Quantum Searching - Grover

PHYS/CSCI 3090

Prof. Alexandra Kolla
Alexandra.Kolla@Colorado.edu
ECES 122

Prof. Graeme Smith
Graeme.Smith@Colorado.edu
JILA S326

https://home.cs.colorado.edu/~alko5368/indexCSCI3090.html
Come see us!

- Alexandra Kolla/ Graeme Smith: Friday 3:00-4:00 pm, over zoom.
- Ariel Shlosberg: Tu/Th 2:00-4:00pm, over zoom
- Steven Kordonowy: Th 11am-12pm, over zoom.
- Matteo Wilczak: Wednesday, 1-2pm, over zoom.
Where do we stand

- We saw Shor’s algorithm, first real and very significant quantum speedup
Today

- Searching for a marked item
- Grover’s algorithm.
The problem

• Suppose we know that exactly one n-bit integer satisfies some condition.
• Namely, we have a special “marked” item $a$, such that, for some function $f : \{0,1\}^n \rightarrow \{0,1\}$, $f(x)=1$ iff $x=a$ and 0 otherwise.
The problem

- Classically?

  how many queries to the database do I need to find a?

  Check everything: n bits, means \( n = 2^k \) 1's to check

  BAD
The problem

- Classically?

- Have to possibly try all $N = 2^n$ integers $x$ to find the one such that $f(x) = 1$.

- Randomly, need to check at least $N/2$ to have probability 50% of success.

- Quantumly: only $\left(\frac{\pi}{4}\right) \sqrt{N}$ queries!
The setup

We have a function $f(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{o.w.} \end{cases}$
The setup

- We have a function $f(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{o.w.} \end{cases}$.
The Trick

\[ U_f (|x\rangle_n \otimes |0\rangle) = |x\rangle_n \otimes |0 \oplus f(x)\rangle = \]
\[ - |x\rangle_n \otimes |0\rangle, \text{ if } f(x) = 0 \]
\[ - |x\rangle_n \otimes |1\rangle, \text{ if } f(x) = 1 \]

\[ U_f |x\rangle_n \otimes |1\rangle = |x\rangle_n \otimes |1 \oplus f(x)\rangle = \]
\[ - |x\rangle_n \otimes |1\rangle, \text{ if } f(x) = 0 \]
\[ - |x\rangle_n \otimes |0\rangle, \text{ if } f(x) = 1 \]
The Trick

1. \[ U_f |x\rangle_n \otimes (|0\rangle + |1\rangle) = ?? \text{ nothing} \]

2. \[ U_f |x\rangle_n \otimes (|0\rangle - |1\rangle) = ?? \text{ (16-17)} \]
The Trick

\[ U_f |x\rangle_n \otimes 1/\sqrt{2} \ (|0\rangle - |1\rangle) = \]
\[ (-1)^f(x) \ |x\rangle_n \otimes 1/\sqrt{2} \ (|0\rangle - |1\rangle) \]

So taking the 1-qubit output register to be \( \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \), we convert a bit flip to a sign change!
The Unitary for Grover

\[ U_f |x\rangle_n \otimes 1/\sqrt{2} (|0\rangle - |1\rangle) = (-1)^{f(x)} |x\rangle_n \otimes 1/\sqrt{2} (|0\rangle - |1\rangle) \]

Multiply the input state by -1 if and only if \( x = a \)
We can forget about the output register since it does not change
The Unitary for Grover

\[ |x\rangle \rightarrow U_f |x\rangle \]

where

\[ V = \text{unitary for 1 query to database} \]

\[ V|x\rangle_n = \begin{cases} 
|x\rangle_n, & x \neq a \\
-|a\rangle, & x = a 
\end{cases} \]

\[ V|a\rangle = -|a\rangle, \quad V|x\rangle = |x\rangle \quad \forall x \neq a \]

Multiply the input state by \(-1\) if and only if \(x=a\)

We can forget about the output register since it does not change.
The Unitary for Grover

\[ |x\rangle \quad n \text{ bit} \quad U_f \quad n \text{ bit} \quad |x\rangle \]

\[ |y\rangle \quad 1 \text{ bit} \quad |y \oplus f(x)\rangle \quad 1 \text{ bit} \]

- \( V |x\rangle_n = \begin{cases} |x\rangle_n, & x \neq a \\ -|a\rangle, & x = a \end{cases} \)

How does \( V \) act on an arbitrary superposition?
Parenthesis-Projections

- **Question:**
  Let $\Pi_a$ be the projection operator on the basis vector $|a\rangle_n$. What is $\Pi_a(\sum_{0<x\leq2^n}|x\rangle_n)$?

