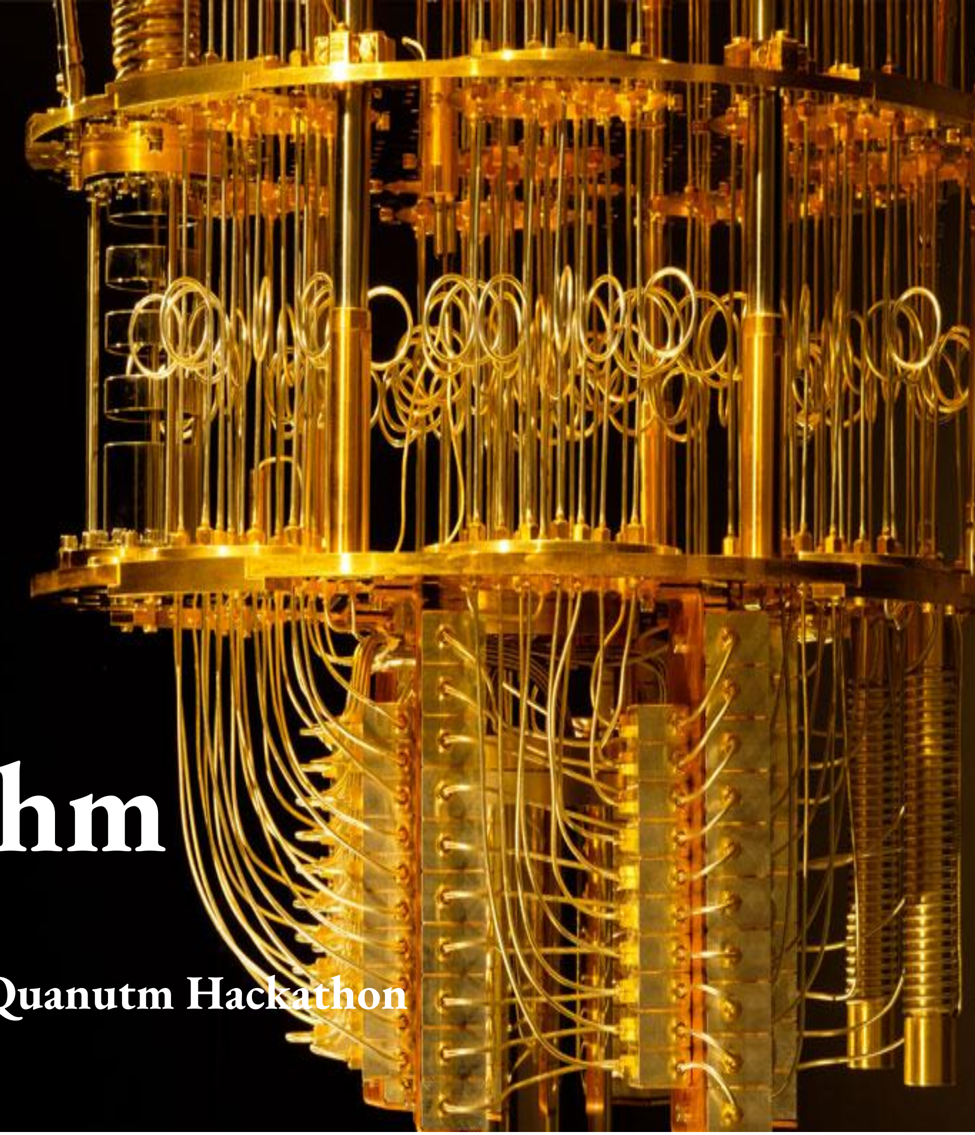
Welcome to the new era of *Quantum Computing*
- where *Quantum Physics* entangles with *Computing*

The Grover's Search Algorithm



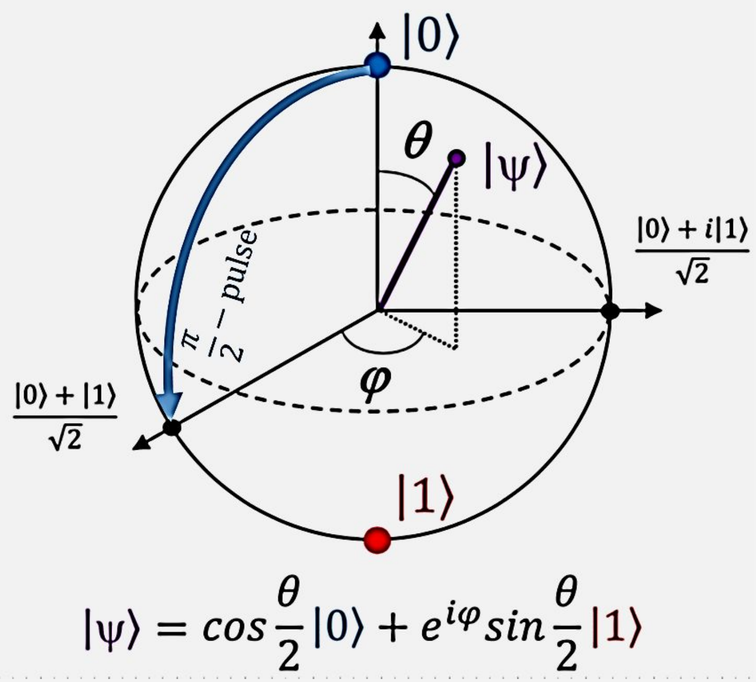
Prepared by Mohammad Aamir Sohail and Erin Diran-Ojo for the ISIT 2025 Quanutm Hackathon

ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY OF MICHIGAN

Hackathon
where quantum computing meets information theory

ISIT JUNE 22-27 ANN ARBOR MICHIGAN

Outline:



1. Motivation: Unstructured Search
2. Introduction-Grover's Algorithm
3. Amplitude Amplification
4. Grover's Circuit
5. References & Further Reading

