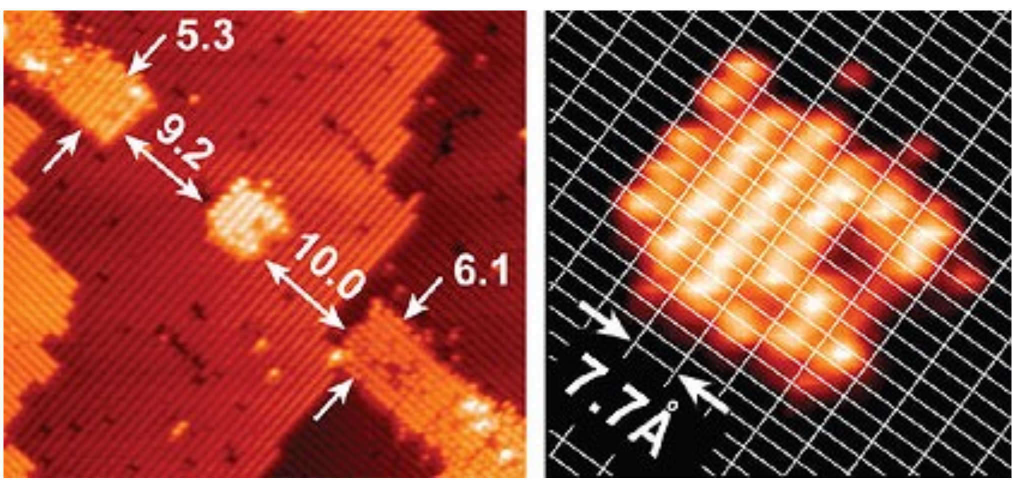
# Introduction to Quantum Computing
## Part II

Emma Strubell

http://cs.umaine.edu/~ema/quantum_tutorial.pdf

April 13, 2011



# Overview

Grover's Algorithm

- Quantum search
- How it works
- A worked example

Simon's algorithm

- Period-finding
- How it works
- An example

# Outline

Grover's Algorithm

- Quantum search
- How it works
- A worked example

Simon's algorithm

- Period-finding
- How it works
- An example

# Step 1: Attain equal superposition

- Begin with a quantum register of $n$ qubits, where $n$ is the number of qubits necessary to represent the search space of size $2^n = N$, all initialized to $|0\rangle$:
$$|0\rangle^{\otimes n} = |0\rangle \tag{1}$$
- First step: put the system into an equal superposition of states, achieved by applying the Hadamard transform $H^{\otimes n}$
$$|\psi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \tag{2}$$
- Requires $\Theta(\lg N) = \Theta(\lg 2^n) = \Theta(n)$ operations, $n$ applications of the elementary Hadamard gate:

# Amplitude amplification: the Grover iteration

- Next series of transformations often referred to as the *Grover iteration*
- Bulk of the algorithm
- Performs *amplitude amplification*
  - Selective shifting of the phase of one state of a quantum system, one that satisfies some condition, at each iteration
  - Performing a phase shift of $\pi$ is equivalent to multiplying the amplitude of that state by $-1$: amplitude for that state changes, but the probability remains the same
  - Subsequent transformations take advantage of difference in amplitude to single state of differing phase, ultimately increasing the probability of the system being in that state
- In order to achieve optimal probability that the state ultimately observed is the correct one, want overall rotation of the phase to be $\frac{\pi}{4}$ radians, which will occur on average after $\frac{\pi}{4}\sqrt{2^n}$ iterations
- The Grover iteration will be repeated $\frac{\pi}{4}\sqrt{2^n}$ times

# The Grover iteration: an oracle query

- First step in Grover iteration is a call to a *quantum oracle*, $\mathcal{O}$, that will modify the system depending on whether it is in the configuration we are searching for
- An oracle is basically a black-box function, and this quantum oracle is a quantum black-box, meaning it can observe and modify the system without collapsing it to a classical state
- If the system is indeed in the correct state, then the oracle will rotate the phase by $\pi$ radians, otherwise it will do nothing
- In this way it marks the correct state for further modification by subsequent operations
- The oracle's effect on $|x\rangle$ may be written simply:

$$|x\rangle \xrightarrow{\mathcal{O}} (-1)^{f(x)} |x\rangle \tag{3}$$

  Where $f(x) = 1$ if $x$ is the correct state, and $f(x) = 0$ otherwise
- The exact implementation of $f(x)$ is dependent on the particular search problem

