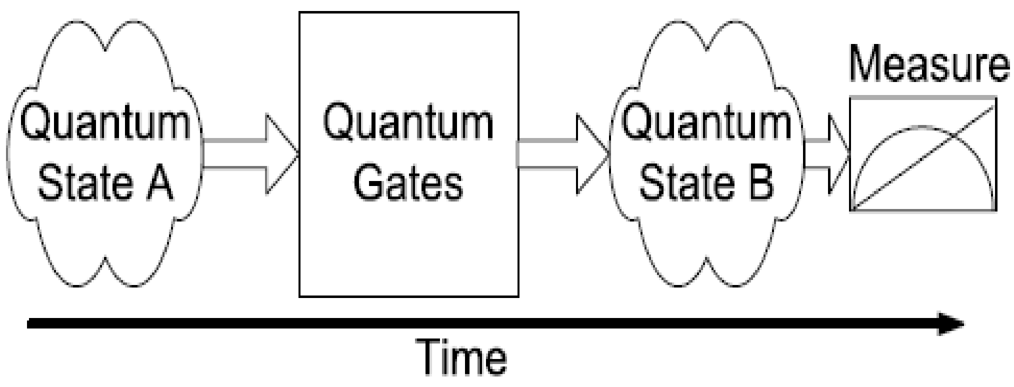
QUANTUM INFORMATION

Deutsch-Jozsa Algorithm
Grover's Algorithm

Y.AADEL

Quantum Algorithm

Quantum circuits are a collection of wires (qubits) and gates that depict the time evolution of a quantum algorithm. The qubits are prepared in a known state and introduced as inputs to the system. The qubits then undergo evolution depicted by the gate operations on them. The evolution ends when the system is subjected to a quantum measurement.



Quantum Algorithm

Most quantum algorithms developed to date are based on four general techniques:

- **QFT** Quantum Fourier Transform: the Deutsch-Jozsa algorithm, Shor's algorithm.
- **Amplitude amplification**: Grover's algorithm.
- **Quantum Simulation:** approximating the Jones polynomial and solving linear equations.
- **Quantum Walk :**
  - element distinctness (**Ambainis)**
  - NAND trees evaluation (**Farhi, Goldstone, Gutmann**)
  - Triangle finding (**F.Magniez et al.)**
  - Evaluating Boolean Formulas (**Farhi et al**.)
  - …

Deutsch-Jozsa Algorithm

The first algorithm to show that quantum computers are capable of solving certain computational problems much more efficiently than classical deterministic computers

The problem

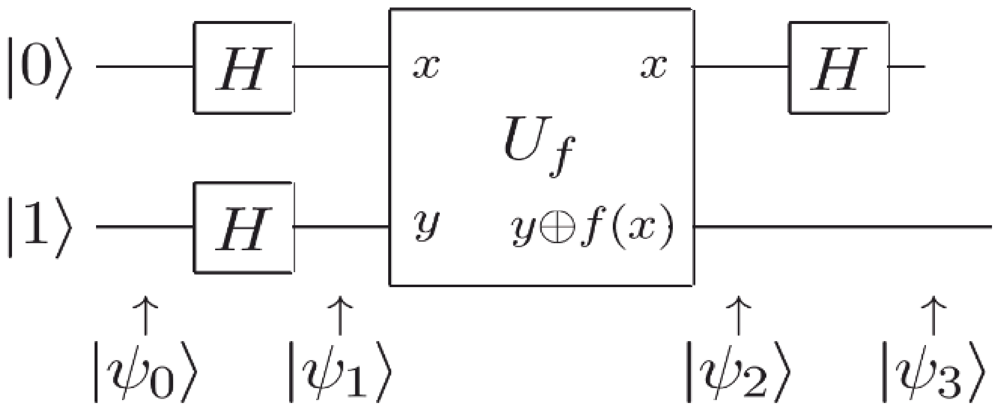
For $N=2^n$ we are given

$$\begin{cases} x \in \{0,1\}^N \\ f : \{0,1\}^N \to \{0,1\} \end{cases}$$

Function f which is one of two kinds, either *f(x) is constant* for all values of x or *f(x) is balanced*, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half.