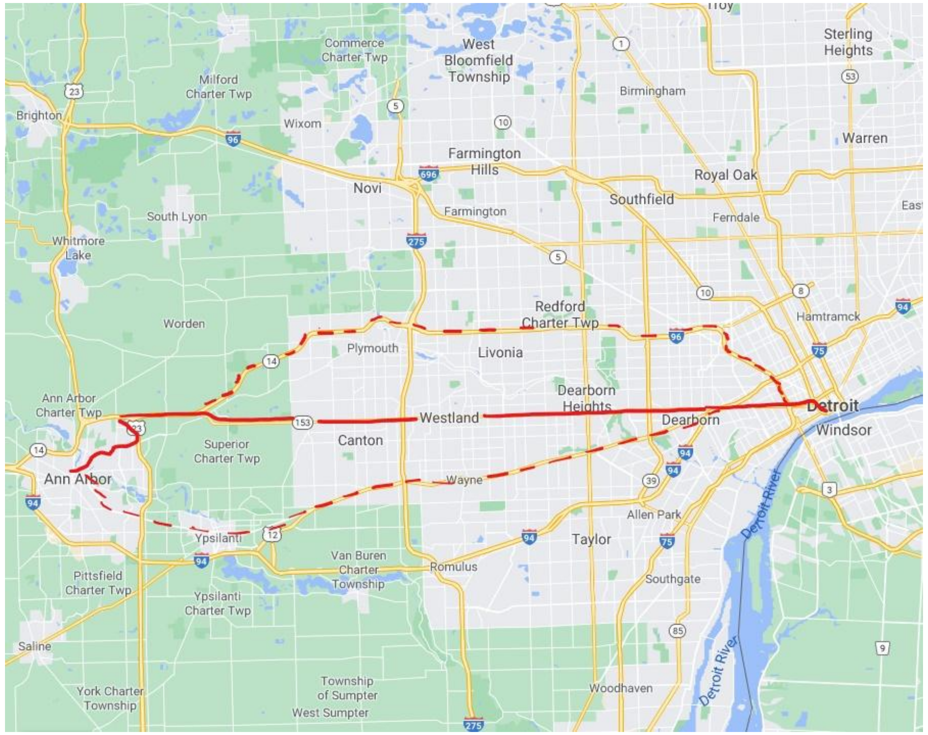
Motivation– Unstructured Search

Suppose we have given a large list of N (unstructured) items.
Among these we wish to find items which is a solution to a certain problem.

# of employees: $N = 2^n$

First Name	Last Name	Position	Company
Thomas	Sneed	Inspector	Sink, Inc.
Betty	Brown	Line Manager	Carp Corp.
Larry	Snopes	CEO	Snopes, LLC
Reginald	Williams	Partner	Williams, Lane & Porter, PC
Wendy	Lane	Clown	Party Hearty
Steve	Linder	Support Representative	Carp Corp
Patrick	Gerald	Attorney	Williams, Lane & Porter, PC
Stanley	Worrell	Store Manager	Quick Tire & Battery
Janet	Mercer	Catering Sales	Pellatino Patries
Sandeep	Khatri	VP Sales	Widget Mania

# of possible paths: $N = 2^n$



Problem 1: Find details of Wendy Lane from a database.

Problem 2: Find the shortest path between Ann Arbor and Detroit.

continued...

Problem: Let $x_1, x_2, x_3, \dots, x_n$ be the variables which take only positive integer value, $0 \leq x_1 \leq M$-1.
Find $x_i's$ such that $(x_1 + x_2 + x_3 + \dots + x_n) = \delta$.

# of possible combinations: $N = M^n$

Naïve Approach:

Define $p(\overline{\boldsymbol{x}}) = (1_n \cdot \overline{\boldsymbol{x}})$ - δ

For each possible $\overline{\boldsymbol{x}}$ = $(x_1, x_2, x_3, \dots, x_n)$,
  Compute $p(\overline{\boldsymbol{x}})$,
  if $p(\overline{\boldsymbol{x}}) = 0$,
  $\longrightarrow$ $\overline{\boldsymbol{x}}$ is a solution
  else
  $\longrightarrow$ $\overline{\boldsymbol{x}}$ is not a solution

Classically ...

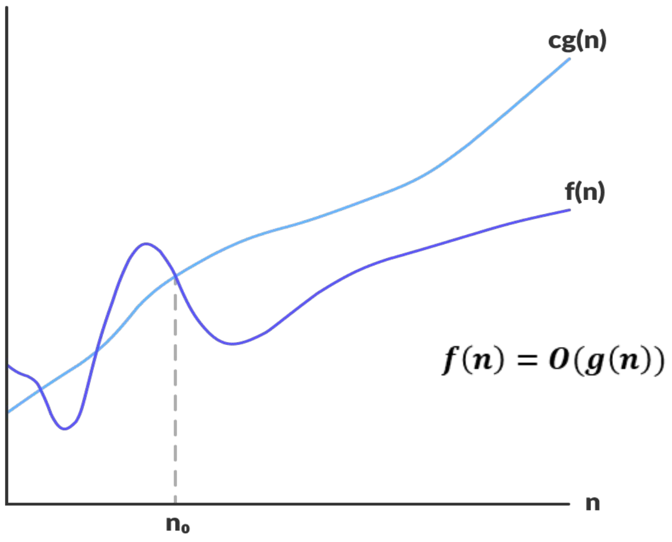
- The performance of the classical search algorithm is $\boldsymbol{O}(\boldsymbol{N})$.
- Using classical computation, in order to search an element in an unstructured list with probability 0.5, one need to traverse at $N/2$ elements.
- Worst case, one need to traverse N elements to find a solution.

Detour : Big-O Notation

Definition:

Let f and g are the functions from the set of real numbers ($\mathbb{R}$) to the set of real numbers ($\mathbb{R}$). We say that $\boldsymbol{f(n) = O(g(n))}$, if there exist positive constant c and n_0 such that-

$$0 \le f(n) \le cg(n), \qquad for\ all\ n \ge n_0$$

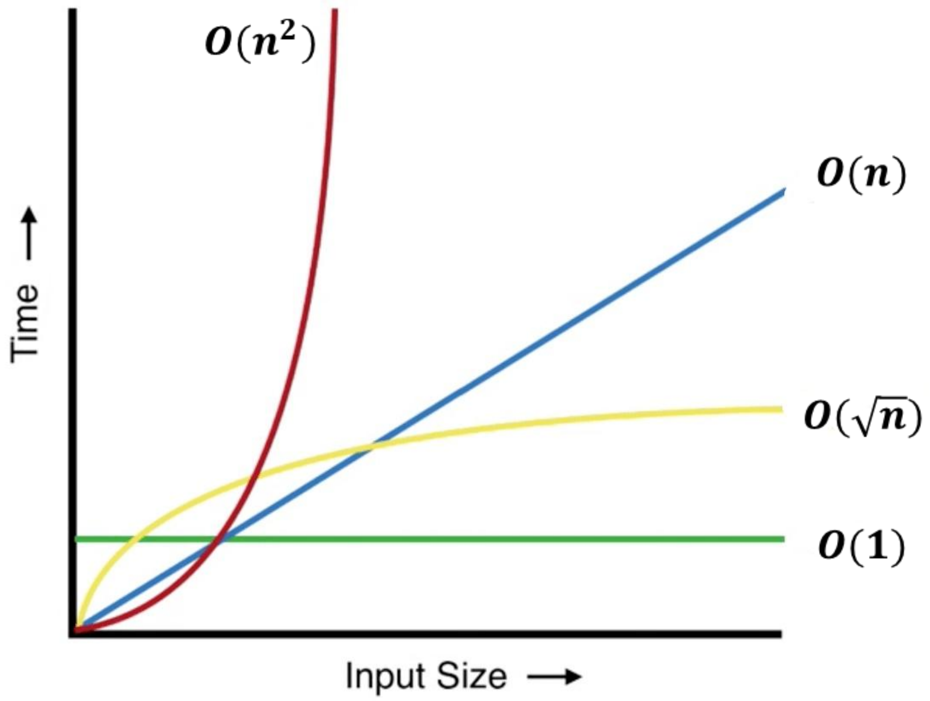


Here, $g(n)$ is an asymptotic upper bound for $f(n)$

Why do we need Big-*O*?

