

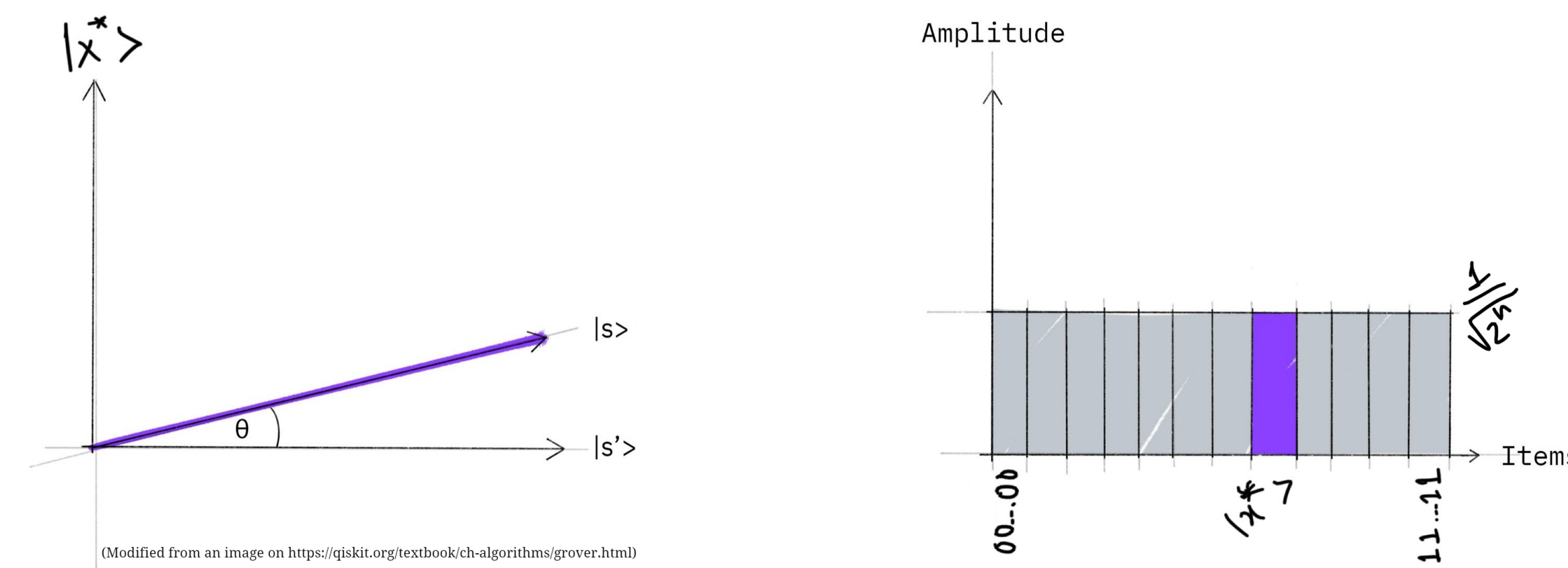
INTRODUCTION

Given a set of 2^n elements, $X = \{x_1, x_2, \dots, x_{2^n}\}$ where $x_i \in \{0, 1\}^n$ is a n -bit string, and a boolean function $f : X \rightarrow \{0, 1\}$, the problem of *unstructured search* is to find solution element(s) $x^* \in X$ such that $f(x^*) = 1$ or to conclude that no such x exists if $f(x) = 0$ for all $x \in X$. It is obvious that any classical brute-force algorithm would require $O(2^n)$ checks to find the solution element x^* if it exists. It is known that unstructured search problem can be solved with only $O(\sqrt{2^n})$ checks using *Grover's Algorithm* in a quantum computer by utilizing the quantum features of superposition and entanglement - providing a quadratic improvement in runtime.

GROVER'S ALGORITHM

Grover's Algorithm performs *amplitude amplification* to get the solution state as follows:

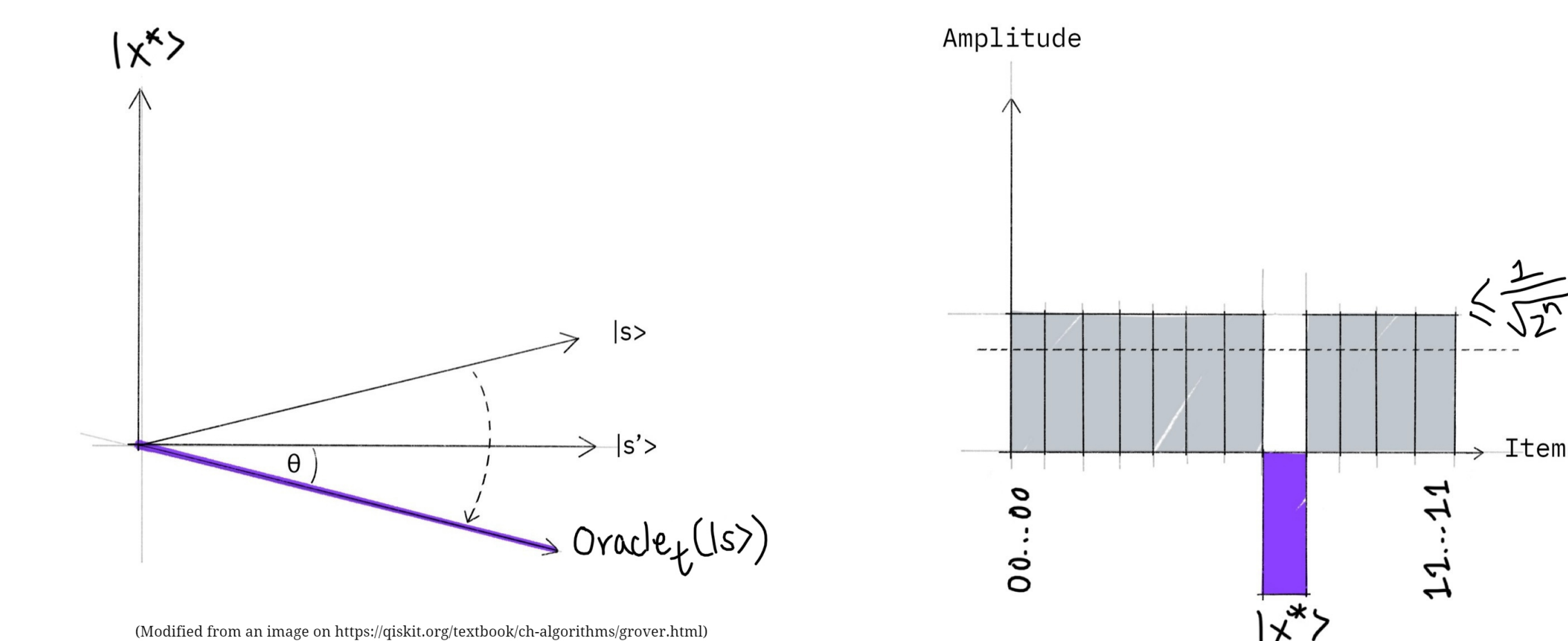
- Start with n qubits that are all initialized to $|0\rangle$ and put these qubits in uniform superposition $|s\rangle$ by applying Hadamard gate $H^{\otimes n}$ to all n qubits. This step: $|s\rangle = H^{\otimes n}|0\rangle^n = \sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle$ can be seen graphically as follows:



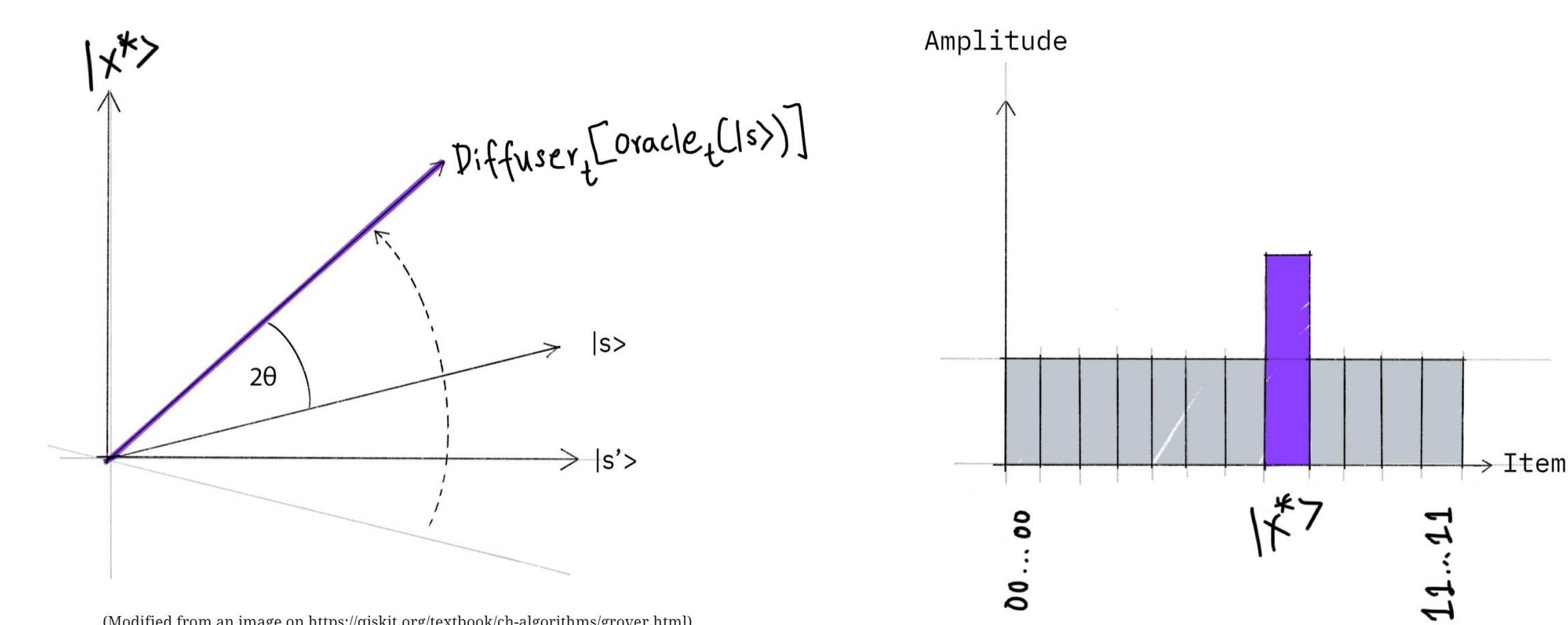
- Apply the *oracle* to the superposed state. This flips the amplitude of the solution state $|x^*\rangle$ and leaves everything else unchanged resulting in the state,

$$\frac{-1}{\sqrt{2^n}} |x^*\rangle + \sum_{\substack{x \in \{0,1\}^n \\ x \neq x^*}} \frac{1}{\sqrt{2^n}} |x\rangle$$

This can be graphically represented as a reflection of $|s\rangle$ about $|s'\rangle$ (vector orthogonal to $|x^*\rangle$ obtained from $|s\rangle$ by removing $|x^*\rangle$ and rescaling). This step lowers the average amplitude (the dotted line) since the amplitude of $|x^*\rangle$ becomes negative.



- Apply the *Grover diffusion operator*. This does another reflection around the lower average amplitude such that the amplitude of $|x^*\rangle$ gets magnified leaving all the other states roughly the same. This reflection, $2|s\rangle\langle s| - I$ can be visualized graphically as,



Steps 2. and 3. can then be repeated $t \geq 1$ times to further increase the amplitude of the target state. In general, about $O(\sqrt{n})$ repetitions suffices.

GROVER'S ALGORITHM: EXAMPLE

Suppose we have $n = 3$ qubits, and the solution state $x^* = |111\rangle$. After the first step we obtain a uniform superposition state where each state $|x\rangle \in \{0, 1\}^n$ has an amplitude equal to $\frac{1}{\sqrt{2^n}} = \frac{1}{\sqrt{8}} = \frac{1}{2\sqrt{2}}$. That is, after the first step we get,

$$|s\rangle = \sum_{|x\rangle \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |x\rangle = \sum_{|x\rangle \in \{0,1\}^n} \frac{1}{2\sqrt{2}} |x\rangle.$$

In the second step, we apply the *oracle* and get the state,

$$\begin{aligned} &= \frac{-1}{2\sqrt{2}} |111\rangle + \sum_{\substack{x \in \{0,1\}^n \\ x \neq |111\rangle}} \frac{1}{2\sqrt{2}} |x\rangle \\ &= |s\rangle - \frac{1}{\sqrt{2}} |111\rangle. \end{aligned}$$

