Grover's Algorithm

Quantum Search Algorithm in $\mathcal{O}(\sqrt{N})$ complexity

C. Haaland

December 30, 2017

Outline

Classical Search

Motivation

- "Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of 0.5, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $N/2$ names."

Classical Search

Motivation

- "Imagine a phone directory containing N names arranged in completely random order. In order to find someone's phone number with a probability of 0.5, any classical algorithm (whether deterministic or probabilistic) will need to look at a minimum of $N/2$ names."
- Consider the function $F : \{0,1\}^3 \to \{0,1\}$,

$$\begin{aligned} F(x,y,z) = &(x \vee y \vee z) \wedge \\ &(\neg x \vee \neg y \vee z) \wedge \\ &(x \vee \neg y \vee \neg z) \wedge \\ &(\neg x \vee y \vee \neg z) \end{aligned}$$

  - Question: For what values of the input does $F(x,y,z) = 1$?

Classical Search

Complexity

- Problems are $\mathcal{O}(N)$ on a classical computer
- Lov Grover published a *quantum algorithm* in 1996 with complexity $\mathcal{O}(\sqrt{N})$.
  - For large N, this represents a significant improvement over the classical case
  - Quantum algorithm cannot guarantee the correct answer, only returns the solution with high probability

Outline

Outline

Notation

- $\mathbf{R}$ is set of real numbers

Notation

- $\mathbf{R}$ is set of real numbers
- $\mathbf{C}$ is set of complex numbers (e.g. $x + iy$)

Notation

- $\mathbf{R}$ is set of real numbers
- $\mathbf{C}$ is set of complex numbers (e.g. $x + iy$)
- $\mathbf{R}^n$ ($\mathbf{C}^n$) indicates column vector of n real (complex) numbers respectively

Notation

- $\mathbf{R}$ is set of real numbers
- $\mathbf{C}$ is set of complex numbers (e.g. $x + iy$)
- $\mathbf{R}^n$ ($\mathbf{C}^n$) indicates column vector of n real (complex) numbers respectively
- z^* is the *complex conjugate*
  - If $z = x + iy$ then $z^* = x - iy$

Notation

- $\mathbf{R}$ is set of real numbers
- $\mathbf{C}$ is set of complex numbers (e.g. $x + iy$)
- $\mathbf{R}^n$ ($\mathbf{C}^n$) indicates column vector of n real (complex) numbers respectively
- z^* is the *complex conjugate*
  - If $z = x + iy$ then $z^* = x - iy$
- $|\psi\rangle$ is *Dirac notation* for a column vector (*ket* vector)

Notation

- $\mathbf{R}$ is set of real numbers
- $\mathbf{C}$ is set of complex numbers (e.g. $x + iy$)
- $\mathbf{R}^n$ ($\mathbf{C}^n$) indicates column vector of n real (complex) numbers respectively
- z^* is the *complex conjugate*
  - If $z = x + iy$ then $z^* = x - iy$
- $|\psi\rangle$ is *Dirac notation* for a column vector (*ket* vector)
- $\langle\psi|$ is *Dirac notation* for a row vector (*bra* vector)

Notation (cont'd)

- $A \in \mathbf{R}^{m \times n}(\mathbf{C}^{m \times n})$ means A is a matrix of real (complex) numbers with m rows and n columns

Notation (cont'd)

- $A \in \mathbf{R}^{m \times n}(\mathbf{C}^{m \times n})$ means A is a matrix of real (complex) numbers with m rows and n columns
  - When $m = n$ we call A an *operator*

Notation (cont'd)

- $A \in \mathbf{R}^{m \times n}(\mathbf{C}^{m \times n})$ means A is a matrix of real (complex) numbers with m rows and n columns
  - When $m = n$ we call A an *operator*
- $A^\dagger$ is *Hermitian*/*adjoint*/*conjugate transpose* of A

Notation (cont'd)

- $A \in \mathbf{R}^{m \times n}(\mathbf{C}^{m \times n})$ means A is a matrix of real (complex) numbers with m rows and n columns
  - When $m = n$ we call A an *operator*
- $A^\dagger$ is *Hermitian*/*adjoint*/*conjugate transpose* of A
  - If a matrix A has elements A_{ij} the matrix $A^\dagger$ has entries A^*_{ji}
  - An example is $\langle\psi| = |\psi\rangle^\dagger$

Notation (cont'd)

- $A \in \mathbf{R}^{m \times n}(\mathbf{C}^{m \times n})$ means A is a matrix of real (complex) numbers with m rows and n columns
  - When $m = n$ we call A an *operator*
- $A^\dagger$ is *Hermitian*/*adjoint*/*conjugate transpose* of A
  - If a matrix A has elements A_{ij} the matrix $A^\dagger$ has entries A^*_{ji}
  - An example is $\langle\psi| = |\psi\rangle^\dagger$
- The quantity $\langle\phi|\psi\rangle$ is called the *inner product*
  - The quantity is a scalar with value $\sum_{i=1}^{n} \phi_i^* \psi_i$

