COMS 4281 - Intro to Quantum Computing

Problem Set 4: Hamiltonians, Algorithms, and Complexity

Due: November 20, 11:59pm.

Collaboration is allowed and encouraged (teams of at most 3). Please read the syllabus carefully for the guidlines regarding collaboration. In particular, everyone must write their own solutions in their own words.

Name: Chandan Suri, UNI: CS4090

Write your collaborators here:

AS6413

Problem 1: Hamiltonian Math

Problem 1.1

Let H be a Hamiltonian and let $|\psi\rangle$ be a ground state, i.e., it minimizes $\langle\psi| H |\psi\rangle$ over all states. Show that $|\psi\rangle$ is an eigenvector.

Solution

To show that ψ is an eigenvector, we would want to prove that $H|\psi\rangle = \lambda|\psi\rangle$ where λ is some scalar value.

Now, let's try and simplify the expression $H|\psi\rangle$:

$$H|\psi\rangle = \left(\sum_j E_j |v_j\rangle\langle v_j|\right)|\psi\rangle$$

Let's simplify this even further:

$$= \sum_j E_j |v_j\rangle\langle v_j|\psi\rangle = \sum_j E_j\alpha_j|v_j\rangle$$

Since, we know that ψ minimizes the equation $\langle\psi| H |\psi\rangle$ which would be the minima and thus the ground energy. The ground energy is composed of the same value such that $\alpha_i^2 + \alpha_j^2 + \alpha_k^2 = 1$ for some i, j, k. Also, the ground energy, $E_{ground} = \alpha_i E_i + \alpha_j E_j + \alpha_k E_k$.

Following this, we can say that $\psi = \alpha_i |v_i\rangle + \alpha_j |v_j\rangle + \alpha_k |v_k\rangle$. In general, there will be some state in existence and when it's the minimum of the same eigenvalue E_j such that $\psi = \alpha_j |v_j\rangle = |v_j\rangle$. Also, we have that, $E_{ground} = |\alpha_j|^2 E_j = E_j$. Since the alphas will be zero for all the terms when $i \neq j$.

$$H |\psi\rangle = E_j \alpha_j |v_j\rangle = E_j |v_j\rangle = E_{ground} |\psi\rangle$$

Thus, ψ is the eigenvector of H and also, the ground energy will be the minimum eigenvalue.

Problem 1.2

Let H be a Hamiltonian and let $|\psi(0)\rangle$ denote some initial state with average energy $E = \langle\psi(0)| H |\psi(0)\rangle$.

Let $|\psi(t)\rangle$ denote the time evolution of $|\psi(0)\rangle$ with respect to the Hamiltonian H. In other words,

$$|\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle .$$

Show that the energy of the state $|\psi(t)\rangle$ with respect to H is still E. In other words, show that time evolution of a state with respect to a Hamiltonian conserves energy.

Solution

As initial state can be shown as $E = \langle\psi(0)| H |\psi(0)\rangle$.

So, throught time evolution, the average energy at time t can be shown as:

$$\langle\psi(t)| H |\psi(t)\rangle$$

Also, if:

$$|\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle$$

Then, $\langle\psi(t)|$ is basically the transposed version of $|\psi(t)\rangle$ and thus, can be written as:

$$\langle\psi(t)| = \langle\psi(0)| e^{+iHt}$$

Using the formulations above, we can write the following:

$$\langle\psi(t)| H |\psi(t)\rangle = \langle\psi(0)| e^{+iHt} H e^{-iHt} |\psi(0)\rangle$$

Solving for $e^{+iHt} H e^{-iHt}$, we get the following:

$$e^{+iHt} H e^{-iHt} = \left(\sum_j e^{E_j t} |v_j\rangle \langle v_j|\right) \left(\sum_j E_j |v_j\rangle \langle v_j|\right) \left(\sum_j e^{-E_j t} |v_j\rangle \langle v_j|\right)$$

Similar to the proof in class, let's simplify the above expression (As some terms will become 1 when summations are merged and some expressions become zero):

$$= \left(\sum_j e^{E_j t} |v_j\rangle \langle v_j| \right) \left(\sum_j e^{-E_j t} E_j |v_j\rangle \langle v_j| \right)$$

Next, we simplify it further:

$$= \left(\sum_j e^{E_j t} e^{-E_j t} E_j |v_j\rangle \langle v_j| \right)$$

After cancelling the terms $e^{E_j t}$ and $e^{-E_j t}$, we will get the following:

$$= \left(\sum_j E_j |v_j\rangle \langle v_j| \right)$$

This is basically H.

