

Quantum Computing

- Week 12 (June 30th – July 1st, 2026)
- Topics:
 - Unstructured Search Problem
 - Grover's algorithm

Unstructured Search

- Search problems: Given a domain D and a Boolean function f , find an $x \in D$ s.t. $f(x) = 1$.
 - How *good* a search algorithm is: How many times f is evaluated.

Unstructured Search

- Search problems: Given a domain D and a Boolean function f , find an $x \in D$ s.t. $f(x) = 1$.
 - How *good* a search algorithm is: How many times f is evaluated.
- Running time: (Suppose that $|D| = 2^n$, namely, exponentially large)
 - The worst case: Brute-force, $O(|D|)$
 - Good cases: D has some **structures**...

Unstructured Search

- Search problems: Given a domain D and a Boolean function f , find an $x \in D$ s.t. $f(x) = 1$.
 - How *good* a search algorithm is: How many times f is evaluated.
- Running time: (Suppose that $|D| = 2^n$, namely, exponentially large)
 - The worst case: Brute-force, $O(|D|)$
 - Good cases: D has some **structures**...
- Polynomial-time ($O(\log |D|) = O(n)$) searching algorithms relying on specific data structures:
 - Binary search in *sorted lists*
 - Binary search in *some tree structures* (binary trees, ...)
 - BFS/DFS in some *graph structures*

Unstructured Search

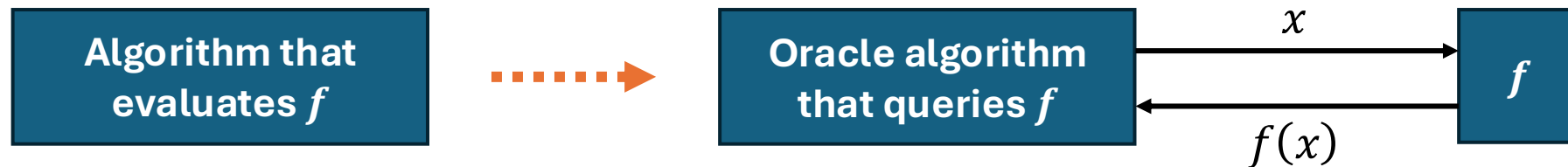
- Search problems: Given a domain D and a Boolean function f , find an $x \in D$ s.t. $f(x) = 1$.
 - How *good* a search algorithm is: How many times f is evaluated.
- Running time: (Suppose that $|D| = 2^n$, namely, exponentially large)
 - **The worst case: Brute-force, $O(|D|)$**
 - Good cases: D has some structures...

Unstructured Search

- Search problems: Given a domain D and a Boolean function f , find an $x \in D$ s.t. $f(x) = 1$.
 - How *good* a search algorithm is: How many times f is evaluated.
- Running time: (Suppose that $|D| = 2^n$, namely, exponentially large)
 - **The worst case: Brute-force, $O(|D|)$**
 - Good cases: D has some structures...
- For unstructured search problems, can quantum computing offer a better solution?
 - Grover's algorithm, **$O(\sqrt{|D|})$ quantum** evaluations on f

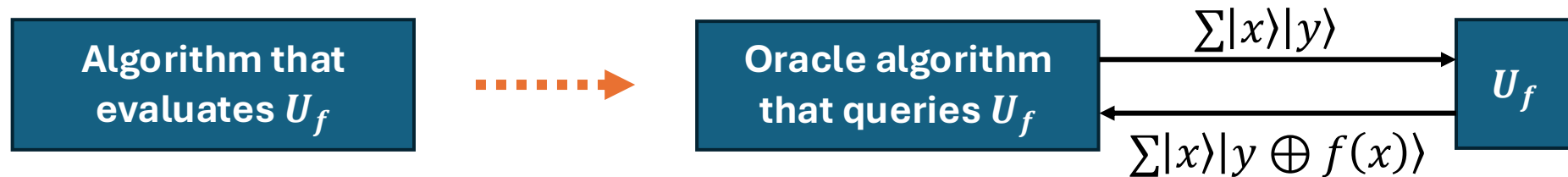
Unstructured Search

- Understand f as an oracle:
 - Reformulate a search algorithm as an oracle algorithm
 - Treat f as an oracle to reflect its black-box nature and the lack of structure
 - Evaluate f once = query the oracle f once