Outline

Vector Norm

- The norm/length/magnitude squared of $|\psi\rangle \in \mathbf{C}^n$ is defined as

$$\langle\psi|\psi\rangle = \sum_{i=1}^{n} \psi_i^* \psi_i = \sum_{i=1}^{n} |\psi_i|^2$$

Vector Norm

- The norm/length/magnitude squared of $|\psi\rangle \in \mathbf{C}^n$ is defined as

$$\langle\psi|\psi\rangle = \sum_{i=1}^{n} \psi_i^* \psi_i = \sum_{i=1}^{n} |\psi_i|^2$$

  - This will always be 1 for a valid quantum mechanical state

Matrices

- From the definition of the adjoint

$$(A|\psi\rangle)^\dagger = (|\psi\rangle)^\dagger A^\dagger = \langle\psi|A^\dagger$$

where $A \in \mathbf{C}^{n\times n}$

Matrices

- From the definition of the adjoint

$$(A|\psi\rangle)^\dagger = (|\psi\rangle)^\dagger A^\dagger = \langle\psi|A^\dagger$$

  where $A \in \mathbf{C}^{n\times n}$
- Because the norm of a quantum state is 1, if $|\phi\rangle = U|\psi\rangle$ then $\langle\phi|\phi\rangle = 1$

Matrices

- From the definition of the adjoint

$$(A|\psi\rangle)^\dagger = (|\psi\rangle)^\dagger A^\dagger = \langle\psi|A^\dagger$$

  where $A \in \mathbf{C}^{n\times n}$
- Because the norm of a quantum state is 1, if $|\phi\rangle = U|\psi\rangle$ then $\langle\phi|\phi\rangle = 1$
  - From this we have $(\langle\psi|U^\dagger)(U|\psi\rangle) = 1$ which means $U^T U = I$

Matrices

- From the definition of the adjoint

$$(A|\psi\rangle)^\dagger = (|\psi\rangle)^\dagger A^\dagger = \langle\psi|A^\dagger$$

  where $A \in \mathbf{C}^{n\times n}$
- Because the norm of a quantum state is 1, if $|\phi\rangle = U|\psi\rangle$ then $\langle\phi|\phi\rangle = 1$
  - From this we have $(\langle\psi|U^\dagger)(U|\psi\rangle) = 1$ which means $U^T U = I$
  - An operator satisfying this property is called *unitary*

Matrices

- From the definition of the adjoint

$$(A|\psi\rangle)^\dagger = (|\psi\rangle)^\dagger A^\dagger = \langle\psi|A^\dagger$$

  where $A \in \mathbf{C}^{n\times n}$
- Because the norm of a quantum state is 1, if $|\phi\rangle = U|\psi\rangle$ then $\langle\phi|\phi\rangle = 1$
  - From this we have $(\langle\psi|U^\dagger)(U|\psi\rangle) = 1$ which means $U^T U = I$
  - An operator satisfying this property is called *unitary*
- Unitary operators are the way in which quantum states are altered or evolved

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},\ \sigma_x = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\ \sigma_y = \begin{bmatrix}0 & i\\ -i & 0\end{bmatrix},\ \sigma_z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$$

Linearity

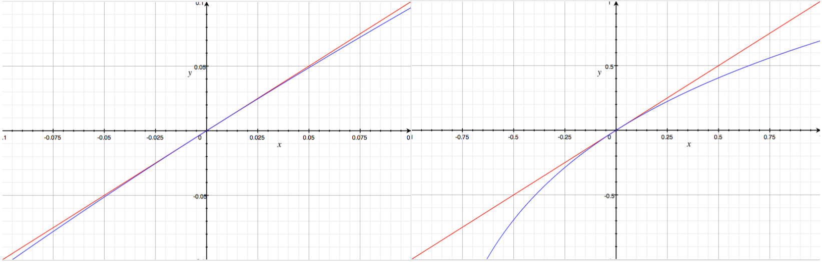
- *Linearity* of a function f means
  - $f(x+y) = f(x) + f(y)$
  - $f(\alpha x) = \alpha f(x)$

Linearity

- *Linearity* of a function f means
  - $f(x+y) = f(x) + f(y)$
  - $f(\alpha x) = \alpha f(x)$
- Matrix multiplication is linear

Linearity

- *Linearity* of a function f means
  - $f(x + y) = f(x) + f(y)$
  - $f(\alpha x) = \alpha f(x)$
- Matrix multiplication is linear
- Common modeling approximation in engineering
  - Example: $\log(1 + x)$ is very nearly x for small x



Linearity & QM

- Linearity is a *fundamental* property of QM
  - *"With classical fields, we often use linear equations, such as the differential equations that allow us to solve for small oscillatory motion of, say, a pendulum. In such a classical case, the linear equation is an approximation; a pendulum with twice the amplitude of oscillation will not oscillate at exactly the same frequency, for example. Hence we cannot take the solution derived at one amplitude of oscillation of the pendulum and merely scale it up for larger amplitudes of oscillation, except as a first approximation. We should emphasize right away, however, that, in quantum mechanics, this linearity of the equations with respect to the quantum mechanical amplitude is not an approximation of any kind; it is apparently an absolute property."-David Miller (Prof. Stanford University)*