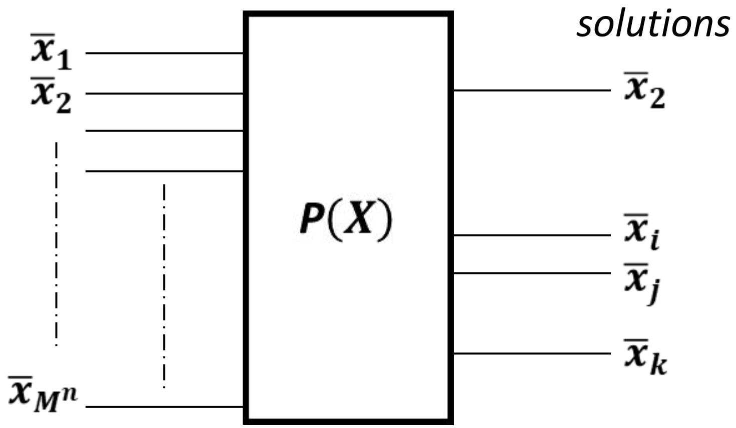
In computer science, it is used to categorize the algorithm based on their scalability.

** *Estimating the worst case running time of an algorithm as a function of the input size* **



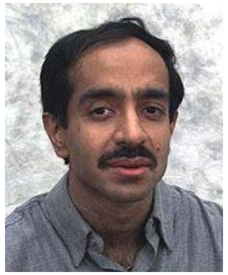
Quantum Search Algorithm

Question:
Can we compute $p(\overline{\boldsymbol{x}})$ *at once for all* possible $\overline{\boldsymbol{x}}$.



"***Quantum Parallelism***" or "***Superposition***"

The Grover's Search Algorithm



Lov Grover published a "*Quantum Unstructured Search Algorithm*" in 1996 with complexity $\boldsymbol{O}(\sqrt{\boldsymbol{N}})$. It's commonly known as the Grover's algorithm.

It provides 'quadratic speedup' over classical algorithm.

Consider a list of million elements, which contains integer 1 to 10^6, in randomised order. We need to traverse the list and find out the integer 59.

Classically: $\sim \frac{10^6}{2} = (5 \times 10^5)$ units of time.
Quantum: $\sqrt{10^6} = 10^3$ units of time.

$\boldsymbol{O}(\sqrt{\boldsymbol{N}})$! *But we are using* ***Quantum Parallelism***

Amplitude Amplification

Let the search space be $S = \{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$**, basis for the N dimensional Hilbert Space.**
Also, $|x_o\rangle \in S$ **be a solution to problem** $p(x)$.

Step 0: ***Uniform Superposition***

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

Steps:

1. Flipping the sign of the x_o
2. Inversion about the mean

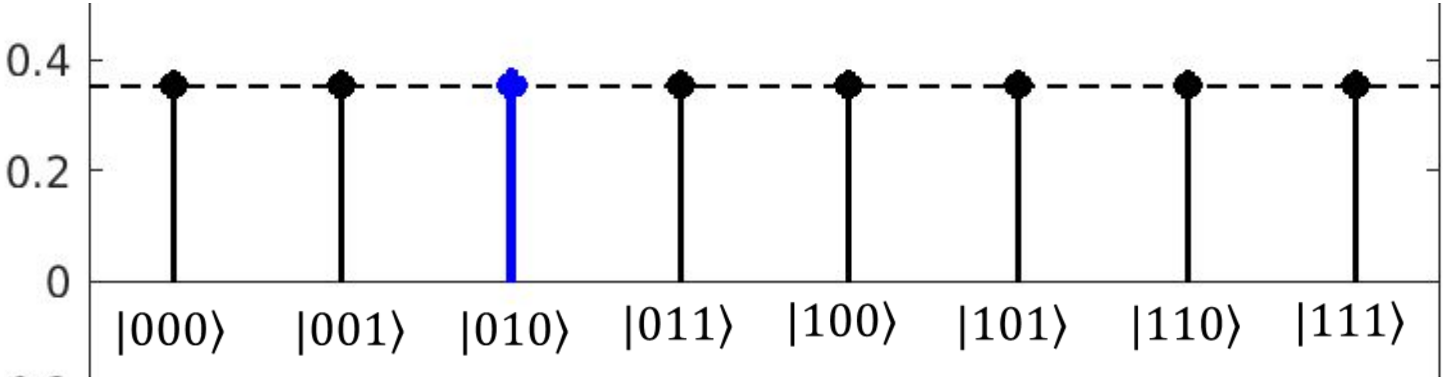
Note: Qbit or **Quantum Bit** is a state vector of 2-dimensional Hilbert Space.
(standard /computational) Basis: $\{|0\rangle, |1\rangle\}$

Consider an example of $n = 3$ qubits quantum system.
$\dim(\mathcal{H}) = N = 2^n = 8$

Basis (search space): $\{|000\rangle, |001\rangle, \ldots, |111\rangle\}$ (i.e. $|0\rangle \to |7\rangle$).

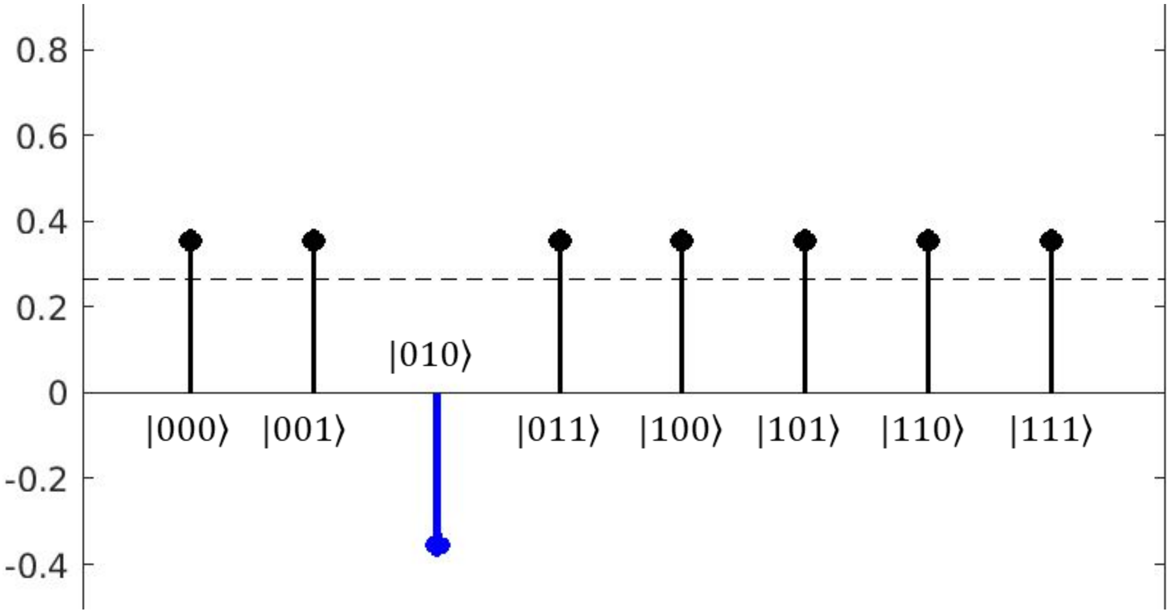
Step 0:

$$|\psi\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{8} |x\rangle = \frac{1}{\sqrt{8}} \{|000\rangle + |001\rangle + \ldots + |111\rangle\}$$

