ITIS 6260/8260 Quantum Computing

Lecture 4: Quantum Search: Grover's Algorithm

Yongge Wang

UNC Charlotte, USA

January 3, 2019

Outline

1. Quantum Search
   - The problem
   - Applications
   - Grover's algorithm
2. Further Discussion on Grover's algorithm
   - BBBV Theorem
   - Collisions

Outline

1. Quantum Search
   - The problem
   - Applications
   - Grover's algorithm
2. Further Discussion on Grover's algorithm
   - BBBV Theorem
   - Collisions

The problem

- Input: Given an oracle function $f : \{0, \cdots, N-1\} \to \{0, 1\}$
- Questions: Is there an x such tht $f(x) = 1$ nad if yes, what is the value of x?
- Classical solution: needs N deterministically query
- Grover's algorithm: $O(\sqrt{N})$ query with $O(\log N)$ qubits and $O(\sqrt{N} \log N)$ gates
- Requires quantum access to f such that we can compute $|x, a\rangle \to |x, a \oplus f(x)\rangle$
- Related Questions: unsorted search

The problem

- Input: Given an oracle function $f : \{0, \cdots, N-1\} \to \{0, 1\}$
- Questions: Is there an x such tht $f(x) = 1$ nad if yes, what is the value of x?
- Classical solution: needs N deterministically query
- Grover's algorithm: $O(\sqrt{N})$ query with $O(\log N)$ qubits and $O(\sqrt{N} \log N)$ gates
- Requires quantum access to f such that we can compute $|x, a\rangle \to |x, a \oplus f(x)\rangle$
- Related Questions: unsorted search

The problem

- Input: Given an oracle function $f : \{0, \cdots, N-1\} \to \{0,1\}$
- Questions: Is there an x such tht $f(x) = 1$ nad if yes, what is the value of x?
- Classical solution: needs N deterministically query
- Grover's algorithm: $O(\sqrt{N})$ query with $O(\log N)$ qubits and $O(\sqrt{N}\log N)$ gates
- Requires quantum access to f such that we can compute $|x, a\rangle \to |x, a \oplus f(x)\rangle$
- Related Questions: unsorted search

The problem

- Input: Given an oracle function $f : \{0, \cdots, N-1\} \to \{0, 1\}$
- Questions: Is there an x such tht $f(x) = 1$ nad if yes, what is the value of x?
- Classical solution: needs N deterministically query
- Grover's algorithm: $O(\sqrt{N})$ query with $O(\log N)$ qubits and $O(\sqrt{N} \log N)$ gates
- Requires quantum access to f such that we can compute $|x, a\rangle \to |x, a \oplus f(x)\rangle$
- Related Questions: unsorted search

The problem

- Input: Given an oracle function $f:\{0,\cdots,N-1\}\to\{0,1\}$
- Questions: Is there an x such tht $f(x)=1$ nad if yes, what is the value of x?
- Classical solution: needs N deterministically query
- Grover's algorithm: $O(\sqrt{N})$ query with $O(\log N)$ qubits and $O(\sqrt{N}\log N)$ gates
- Requires quantum access to f such that we can compute $|x,a\rangle\to|x,a\oplus f(x)\rangle$
- Related Questions: unsorted search

The problem

- Input: Given an oracle function $f : \{0, \cdots, N-1\} \to \{0, 1\}$
- Questions: Is there an x such tht $f(x) = 1$ nad if yes, what is the value of x?
- Classical solution: needs N deterministically query
- Grover's algorithm: $O(\sqrt{N})$ query with $O(\log N)$ qubits and $O(\sqrt{N} \log N)$ gates
- Requires quantum access to f such that we can compute $|x, a\rangle \to |x, a \oplus f(x)\rangle$
- Related Questions: unsorted search

Solve NP-Problems

- Let $N = 2^n$ and $f(x)$ be the SAT problem
- Grover's algorithm could solve SAT in $O(2^{n/2}\text{poly}(n))$ times with $2^{n/2}$ querries where the query checks whehter a given x satisfies the circuit formula