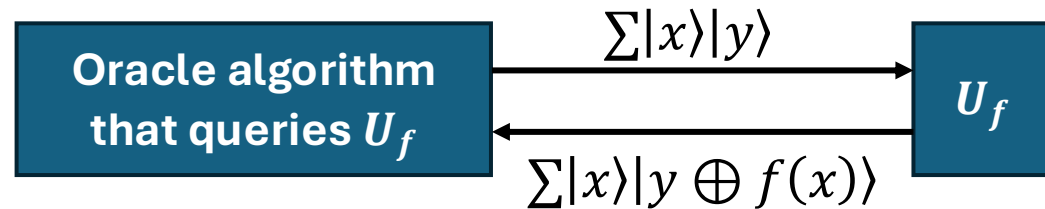
Unstructured Search

- Understand f as a *quantum-accessible* oracle:
 - ...
 - Evaluate U_f once = query the oracle U_f once



Unstructured Search

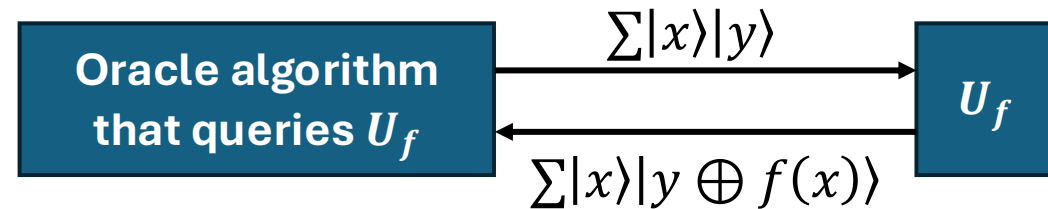
- Transform a “standard oracle” into a “phase oracle”
- Understand f as a *quantum-accessible* oracle:



- Query U_f on $\sum |x\rangle |0\rangle$, then get $\sum |x\rangle |f(x)\rangle$
- Question: Query U_f on $\sum |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$, then get...

Unstructured Search

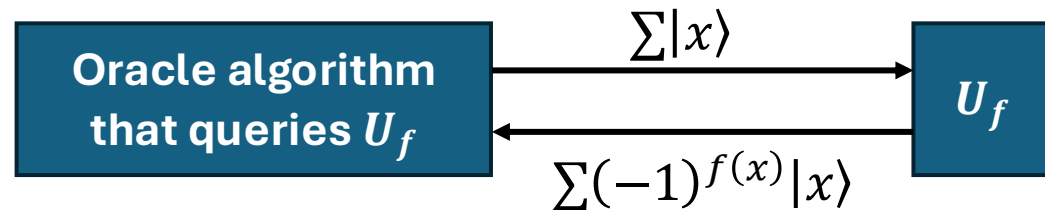
- Transform a “standard oracle” into a “phase oracle”
- Understand f as a *quantum-accessible* oracle:



- Query U_f on $\sum |x\rangle |0\rangle$, then get $\sum |x\rangle |f(x)\rangle$
- Question: Query U_f on $\sum |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$, then get $\sum (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

Unstructured Search

- Transform a “standard oracle” into a “phase oracle”
- Phase oracle:



- Query U_f on $\sum |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$, then get $\sum (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$
- Ignore the last qubit $\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$