# The Grover iteration: diffusion transform

- Grover refers to the next part of the iteration as the *diffusion transform*
- Performs *inversion about the average*, transforming the amplitude of each state so that it is as far above the average as it was below the average prior to the transformation
- Consists of another application of the Hadamard transform $H^{\otimes n}$, followed by a conditional phase shift that shifts every state except $|0\rangle$ by $-1$, followed by yet another Hadamard transform
- The conditional phase shift can be represented by the unitary operator $2|0\rangle\langle 0| - I$:

$$[2|0\rangle\langle 0| - I]|0\rangle = 2|0\rangle\langle 0|0\rangle - I = |0\rangle \quad (4a)$$

$$[2|0\rangle\langle 0| - I]|x\rangle = 2|0\rangle\langle 0|x\rangle - I = -|x\rangle \quad (4b)$$

# The Grover iteration: bringing it all together

- The entire diffusion transform, using the notation $|\psi\rangle$ from equation 2, can be written:

$$H^{\otimes n}\left[2\left|0\right\rangle\left\langle 0\right| - I\right]H^{\otimes n} = 2H^{\otimes n}\left|0\right\rangle\left\langle 0\right|H^{\otimes n} - I = 2\left|\psi\right\rangle\left\langle\psi\right| - I \quad (5)$$

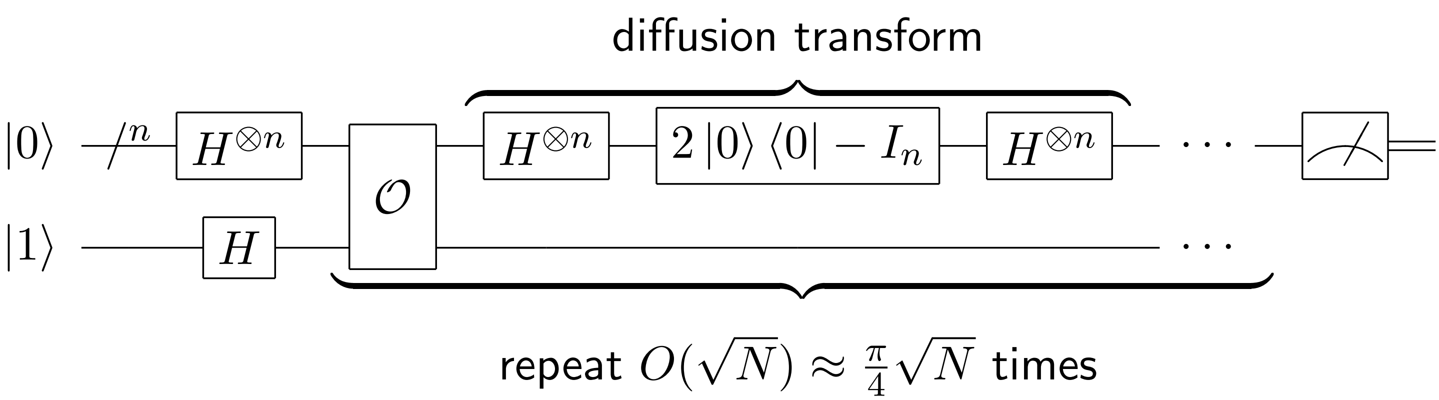
  And the entire Grover iteration:

$$\left[2\left|\psi\right\rangle\left\langle\psi\right| - I\right]\mathcal{O} \quad (6)$$

- The exact runtime of the oracle depends on the specific problem and implementation, so a call to $\mathcal{O}$ is viewed as one elementary operation
- Total runtime of a single Grover iteration is $O(n)$:
  - $O(2n)$ from the two Hadamard transforms
  - $O(n)$ gates to perform the conditional phase shift
- The runtime of Grover's entire algorithm, performing $O(\sqrt{N}) = O(\sqrt{2^n}) = O(2^{\frac{n}{2}})$ iterations each requiring $O(n)$ gates, is $O(2^{\frac{n}{2}})$.