Outline

Quantum State

Single Particle System

- Single particle can be in one of two states

Quantum State

Single Particle System

- Single particle can be in one of two states
  - Electron, for example, can be spin up, $|0\rangle$, or spin down, $|1\rangle$

Quantum State

Single Particle System

- Single particle can be in one of two states
  - Electron, for example, can be spin up, $|0\rangle$, or spin down, $|1\rangle$
  - Particle encodes a single quantum bit or *qubit*

Quantum State

Single Particle System

- Single particle can be in one of two states
  - Electron, for example, can be spin up, $|0\rangle$, or spin down, $|1\rangle$
  - Particle encodes a single quantum bit or *qubit*
  - A qubit is a vector in $\mathbf{C}^2$ represented as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Quantum State

Single Particle System

- Single particle can be in one of two states
  - Electron, for example, can be spin up, $|0\rangle$, or spin down, $|1\rangle$
  - Particle encodes a single quantum bit or *qubit*
  - A qubit is a vector in $\mathbf{C}^2$ represented as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Measuring, we will find the particle in *exactly* one of the two states

Quantum State

Single Particle System

- Single particle can be in one of two states
  - Electron, for example, can be spin up, $|0\rangle$, or spin down, $|1\rangle$
  - Particle encodes a single quantum bit or *qubit*
  - A qubit is a vector in $\mathbf{C}^2$ represented as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \; |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Measuring, we will find the particle in *exactly* one of the two states
- Before measurement this is *not* true!

Quantum State

Single Particle System

- Single particle can be in one of two states
  - Electron, for example, can be spin up, $|0\rangle$, or spin down, $|1\rangle$
  - Particle encodes a single quantum bit or *qubit*
  - A qubit is a vector in $\mathbf{C}^2$ represented as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Measuring, we will find the particle in *exactly* one of the two states
- Before measurement this is *not* true!
  - Particle exists in a *linear superposition* of these states

Quantum State

Single Particle System

- Single particle can be in one of two states
  - Electron, for example, can be spin up, $|0\rangle$, or spin down, $|1\rangle$
  - Particle encodes a single quantum bit or *qubit*
  - A qubit is a vector in $\mathbf{C}^2$ represented as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Measuring, we will find the particle in *exactly* one of the two states
- Before measurement this is *not* true!
  - Particle exists in a *linear superposition* of these states
  - State will be $|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$
    - $\psi_0, \psi_1 \in \mathbf{C}$ and $|\psi_0|^2 + |\psi_1|^2 = 1$

Quantum State

Single Particle System

- Single particle can be in one of two states
  - Electron, for example, can be spin up, $|0\rangle$, or spin down, $|1\rangle$
  - Particle encodes a single quantum bit or *qubit*
  - A qubit is a vector in $\mathbf{C}^2$ represented as

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Measuring, we will find the particle in *exactly* one of the two states
- Before measurement this is *not* true!
  - Particle exists in a *linear superposition* of these states
  - State will be $|\psi\rangle = \psi_0|0\rangle + \psi_1|1\rangle$
    - $\psi_0, \psi_1 \in \mathbf{C}$ and $|\psi_0|^2 + |\psi_1|^2 = 1$
  - Classical analogy is Schrodinger's cat that is both alive and dead

Quantum State

Multi-Particle System

- Suppose we have n particles each of which can be in one of two states

Quantum State

Multi-Particle System

- Suppose we have n particles each of which can be in one of two states
  - The system represents n qubits of information

Quantum State

Multi-Particle System

- Suppose we have n particles each of which can be in one of two states
  - The system represents n qubits of information
  - There are $N = 2^n$ possible different states $|0\ldots00\rangle, |0\ldots01\rangle, |0\ldots10\rangle, \ldots, |1\ldots11\rangle$

Quantum State

Multi-Particle System

- Suppose we have n particles each of which can be in one of two states
  - The system represents n qubits of information
  - There are $N = 2^n$ possible different states $|0\ldots00\rangle, |0\ldots01\rangle, |0\ldots10\rangle, \ldots, |1\ldots11\rangle$
  - Each state is a standard basis vector in $\mathbf{R}^N$ (i.e. one component equal to 1 and the rest 0)
    - **Note**: The vector components are *not* the same as the entries of the Dirac notation

Quantum State

Multi-Particle System

- Suppose we have n particles each of which can be in one of two states
  - The system represents n qubits of information
  - There are $N = 2^n$ possible different states $|0\ldots00\rangle, |0\ldots01\rangle, |0\ldots10\rangle, \ldots, |1\ldots11\rangle$
  - Each state is a standard basis vector in $\mathbf{R}^N$ (i.e. one component equal to 1 and the rest 0)
    - **Note**: The vector components are *not* the same as the entries of the Dirac notation
- Measuring, we will find the system to be in one of $N = 2^n$ possible states $|\psi\rangle \in \mathbf{R}^N$