Unstructured Search

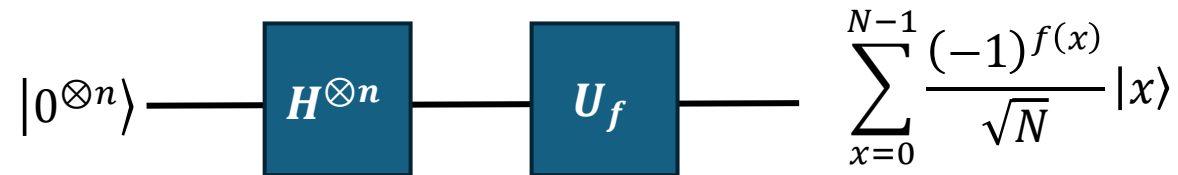
- Reformulate unstructured search problems
- Given a domain D and **a phase oracle** $U_f: |x\rangle \mapsto (-1)^{f(x)}|x\rangle$, find an $x \in D$ s.t. $f(x) = 1$.
 - Let $|D| = N = 2^n$ for some integer n
 - Suppose that there is only one $x_0 \in D$ s.t. $f(x_0) = 1$

Unstructured Search

- Reformulate unstructured search problems
- Given a domain D and a phase oracle $U_f: |x\rangle \mapsto (-1)^{f(x)}|x\rangle$, find an $x \in D$ s.t. $f(x) = 1$.
 - Let $|D| = N = 2^n$ for some integer n
 - Suppose that there is **only one** $x_0 \in D$ s.t. $f(x_0) = 1$

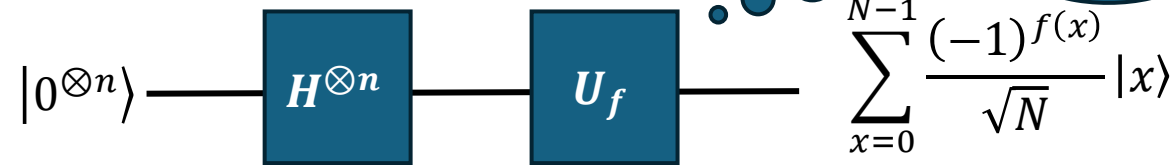
Amplitude Amplification

- Reformulate unstructured search problems
- Given a domain D and a phase oracle $U_f: |x\rangle \mapsto (-1)^{f(x)}|x\rangle$, find an $x \in D$ s.t. $f(x) = 1$.
 - Let $|D| = N = 2^n$ for some integer n
 - Suppose that there is only one $x_0 \in D$ s.t. $f(x_0) = 1$
- Starting point:



Amplitude Amplification

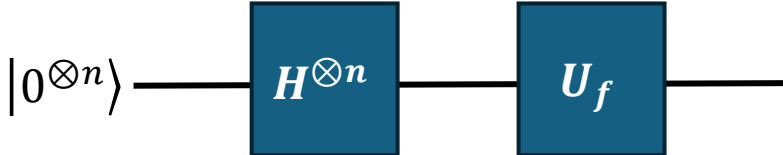
- Reformulate unstructured search problems
- Given a domain D and a phase oracle $U_f: |x\rangle \mapsto (-1)^{f(x)}|x\rangle$, find an $x \in D$ s.t. $f(x) = 1$.
 - Let $|D| = N = 2^n$ for some integer n
 - Suppose that there is only one $x_0 \in D$ s.t. $f(x_0) = 1$
- Starting point:



Amplitude Amplification

- Reformulate unstructured search problems
- Given a domain D and a phase oracle $U_f: |x\rangle \mapsto (-1)^{f(x)}|x\rangle$, find an $x \in D$ s.t. $f(x) = 1$.
 - Let $|D| = N = 2^n$ for some integer n
 - Suppose that there is only one $x_0 \in D$ s.t. $f(x_0) = 1$

- Starting point:


$$\begin{aligned} & |0^{\otimes n}\rangle \xrightarrow{H^{\otimes n}} \xrightarrow{U_f} \sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{\sqrt{N}} |x\rangle \\ & = \sum_{\substack{x=0 \\ x \neq x_0}}^{N-1} \frac{1}{\sqrt{N}} |x\rangle + \frac{(-1)}{\sqrt{N}} |x_0\rangle \end{aligned}$$