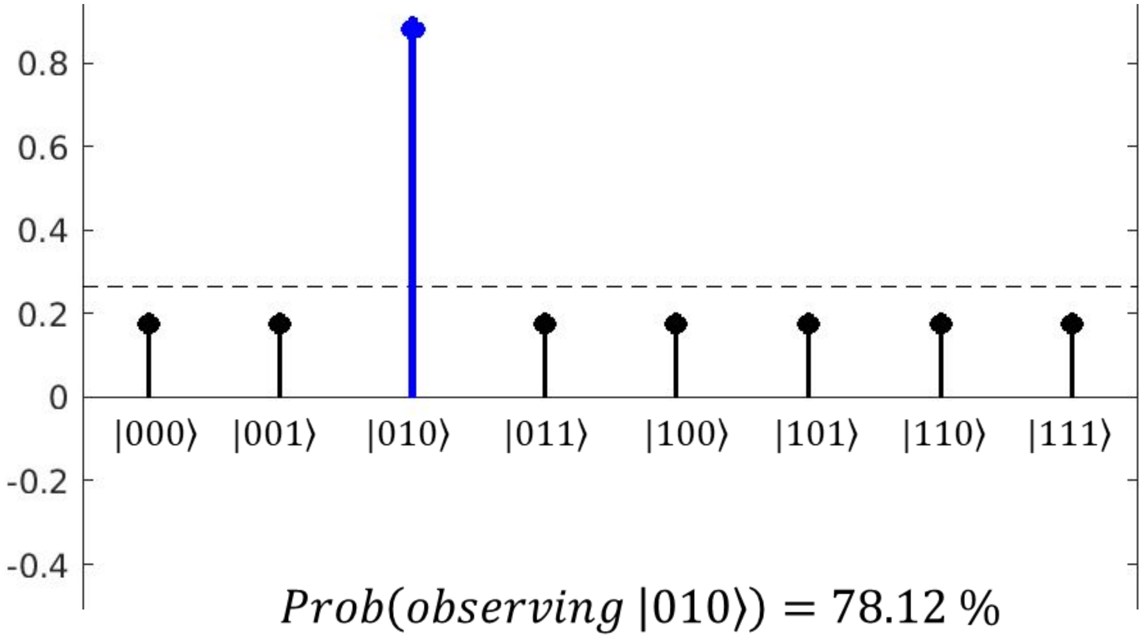


Amplitude Amplification continued …

Step 1: Flipping the sign



Step 2: Inversion about the mean

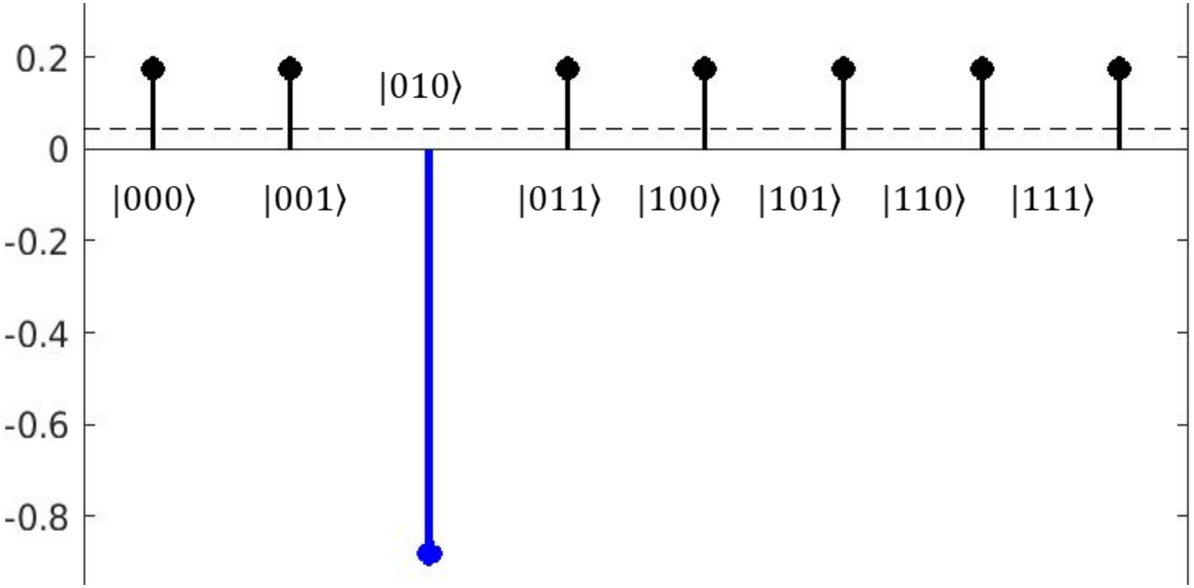


Note: y-axis represents prob. amplitude

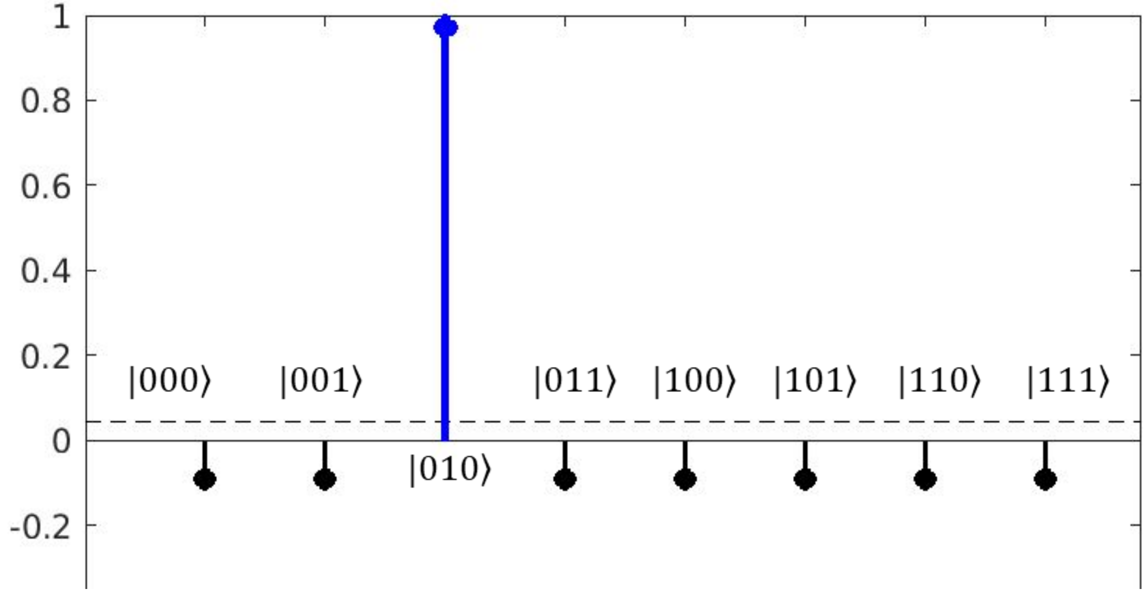
Amplitude Amplification continued ...