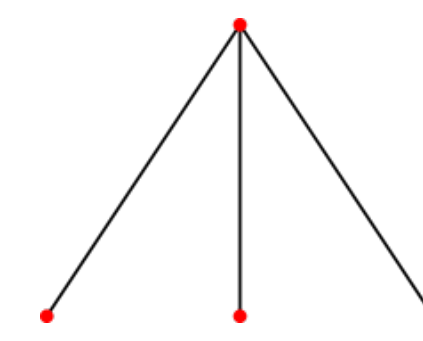
In the third step, we apply *Grover diffusion* and get,

$$\begin{aligned} &= [2|s\rangle\langle s| - I](|s\rangle - \frac{1}{\sqrt{2}} |111\rangle) \\ &= 2|s\rangle\langle s|s\rangle - |s\rangle - 2|s\rangle\langle s|111\rangle \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} |111\rangle \\ &= \frac{1}{2} |s\rangle + \frac{1}{\sqrt{2}} |111\rangle; \quad (\langle s|s\rangle = 1, \langle s|111\rangle = \frac{1}{2\sqrt{2}}) \\ &= \frac{1}{2} \left[\frac{1}{2\sqrt{2}} \sum_{|x\rangle \in \{0,1\}^n} |x\rangle \right] + \frac{1}{\sqrt{2}} |111\rangle \\ &= \frac{1}{4\sqrt{2}} \sum_{\substack{|x\rangle \in \{0,1\}^n \\ |x\rangle \neq |111\rangle}} |x\rangle + \frac{5}{4\sqrt{2}} |111\rangle. \end{aligned}$$

We can observe that after a single iteration of Grover's algorithm the amplitude of solution state $x^* = |111\rangle$ gets amplified from $\frac{1}{2\sqrt{2}} \approx 0.35$ to $\frac{5}{4\sqrt{2}} \approx 0.88$ while the amplitude of other states gets reduced to $\frac{1}{4\sqrt{2}} \approx 0.17$. Amplitude of a state is analogous to the probability that the state gets measured.

IDENTIFYING CLAWS USING GROVER'S ALGORITHM

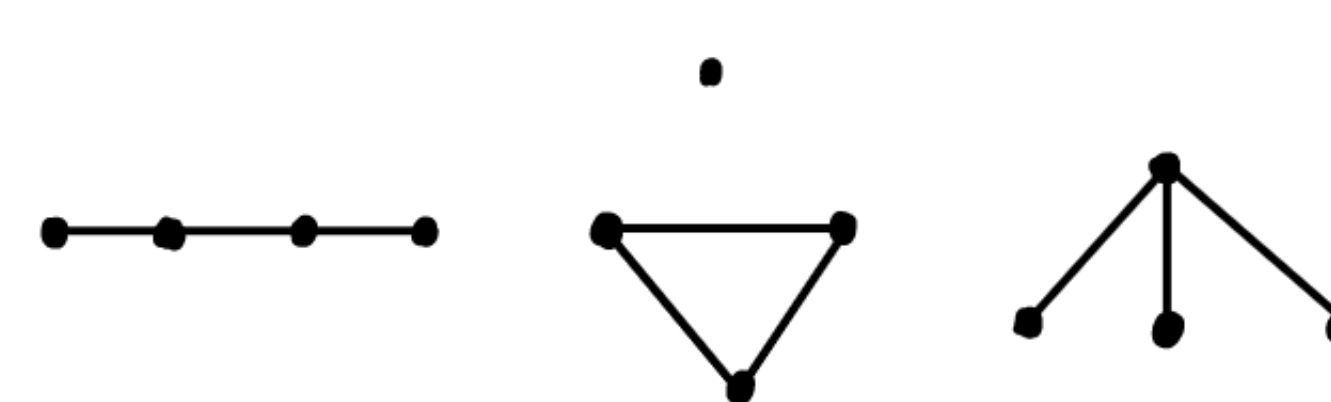
A *claw* is a complete bipartite graph $K_{1,3}$ comprising of three edges, three leaves and a central vertex as shown below. A *claw-free* graph is a graph in which no induced subgraph is a claw.



In practice, the oracle part of Grover's Algorithm can be implemented by using a checking circuit (a quantum circuit that can check whether a particular state is a solution) with ancillary qubits along with *phase kickback* and *uncomputation*. In this particular case of identifying claws in graph, the checking circuit can be implemented by defining a claw as a state x^* that satisfies the following conditions:

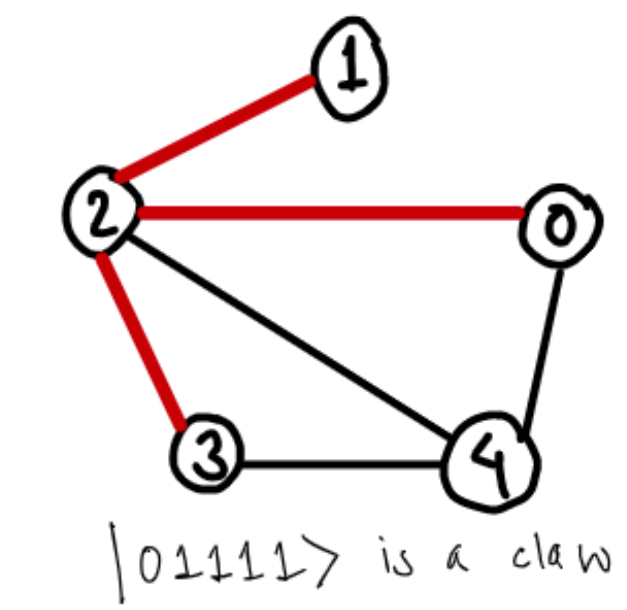
- The state has exactly 4 nodes.
- The state has exactly 3 edges.
- Every node in the state has an odd number of edges connected to it.

The third condition is added in order to distinguish between the following three cases where (i) and (ii) are satisfied, but only one of them is actually a claw.