- Goal: Boost the **amplitude** of the *marked state* $|x_0\rangle$

Amplitude Amplification

- Consider the following quantum circuit:



- The phase gate: $|x\rangle \mapsto (-1)^x|x\rangle$

Amplitude Amplification

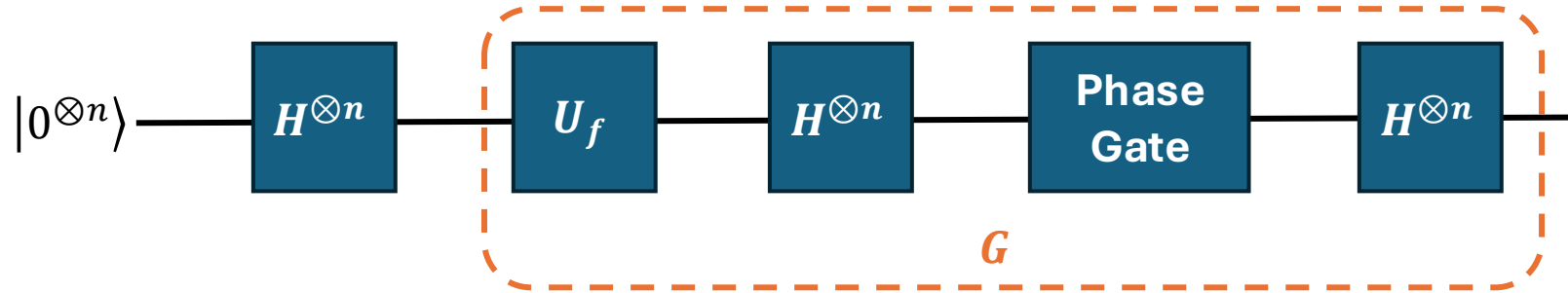
- Consider the following quantum circuit:



- The phase gate: $|x\rangle \mapsto (-1)^x|x\rangle$

Amplitude Amplification

- Consider the following quantum circuit:

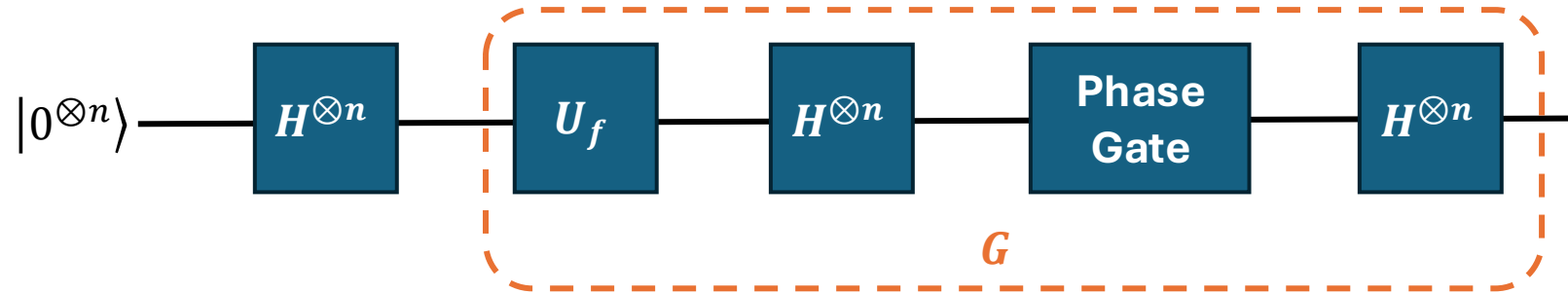


- The phase gate: $|x\rangle \mapsto (-1)^x|x\rangle$

$H^{\otimes n}|\mathbf{0}\rangle$ ——— G ——— $(1 - \frac{4}{N})H^{\otimes n}|\mathbf{0}\rangle + \frac{2}{\sqrt{N}}|x_0\rangle$