Solve NP-Problems

- Let $N = 2^n$ and $f(x)$ be the SAT problem
- Grover's algorithm could solve SAT in $O(2^{n/2}\text{poly}(n))$ times with $2^{n/2}$ querries where the query checks whehter a given x satisfies the circuit formula

Search databases

- $f(x) = 1$ if the person x meets the criteria and 0 otherwise.
- quadratic speed up in search an un-ordered database

Search databases

- $f(x) = 1$ if the person x meets the criteria and 0 otherwise.
- quadratic speed up in search an un-ordered database

Grover's algorithm

- Let $2^n = N$ and initialize all n-qubits to $|0\rangle$.

$$|0\rangle^{\otimes n} = |0 \cdots 0\rangle$$

- Use the Hardamard transform $H^{\otimes n}$ (that is, n applications of Hadamard gate) to obtain

$$|\phi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

Grover's algorithm

- Let $2^n = N$ and initialize all n-qubits to $|0\rangle$.

$$|0\rangle^{\otimes n} = |0\cdots 0\rangle$$

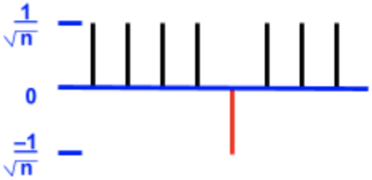
- Use the Hardamard transform $H^{\otimes n}$ (that is, n applications of Hadamard gate) to obtain

$$|\phi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$$

Grover's algorithm

- Query the oracle circuit U_f for implementing f and a unitary transformation that flips the amplitude of the marked item:

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

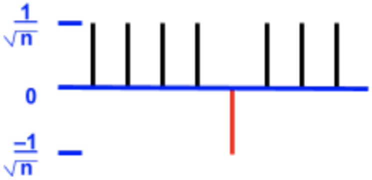


- Note that if one can apply the phase oracle to compute $|x, a\rangle \rightarrow |x, a \oplus f(x)\rangle$, then one can compute $|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$ similarly

Grover's algorithm

- Query the oracle circuit U_f for implementing f and a unitary transformation that flips the amplitude of the marked item:

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

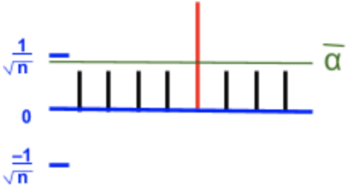


- Note that if one can apply the phase oracle to compute $|x, a\rangle \rightarrow |x, a \oplus f(x)\rangle$, then one can compute $|x\rangle \rightarrow (-1)^{f(x)}|x\rangle$ similarly

Grover diffusion transform

- Let $\bar{\alpha} = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \alpha_x$
- the unitary matrix D will map α_x to $2\bar{\alpha} - \alpha_x$

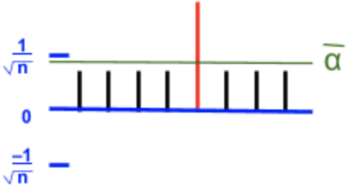
$$D = \begin{bmatrix} \frac{2}{2^n} - 1 & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} - 1 & \cdots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} - 1 \end{bmatrix}$$



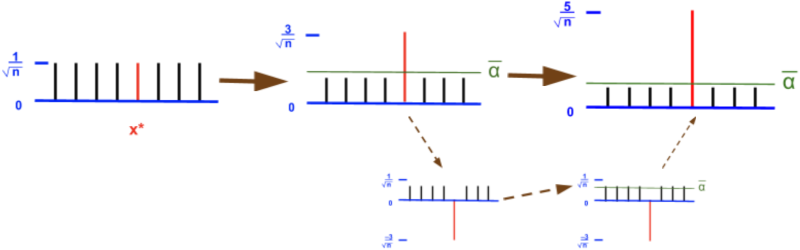
Grover diffusion transform

- Let $\bar{\alpha} = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \alpha_x$
- the unitary matrix D will map α_x to $2\bar{\alpha} - \alpha_x$

$$D = \begin{bmatrix} \frac{2}{2^n} - 1 & \frac{2}{2^n} & \cdots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} - 1 & \cdots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \cdots & \frac{2}{2^n} - 1 \end{bmatrix}$$