Quantum State

Multi-Particle System

- Suppose we have n particles each of which can be in one of two states
  - The system represents n qubits of information
  - There are $N = 2^n$ possible different states $|0\ldots00\rangle, |0\ldots01\rangle, |0\ldots10\rangle, \ldots, |1\ldots11\rangle$
  - Each state is a standard basis vector in $\mathbf{R}^N$ (i.e. one component equal to 1 and the rest 0)
    - **Note**: The vector components are *not* the same as the entries of the Dirac notation
- Measuring, we will find the system to be in one of $N = 2^n$ possible states $|\psi\rangle \in \mathbf{R}^N$
- Before measurement, it will be in a *linear superposition* of these states

Quantum State

Multi-Particle System

- Suppose we have n particles each of which can be in one of two states
  - The system represents n qubits of information
  - There are $N = 2^n$ possible different states $|0\dots00\rangle, |0\dots01\rangle, |0\dots10\rangle, \dots, |1\dots11\rangle$
  - Each state is a standard basis vector in $\mathbf{R}^N$ (i.e. one component equal to 1 and the rest 0)
    - **Note**: The vector components are *not* the same as the entries of the Dirac notation
- Measuring, we will find the system to be in one of $N = 2^n$ possible states $|\psi\rangle \in \mathbf{R}^N$
- Before measurement, it will be in a *linear superposition* of these states
  - Its state will be $|\psi\rangle = \psi_0|0\dots00\rangle + \psi_1|0\dots01\rangle + \cdots + \psi_{N-1}|1\dots11\rangle$ where $\psi_i \in \mathbf{C}$ and $\sum_{i=0}^{N-1} |\psi_i|^2 = 1$

Born Rule

- What are the coefficients ψ_i respresenting physically?

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!
- Squared magnitude is the *probability* of measuring the system in state i

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!
- Squared magnitude is the *probability* of measuring the system in state i
- This interpretation is called the *Born Rule*

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!
- Squared magnitude is the *probability* of measuring the system in state i
- This interpretation is called the *Born Rule*
  - This is empirical and more like a postulate

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!
- Squared magnitude is the *probability* of measuring the system in state i
- This interpretation is called the *Born Rule*
  - This is empirical and more like a postulate
  - Many attempts to derive it from first principles

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!
- Squared magnitude is the *probability* of measuring the system in state *i*
- This interpretation is called the *Born Rule*
  - This is empirical and more like a postulate
  - Many attempts to derive it from first principles
- Are we sure it's *completely* random?

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!
- Squared magnitude is the *probability* of measuring the system in state i
- This interpretation is called the *Born Rule*
  - This is empirical and more like a postulate
  - Many attempts to derive it from first principles
- Are we sure it's *completely* random?
  - As far as we can tell, it is actually random (cf. Bell's Inequalities)

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!
- Squared magnitude is the *probability* of measuring the system in state *i*
- This interpretation is called the *Born Rule*
  - This is empirical and more like a postulate
  - Many attempts to derive it from first principles
- Are we sure it's *completely* random?
  - As far as we can tell, it is actually random (cf. Bell's Inequalities)
- Some interpretations of this phenomenon are

Born Rule

- What are the coefficients ψ_i respresenting physically?
  - ψ_i cannot be measured, but $|\psi_i|^2$ can!
- Squared magnitude is the *probability* of measuring the system in state i
- This interpretation is called the *Born Rule*
  - This is empirical and more like a postulate
  - Many attempts to derive it from first principles
- Are we sure it's *completely* random?
  - As far as we can tell, it is actually random (cf. Bell's Inequalities)
- Some interpretations of this phenomenon are
  - Copenhagen Interpretation
  - Many World's Hypothesis
  - Quantum Decoherence

Quantum Measurement

Wave Particle Duality

- A wave (of water say) impinging on a screen with two openings will yield a diffraction pattern

Quantum Measurement

Wave Particle Duality

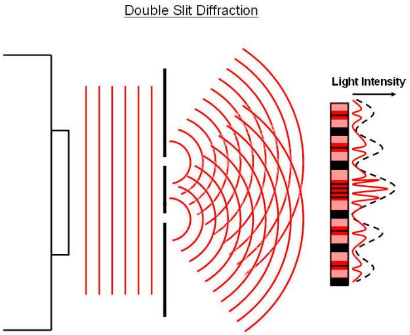
- A wave (of water say) impinging on a screen with two openings will yield a diffraction pattern
  - Each opening becomes the source of a new wave front

- A wave (of water say) impinging on a screen with two openings will yield a diffraction pattern
  - Each opening becomes the source of a new wave front
  - The two waves *interfere* with each other forming alternating peaks and troughs

Quantum Measurement

Wave Particle Duality

- A wave (of water say) impinging on a screen with two openings will yield a diffraction pattern
  - Each opening becomes the source of a new wave front
  - The two waves *interfere* with each other forming alternating peaks and troughs



Quantum Measurement (cont'd)