Amplitude Amplification

- Consider the following quantum circuit:

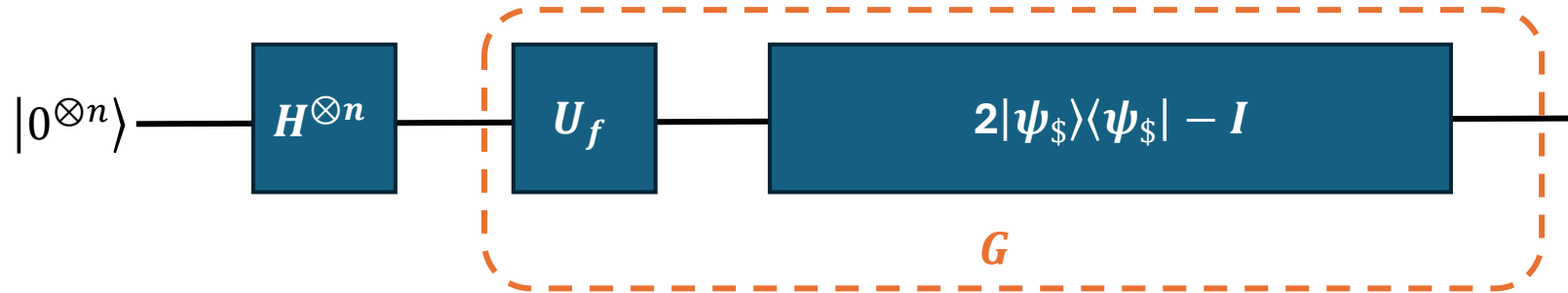


- The phase gate: $|x\rangle \mapsto (-1)^x |x\rangle$
- Let $|x_0^\perp\rangle := \sum_{x \neq x_0} \frac{1}{\sqrt{N-1}} |x\rangle$

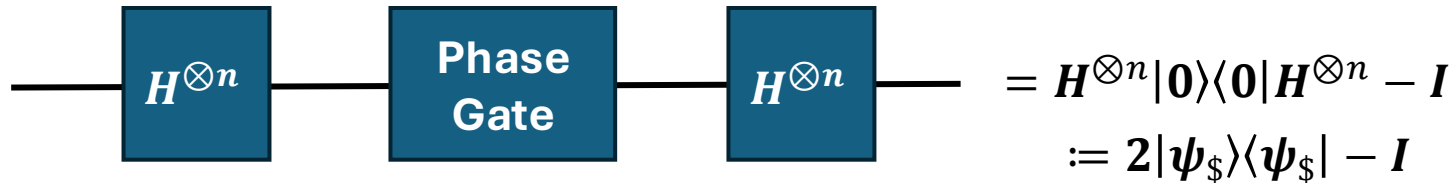
$$\begin{aligned}
 & H^{\otimes n} |0\rangle \quad \longrightarrow \quad \boxed{G} \quad \longrightarrow \quad \left(1 - \frac{4}{N}\right) H^{\otimes n} |0\rangle + \frac{2}{\sqrt{N}} |x_0\rangle \\
 & = \frac{\sqrt{N-1}}{\sqrt{N}} |x_0^\perp\rangle + \frac{1}{\sqrt{N}} |x_0\rangle \qquad \qquad \qquad = \left(1 - \frac{4}{N}\right) \frac{\sqrt{N-1}}{\sqrt{N}} |x_0^\perp\rangle + \left(3 - \frac{4}{N}\right) \frac{1}{\sqrt{N}} |x_0\rangle
 \end{aligned}$$

Amplitude Amplification

- Consider the following quantum circuit:



- Observation (**Exercise**):



Amplitude Amplification

- Change the view:

$$H^{\otimes n}|\mathbf{0}\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|x_0^\perp\rangle + \frac{1}{\sqrt{N}}|x_0\rangle \longrightarrow \boxed{G = (2|\psi_\$ \rangle \langle \psi_\$ | - I)U_f} \longrightarrow$$