Repeat Grover diffusion operator $\frac{\pi}{4}\sqrt{N}$ times

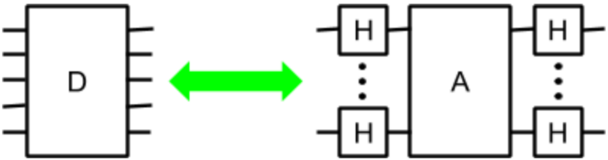


Implement Grover diffusion transform D

- Let A be the conditional phase shift that shifts every state except $|0\rangle$ by -1

$$A = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & \ddots & \\ & & & -1 \end{bmatrix}$$

- Then

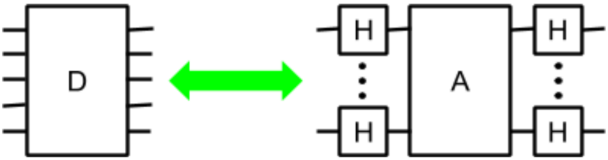


Implement Grover diffusion transform D

- Let A be the conditional phase shift that shifts every state except $|0\rangle$ by -1

$$A = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & \ddots & \\ & & & -1 \end{bmatrix}$$

- Then



Another look at diffusion transform D

- Note that A can be rewritten as $2|0\rangle\langle 0| - I$.

$$(2|0\rangle\langle 0| - I)\,|0\rangle = 2|0\rangle\langle 0||0\rangle - |0\rangle = |0\rangle$$
$$(2|0\rangle\langle 0| - I)\,|x\rangle = 2|0\rangle\langle 0|x\rangle - |x\rangle = -|x\rangle$$

- Thus we have

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

where $|\phi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$

Another look at diffusion transform D

- Note that A can be rewritten as $2|0\rangle\langle 0| - I$.

$$(2|0\rangle\langle 0| - I)\,|0\rangle = 2|0\rangle\langle 0||0\rangle - |0\rangle = |0\rangle$$
$$(2|0\rangle\langle 0| - I)\,|x\rangle = 2|0\rangle\langle 0|x\rangle - |x\rangle = -|x\rangle$$

- Thus we have

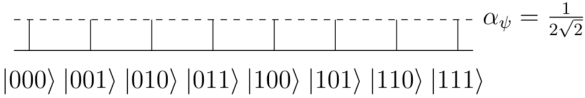
$$D = H^{\otimes n}(2|0\rangle\langle 0| - I)\,H^{\otimes n} = 2H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I = 2|\phi\rangle\langle\phi| - I$$

where $|\phi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$

Grover's algorithm by example

- Let $N = 8 = 2^3$ and the target string is $x_0 = 011$
- initialze the qubits to $|000\rangle$ and apply Hardamard transform to obtain

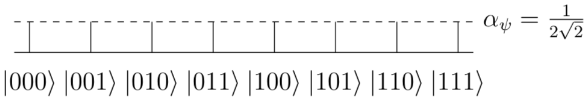
$$H^{\otimes 3}|000\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \cdots + \frac{1}{2\sqrt{2}}|111\rangle = \frac{1}{2\sqrt{2}}\sum_{x=0}^{7}|x\rangle = |\phi\rangle$$



Grover's algorithm by example

- Let $N = 8 = 2^3$ and the target string is $x_0 = 011$
- initialze the qubits to $|000\rangle$ and apply Hardamard transform to obtain