Wave Particle Duality

- Perform the same experiment with an electron gun

Quantum Measurement (cont'd)

Wave Particle Duality

- Perform the same experiment with an electron gun
  - A diffraction pattern is observed!
  - This indicates electrons are like waves

Quantum Measurement (cont'd)

Wave Particle Duality

- Perform the same experiment with an electron gun
  - A diffraction pattern is observed!
  - This indicates electrons are like waves
- Now we have an apparatus that can shoot only a single electron at a time

Quantum Measurement (cont'd)

Wave Particle Duality

- Perform the same experiment with an electron gun
  - A diffraction pattern is observed!
  - This indicates electrons are like waves
- Now we have an apparatus that can shoot only a single electron at a time
  - A diffraction pattern! The electron is interfering with itself

Quantum Measurement (cont'd)

Wave Particle Duality

- Perform the same experiment with an electron gun
  - A diffraction pattern is observed!
  - This indicates electrons are like waves
- Now we have an apparatus that can shoot only a single electron at a time
  - A diffraction pattern! The electron is interfering with itself
- A measurement device is placed on one of the slits to see which one the electron went through

Quantum Measurement (cont'd)

Wave Particle Duality

- Perform the same experiment with an electron gun
  - A diffraction pattern is observed!
  - This indicates electrons are like waves
- Now we have an apparatus that can shoot only a single electron at a time
  - A diffraction pattern! The electron is interfering with itself
- A measurement device is placed on one of the slits to see which one the electron went through
  - Diffraction pattern is gone.
  - Electron behaves like a particle that goes through one slit or the other when measured
  - The act of measurement has altered the outcome

Outline

Outline

Grover's Algorithm

Function Inversion

- Often framed in the context of unstructured database search

Grover's Algorithm

Function Inversion

- Often framed in the context of unstructured database search
- More precisely, searches a function for a *single* satisfying input

Grover's Algorithm

Function Inversion

- Often framed in the context of unstructured database search
- More precisely, searches a function for a *single* satisfying input
  - Given y, find *the* corresponding x such that $f(x) = y$.
  - Invert the function $f(\cdot)$
  - To search an *explicit list* (i.e. unstructured database), need a function backing it

Grover's Algorithm

Function Inversion

- Often framed in the context of unstructured database search
- More precisely, searches a function for a *single* satisfying input
  - Given y, find *the* corresponding x such that $f(x) = y$.
  - Invert the function $f(\cdot)$
  - To search an *explicit list* (i.e. unstructured database), need a function backing it
- If there is no solution or multiple solutions, algorithm does not work out of the box

Grover's Algorithm

Algorithm

- We search for index $|\omega\rangle$

Grover's Algorithm

Algorithm

- We search for index $|\omega\rangle$
- Initialize n qubits to quantum state $|s\rangle \in \mathbf{R}^N$ $(N = 2^n)$ which is the uniform superposition of states

Grover's Algorithm

Algorithm

- We search for index $|\omega\rangle$
- Initialize n qubits to quantum state $|s\rangle \in \mathbf{R}^N$ ($N = 2^n$) which is the uniform superposition of states

$$|s\rangle \triangleq \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |x\rangle = \frac{1}{\sqrt{N}} \mathbf{1}$$

Grover's Algorithm

Algorithm

- We search for index $|\omega\rangle$
- Initialize n qubits to quantum state $|s\rangle \in \mathbf{R}^N$ $(N = 2^n)$ which is the uniform superposition of states

$$|s\rangle \triangleq \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |x\rangle = \frac{1}{\sqrt{N}} \mathbf{1}$$

- Repeat $r = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ times

Grover's Algorithm

Algorithm

- We search for index $|\omega\rangle$
- Initialize n qubits to quantum state $|s\rangle \in \mathbf{R}^N$ $(N = 2^n)$ which is the uniform superposition of states

$$|s\rangle \triangleq \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |x\rangle = \frac{1}{\sqrt{N}}\mathbf{1}$$

- Repeat $r = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ times
  - Define the oracle operator $U_\omega \in \mathbf{R}^{n\times n}$ as

$$U_\omega = I - 2|\omega\rangle\langle\omega| = \mathbf{diag}(\underbrace{1, 1, \ldots, -1, \ldots, 1, 1}_{0,1,\ldots,\omega,\ldots,N-2,N-1})$$

    Apply the operator U_ω to the qubit state

Grover's Algorithm

Algorithm

- We search for index $|\omega\rangle$
- Initialize n qubits to quantum state $|s\rangle \in \mathbf{R}^N$ $(N = 2^n)$ which is the uniform superposition of states

$$|s\rangle \triangleq \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |x\rangle = \frac{1}{\sqrt{N}} \mathbf{1}$$

- Repeat $r = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ times
  - Define the oracle operator $U_\omega \in \mathbf{R}^{n \times n}$ as

    $$U_\omega = I - 2|\omega\rangle\langle\omega| = \mathbf{diag}(\underbrace{1, 1, \ldots, -1, \ldots, 1, 1}_{0,1,\ldots,\omega,\ldots,N-2,N-1})$$