Thus, the expression becomes:

$$\langle \psi(t)| H |\psi(t)\rangle = \langle \psi(0)| H |\psi(0)\rangle$$

As we can see, this is the same as the initial average energy and thus, the energy is conserved.

Hence Proved!

Problem 2: The 1D Ising model

Problem 2.1

Recall the 1-dimensional Ising model, which is a Hamiltonian describing a bunch of magnets on a line:

$$H = \sum_{j=1}^{n-1} Z_j \otimes Z_{j+1} + \mu \sum_{i=1}^{n} Z_i$$

where $\mu \in \mathbb{R}$ is a real parameter that represents the strength of the global magnetic field relative to the interactions between neighboring magnets.

Fix a string $x \in \{0,1\}^n$ and consider the corresponding n-qubit basis state $|x\rangle = |x_1, \ldots, x_n\rangle$.

Give a formula for the quantity $\langle x| H |x\rangle$ in terms of the strings x and the parameter μ.

Use this to deduce the spectral decomposition (i.e. find its eigenvectors and eigenvalues) of H, as a function of μ.

Solution

The formulation for $\langle x| H |x\rangle$ can be written as (using the formulation used in the class):

$$\langle x| H |x\rangle = \sum_{j=1}^{n-1} \langle x| Z_j \otimes Z_{j+1} |x\rangle + \mu \sum_{i=1}^{n} \langle x| Z_i |x\rangle$$

Let's take the first part of the expression as A and second part as B.

Now, let's simplify A:

$$A = \sum_{j=1}^{n-1} \langle x| Z_j \otimes Z_{j+1} |x\rangle = \sum_{j=1}^{n-1} \langle x| \Big(|00\rangle_j \langle 00|_{j+1} + |11\rangle_j \langle 11|_{j+1} - |01\rangle_j \langle 01|_{j+1} - |10\rangle_j \langle 10|_{j+}$$

As the jth and $(j+1)th$ will be the only bits interacting with the Z's and giving an output and thus, we can simplify the above expression as:

$$= \sum_{j=1}^{n-1} \left\langle x_j x_{j+1} \right| |00\rangle \langle 00| \left| x_j x_{j+1} \right\rangle + \left\langle x_j x_{j+1} \right| |11\rangle \langle 11| \left| x_j x_{j+1} \right\rangle - \left\langle x_j x_{j+1} \right| |01\rangle \langle 01| \left| x_j x_{j+1} \right\rangle -$$

This can be simplied further as:

$$A = \sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2$$

Let's simplify B now:

$$B = \mu \sum_{i=1}^{n} \langle x| Z_i |x\rangle = \mu \sum_{i=1}^{n} \langle x| \left(|0\rangle \langle 0|_i - |1\rangle \langle 1|_i \right) |x\rangle$$

Simplifying this further similarly as we simplied A above will give us:

$$B = \mu \sum_{i=1}^{n} |\langle x_i|0\rangle|^2 - |\langle x_i|1\rangle|^2$$

Putting the expressions for A and B in the original equation gives us:

$$\langle x| H |x\rangle = \sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2 + \mu \sum_{i=1}^{n} |\langle x_i$$

This is the final expression. Alternatively, we can also write the same as:

$$\langle x| H |x\rangle = \left[\sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2 + \mu(|\langle x_j|0 \right.$$

In the above expression, the minimum energy configurations can be computed using some $|x\rangle$ and μ that minimize the above expression.

Problem 2.2

Suppose $\mu = 0$. What is the minimum energy of H and what are the ground states of H? What is the maximum energy of H and what states achieve the maximum energy?

Solution

If $\mu = 0$, then the second part of the expression for the global magnetic field will collapse to zero and thus, the expression left becomes:

$$\langle x| H |x\rangle = \sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2$$

For the Minimum case:

Whenever the bits are alternating in the state like $|x\rangle = |010...\rangle$ or $|x\rangle = |101...\rangle$, then this would minimize the same and as can be seen clearly from the expression above, the minimizing terms will become all 1 and thus, summing them up for $n-1$ cases and would give us $n-1$, but because of the negative sign it would become $1-n$. Thus, the minimum energy states will be the ones with alternating bits and the minimum energy of H will be $1-n$.

For the Maximum case:

Whenever all the bits are either equal to 0 or 1, that would zero out the negative parts of the expression above (the second half of the expression with negative signs) and thus, summing them up would give us $n-1$. In this case the maximum energy becomes $n-1$. This is actually the case for maximum energy as even if 2 alternating bits are there and that would minimize the energy because of the minimizing terms (negative signed). The states achieving the same will be of the form $|x\rangle = \{0\}^n$ or $|x\rangle = \{1\}^n$.