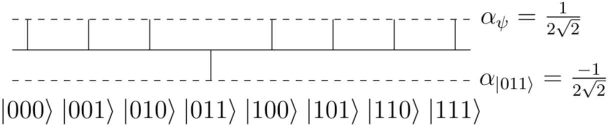
$$H^{\otimes 3}|000\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \cdots + \frac{1}{2\sqrt{2}}|111\rangle = \frac{1}{2\sqrt{2}}\sum_{x=0}^{7}|x\rangle = |\phi\rangle$$



Grover's algorithm by example

- We need to apply Grover's difussion transform D $\lfloor \frac{\pi}{4}\sqrt{8} \rfloor = 2$ times
- The oracle query negates the amplitude of the state $|011\rangle$, giving the configuration

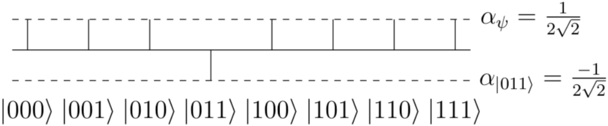
$$|x\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \cdots - \frac{1}{2\sqrt{2}}|011\rangle + \cdots + \frac{1}{2\sqrt{2}}|111\rangle$$



Grover's algorithm by example

- We need to apply Grover's difussion transform D $\lfloor \frac{\pi}{4}\sqrt{8} \rfloor = 2$ times
- The oracle query negates the amplitude of the state $|011\rangle$, giving the configuration

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



Grover's algorithm by example

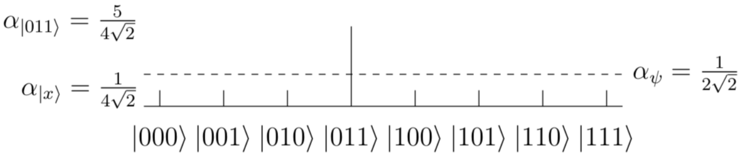
- Perform the diffusion transform $2|\phi\rangle\langle\phi| - I$ to the configuration $|x\rangle = |\phi\rangle - \frac{1}{\sqrt{2}}|011\rangle$

$$
\begin{aligned}
&(2|\phi\rangle\langle\phi| - I)\left(|\phi\rangle - \frac{1}{\sqrt{2}}|011\rangle\right) \\
&= 2|\phi\rangle\langle\phi|\phi\rangle - |\phi\rangle - \frac{2}{\sqrt{2}}|\phi\rangle\langle\phi|011\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= 2|\phi\rangle - |\phi\rangle - \frac{2}{\sqrt{2}}|\phi\rangle\langle\phi|011\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= |\phi\rangle - \frac{2}{\sqrt{2}}|\phi\rangle\langle\phi|011\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= |\phi\rangle - \frac{2}{\sqrt{2}}|\phi\rangle\frac{1}{2\sqrt{2}} + \frac{1}{\sqrt{2}}|011\rangle \\
&= \frac{1}{2}|\phi\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= \frac{1}{2}\frac{1}{2\sqrt{2}}\sum_{x=0}^{7}|x\rangle + \frac{1}{\sqrt{2}}|011\rangle \\
&= \frac{1}{4\sqrt{2}}\sum_{x=0,x\neq 3}^{7}|x\rangle + \frac{5}{4\sqrt{2}}|011\rangle
\end{aligned}
$$

Grover's algorithm by example

- After the first iteration, we get

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



Grover's algorithm by example

- Apply the second oracle query, we get

$$
\begin{aligned}
|x\rangle &= \tfrac{1}{4\sqrt{2}}|000\rangle + \cdots - \tfrac{5}{4\sqrt{2}}|011\rangle + \cdots + \tfrac{1}{4\sqrt{2}}|111\rangle \\
&= \frac{1}{4\sqrt{2}} \sum_{x=0, x\neq 3}^{7} |x\rangle - \frac{5}{4\sqrt{2}}|011\rangle \\
&= \frac{1}{4\sqrt{2}} \sum_{x=0}^{7} |x\rangle - \frac{6}{4\sqrt{2}}|011\rangle \\
&= \frac{1}{2}|\phi\rangle - \frac{3}{2\sqrt{2}}|011\rangle
\end{aligned}
$$