    Apply the operator U_ω to the qubit state
  - Define the operator $U_s \in \mathbf{R}^{n \times n}$ as

    $$U_s = 2|s\rangle\langle s| - I$$

    Apply the operator U_s to the qubit state

Grover's Algorithm

Algorithm

- We search for index $|\omega\rangle$
- Initialize n qubits to quantum state $|s\rangle \in \mathbf{R}^N$ ($N = 2^n$) which is the uniform superposition of states

$$|s\rangle \triangleq \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |x\rangle = \frac{1}{\sqrt{N}} \mathbf{1}$$

- Repeat $r = \left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$ times
  - Define the oracle operator $U_\omega \in \mathbf{R}^{n \times n}$ as

    $$U_\omega = I - 2|\omega\rangle\langle\omega| = \mathbf{diag}(\underbrace{1, 1, \ldots, -1, , \ldots, 1, 1}_{0,1,\ldots,\omega,\ldots,N-2,N-1})$$

    Apply the operator U_ω to the qubit state
  - Define the operator $U_s \in \mathbf{R}^{n \times n}$ as

    $$U_s = 2|s\rangle\langle s| - I$$

    Apply the operator U_s to the qubit state
- Measure qubits

Inversion About the Mean

- The operator U_s can be written as

$$U_s = \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} - 1 \end{bmatrix}$$

- Applying the operator to $|x\rangle$ gives the update

$$x_i \leftarrow -x_i + \frac{2}{N} \sum_{j=1}^{N} x_j$$

- Adds twice the mean of the coefficients to negation of each state
- State x_ω was already negated which boosts its value.

Grover's Example

N=4

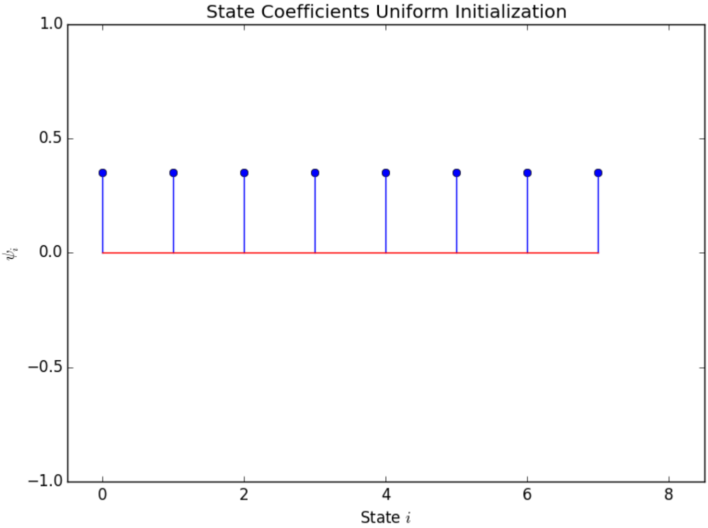
- For the case of $N = 4$ we need only compute $r = \left\lfloor \frac{\pi}{4}\sqrt{4} \right\rfloor = 1$ iteration

$$U_\omega|s\rangle = (I - 2|\omega\rangle\langle\omega|)|s\rangle = |s\rangle - 2|\omega\rangle\langle\omega|s\rangle = |s\rangle - 2|\omega\rangle(1/\sqrt{4})$$

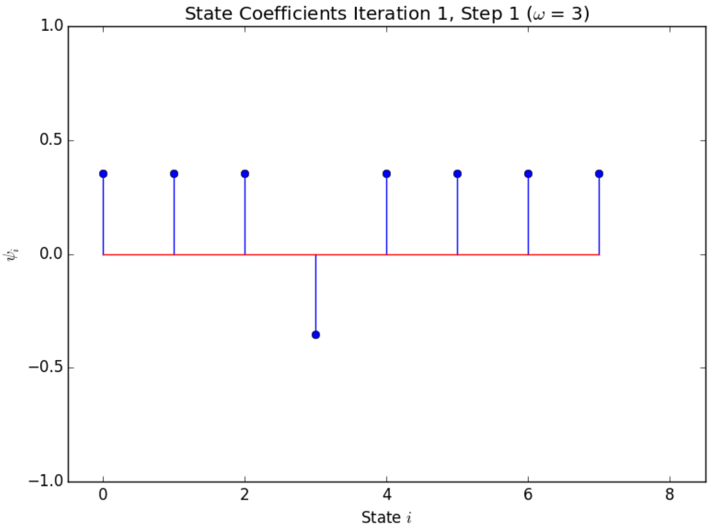
$$\begin{aligned} U_s\left(|s\rangle - \frac{2}{\sqrt{4}}|\omega\rangle\right) &= (2|s\rangle\langle s| - I)\,(|s\rangle - |\omega\rangle) \\ &= 2|s\rangle\langle s|s\rangle - |s\rangle - |s\rangle\langle s|\omega\rangle + |\omega\rangle \\ &= 2|s\rangle - |s\rangle - |s\rangle - |\omega\rangle \\ &= |\omega\rangle \end{aligned}$$