The goal is to find out whether f(x) is balanced or constant

Deutsch-Jozsa Algorithm



Circuit Deutsch-Jozsa for one qubit

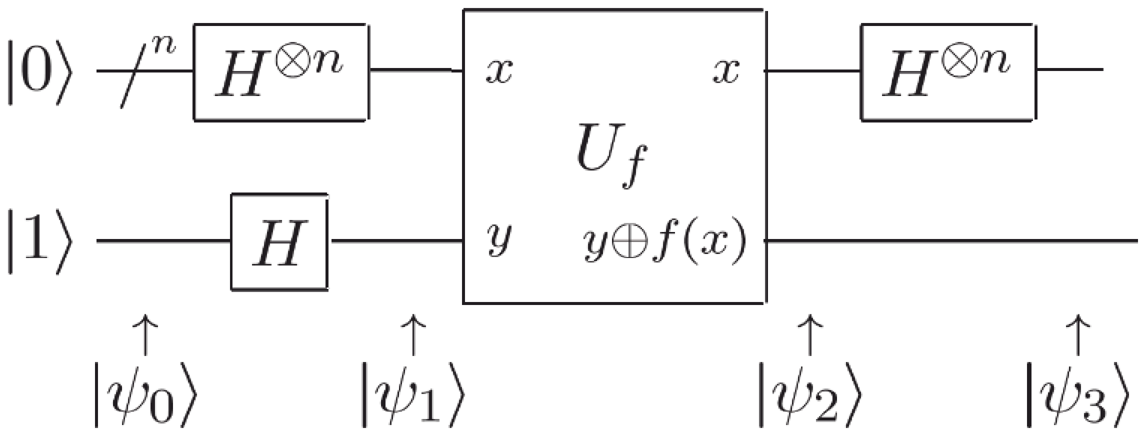
$$|\psi_1\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = (-1)^{f(0)} \frac{1}{2}\left[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right] \otimes (|0\rangle - |1\rangle)$$

$$\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right) \xrightarrow{H} \frac{1}{2}\left(|0\rangle + |1\rangle + (-1)^{f(0)\oplus f(1)}(|0\rangle - |1\rangle)\right)$$

after measure the first qubit we conclure that f constant or balanced

Deutsch-Jozsa Algorithm



Deutsch-Jozsa Circuit for n qubit

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x.z+f(x)}}{2^n} |z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Classically we get the solution after $2^{n-1}+1$evaluations

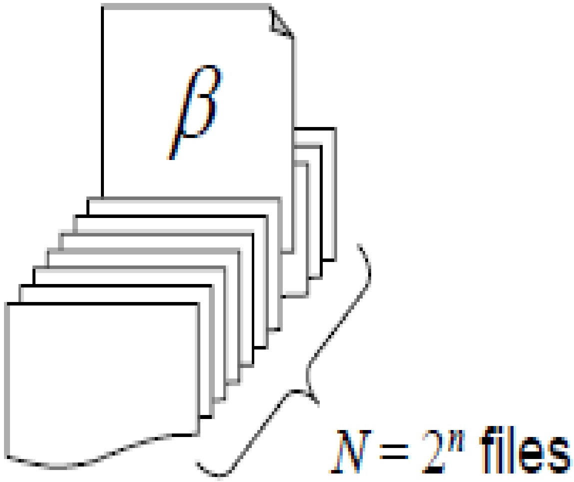
With Deutsch-Jozsa algorithm we get the solution after one evaluation → ***Exponential acceleration***

No application

Grover's Algorithm

- Database searching:

Find the desired file indexed as "β" among N files



Grover's Algorithm

- The problem addressed by Grover's algorithm can be viewed as trying to find a marked element in an unstructured database of size N. To solve this problem a classical algorithm need, on average ***O(N/2)*** evaluations and ***O(N)*** in the worst case.

- But with using Grover's algorithm, a quantum computer can realize the same task using only $O(\sqrt{N})$ evaluations.