Grover's algorithm by example

- Apply the second diffusion transform $2|\phi\rangle\langle\phi| - I$

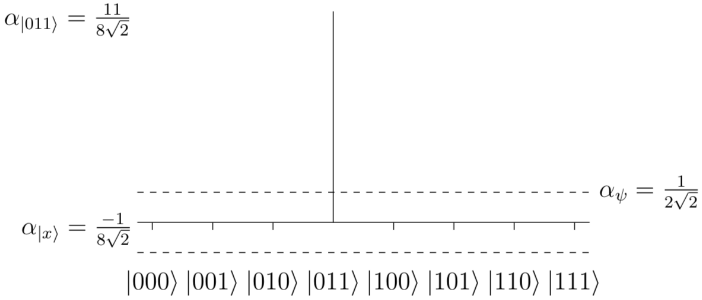
$$
\begin{aligned}
&(2|\phi\rangle\langle\phi| - I)\left(\frac{1}{2}|\phi\rangle - \frac{3}{2\sqrt{2}}|011\rangle\right) \\
&= |\phi\rangle\langle\phi|\phi\rangle - \tfrac{1}{2}|\phi\rangle - \tfrac{3}{\sqrt{2}}|\phi\rangle\langle\phi|011\rangle + \tfrac{3}{\sqrt{2}}|011\rangle \\
&= |\phi\rangle - \tfrac{1}{2}|\phi\rangle - \tfrac{3}{\sqrt{2}}\tfrac{1}{2\sqrt{2}}|\phi\rangle + \tfrac{3}{\sqrt{2}}|011\rangle \\
&= -\tfrac{1}{4}|\phi\rangle + \tfrac{3}{\sqrt{2}}|011\rangle \\
&= -\tfrac{1}{4}\left(\frac{1}{2\sqrt{2}}\sum_{x=0,x\neq 3}^{7}|x\rangle + \frac{1}{2\sqrt{2}}|011\rangle\right) + \tfrac{3}{\sqrt{2}}|011\rangle \\
&= -\frac{1}{8\sqrt{2}}\sum_{x=0,x\neq 3}^{7}|x\rangle + \frac{11}{8\sqrt{2}}|011\rangle
\end{aligned}
$$

Grover's algorithm by example

- After the second iteration, we get

$$|x\rangle = -\frac{1}{8\sqrt{2}}|000\rangle - \cdots + \frac{11}{8\sqrt{2}}|011\rangle - \cdots - \frac{1}{8\sqrt{2}}|111\rangle$$

- $|\frac{11}{8\sqrt{2}}|^2 = 121/128 \simeq 0.945$

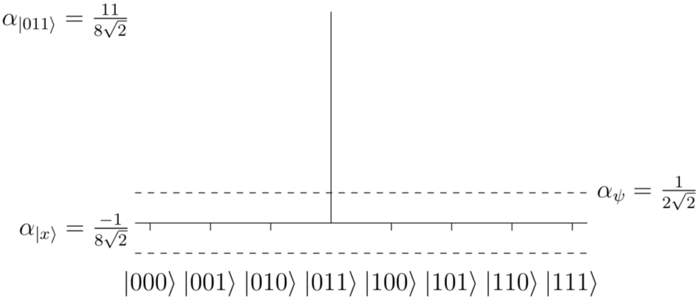


Grover's algorithm by example

- After the second iteration, we get

$$|x\rangle = -\frac{1}{8\sqrt{2}}|000\rangle - \cdots + \frac{11}{8\sqrt{2}}|011\rangle - \cdots - \frac{1}{8\sqrt{2}}|111\rangle$$

- $|\frac{11}{8\sqrt{2}}|^2 = 121/128 \simeq 0.945$



BBBV Theorem

- (Bennett, Bernstein, Brassard, Vazirani 1994: Informal Description) Grover's algorithm is asymptotically optimal for the black-box unordered search problem.