Amplitude Amplification

- Change the view:

$$H^{\otimes n}|\mathbf{0}\rangle = \cos(\theta) |x_0^\perp\rangle + \sin \theta |x_0\rangle \quad \text{---} \quad \boxed{G = (2|\psi_\$ \rangle \langle \psi_\$ | - I)U_f} \quad \text{---}$$

- We have: $G(\cos(\theta) |x_0^\perp\rangle + \sin \theta |x_0\rangle) = (2|\psi_\$ \rangle \langle \psi_\$ | - I)U_f(\cos(\theta) |x_0^\perp\rangle + \sin \theta |x_0\rangle)$
 $= \cos(3\theta) |x_0^\perp\rangle + \sin(3\theta) |x_0\rangle$

Amplitude Amplification

- Change the view:

$$H^{\otimes n}|\mathbf{0}\rangle = \cos(\theta) |x_0^\perp\rangle + \sin \theta |x_0\rangle \quad \text{---} \quad \boxed{G = (2|\psi_\$ \rangle \langle \psi_\$ | - I)U_f} \quad \text{---}$$

- More generally:

$$G^k(\cos(\theta) |x_0^\perp\rangle + \sin \theta |x_0\rangle) = \cos((1 + 2k)\theta) |x_0^\perp\rangle + \sin((1 + 2k)\theta) |x_0\rangle$$

- Grover's algorithm: Apply the unitary G many times so that $\sin((1 + 2k)\theta)$ is noticeable

Amplitude Amplification

- Change the view:

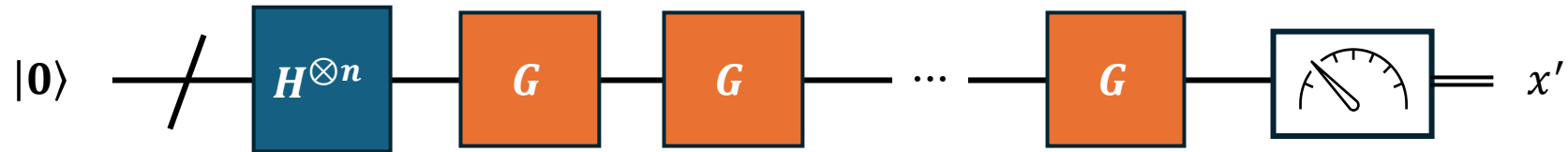
$$H^{\otimes n}|\mathbf{0}\rangle = \cos(\theta) |x_0^\perp\rangle + \sin \theta |x_0\rangle \quad \text{---} \quad \boxed{G = (2|\psi_\$ \rangle \langle \psi_\$ | - I)U_f} \quad \text{---}$$

- More generally:

$$G^k(\cos(\theta) |x_0^\perp\rangle + \sin \theta |x_0\rangle) = \cos((1 + 2k)\theta) |x_0^\perp\rangle + \sin((1 + 2k)\theta) |x_0\rangle$$

- Grover's algorithm: Apply the unitary G many times so that $\sin((1 + 2k)\theta)$ is noticeable
- **Theorem (Informal):** $\sin((1 + 2k)\theta)$ is noticeable if $k = O(\sqrt{N})$.

