 2θ towards the $|\beta\rangle$ axis. Let us observe that our goal is to reach $|\beta\rangle$ and thus we'd want our final angle to be $\frac{\pi}{2}$. Let us consider the state $|\psi_t\rangle$ after t iterations:

$$|\psi_t\rangle = \cos\Big((2t+1)\theta\Big)|\alpha\rangle + \sin\Big((2t+1)\theta\Big)|\beta\rangle \approx$$
$$\cos\Big((2t+1)\sqrt{\frac{K}{N}}\Big)|\alpha\rangle + \sin\Big((2t+1)\sqrt{\frac{K}{N}}\Big)|\beta\rangle$$

Now, for our condition to hold, let for $t = T$:

$$(2T+1)\sqrt{\frac{K}{N}} = \frac{\pi}{2}$$

Thus, for us to return an index of a marked item we must have:

$$T = \left\lfloor \frac{\pi\sqrt{\frac{N}{K}}}{4} - \frac{1}{2} \right\rfloor$$

And thus $\mathcal{A}_K$ has performs $O\Big(\sqrt{\frac{N}{K}}\Big)$ iterations and returns an index of a marked item with a probability close to 1. □

(2)

We are to show that if K is unknown but lies between 2^j to 2^{j+1} for a given j, there is an algorithm that finds a marked element with a probability of at least $\frac{1}{2}$, with the same running time. To answer this question, we will use the algorithm $\mathcal{A}_{K_T}$ from the previous section, but with the largest value that K can get in the given range. Let us denote with K the actual number of marked items in the input.
Given N, and j let $K' = 2^{j+1}$ and let us define the algorithm which we will denote $\mathcal{A}_{K'}$ by running $\mathcal{A}_{K_T}$ with $T = T_{K'} = \left\lfloor \frac{\pi\sqrt{N/K'}}{4} - \frac{1}{2} \right\rfloor$.

Claim 3. *Given N and j such that $2^j \leq K \leq 2^{j+1}$, the algorithm $\mathcal{A}_{K'}$ returns an index of a marked item and runs in a running time of $O\Big(\sqrt{\frac{N}{K}}\Big)$ with probability of at least $1/2$.*

Proof. First of all, since $T_{K'}$ is finite - $\mathcal{A}_{K'}$ halts. Let us denote with $T_{\frac{1}{2}}$ the number of iterations needed with $\mathcal{A}_{K'}$ to obtain a probability of success of exactly $\frac{1}{2}$ with the required running time. Like we did before, let us denote the angle between $|\psi_0\rangle$ and $|\alpha\rangle$ as θ and based on the same reasoning as before, we have that $\sin(\theta) = \sqrt{\frac{K}{N}}$ and once again using small angle approximation, we'll have $\theta \approx \sqrt{\frac{K}{N}}$. Let us recall the expression we devised in the previous section for $|\psi_t\rangle$ and let us observe that a probability of $\frac{1}{2}$ is obtained if the squared absolute value of coefficient of $|\beta\rangle$ in $|\psi_t\rangle$ is equal to $\frac{1}{2}$. Since $\sin(\pi/4) = 1/\sqrt{2}$ and $(1/\sqrt{2})^2 = 1/2$, the corresponding angle we end up with after running the algorithm $\mathcal{A}_{K'}$ with $T_{\frac{1}{2}}$ iterations is $\pi/4$.

Lemma 3. *Let us denote φ to be the final angle of $|\psi_{T_{K'}}\rangle$ about the $|\alpha\rangle$ axis when the algorithm $\mathcal{A}_{K'}$ is over. Then $\frac{\pi}{2} \geq \varphi > \frac{\pi}{4}$.*

Proof. Let us break down the proof into the two bounds:

- Lower bound: By the expression for $|\psi_t\rangle$ we have that the total angle for t iterations increases linearly with t. Thus in order to prove that $\varphi > \frac{\pi}{4}$ - it suffices to prove that $T_{K'} > T_{\frac{1}{2}}$. As we calculated before, we have:

$$T_{K'} = \left\lfloor \frac{\pi\sqrt{N/K'}}{4} - \frac{1}{2} \right\rfloor$$

Now let us calculate the value for $T_{\frac{1}{2}}$. In order to do so, we'll equate the angle after $T_{\frac{1}{2}}$ iterations to $\pi/4$:

$$\pi/4 = (2T_{\frac{1}{2}} + 1)\theta \approx (2T_{\frac{1}{2}} + 1)\sqrt{K/N}$$

Solving for $T_{\frac{1}{2}}$, we have:

$$T_{\frac{1}{2}} = \left\lfloor \frac{1}{2}\frac{\pi\sqrt{N/K}}{4} - \frac{1}{2} \right\rfloor$$