Collisions

- Given a quantum black-box access to a function $f: \{0, \cdots, N-1\} \to \{0, \cdots, N-1\}$ and f is promised to be two-to-one. Find x and y such that $f(x) = f(y)$.
- Traditionally, the birthday attack shows that we need approximately $\sqrt{N}$ queries to find a collision
- (Brassard, Hoyer, Tapp 1997) An $O(\sqrt[3]{N})$-step algorithm
  1. pick $\sqrt[3]{N}$ random inputs to f, query them classically, and sort the results for fast lookup.
  2. run Grover's algorithm on $\sqrt[3]{N^2}$ more random inputs to f. In this Grover's search, cound each input x as "marked" iff $f(x) = f(y)$ for one of the $\sqrt[3]{N^2}$ inputs y that was already queried in the first step

Collisions

- Given a quantum black-box access to a function $f:\{0,\cdots,N-1\}\to\{0,\cdots,N-1\}$ and f is promised to be two-to-one. Find x and y such that $f(x)=f(y)$.
- Traditionally, the birthday attack shows that we need approximately $\sqrt{N}$ queries to find a collision
- (Brassard, Hoyer, Tapp 1997) An $O(\sqrt[3]{N})$-step algorithm
  1. pick $\sqrt[3]{N}$ random inputs to f, query them classically, and sort the results for fast lookup.
  2. run Grover's algorithm on $\sqrt[3]{N^2}$ more random inputs to f. In this Grover's search, cound each input x as "marked" iff $f(x)=f(y)$ for one of the $\sqrt[3]{N^2}$ inputs y that was already queried in the first step

Collisions

- Given a quantum black-box access to a function $f : \{0, \cdots, N-1\} \to \{0, \cdots, N-1\}$ and f is promised to be two-to-one. Find x and y such that $f(x) = f(y)$.
- Traditionally, the birthday attack shows that we need approximately $\sqrt{N}$ queries to find a collision
- (Brassard, Hoyer, Tapp 1997) An $O(\sqrt[3]{N})$-step algorithm
  1. pick $\sqrt[3]{N}$ random inputs to f, query them classically, and sort the results for fast lookup.
  2. run Grover's algorithm on $\sqrt[3]{N^2}$ more random inputs to f. In this Grover's search, cound each input x as "marked" iff $f(x) = f(y)$ for one of the $\sqrt[3]{N^2}$ inputs y that was already queried in the first step

Collisions

- Given a quantum black-box access to a function $f : \{0, \cdots, N-1\} \to \{0, \cdots, N-1\}$ and f is promised to be two-to-one. Find x and y such that $f(x) = f(y)$.
- Traditionally, the birthday attack shows that we need approximately $\sqrt{N}$ queries to find a collision
- (Brassard, Hoyer, Tapp 1997) An $O(\sqrt[3]{N})$-step algorithm
  1. pick $\sqrt[3]{N}$ random inputs to f, query them classically, and sort the results for fast lookup.
  2. run Grover's algorithm on $\sqrt[3]{N^2}$ more random inputs to f. In this Grover's search, cound each input x as "marked" iff $f(x) = f(y)$ for one of the $\sqrt[3]{N^2}$ inputs y that was already queried in the first step

Collisions

- Given a quantum black-box access to a function $f : \{0, \cdots, N-1\} \rightarrow \{0, \cdots, N-1\}$ and f is promised to be two-to-one. Find x and y such that $f(x) = f(y)$.
- Traditionally, the birthday attack shows that we need approximately $\sqrt{N}$ queries to find a collision
- (Brassard, Hoyer, Tapp 1997) An $O(\sqrt[3]{N})$-step algorithm
  1. pick $\sqrt[3]{N}$ random inputs to f, query them classically, and sort the results for fast lookup.
  2. run Grover's algorithm on $\sqrt[3]{N^2}$ more random inputs to f. In this Grover's search, cound each input x as "marked" iff $f(x) = f(y)$ for one of the $\sqrt[3]{N^2}$ inputs y that was already queried in the first step

Q&A

Q&A?