Grover's Algorithm

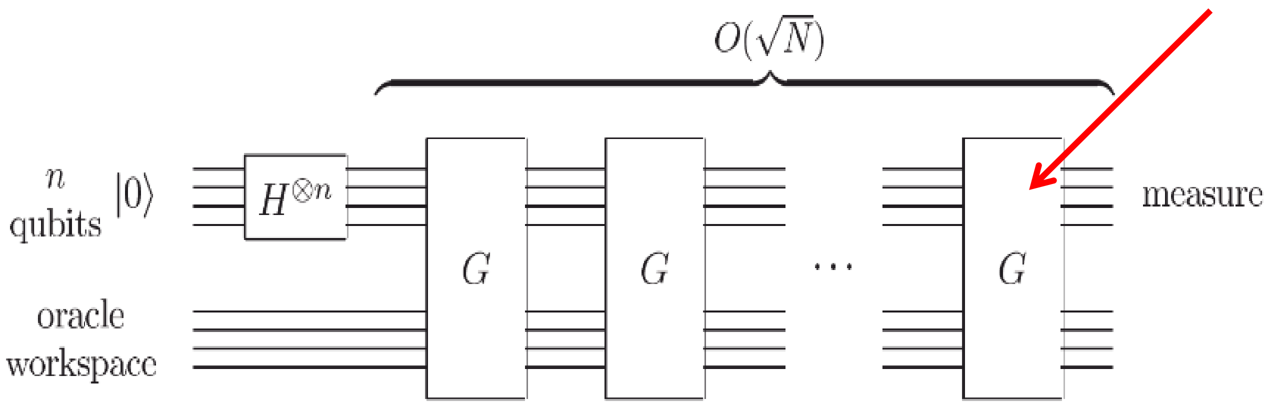
The protocol for the Grover's algorithm is described in Fig 1 for n qubits

Grover's search algorithm begins with the initialized state $|0\rangle^{\otimes n}$

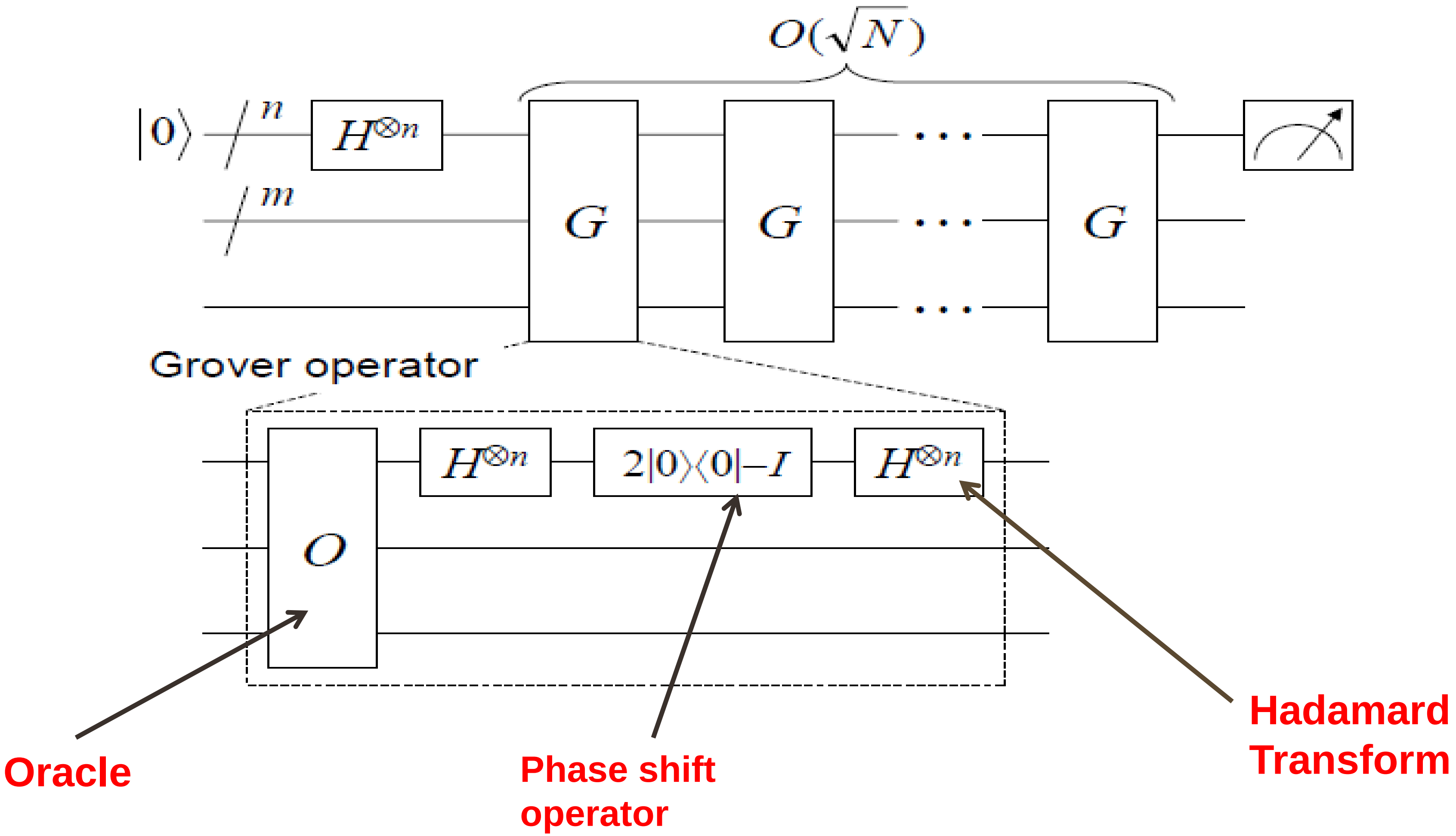
The Hadamard transform is used to get an equal superposition state.