Iteration # 2

Step 1: Flipping the sign



Step 2: Inversion about the mean

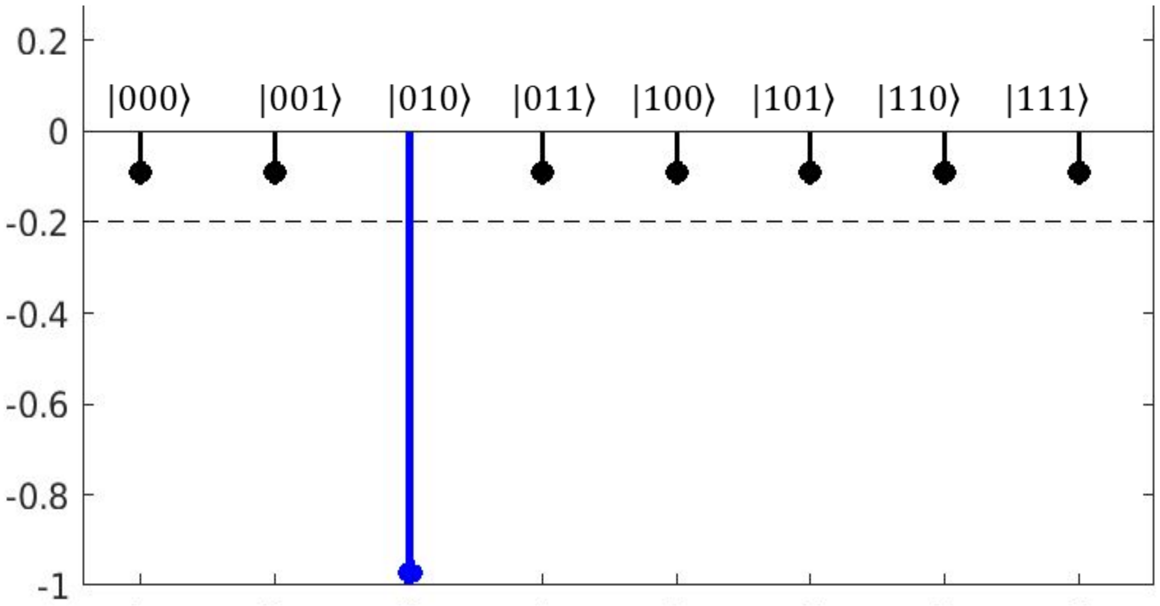


$Prob(observing\ |010\rangle) = 94.53\ \%$

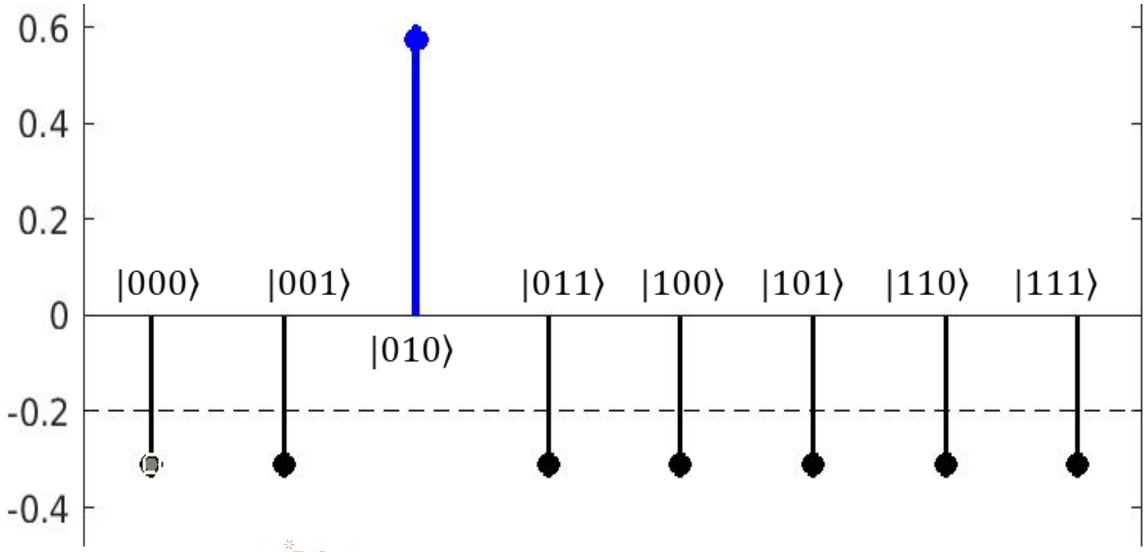
Amplitude Amplification continued …

Iteration # 3

Step 1: Flipping the sign



Step 2: Inversion about the mean



$Prob(observing\ |010\rangle) = 33.01\ \%$

Performance Analysis:

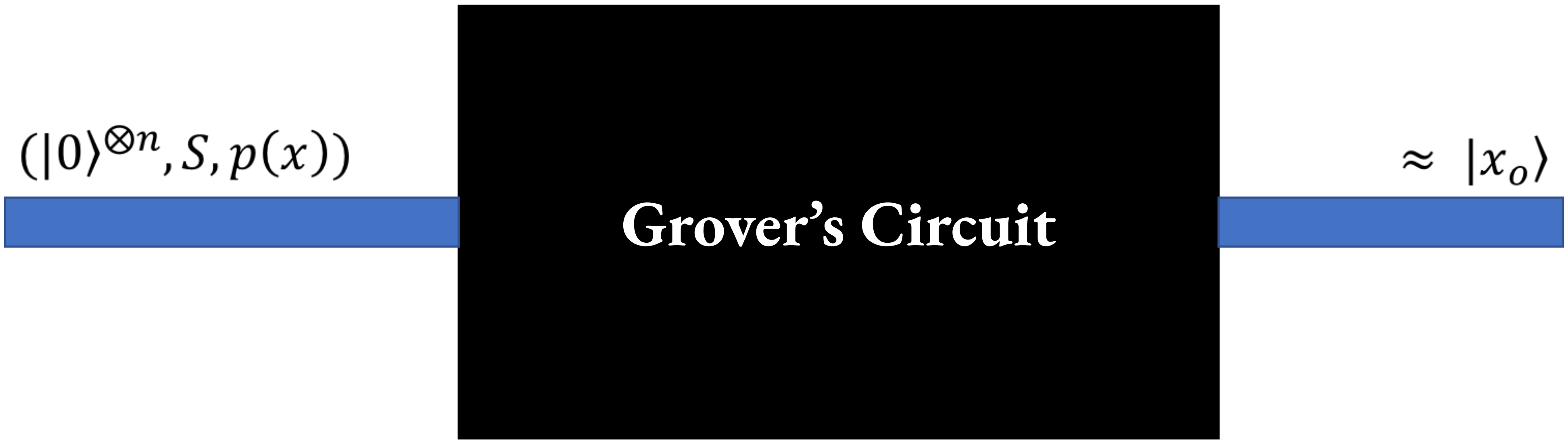
upper bound on the # of iterations: $itr \leq \left\lceil \frac{\pi}{4}\sqrt{\frac{N}{M}} \right\rceil\ i.e.\ O\left(\sqrt{\frac{N}{M}}\right),$