- Measure the system to get the answer

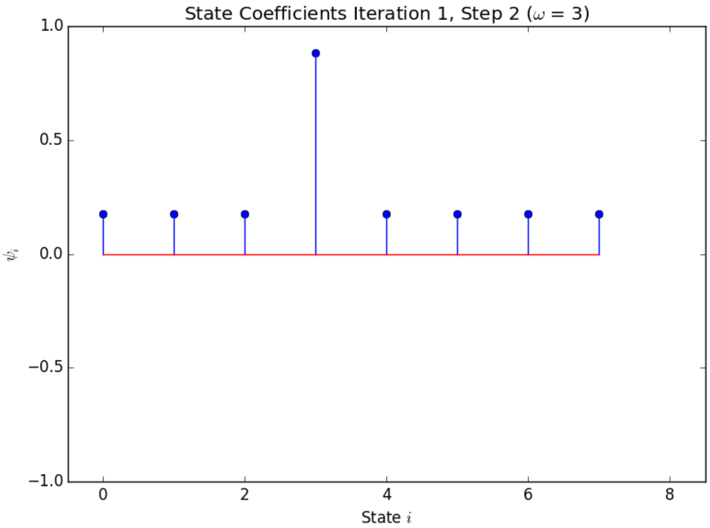
Grover's Illustration (N=8, ω=3)



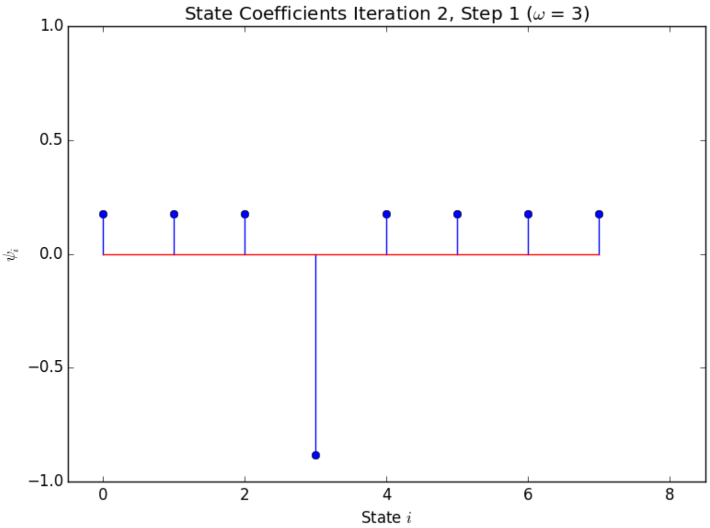
Grover's Illustration (N=8, ω=3)



Grover's Illustration (N=8, ω=3)

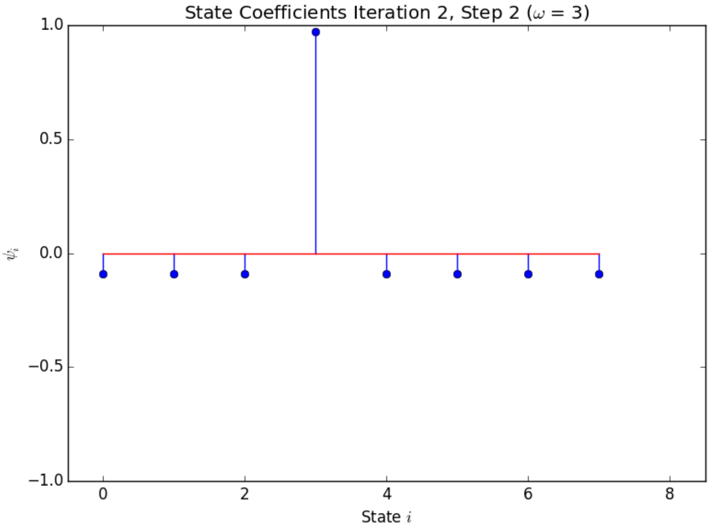


Grover's Illustration (N=8, ω=3)



Grover's Illustration (N=8, ω=3)

Graphical



Grover's Algorithm

Notes

- If the solution does not exist, an answer is returned at random

Grover's Algorithm

Notes

- If the solution does not exist, an answer is returned at random
- Performing more iterations will degrade the solution probability

Grover's Algorithm

Notes

- If the solution does not exist, an answer is returned at random
- Performing more iterations will degrade the solution probability
- Multiple solutions will change the optimal number of iterations needed

The Quantum Oracle

- The oracle is a (problem dependent) function such that $f(\omega) = 1$ and 0 otherwise

The Quantum Oracle

- The oracle is a (problem dependent) function such that $f(\omega) = 1$ and 0 otherwise
  - Each state is then multiplied with $(-1)^{f(x)}$ to "mark" the solution

The Quantum Oracle

- The oracle is a (problem dependent) function such that $f(\omega) = 1$ and 0 otherwise
  - Each state is then multiplied with $(-1)^{f(x)}$ to "mark" the solution
- Quantum oracle must be able to evaluate on the superposition of indices