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

The Grover operator



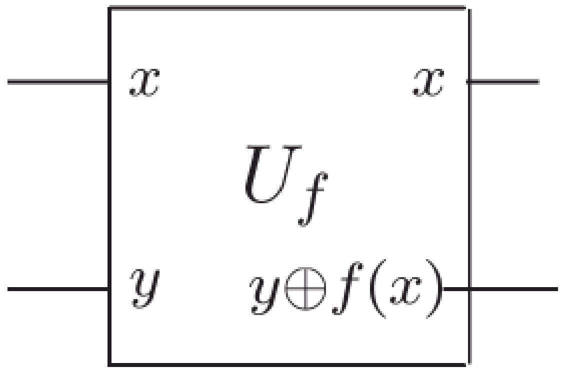
Grover's Algorithm



$$|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle$$

Grover's Algorithm

Oracle :

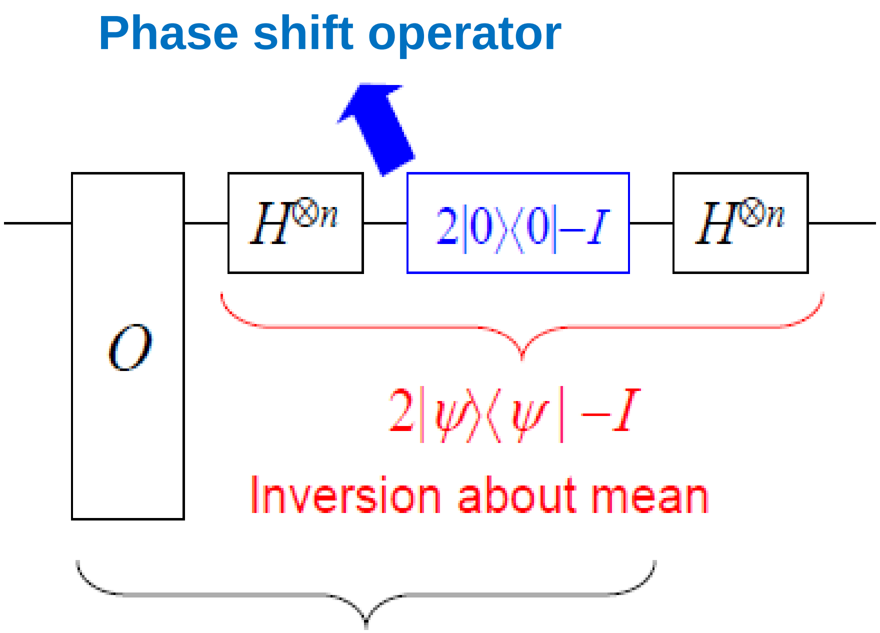


$$U_f \left| x, y \right\rangle \rightarrow \left| x, y \oplus f(x) \right\rangle$$

With *f* is a Boolean function $f(x) : \{0,1\}^n \rightarrow \{0,1\}$

$$\left| x \right\rangle \left(\frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \right) \xrightarrow{O} (-1)^{f(x)} \left| x \right\rangle \left(\frac{\left| 0 \right\rangle - \left| 1 \right\rangle}{\sqrt{2}} \right)$$