$here\ N\ is\ the\ dimension\ of\ search\ space, M\ is\ the\ \#\ of\ solution\ of\ p(x).$

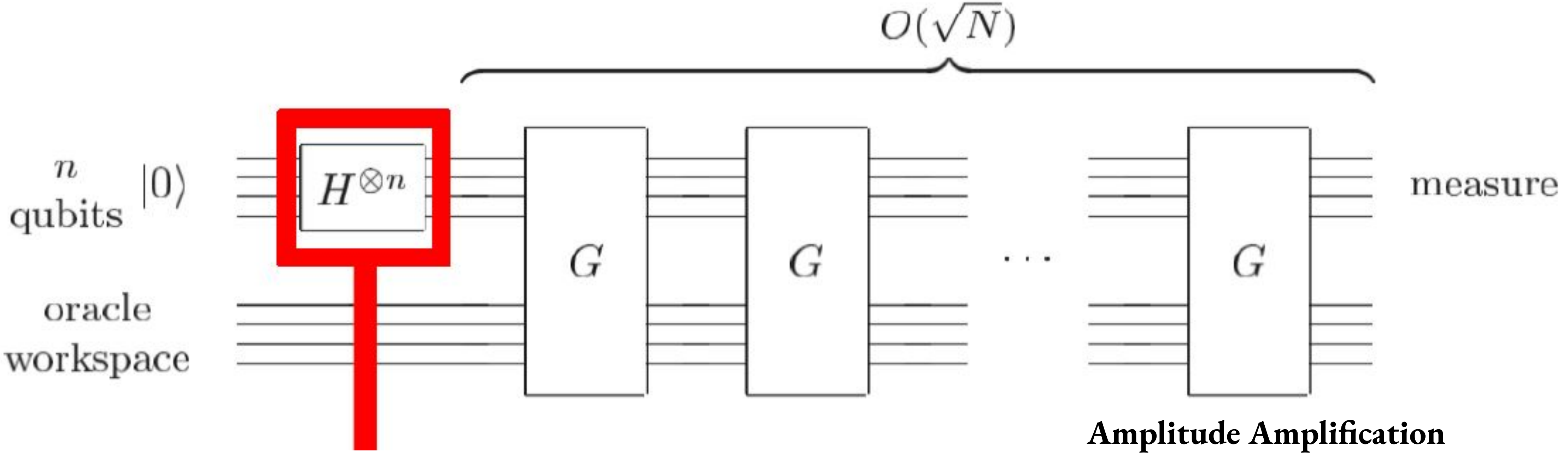
**** Geometrical Interpretation, Chp.6, Neilson and Chuang, Quantum Computation and Quantum Information*

Grover's Circuit

Let the search space be $S = \{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$**, basis for the N dimensional Hilbert Space.**
Also, $|x_o\rangle \in S$ **be a solution to problem** $p(x)$.



The Algorithm: breaking it down …



Amplitude Amplification

Hadamard Gate,

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$H|0\rangle = \frac{1}{\sqrt{2}}\{|0\rangle + |1\rangle\}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\{|0\rangle - |1\rangle\}$$

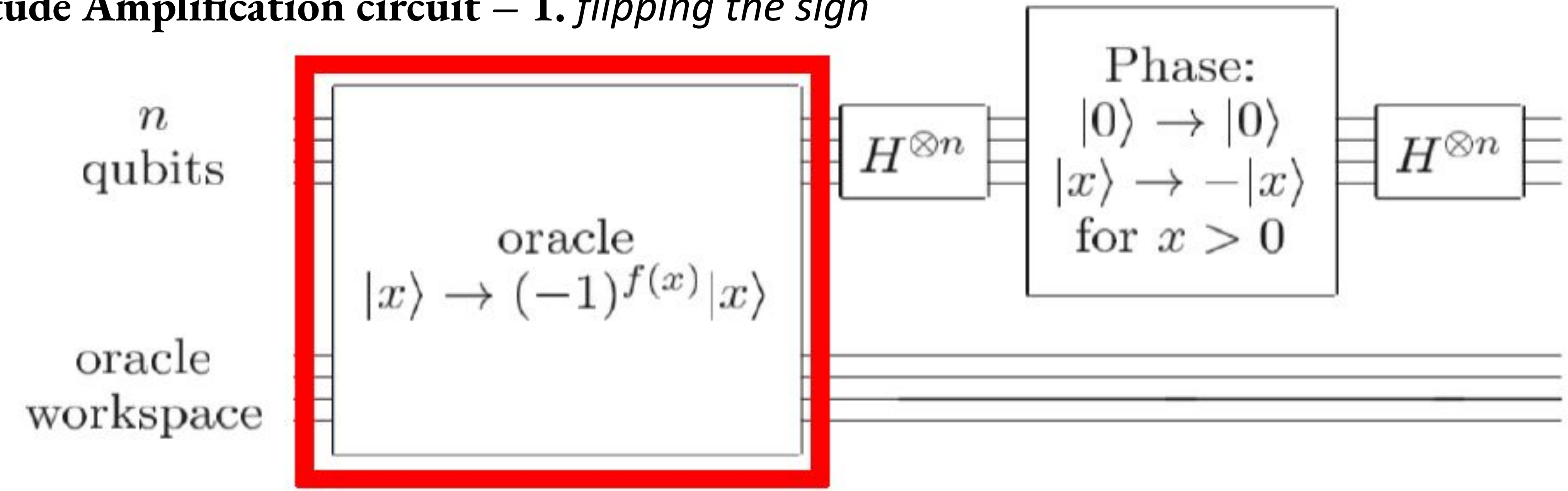
$$\Rightarrow H^{\otimes n}|0\rangle^{\otimes n} = |\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

Example: $\boldsymbol{n = 3\ qubits, N = 2^n = 8.}$

$$H^{\otimes 3}|0\rangle^{\otimes 3} = |\psi\rangle = \frac{1}{\sqrt{8}}\sum_{x=0}^{8}|x\rangle = \frac{1}{\sqrt{8}}\{|000\rangle + |001\rangle + |010\rangle + |011\rangle + |101\rangle + |110\rangle + |111\rangle\}$$

The Algorithm: breaking it down …

Amplitude Amplification circuit – 1. *flipping the sign*



oracle:

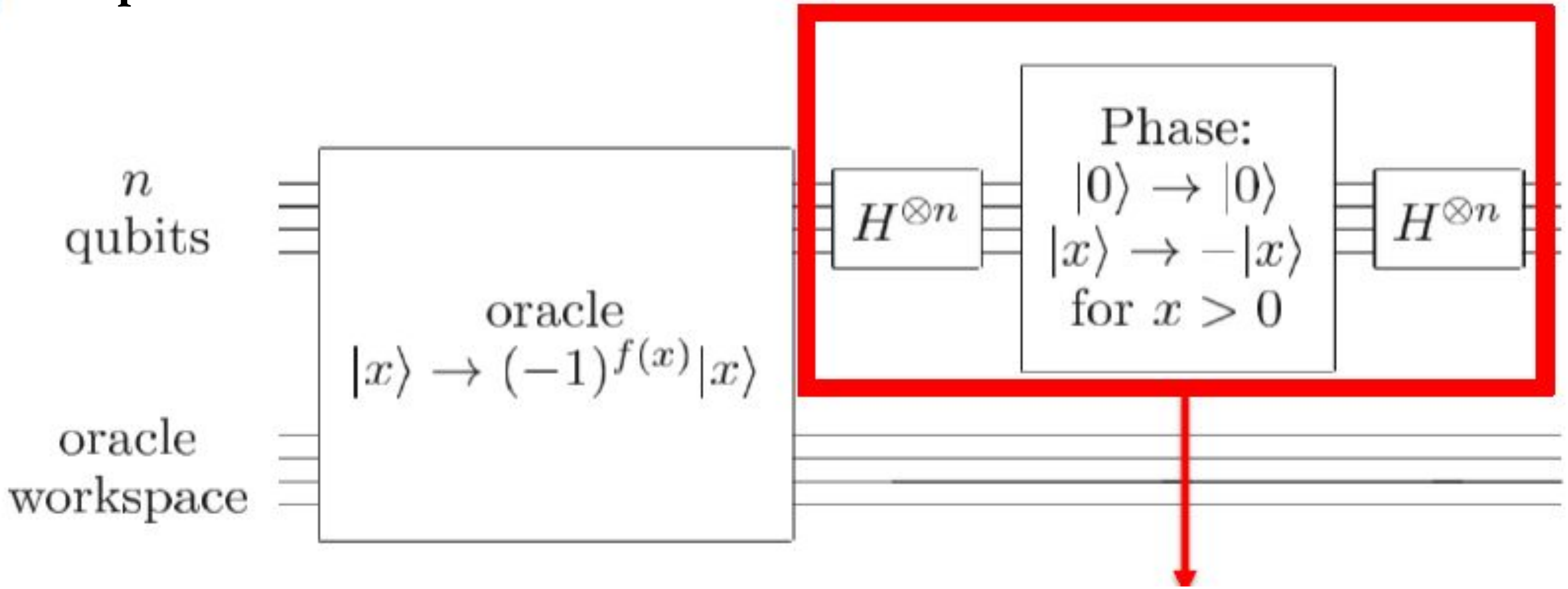
$$f(x) = \begin{cases} 1, & |x\rangle = |010\rangle \\ 0, & |x\rangle \neq |010\rangle \end{cases}$$

Example: $n = 3\ qubits, N = 2^n = 8, |x_0\rangle = |010\rangle$

$$|\psi_1\rangle = \frac{1}{\sqrt{8}}\{|000\rangle + |001\rangle - |010\rangle + |011\rangle + |101\rangle + |110\rangle + |111\rangle\}$$

The Algorithm: breaking it down ...

Amplitude Amplification circuit – 2. *inversion about mean)*



Diffusion Operator

$$D = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = (2|\psi\rangle\langle\psi| - I)$$

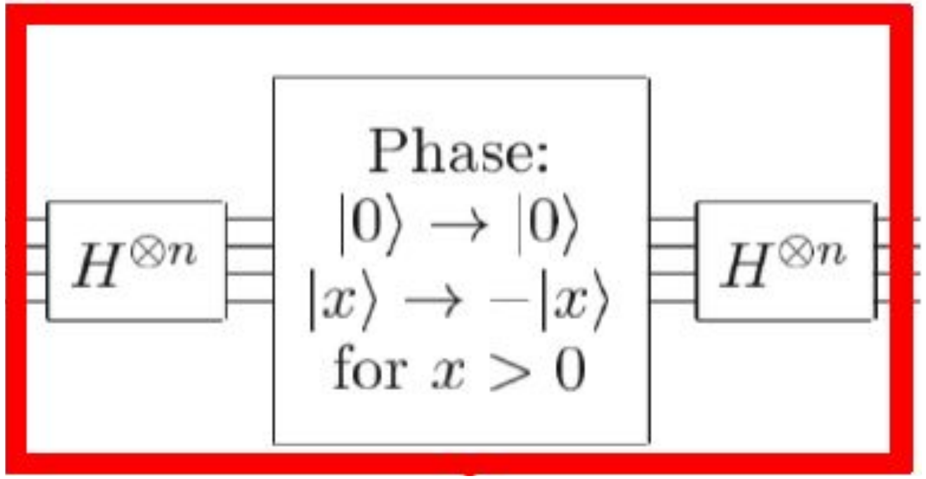
$$|\psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$$

Example: $n = 3\ qubits, N = 2^n = 8, |x_0\rangle = |010\rangle$

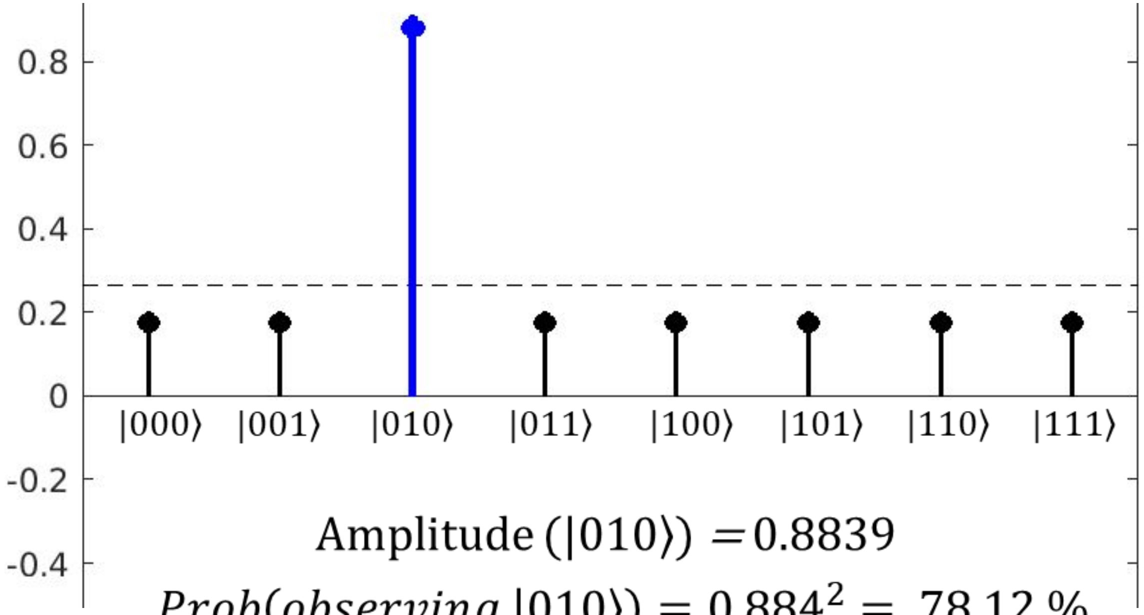
$$|\psi_2\rangle = (2|\psi\rangle\langle\psi| - I)|\psi_1\rangle = [(2|\psi\rangle\langle\psi| - I)\mathrm{Oracle}]|\psi\rangle = \mathrm{G}\,|\psi\rangle$$

The Algorithm: breaking it down ...