Since $K' = 2^{j+1}$ and $2^j \leq K \leq 2^{j+1}$ we have that $K' \leq 2K$. Thus:

$$T_{K'} = \left\lfloor \frac{\pi\sqrt{N/K'}}{4} - \frac{1}{2} \right\rfloor \geq \left\lfloor \frac{\pi\sqrt{N/(2K)}}{4} - \frac{1}{2} \right\rfloor =$$
$$\left\lfloor \frac{1}{\sqrt{2}}\frac{\pi\sqrt{N/K}}{4} - \frac{1}{2} \right\rfloor > \left\lfloor \frac{1}{2}\frac{\pi\sqrt{N/K}}{4} - \frac{1}{2} \right\rfloor = T_{\frac{1}{2}}$$

- Upper bound: Now, let us prove that $\varphi \leq \frac{\pi}{2}$. Let $T_K = \left\lfloor \frac{\pi\sqrt{\frac{N}{K}}}{4} - \frac{1}{2} \right\rfloor$ be the number of iterations the algorithm $\mathcal{A}_{K'}$ runs using the actual unknown number K and let us denote ζ to be the final angle when running the algorithm $\mathcal{A}_{K'}$ for T_K iterations. By the reasoning we discussed earlier, ζ is the closest we can get to the desired angle of $\pi/2$ and thus we assume $\zeta \approx \pi/2$. Thus it suffices to prove that $\varphi \leq \zeta$. As mentioned, by the definition of $|\psi_t\rangle$, we have that the angle after t iterations is $(2t+1)\sqrt{\frac{K}{N}}$. Since $K' \geq K$, by the definition of $T_{K'}$ and T_K, we'll have that $T_{K'} \leq T_K$. Thus:

$$\varphi = (2T_{K'} + 1)\sqrt{\frac{K}{N}} \leq (2T_K + 1)\sqrt{\frac{K}{N}} = \zeta$$

□

Let us go back to the proof of the main claim. Let us recall that the probability of measuring a state is the squared absolute value of its coefficient and let us recall that our goal is to get as close as we can to $|\beta\rangle$ so when measuring $|\psi_{T_{K'}}\rangle$ we'll get a marked item. Using the definition of $|\psi_t\rangle$ we have that the probability of measuring $|\beta\rangle$ by $|\psi_{T_{K'}}\rangle$ is $P_{|\beta\rangle} = |\sin(\varphi)|^2$. Using the lemma and the fact that in the interval $[\pi/4, \pi/2]$, the function $sin(x)$ is monotonically increasing:

$$1/2 = |\sin(\pi/4)|^2 \geq |\sin(\varphi)|^2 \geq |\sin(\pi/2)|^2 = 1$$

and thus:

$$1/2 \geq P_{|\beta\rangle} \geq 1$$

Moreover, we have that the total running time is $O\left(\sqrt{\frac{N}{K'}}\right)$. Since $K' \geq K$ we have that $O\left(\sqrt{\frac{N}{K'}}\right) = O\left(\sqrt{\frac{N}{K}}\right)$ as required. □

(3)

In this section we are asked to iterate over the possible values of j in a certain order, to end up with a total running time of $O\left(\sqrt{\frac{N}{K}}\right)$ with probability 1/2. To do so, we'll use the algorithm $\mathcal{A}_{K'}$ from the previous section and with it iterate all the possible values of j **from top to bottom**. Since $K < N$ and $\mathcal{A}_{K'}$ always sets $K' = 2^{j+1}$ for a given j, the maximal value j can have is $\lfloor \log(N) \rfloor - 1$, so that's the initial value our new algorithm will start with for j.
Let us define the algorithm $\mathcal{A}_j$:

1. Let us define:
   (a) A boolean variable named **found** and initialize it with the value **False**
   (b) An index j and initialize it with the value $\lfloor \log(N) - 1 \rfloor$
2. While **found** is False, perform:
   (a) Run the algorithm $\mathcal{A}_{K'}$ with the current value of j, which will return the result of the measurement as stated, which is an index that we will denote as r
   (b) With the oracle, access x in the position r and denote it x_r
   (c) If $x_r = 1$:
      i. Set **found** to be True

   else:
      i. Set j to be $j - 1$
3. Return x_r

Claim 4. *Given N, the algorithm $\mathcal{A}_j$ returns a marked item with a running time of $O\left(\sqrt{\frac{N}{K}}\right)$ with a probability of* 1/2.

Proof. To prove so, we'll use several lemmas.

Lemma 4. *Given N, the algorithm $\mathcal{A}_j$ halts and returns a marked item with a probability of at least* 1/2.