Problem 2.3

Suppose $\mu = 1$. What is the ground energy and ground states of H? What about when $\mu = -1$?

Solution

For $\mu = 1$:

The expression in the first part will become:

$$\langle x| H |x\rangle = \left[\sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2 + |\langle x_j|0\rangle|^2\right.$$

This can also be written as:

$$\langle x| H |x\rangle = \left[\sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 + |\langle x_j|0\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2\right.$$

For finding the minimum energy and the ground states, we need to look into 2 cases here:

When n is even: In this case to minimize the energy we will need the part of the expression with negative sign to give the output and thus, similarly to the problem 2.2 case the part of the expression with positive sign will zero out and the single bit states will cancel out when summed over the whole n-bit string. Thus, the minimum energy of H beccomes $1-n$. The ground state will be the one with alternating bits and will be of the form $|x\rangle = |010...\rangle$ or $|x\rangle = |101...\rangle$.

When n is odd: In this case, to minimize the energy, we should again consider the state with alternating bits. The difference is that, now the expression out of the summation will yield 1 when the alternating bit string state starts with zero and thus, ends with zero as well. But, we need -1 from there, thus, the state should start with 1 and have alternating bits. This will make the expression $|\langle x_n|1\rangle|^2$ yield 1 and thus, the minimum energy will become $1-n-1=-n$. The ground state as explained above will be: $|x\rangle = |1010...1\rangle$.

For $\mu = -1$:

The expression in the first part will become:

$$\langle x|\, H\, |x\rangle = \left[\sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2 - |\langle x_j|0\rangle|^2\right.$$

This can also be written as:

$$\langle x|\, H\, |x\rangle = \left[\sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 + |\langle x_j|1\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2\right.$$

Again, for finding the mimimum energy and the ground states, we will have to consider 2 cases:

When n is even: In this case to minimize the energy we will need the part of the expression with negative sign to give the output and thus, similarly to the problem 2.2 case the part of the expression with positive sign will zero out and the single bit states will cancel out when summed over the whole n-bit string. Thus, the minimum energy of H beccomes $1-n$. The ground state will be the one with alternating bits and will be of the form $|x\rangle = |010...\rangle$ or $|x\rangle = |101...\rangle$.

When n is odd: In this case, to minimize the energy, we should again consider the state with alternating bits. The difference is that, now the expression out of the summation will yield 1 when the alternating bit string state starts with one and thus, ends with one as well. But, we need -1 from there, thus, the state should start with 0 and have alternating bits. This will make the expression $|\langle x_n|0\rangle|^2$ yield 1 and thus, the minimum energy will become $1-n-1=-n$. The ground state as explained above will be: $|x\rangle = |0101...0\rangle$.

Problem 2.4

Give a qualitative description of what the ground states of H are, depending on μ. What happens as $\mu \to \infty$ or $\mu \to -\infty$? Are there "critical points" of μ where the behavior of the

ground states seem to change?

Solution

We know by now that to minimize the energy we would need some kind of n-bit string/state that has alternating bits. That will also be the ground state of H in the minima case.

Considering the expression below:

$$\langle x| H |x\rangle = \sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2 + \mu \sum_{i=1}^{n} |\langle x_i$$

Let's break the above expression into 2 different expressions as:

$$A = \sum_{j=1}^{n-1} |\langle x_j x_{j+1}|00\rangle|^2 + |\langle x_j x_{j+1}|11\rangle|^2 - |\langle x_j x_{j+1}|01\rangle|^2 - |\langle x_j x_{j+1}|10\rangle|^2$$

and,

$$B = \mu \sum_{i=1}^{n} |\langle x_i|0\rangle|^2 - |\langle x_i|1\rangle|^2$$

When μ tends to infinity or negative infinity, the expression A will be overpowered by the seccond expression B and thus, the main effect will be due to the B expression that is for the global magnetic field. Thus, the minimum energy will solely depend on B. So,

When $\mu \to \infty$: Then, the minimum energy should be $-\infty$ and for the same I will have to zero out the positive signed expression and thus, the ground states for H will be composed of all 1's: $|x\rangle = \{1\}^n$.

When $\mu \to -\infty$: Then, the minimum energy should be $-\infty$ and for the same I will have to zero out the negative signed expression and thus, the ground states for H will be composed of all 0's: $|x\rangle = \{0\}^n$.