- **Definition:** we denote $\Pi_a$ with $|a\rangle\langle a|$
Parenthesis-Projections, II

- Question:
  Let $|Y\rangle = \sum_{0<x \leq 2^n} y_x |x\rangle_n$ be an arbitrary superposition. How can we express the coefficients $y_x$ as inner products?

\[
y_x = \langle x|Y\rangle
\]

\[
|Y\rangle = \sum_{0<x \leq 2^n} |x\rangle \langle x|Y\rangle
\]
Parenthesis-Projections,II

• Question:
Let \( |Y\rangle = \sum_{0 < x \leq 2^n} y_x |x\rangle_n \) be an arbitrary superposition. How can we express the coefficients \( y_x \) as inner products?

\[
y_x = \langle x | Y \rangle
\]

So \( |Y\rangle = \sum_{0 < x \leq 2^n} |x\rangle \langle x | Y \rangle \)
Parenthesis-Projections, II

• Question:
  What is $\Pi_a |Y\rangle$? (or, equivalently, $|a\rangle\langle a| |Y\rangle$?

\[
\Pi_a |Y\rangle = |a\rangle |x\rangle \sum_l |x\rangle \langle x| |Y\rangle
= \sum_x |a\rangle |x\rangle |x| |Y\rangle
\]

\[
|Y\rangle = \sum_{0<x\leq 2^n} |x\rangle \langle x| |Y\rangle
\]
The Unitary for Grover

\[ U_f \]

|\( |x\rangle \rangle \text{ 1 bit } n \text{ bit} |\)
|\( |y\rangle \rangle \text{ 1 bit } |\)

\[ U_f \]

|\( |x\rangle \rangle n \text{ bit} |\)
|\( |y\rangle \rangle \text{ 1 bit} |\)

|\( |y\oplus f(x)\rangle \rangle |\)

- \( V |x\rangle_n = \begin{cases} |x\rangle_n, & x \neq a \\ -|a\rangle, & x = a \end{cases} \)

How does \( V \) act on an arbitrary superposition
\( |Y\rangle = \sum_{0 < x < 2^n} |x\rangle \langle x|Y\rangle? \)
The Unitary for Grover

How does $V$ act on an arbitrary superposition $|Y\rangle = \sum_{0<x\leq2^n} |x\rangle \langle x|Y\rangle$?

Changes the sign of the component along $|a\rangle$, while leaving unchanged the component orthogonal to $|a\rangle$.

\[ V |x\rangle_n = \begin{cases} |x\rangle_n, & x \neq a \\ -|a\rangle, & x = a \end{cases} \]
The Unitary for Grover

\[ |x\rangle \quad \text{n bit} \]
\[ |y\rangle \quad \text{1 bit} \]

\[ \text{U}_f \]

\[ |x\rangle \quad \text{n bit} \]
\[ |y\rangle \quad \text{1 bit} \]

\[ |y \oplus f(x)\rangle \]

- \[ V |x\rangle_n = \begin{cases} |x\rangle_n, & x \neq a \\ -|a\rangle, & x = a \end{cases} \]

So, at the end, \[ V |Y\rangle = \sum_{0 < x \leq 2^n, x \neq a} |x\rangle \langle x | Y \rangle - |a\rangle \langle a | Y \rangle \]
The Unitary for Grover

\[ |x\rangle \text{ n bit} \quad U_f \quad |x\rangle \text{ n bit} \]

\[ |y\rangle \text{ n bit} \quad U_f \quad |y \oplus f(x)\rangle \text{ n bit} \]

- \[ V |x\rangle_n = \begin{cases} |x\rangle_n, & x \neq a \\ -|a\rangle, & x = a \end{cases} \]

\[ V |Y\rangle = V \sum_{0 < x \leq 2^n} |x\rangle\langle x|Y\rangle = |Y\rangle - 2|a\rangle\langle a|Y\rangle \]
The Unitary for Grover

\[ |x\rangle \quad \begin{array}{c} \text{1 bit n bit} \end{array} \quad U_f \quad \begin{array}{c} \text{n bit} \end{array} \quad |x\rangle \]

\[ |y \oplus f(x)\rangle \]

\[ \mathcal{V} = I - 2|a\rangle\langle a| \]

\[ \mathcal{V}|Y\rangle = \mathcal{V} \sum_{0 < x \leq 2^n} |x\rangle\langle x|Y\rangle = |Y\rangle - 2|a\rangle\langle a|Y\rangle \]
The Uniform Input Superposition

- Recall: \( H^\otimes n \ket{0}_n = \frac{1}{2^{n/2}} \sum_{0 < x \leq 2^n} \ket{x}_n \)