Grover's Algorithm



$$G=(2|\psi\rangle\langle\psi|-I)O$$

$$\begin{cases} |0\rangle \rightarrow |0\rangle \\ |x\rangle \rightarrow -|x\rangle \qquad x \neq 0 \end{cases}$$

$$\begin{aligned} &H^{\otimes n}\left(2|0\rangle\langle 0|-I\right)H^{\otimes n} \\ &=2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n}-H^{\otimes n}H^{\otimes n} \\ &=2|\psi\rangle\langle\psi|-I \end{aligned}$$

Grover's Algorithm

Geometric Visualization

In fact, the Grover iteration can be viewed as a rotation in the two-dimensional space spanned by the starting state vector $|\psi\rangle$ and the state consisting of a uniform superposition of solutions to the search problem.

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

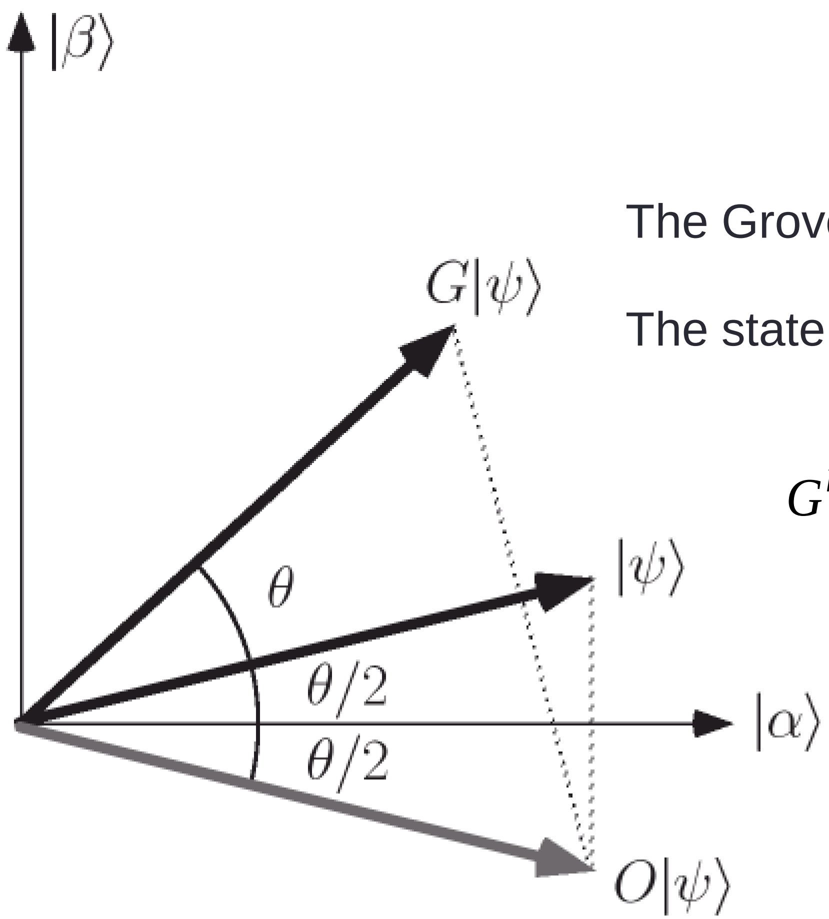
$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum |x\rangle$$

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum |x\rangle$$

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\alpha\rangle + \sqrt{\frac{M}{N}} |\beta\rangle$$

Grover's Algorithm

Geometric Visualization



Let $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$

$$|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$$

The Grover iteration $G = \left(2|\psi\rangle\langle\psi| - I\right)O$

The state after repeating the Grover iteration *k* times

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

After repeated Grover iteration, the state vector gets close to $|\beta\rangle$

Grover's Algorithm

Algorithm & procedure

$$|0\rangle^{\otimes n}|1\rangle$$

Initial state

$$\rightarrow \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Apply the Hadamard Transform for initial state

$$\rightarrow \left[\left(2|\psi\rangle\langle\psi|-I\right)O\right]^R \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