For the critical points:

We know that the minima of A is when the state has alternating bits and the minimum value of A in those cases is $1 - n$. Also, if n is even, then B computes to zero. If $\mu > 1$, then, wherever we can minimize B at the expense of A will be the minimum. Also, note that maximum value of A is $n - 1$. Hence, wherever $B < 1 - n - (n - 1)$: $B < -2n + 2$ in the even case, A can be disregarded. If the case is like all the bits are either 0 or 1, then, if $|x\rangle = \{1\}^n$ and $\mu > 2$ or $|x\rangle = \{0\}^n$ and $\mu < -2$, then A is equal to $n - 1$ and $B < -2n + 2$. Then same arguments follows for the n being odd case, where $B < -2n + 1$. Thus, behavior always changes at either $\mu = \{-2, 0, 2\}$. These are thus, the critical points. Also, as we saw behavior changes for the cases of μ tends to ∞ or $-\infty$, thus, these are also the critical points for value of μ that changes the bahavior.

Problem 3: Quantum Graph Algorithms

Problem 3.1

In this problem you will design a quantum query algorithm to determine whether a graph is connected (i.e. there is a path between every pair of vertices). Let G be an n-vertex undirected graph and let A denote the $n \times n$ adjacency matrix for G (i.e., $A_{ij} = 1$ if and only if there is an edge between vertices i and j in the graph). Suppose you are given access to an oracle V that, on a basis state $|i, j, a\rangle$ for some $i, j \in [n]$ and $a \in \{0, 1\}$, maps it to the state $|i, j, a \oplus A_{ij}\rangle$. In other words, if (i, j) is an edge in the graph, then $V|i, j, a\rangle = |i, j, a \oplus 1\rangle$, and otherwise $V|i, j, a\rangle = |i, j, a\rangle$.

Design and analyze a quantum algorithm that makes at most $O(n^{3/2} \log n)$ calls to the oracle V and determines if the graph G is connected with probability at least 99%. To design your algorithm, you may use any classical graph algorithm (depth-first search, breadth-first search, etc.), combined with any of the quantum algorithms we have learned in class as a subroutine.

This constitutes a quantum speedup, because any **classical** algorithm must make $\Omega(n^2)$ queries to the adjacency matrix A to determine whether a graph is connected (even if the algorithm is randomized).

Hint: if you use Grover's algorithm that makes $O(\sqrt{n})$ queries as we've learned about it in class, be mindful that it has some probability of error. In general, if the number of solutions are not known ahead of time, then there is some constant probability of error (say at least 1%).

Solution

Algorithm:

Input: Quantum Oracle O

Output: connected if graph G is connected, not connected otherwise

$E_T \leftarrow \phi$

$T \leftarrow (V, E_T)$

while $c(T) \neq 1$:

Find e $\in E$ / E_T using quantum search

If e is found:

$E_T \leftarrow E_T \cup \{e\}$

else:

return not-connected

return connected

This is the algorithm above.

Explanation:

E_T is used for storing the edges of the spanning tree and T is the initial spanning tree wherein edges are added to it one by one. V is the set of vertices here. Using quantum search, we find an edge in the graph such that adding that found edge to tree T reduces the $c(T)$. $c(T)$ is a function here that computes the number of connected components in the graph. If at any point in time, no such edge can be found such that adding it to the set of edges reduces the number of connected components, then that it means that the graph is not connected and might have more than 1 connected component. If we come out of the loop at the end, that means that the graph is connected.

Correctness of the algorithm:

As explained above, assuming the correctness of the quantum subroutine, proving the correctness of the whole algorithm is trivial.

For the quantum subroutine, we will be creating a new oracle which will be responsible for searching for an edge e such that adding the edge to E_T will reduce $c(T)$. This will be basically like from the unstructured search problem. The function responsible for getting that edge can be defined as:

$$f(e) = \begin{cases} 1 & \text{if } c((V, E_T \cup e)) < c(T) \\ 0 & \text{otherwise} \end{cases}$$

The function f shown above ias basically a simple memory based operation and doesn't make any query to another oracle on it's own. The oracle can then be shown as (using the function above):

$$O(v_i, v_j) = A(v_i, v_j) \times f(e_{ij})$$

Here, A is the original adjacency matrix oracle for the graph, O is the oracle, e_{ij} is the supposed edge between the vertices v_i and v_j, and f is the function stated as above.