Amplitude Amplification circuit – 2. *inversion about mean*



$$\mathbf{(2|\psi_1\rangle\langle\psi_1| - I)}$$



Amplitude $(|010\rangle) = 0.8839$

$Prob(observing\ |010\rangle) = 0.884^2 = 78.12\ \%$

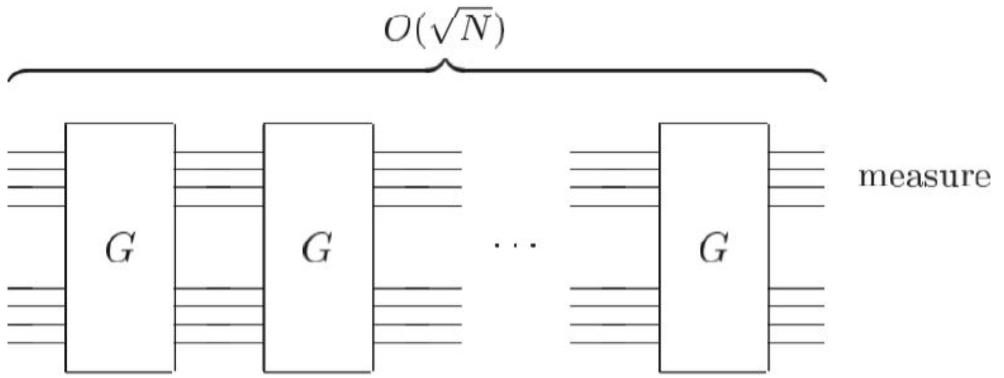
Example: $\boldsymbol{n = 3\ qubits, N = 2^n = 8, |x_0\rangle = |010\rangle}$

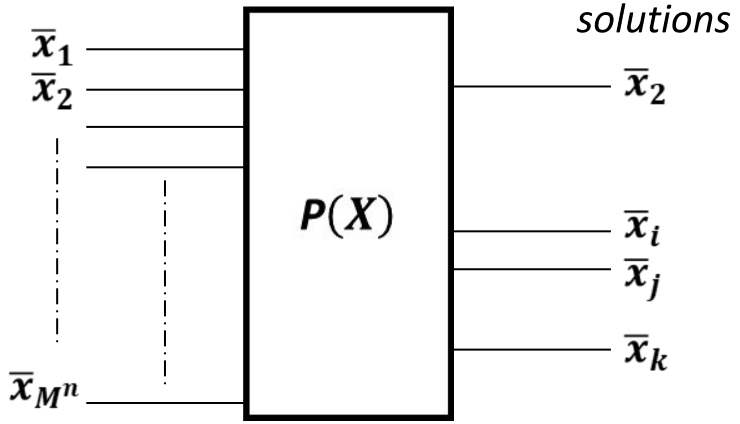
$$|\psi_1\rangle = \frac{1}{\sqrt{8}}\{|000\rangle + |001\rangle - |010\rangle + |011\rangle + |101\rangle + |110\rangle + |111\rangle\}$$

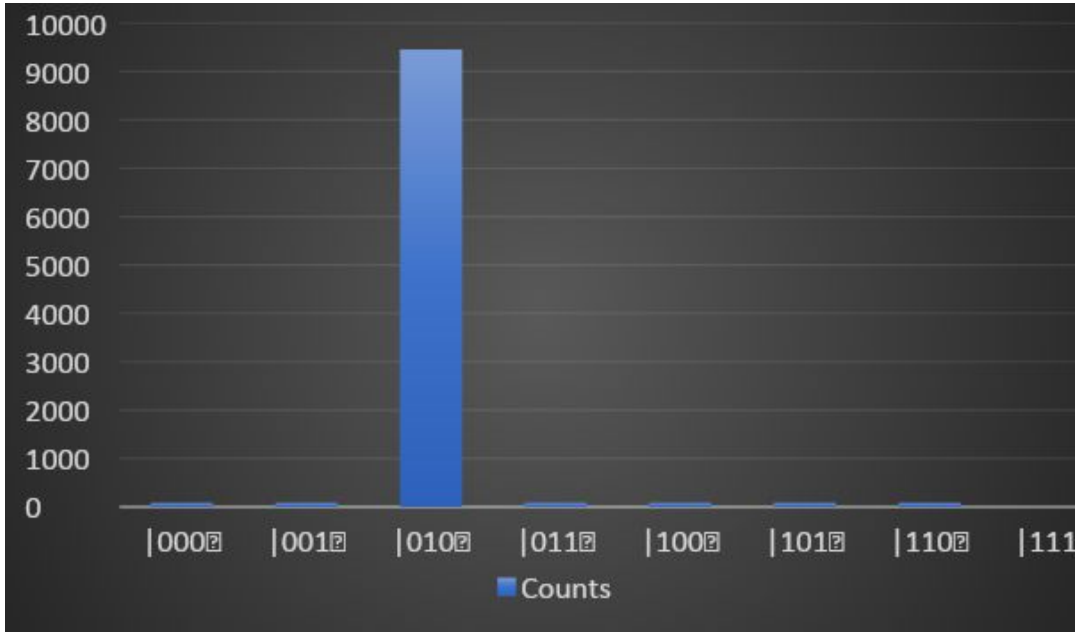
$$(2|\psi_1\rangle\langle\psi_1| - I)|\psi_1\rangle = 0.1768 * \{|000\rangle + |001\rangle + |011\rangle + |101\rangle + |110\rangle + |111\rangle\} + 0.8839 * |010\rangle$$

Conclusion

The Grover's Algorithm







Summary:

- Superposition
- Amplitude Amplification:
  - Flipping the sign
  - Inversion about mean
- Repeat the above process $O(\sqrt{N})$ times
- Perform Measurement

Applications:

- Finding minimum
- Cryptography – finding keys

References

- Grover’s Algorithm, Chapter 3, Section-3.10, Qiskit Notebook.
  https://qiskit.org/textbook/ch-algorithms/grover.html
- Lecture 4- Grover’s Algorithm, Quantum Computation-Fall 2015, John Wright (CMU).
  https://www.cs.cmu.edu/~odonnell/quantum15/lecture04.pdf
- The Grover’s Algorithm, QSIT16-talks, Camilo Zapata, Xiao yang.
  https://qudev.phys.ethz.ch/static/content/QSIT16/talks/Grover_QSIT.pdf

Further Reading

- Quantum Computation and Quantum Information, Neilson and Chuang
- Dancing with Qubits, Robert S. Tutor
- Quantum Algorithms for Beginners (https://arxiv.org/pdf/1804.03719.pdf)