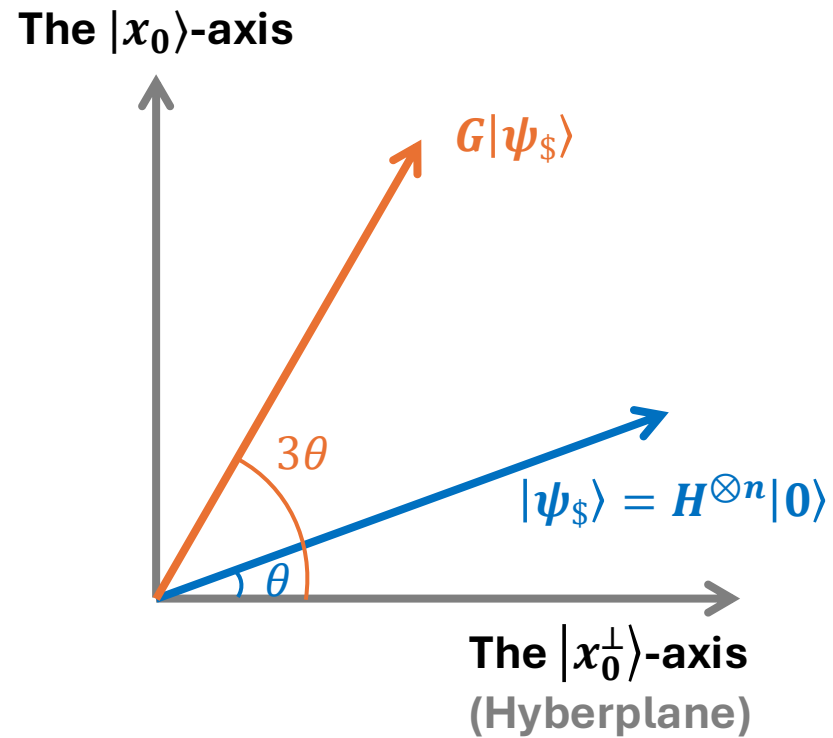
Grover Search Algorithm



- Apply G about $O(\sqrt{N})$ times to make $\Pr[x' = x_0]$ noticeable (e.g., $\geq \frac{1}{2}$)