Apply the Grover iteration R time

$$\approx |x_0\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]$$

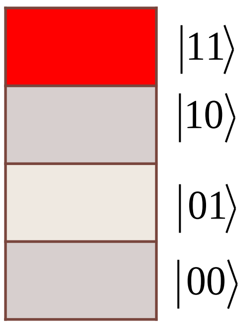
$$R = \left\lceil \frac{\pi\sqrt{N}}{4} \right\rceil$$

$$x_0$$

Measure the first n qubit

Grover's Algorithm

Special case



$$|\psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$$

$$G = \left(2|\psi\rangle\langle\psi| - I\right)O$$

$$O|\psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$$

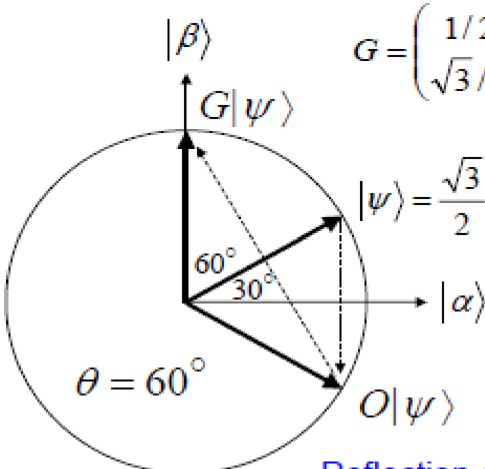
$$G|\psi\rangle = \left(2|\psi\rangle\langle\psi| - I\right)O|\psi\rangle$$

$$G|\psi\rangle = \left(2|\psi\rangle\langle\psi| - I\right)\left(\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle\right)$$

$$= |11\rangle$$

Rotation by 60 degrees

$$G = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$$



$$|\psi\rangle = \frac{\sqrt{3}}{2}|\alpha\rangle + \frac{1}{2}|\beta\rangle$$

$$O = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Reflection about the $|\alpha\rangle$-axis

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$$

Grover's Algorithm

Performance & drawback

$$G^k|\psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

$$\frac{2k+1}{2}\theta \approx \frac{\pi}{2}$$

With

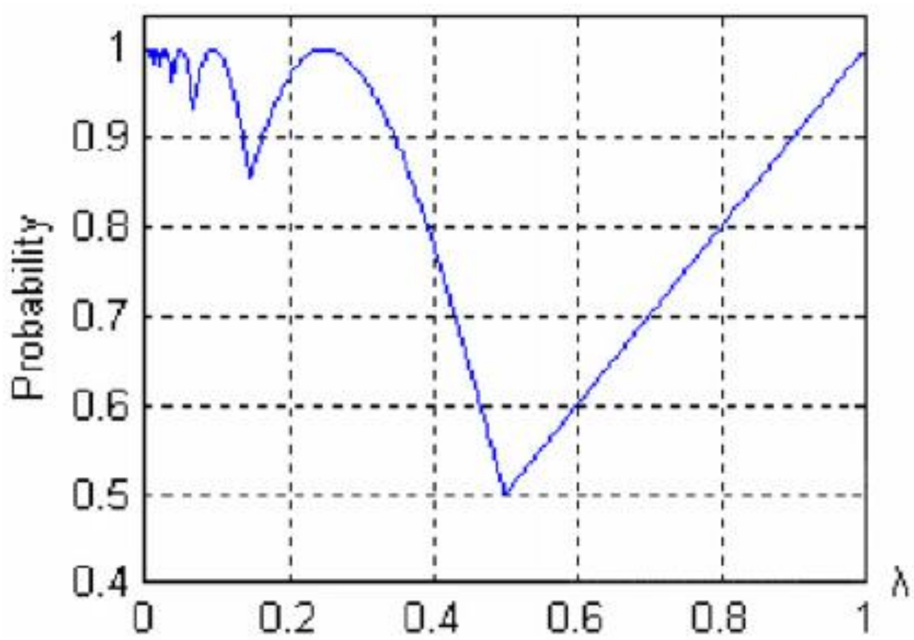
$$\sin\left(\frac{\theta}{2}\right) = \sqrt{\frac{M}{N}}$$

Let $\lambda = M/N$ and let *CI(x)* denote the integer closest to the real number x.
Then repeating the Grover iteration

$$k = CI\left(\frac{\arccos\sqrt{\lambda}}{2\arcsin\sqrt{\lambda}}\right)$$

Grover's Algorithm

Performance & drawback



The success probability curve of Grover's algorithm

The Grover's algorithm is no longer useful when $\lambda > 0.25$