The Quantum Oracle

- The oracle is a (problem dependent) function such that $f(\omega) = 1$ and 0 otherwise
  - Each state is then multiplied with $(-1)^{f(x)}$ to "mark" the solution
- Quantum oracle must be able to evaluate on the superposition of indices
  - Classically, we can only evaluate one query at a time

The Quantum Oracle

- The oracle is a (problem dependent) function such that $f(\omega) = 1$ and 0 otherwise
  - Each state is then multiplied with $(-1)^{f(x)}$ to "mark" the solution
- Quantum oracle must be able to evaluate on the superposition of indices
  - Classically, we can only evaluate one query at a time
  - QM has natural parallelism; if f can evaluate x or y, then we can evaluate $f\left(\frac{1}{\sqrt{2}}(x+y)\right)$

The Quantum Oracle

- The oracle is a (problem dependent) function such that $f(\omega) = 1$ and 0 otherwise
  - Each state is then multiplied with $(-1)^{f(x)}$ to "mark" the solution
- Quantum oracle must be able to evaluate on the superposition of indices
  - Classically, we can only evaluate one query at a time
  - QM has natural parallelism; if f can evaluate x or y, then we can evaluate $f\left(\frac{1}{\sqrt{2}}(x+y)\right)$
- A quantum circuit with *quantum gates* can be built to evaluate the predicate

The Quantum Oracle

- The oracle is a (problem dependent) function such that $f(\omega) = 1$ and 0 otherwise
  - Each state is then multiplied with $(-1)^{f(x)}$ to "mark" the solution
- Quantum oracle must be able to evaluate on the superposition of indices
  - Classically, we can only evaluate one query at a time
  - QM has natural parallelism; if f can evaluate x or y, then we can evaluate $f\left(\frac{1}{\sqrt{2}}(x+y)\right)$
- A quantum circuit with *quantum gates* can be built to evaluate the predicate
  - Gates such as Hadamard, Pauli Spin, Phase shift, CNOT etc (all are unitary operators) used to build oracles

The Quantum Oracle

- The oracle is a (problem dependent) function such that $f(\omega) = 1$ and 0 otherwise
  - Each state is then multiplied with $(-1)^{f(x)}$ to "mark" the solution
- Quantum oracle must be able to evaluate on the superposition of indices
  - Classically, we can only evaluate one query at a time
  - QM has natural parallelism; if f can evaluate x or y, then we can evaluate $f\left(\frac{1}{\sqrt{2}}(x+y)\right)$
- A quantum circuit with *quantum gates* can be built to evaluate the predicate
  - Gates such as Hadamard, Pauli Spin, Phase shift, CNOT etc (all are unitary operators) used to build oracles
  - Programming a quantum computer is more like programming an FPGA than writing software

Usefulness of Grover's

- The $\mathcal{O}(\sqrt{N})$ bound assumes predicate can be evaluated on superposition of all states

Usefulness of Grover's

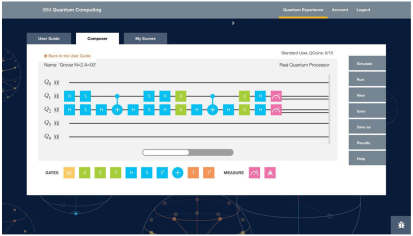
- The $\mathcal{O}(\sqrt{N})$ bound assumes predicate can be evaluated on superposition of all states
- $f(\cdot)$ must be implemented in quantum hardware using *quantum gates*
  - May be difficult to find compact gate representation
  - Problems like database search must first convert to an *implicit* list
  - Cost of evaluating $f(\cdot)$ may dominate

Current State of Quantum Computing

- IBM claims to have a working prototype of a 50 qubit quantum computer

Current State of Quantum Computing

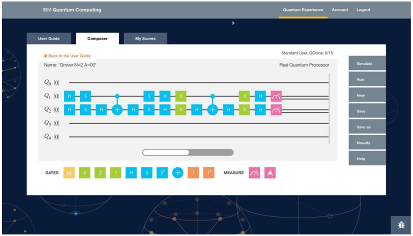
- IBM claims to have a working prototype of a 50 qubit quantum computer



- *D Wave* solves optimization problems by exploiting QM effects

Current State of Quantum Computing

- IBM claims to have a working prototype of a 50 qubit quantum computer



- *D Wave* solves optimization problems by exploiting QM effects
- Much of quantum computing is still theoretical and uses simulation
  - Q#, Libquantum, IBM Q etc
  - Simulation requires *lots* of memory (e.g. 32 qubits implies $2 \cdot 2^{32}$ real numbers)

Outline

References

- https://en.wikipedia.org/wiki/Grover%27s_algorithm
- https://quantiki.org/wiki/grovers-search-algorithm
- *Quantum Mechanics for Scientists and Engineers* - David Miller
- https://web.eecs.umich.edu/ imarkov/pubs/jour/cise05-grov.pdf