Proof. Step 2.a of the algorithm $\mathcal{A}_j$ will result in a value of r which by the correctness proof for the algorithm $\mathcal{A}_{K'}$ will be a marked item with a probability of at least 1/2. Thus in step 2.c we'll have that x_r will be a marked item and thus equal to 1 - with a probability of at least 1/2. Thus the algorithm $\mathcal{A}_j$ will halt and return a marked item with a probability of at least 1/2. □

Lemma 5. *Given N, the algorithm $\mathcal{A}_j$ has a running time of $O\left(\sqrt{\frac{N}{K}}\right)$ with a probability of* 1/2.

Proof. Let us perform a time-complexity analysis of $\mathcal{A}_j$:

- Step 1 initializes variables and thus is done with 0(1) steps.
- Step 2.a uses the algorithm $\mathcal{A}_{K'}$ which we showed that runs for $O\left(\sqrt{\frac{N}{K'}}\right)$ steps. We specifically use the running time of $O\left(\sqrt{\frac{N}{K'}}\right)$ for $\mathcal{A}_{K'}$ (as we showed in its correctness proof that it is a tighter bound on its running time). Since for a given value of j we use $K' = 2^{j+1}$ for $\mathcal{A}_{K'}$, we have that the running time of step 2.a is:

$$O\left(\sqrt{\frac{N}{K'}}\right) = O\left(\sqrt{\frac{N}{2^{j+1}}}\right)$$

- Step 2.b uses the oracle access and thus is done in $O(1)$ steps.
- Step 2.c assigns values to variables and thus is performed in $O(1)$ steps.
- The while loop in step 2 is performed up until x_r is a marked item. Let us evaluate the value of j for which this happens with a probability of at least $1/2$ - which we will denote j_F. By the correctness proof of $\mathcal{A}_{K'}$, we have that for a given j such that $2^j \leq K \leq 2^{j+1}$, $\mathcal{A}_{K'}$ returns an index of a marked item with a probability of at least $1/2$. Thus j_F will have to be such that $2^{j_F} \leq K \leq 2^{j_F+1}$. So with a probability of at least $1/2$ - the while loop in step 2 of $\mathcal{A}_j$ will run up to the point where $j = \lfloor \log(K) \rfloor$ so that step 2.a will run $\mathcal{A}_{K'}$ with $K' = 2^{j_F+1} = 2^{\lfloor \log(K) \rfloor + 1} \approx 2K$. Finally, we conclude that step 2 runs for values of j from $\lfloor \log(N) \rfloor - 1$ up to $\lfloor \log(K) \rfloor$.

Thus the final running time of $\mathcal{A}_j$ is $O(S)$ where:

$$S = \sum_{j=\lfloor \log(K) \rfloor}^{\lfloor \log(N) \rfloor - 1} \sqrt{\frac{N}{2^{j+1}}} = \sqrt{N} \sum_{j=1}^{\lfloor \log(N) \rfloor - \lfloor \log(K) \rfloor} \frac{1}{\sqrt{2^{j+\lfloor \log(K) \rfloor}}} = \sqrt{\frac{N}{2^{\lfloor \log(K) \rfloor}}} \sum_{j=1}^{\lfloor \log(N) \rfloor - \lfloor \log(K) \rfloor} \frac{1}{\sqrt{2^j}}$$

Let us observe that we result in a geometric series where the formula for its sum is:

$$\sum_{j=1}^{p} q^j = \frac{1 - q^{p-1}}{1 - q}$$

For S, we have $q = \frac{1}{\sqrt{2}}$ and $p = \lfloor \log(N) \rfloor - \lfloor \log(K) \rfloor$ and thus:

$$\begin{aligned}
S &= \sqrt{\frac{N}{2^{\lfloor \log(K) \rfloor}}} \frac{1 - \frac{1}{\sqrt{2}}^{\lfloor \log(N) \rfloor - \lfloor \log(K) \rfloor - 1}}{1 - \frac{1}{\sqrt{2}}} = \\
&\sqrt{\frac{N}{2^{\lfloor \log(K) \rfloor}}} \frac{\sqrt{2}}{\sqrt{2} - 1} \left(1 - 2^{-\frac{1}{2}\left(\lfloor \log(N) \rfloor - \lfloor \log(K) \rfloor - 1 \right)} \right) = \\
&\sqrt{\frac{N}{2^{\lfloor \log(K) \rfloor}}} \frac{\sqrt{2}}{\sqrt{2} - 1} \left(1 - \sqrt{2} \cdot \left(2^{\left(\lfloor \log(K) \rfloor - \lfloor \log(N) \rfloor \right)} \right)^{\frac{1}{2}} \right) \approx \\
&\sqrt{\frac{N}{2^{\log(K)}}} \frac{\sqrt{2}}{\sqrt{2} - 1} \left(1 - \sqrt{2} \cdot \left(2^{\left(\log(K) - \log(N) \right)} \right)^{\frac{1}{2}} \right) = \\
&\sqrt{\frac{N}{K}} \frac{\sqrt{2}}{\sqrt{2} - 1} \left(1 - \sqrt{2} \cdot \sqrt{\frac{K}{N}} \right) = \frac{\sqrt{2}}{\sqrt{2} - 1} \left(\sqrt{\frac{N}{K}} - \sqrt{2} \right)
\end{aligned}$$