Two vertices from the graph G can be chosen in $O(n^2)$ ways and and the oracle will only return 1 if such an edge exists in the graph G and reduces the number of connected components in T. Let's say there are k such edges, then we can solve the same by making $\sqrt{\frac{n^2}{k}}$ queries to the oracle O and consequently to A as well.

Next, to get the worst-case bound, we will consider a fully connected graph which makes the loop run $n-1$ times. Initially, the number of edges as a solution will be bound by $n-1$ from below but as the loop runs, this bound will also get reduced by 1 at least in each iteration of the while loop. Thus, the number of calls that are made to the oracle will be upper bound by:

$$\sum_{k=2}^{n} \sqrt{\frac{n^2}{k-1}} = n \sum_{k=2}^{n} \frac{1}{\sqrt{k-1}} = n \sum_{k=1}^{n-1} \frac{1}{\sqrt{k}} \leq n\sqrt{n-1} \left(\sum_{k=1}^{n-1} \frac{1}{k} \right)^{0.5} \leq n\sqrt{n-1}\sqrt{1+\log(n}$$

The simplication above is made using CZ inequality for conveerting the equation into an inequality and the last one represented in the form of a logarithm is taken from stack exchange. Thus, as seen above, it is tightly bound as $O(n^{1.5}logn)$ time.

Problem 3.2

Show that any quantum algorithm must make at least $\Omega(\sqrt{n})$ queries to the oracle V in order to determine whether the graph G is connected.

Hint: You can assume the optimality of Grover's algorithm for unstructured search.

Bonus: Prove that $\Omega(n)$ queries to the oracle V are needed.

Solution

Let us assume that the Grover's algorithm is optimal for the decision version of the unstructured search problem. This would mean that it is not possible for us to devise an algorithm that makes less than $\Omega(\sqrt{n})$ queries to the oracle for deciding of a marked solution exists.

Now, let's construct a decision version of the graph connectivity problem. Essentially, this would mean that we want to find out whether a marked solution exists for a function $f : \{0,1\}^n \to \{0,1\}$.

Let's say we have a graph $G = (V, E)$ where each vertex would correpond to an n-bit string. An oracle will be setup which will output 1 when 2 vertices that are inputted to it have an edge in between them in the graph. This would be the case when both the n-bit strings correponding to those vertices output a zero by f. Thus, an oracle corresponding to this graph connectivity problem can be formulated as:

$$O(v_i, v_j) = \begin{cases} 1 & \text{if } f(x_i) = f(x_j) = 0 \\ 0 & \text{otherwise} \end{cases}$$

Above, v_i is the vertex corresponding to the n-bit string s_i.

Thus, this will yield a graph such that all the marked inputs form a clique of the graph G and all the non-marked inputs are the vertices with a degree of 0. This formulation helps us with the decision whether the graph is a connected one or not as if there is single marked input present, then that would mean that rge graph is not connected. Consequently, the graph will be connected if there are no marked inputs.

Thus, this shows us that it is possible to solve the original decision version of the unstructured search problem using the hypothesis for the graph connectivity algorithm above. However, note

that this algorithm makes less than $\Omega(\sqrt{n})$ to the oracle to make the decision. Consequently, this also shows that less than $\Omega(\sqrt{n})$ queries will be made to f.

As the proposed hypothesis and finding above would contradict the optimality of the Grover's algorithm. Hence, such an algorithm cannot exist!

Problem 4: NP-hardness of estimating output probabilities

Suppose that there existed a classical algorithm A that does the following amazing thing: when given input (C, x) where C describes a quantum circuit acting on n qubits with m gates, and x is an n-bit string, it outputs a number α such that

$$|\alpha - p(C, x)| \leq 2^{-10n}$$

where

$$p(C, x) = |\langle x| C |0^n\rangle|^2.$$

is the probability that, when measuring the final state of C on all the all zeroes input, yields measurement outcome x. In other words, the output of the algorithm A on (C, x) is a number that equal to $p(C, x)$ up to $10n$ digits of precision. Furthermore, the algorithm A runs in time polynomial in n and m.

Show that this would imply $\mathsf{P} = \mathsf{NP}$ by showing that, if such an amazing algorithm A existed, then one could use A to solve 3SAT (or your favorite NP-complete problem) in polynomial time. Therefore, one shouldn't expect it to be possible to efficiently calculate output probabilities of general quantum circuits. Recall that in the 3SAT problem, you're given a boolean formula of the form $(x_1 \vee x_2 \vee \neg x_5) \wedge (\neg x_7 \vee x_1 \vee \neg x_{11}) \wedge \cdots$, and the goal is to determine whether there exists an assignment to the variables that satisfies the formula.