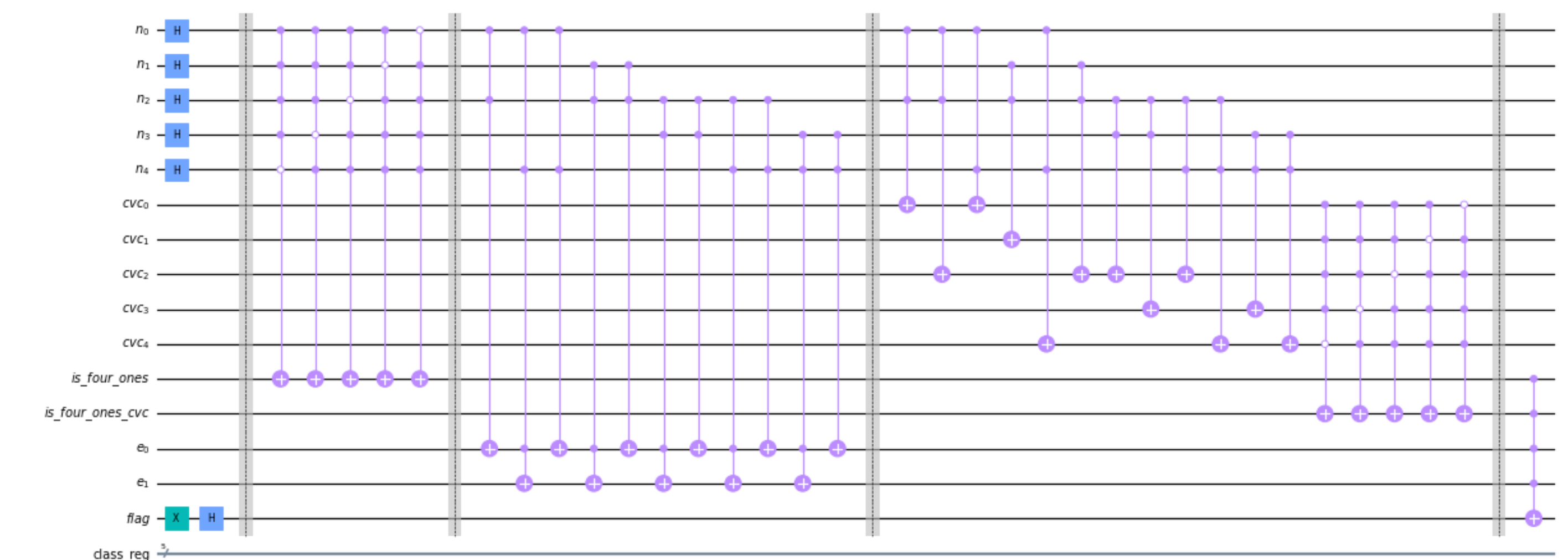


CONTINUED

So, if we have a graph with a claw (in red) as in the following example,

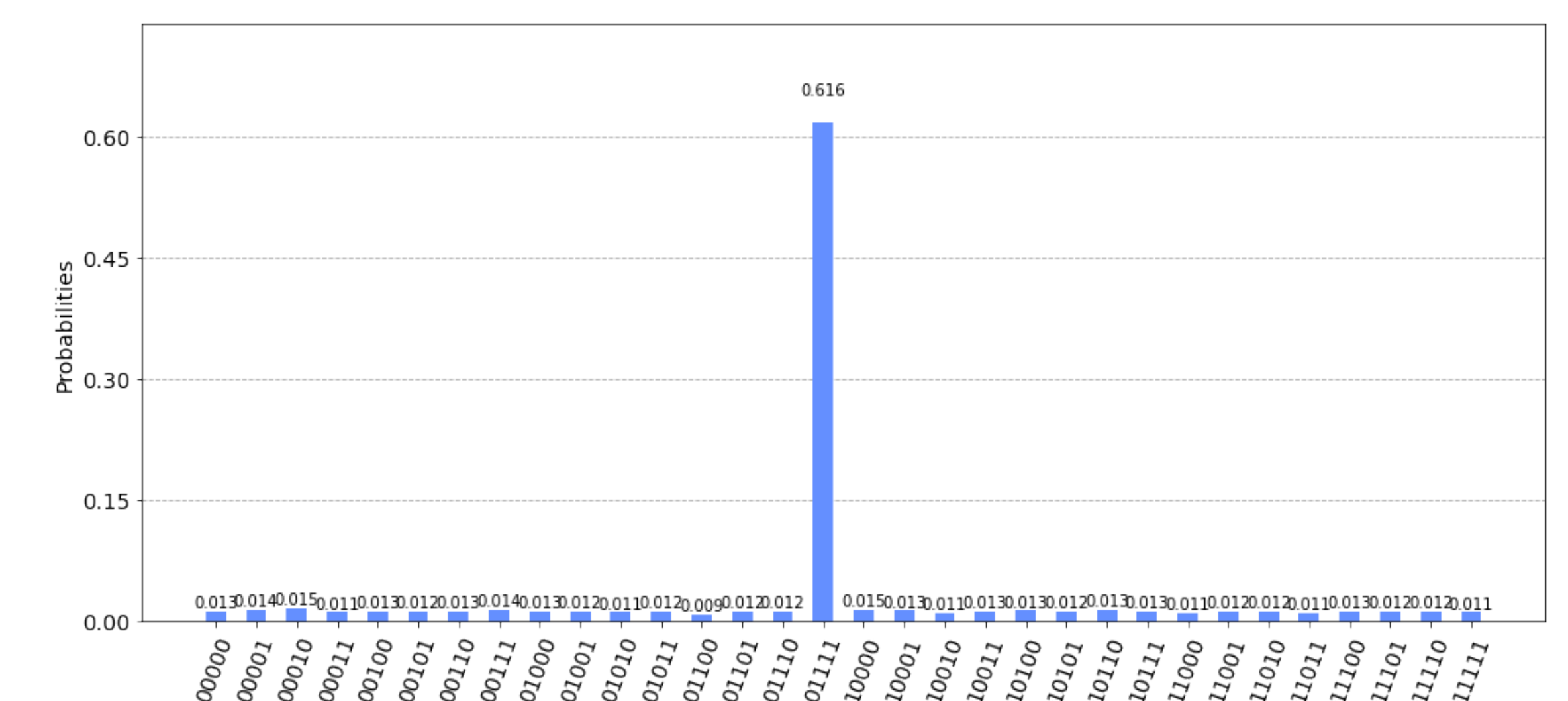


we can use Qiskit to implement Grover's algorithm for the graph by using the following circuit.



Here, the first five qubits represent each of the five nodes in the graph. These are initialized by applying Hadamard gates. The first segment within the two barriers (dotted vertical lines) checks the condition (i) for the claw, that is, if the state has exactly four nodes. The second segment checks condition (ii), that is, if the state has exactly three edges. The third segment checks condition (iii), that is, if every node in the state has an odd number of edges connected to it. The final segment completes the oracle by applying a negative sign to the state x^* that satisfies all of the three conditions by using the *phase kickback* phenomenon. The circuit is completed by following the circuit segment above with *uncomputation* (reset the ancillary qubits), Grover diffusion (reflect and maximize x^*) and measurement.

The result obtained from 10000 simulated runs with oracle and diffusion applied twice using the above circuit and graph is as follows.



It can be observed that the probability of measuring the solution state, $x^* = |01111\rangle$ is amplified. The graph presented has only a single claw, however the circuit also works for graphs with multiple claws with the probability of all the claws maximized together. In the case where there are no claws in the graph (claw-free graph), the result is a uniform probability distribution with all 2^n states having equal probability of being measured.

REFERENCES

- <https://qiskit.org/textbook/ch-algorithms/grover.html>
- <https://www.cs.cmu.edu/~odonnell/quantum15/lecture04.pdf>