# Circuit diagram overview

- Once the Grover iteration has been performed $O(\sqrt{N})$ times, a classical measurement is performed to determine the result, which will be correct with probability $O(1)$



# Grover's algorithm on 3 qubits

- Consider a system consisting of $N = 8 = 2^3$ states
- The state we are searching for, $x_0$, is represented by the bit string 011
- To describe this system, $n = 3$ qubits are required:

$$|x\rangle = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle$$
$$+ \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle$$

  where $\alpha_i$ is the amplitude of the state $|i\rangle$
- Grover's algorithm begins with a system initialized to 0:

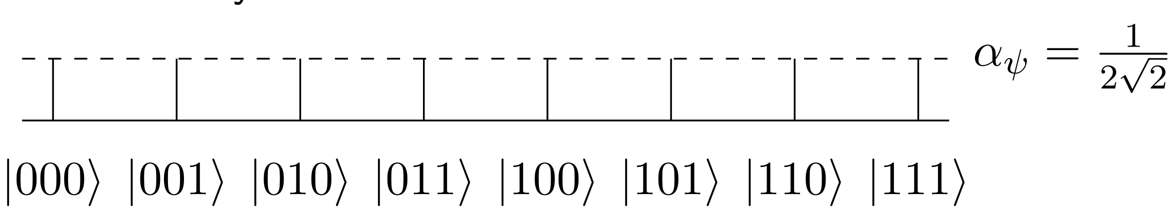
$$1 |000\rangle$$

# Attain equal superposition

- apply the Hadamard transformation to obtain equal amplitudes associated with each state of $1/\sqrt{N} = 1/\sqrt{8} = 1/2\sqrt{2}$, and thus also equal probability of being in any of the 8 possible states:

$$\begin{aligned} H^3 |000\rangle &= \frac{1}{2\sqrt{2}} |000\rangle + \frac{1}{2\sqrt{2}} |001\rangle + \ldots + \frac{1}{2\sqrt{2}} |111\rangle \\ &= \frac{1}{2\sqrt{2}} \sum_{x=0}^{7} |x\rangle \\ &= |\psi\rangle \end{aligned}$$

- Geometrically:

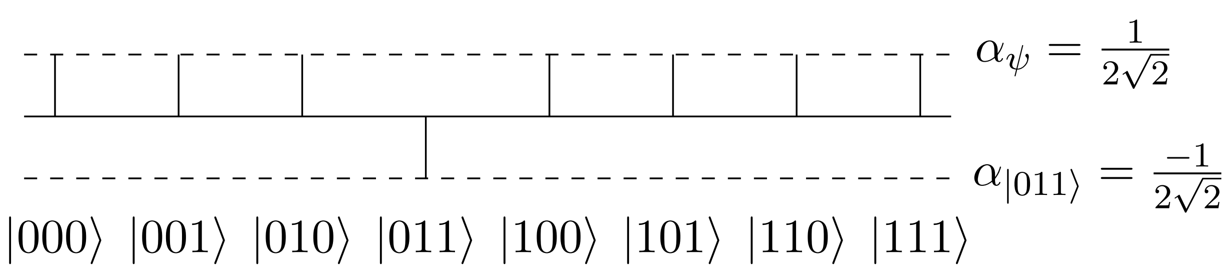


# Two Grover iterations: the first Hadamard

- It is optimal to perform 2 Grover iterations: $\frac{\pi}{4}\sqrt{8} = \frac{2\pi}{4}\sqrt{2} = \frac{\pi}{2}\sqrt{2} \approx 2.22$ rounds to 2 iterations.
- At each iteration, the first step is to query $\mathcal{O}$, then perform inversion about the average, the diffusion transform.
- The oracle query will negate the amplitude of the state $|x_0\rangle$, in this case $|011\rangle$, giving the configuration:

$$|x\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \frac{1}{2\sqrt{2}}|001\rangle + \frac{1}{2\sqrt{2}}|010\rangle - \frac{1}{2\sqrt{2}}|011\rangle + \ldots + \frac{1}{2\sqrt{2}}|111\rangle$$

- With geometric representation:



# Diffusion transform

- Now perform the diffusion transform $2|\psi\rangle\langle\psi| - I$, which will increase the amplitudes by their difference from the average, decreasing if the difference is negative:

$$
\begin{aligned}
&[2|\psi\rangle\langle\psi| - I]\,|x\rangle \\
&= [2|\psi\rangle\langle\psi| - I]\left[|\psi\rangle - \frac{2}{2\sqrt{2}}|011\rangle\right] \\
&= 2|\psi\rangle\langle\psi|\psi\rangle - |\psi\rangle - \frac{2}{\sqrt{2}}|\psi\rangle\langle\psi|011\rangle + \frac{1}{\sqrt{2}}|011\rangle
\end{aligned}
$$

- Note that $\langle\psi|\psi\rangle = 8\frac{1}{2\sqrt{2}}\left[\frac{1}{2\sqrt{2}}\right] = 1$
- Since $|011\rangle$ is one of the basis vectors, we can use the identity $\langle\psi|011\rangle = \langle 011|\psi\rangle = \frac{1}{2\sqrt{2}}$

# Diffusion transform continued

- Final result of the diffusion transform:

$$
\begin{aligned}
&= 2\,|\psi\rangle - |\psi\rangle - \frac{2}{\sqrt{2}}\left(\frac{1}{2\sqrt{2}}\right)|\psi\rangle + \frac{1}{\sqrt{2}}\,|011\rangle \\
&= |\psi\rangle - \frac{1}{2}\,|\psi\rangle + \frac{1}{\sqrt{2}}\,|011\rangle \\
&= \frac{1}{2}\,|\psi\rangle + \frac{1}{\sqrt{2}}\,|011\rangle
\end{aligned}
$$

- Substituting for $|\psi\rangle$ gives:

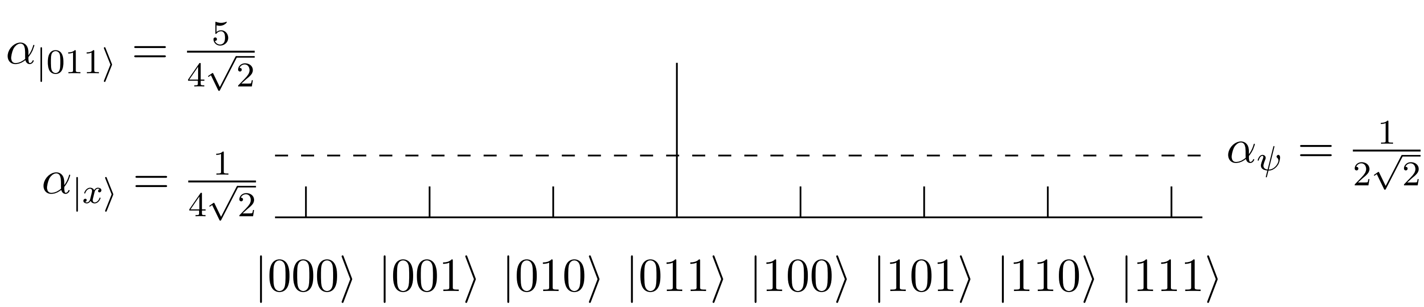
$$
\begin{aligned}
&= \frac{1}{2}\left[\frac{1}{2\sqrt{2}}\sum_{x=0}^{7}|x\rangle\right] + \frac{1}{\sqrt{2}}\,|011\rangle \\
&= \frac{1}{4\sqrt{2}}\sum_{\substack{x=0 \\ x\neq 3}}^{7}|x\rangle + \frac{5}{4\sqrt{2}}\,|011\rangle
\end{aligned}
$$

# Geometric result of the diffusion transform

- Can also be written:

$$|x\rangle = \frac{1}{4\sqrt{2}}|000\rangle + \frac{1}{4\sqrt{2}}|001\rangle + \frac{1}{4\sqrt{2}}|010\rangle + \frac{5}{4\sqrt{2}}|011\rangle + \ldots + \frac{1}{4\sqrt{2}}|111\rangle$$

- Geometric representation:



# The second Grover iteration

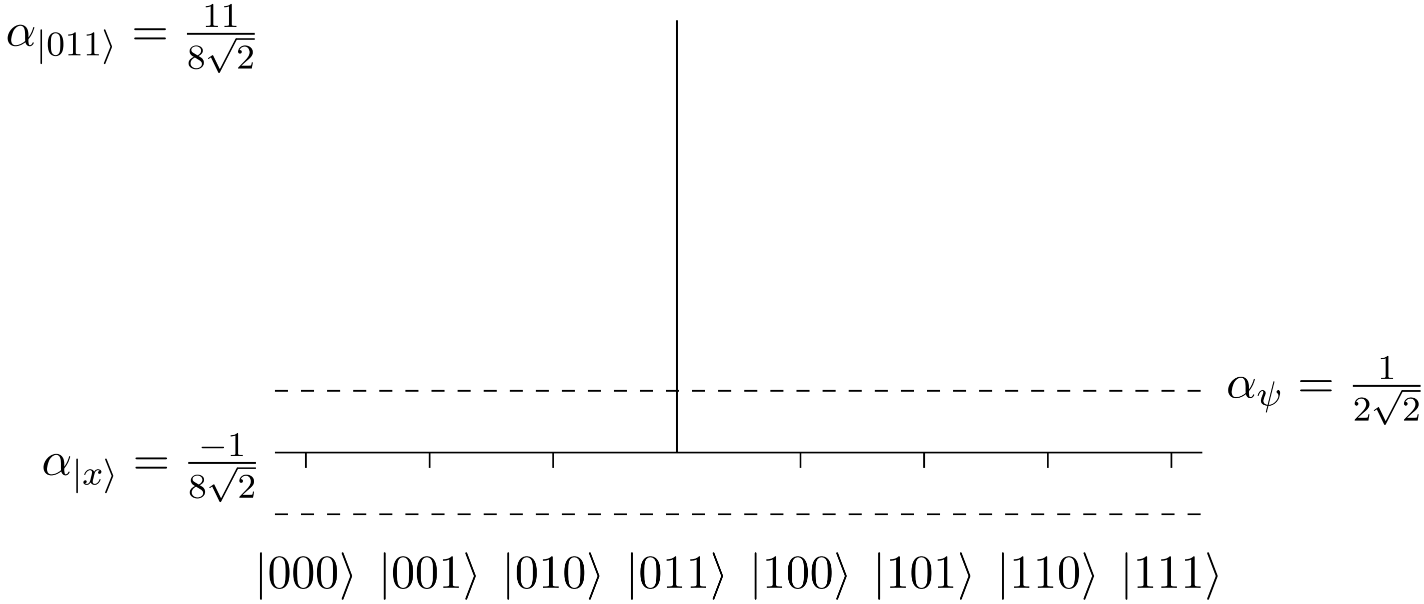
- I will spare you the details, as they are very similar. Result:

$$[2|\psi\rangle\langle\psi| - I]\left[\frac{1}{2}|\psi\rangle - \frac{3}{2\sqrt{2}}|011\rangle\right] = -\frac{1}{8\sqrt{2}}\sum_{\substack{x=0\\x\neq 3}}^{7}|x\rangle + \frac{11}{8\sqrt{2}}|011\rangle$$

- Longer format:

$$|x\rangle = -\frac{1}{8\sqrt{2}}|000\rangle - \frac{1}{8\sqrt{2}}|001\rangle - \frac{1}{8\sqrt{2}}|010\rangle + \frac{11}{8\sqrt{2}}|011\rangle - \ldots - \frac{1}{8\sqrt{2}}|111\rangle \quad (7)$$

# Geometrically, the success of the algorithm is clear



# Final answer

- When the system is observed, the probability that the state representative of the corrct solution, $|011\rangle$, will be measured is $|\frac{11}{8\sqrt{2}}|^2 = 121/128 \approx 94.5\%$
- The probability of finding an incorrect state is $|\frac{-\sqrt{7}}{8\sqrt{2}}|^2 = 7/128 \approx 5.5\%$
- Grover's algorithm is more than 17 times more likely to give the correct answer than an incorrect one with an input size of $N = 8$
- Error only decreases as the input size increases
- Although Grover's algorithm is probabilistic, the error truly becomes negligible as $N$ grows large.