Hint: you'll want show that for an instance φ of a NP-complete problem (such as 3SAT), you can transform that problem into a polynomial-sized quantum circuit C_φ such that the answer to the problem φ (whether it's satisfiable, graph colorable, etc.) can be encoded into the probability of some outcome of measuring the circuit C_φ on the all zeroes input.

Solution

Initially, the input that we have is $|0\rangle^{\otimes n}$. We will pass this through the hadamard gates $H^{\otimes n}$. This will give us a uniform superposition over all the n-bit binary strings. At this point, the probability of measuring any state is $\frac{1}{2^n}$ because of the superposition. Then we put this through one interation of the amplitude magnification like Grover's search, and then use the amazing algorithm A to measure this simple circuit. Also, note that the desired probability of failure is β.

Claim:

For $1 \leq M < N/4$ and any non-solution string $|x\rangle$, $\alpha < \frac{1}{2^n} - 2^{-10n}$.

Proof:

The probability of each non-solution string after one iteration of amplitude magnification is $(\cos^2 3\theta)/(N-M)$. Therefore the change in the probability is:

$$\frac{\cos^2\theta}{N-M} - \frac{\cos^2 3\theta}{N-M} = \frac{1}{N-M}(\cos\theta - \cos 3\theta)\,(\cos\theta + \cos 3\theta)$$

This can be further simplified using trigonometric identities as:

$$= \frac{4}{N-M}(\sin 2\theta \sin\theta)\,(\cos 2\theta \cos\theta)$$

Solving trigonometric formulations for the elements in the formula above, we can write the same as:

$$= \frac{8}{N-M} \times \frac{M}{N} \times \frac{N-M}{N} \times (2.\frac{N-M}{N} - 1)$$

Since, $M < N/4$, we can simplify the above formulation as an inequality as: $$

> \frac{8}{N - M} \times \frac{M}{N} \times \frac{N - M}{N} \times (\frac{1}{2} + \frac{2}{N}) $$

Also, since $M \geq 1$, we can simplify this further as:

$$\geq \frac{4}{N^2} + \frac{16}{N^3}$$

Next, since $N \geq 2$, $$

> \frac{20}{N^3} $$

This is equivalent to:

$$= \frac{20}{2^{3n}}$$

This, in turn is actually greater than the following as we can obviously see: $$

> \frac{1}{2^{10n}} $$

Thus, we have proved the claim the above.

Another Claim:

If $M > N/4$, After randomly sampling $\log_{(3/4)}(1/\delta)$ n-bit strings and finding them all for a 3-SAT problem that is not satisfiable, we can say that the probability for this is at least $1 - \delta$.

Proof:

Probability of k consecutive failures is at least $\left(\frac{3}{4}\right)^k$. If we bound the same by δ and take logarithms on both the sides of the inequality, we can prove the claim above.

Explanation or Procedure:

Firstly, let's say we take a string $|x\rangle$. Next, we will check if this string satisfies our classical 3-SAT problem or circuit. If it is able to do the same, then we are done here and we output probability as 1.

If it wasn't able to satisfy, we will follow the procedure or the algorithm as explained above. So, we will pass $|0\rangle^{\otimes n}$ through $H^{\otimes n}$. Then, we will do one single iteration of the amplitude amplification. Following that, we will measure the probability of $|x\rangle$ using the amazing algorithm A. If A returns a probability less than $\frac{1}{2^n} - 2^{-10n}$, then it means that there exists some M solutions such that $1 \leq M < N/4$. This time we will output 1 as well. Considering the other case, if A returns a probability greater than or equal to $\frac{1}{2^n} - 2^{-10n}$, then this means that either there are no solutions possible or there are at least $N/4$ solutions. Now, we can randomly sample a lot of bit strings and check if they satisfy our circuit. If any of them does satisfy the circuit, then we can for sure say that the circuit is satisfiable with a probability of 1. Otherwise, we can say that with at least $1 - (\frac{3}{4})^k$ probability that the circuit is not satisfiable.

Time and Circuit Complexity:

For the complete circuit, we require n Hadamard gates, a quantum oracle specific to the 3-SAT problem requiring $O(n^3)$ gates, a diffusion operator gate and a classical 3-SAT circuit. Clearly, our classical and quantum gates are polynomial.

Also, we make only one query to the quantum oracle and use the classical circuit at most $1 + \log_{(3/4)}(1/\delta)$ times, which is again polynomial in n.