And thus the final running time of $\mathcal{A}_j$ is $O\left(\sqrt{\frac{N}{K}} \right)$ with a probability of at least a $1/2$. □

Both of these two lemmas form the proof of the main claim. □

Question 4 - Lower Bound on quantum search with ancillary qubits

In class we proved that a quantum algorithm for the search problem must apply $\Omega(\sqrt{N})$ queries in order to solve the search problem with high probability. We assumed that the algorithm does not use any ancillary qubits. The goal of this exercise is to show that the same conclusion holds without this assumption.

(1)

For $t = 1, ..., T$ let $|\psi_t\rangle = \sum_{i\in\{0,1\},z} \alpha_{i,z,t}|i, z\rangle$ the state after applying $U_t \cdots U_0$ (which can be viewed as the state at the t step of the algorithm, when the oracle is not applied, or, equivalently, that there are no marked items). Here, z represents the ancillary qubits. Let $p_i = \frac{1}{T}\sum_{z,t} |\alpha_{i,z,t}|^2$ be the probability of measuring i at the leftmost qubit.

Claim 5. *There exists an index i^* such that $p_{i^*} \leq \frac{1}{N}$.*

Proof. Since p_i is an expression that represents the probability of measuring i at the leftmost qubit, it must hold that:

$$\sum_{i\in\{0,1\}^n} p_i = 1$$

Thus, the minimal value of p_i must be at most the value for an individual probability at the case of uniform distribution. Let us observe that the number of possible values for i is $2^n = N$. Let:

$$i^* = \arg\min_{i\in 0,1^n} p_i$$

Thus we have:

$$\frac{1}{T}\sum_{z,t} |\alpha_{i^*,z,t}|^2 = p_{i^*} \leq \frac{1}{N}$$

□

(2)

Claim 6. *It holds that: $\sum_{t=1}^{T} \sqrt{\sum_z |\alpha_{i^*,z,t}|^2} \leq \frac{T}{\sqrt{N}}$.*

Proof. Let us define a vector $u \in \mathbb{R}^T$ using the index i^* declared at the previous section, such that for $t = 1, ..., T$:

$$u_t = \sqrt{\sum_z |\alpha_{i^*,z,t}|^2}$$

and let us define $v = (1, 1, ...1) \in \mathbb{R}^T$. Let us consider the vectors' norms:

$$||u|| = \sqrt{\sum_{t=1}^{T}\sum_z |\alpha_{i^*,z,t}|^2} \; ; \; ||v|| = \sqrt{\sum_{t=1}^{T} 1^2} = \sqrt{T}$$

Let us consider the inner product of the two vectors:

$$\langle u, v\rangle = \sum_{t=1}^{T} \sqrt{\sum_z |\alpha_{i^*,z,t}|^2}$$

Let us recall Cauchy-Schwarz inequality for two vectors u, v of an inner product space:

$$|\langle u, v\rangle| \leq ||u|| \cdot ||v||$$

Thus we have:

$$\sum_{t=1}^{T} \sqrt{\sum_{z} |\alpha_{i^*,z,t}|^2} \leq \sqrt{\sum_{t=1}^{T} \sum_{z} |\alpha_{i^*,z,t}|^2} \cdot \sqrt{T} = \sqrt{\sum_{z,t} |\alpha_{i^*,z,t}|^2} \cdot \sqrt{T}$$

From the result of the previous section we have:

$$\frac{1}{T} \sum_{z,t} |\alpha_{i^*,z,t}|^2 \leq \frac{1}{N} \rightarrow \sqrt{\sum_{z,t} |\alpha_{i^*,z,t}|^2} \leq \sqrt{\frac{T}{N}}$$

So using the last two inequalities:

$$\sum_{t=1}^{T} \sqrt{\sum_{z} |\alpha_{i^*,z,t}|^2} \leq \sqrt{\sum_{z,t} |\alpha_{i^*,z,t}|^2} \cdot \sqrt{T} \leq \sqrt{\frac{T}{N}} \cdot \sqrt{T} = \frac{T}{\sqrt{N}}$$

And finally we have:

$$\sum_{t=1}^{T} \sqrt{\sum_{z} |\alpha_{i^*,z,t}|^2} \leq \frac{T}{\sqrt{N}}$$

□

Based on these two sections - we conclude that the addition of ancillary qubits does not change the behaviour of the lower bound and thus we arrive at the expected realization that any quantum algorithm for the search problem must apply $\Omega(\sqrt{N})$ queries in order to solve the search problem with high probability.