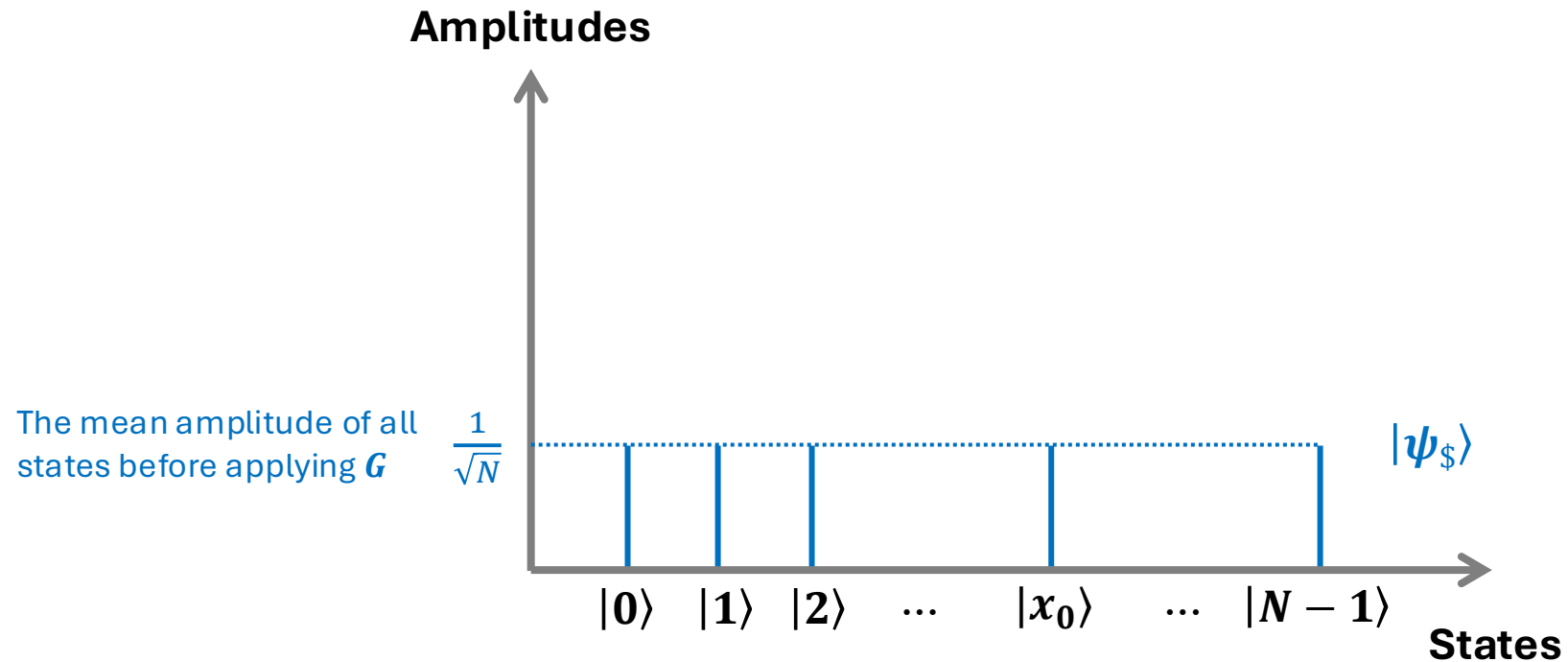
Grover Search Algorithm

- Two ways to understand the process of amplitude amplification:



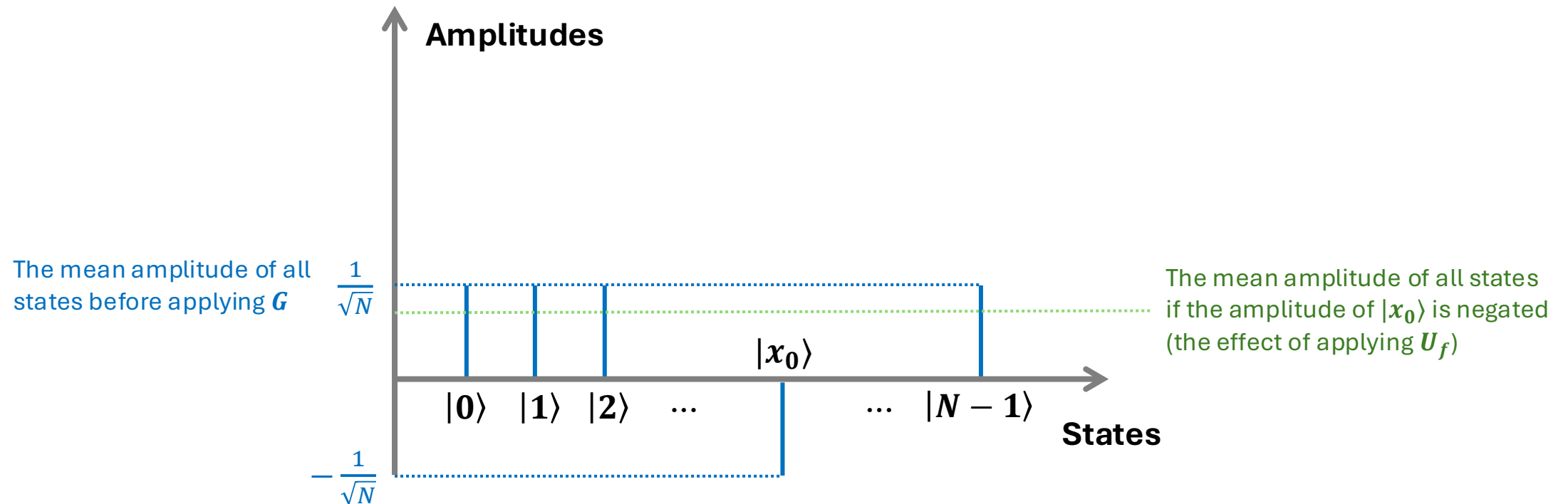
Grover Search Algorithm

- Two ways to understand the process of amplitude amplification: $|\psi_s\rangle$



Grover Search Algorithm

- Two ways to understand the process of amplitude amplification: $U_f|\psi\rangle$



Grover Search Algorithm

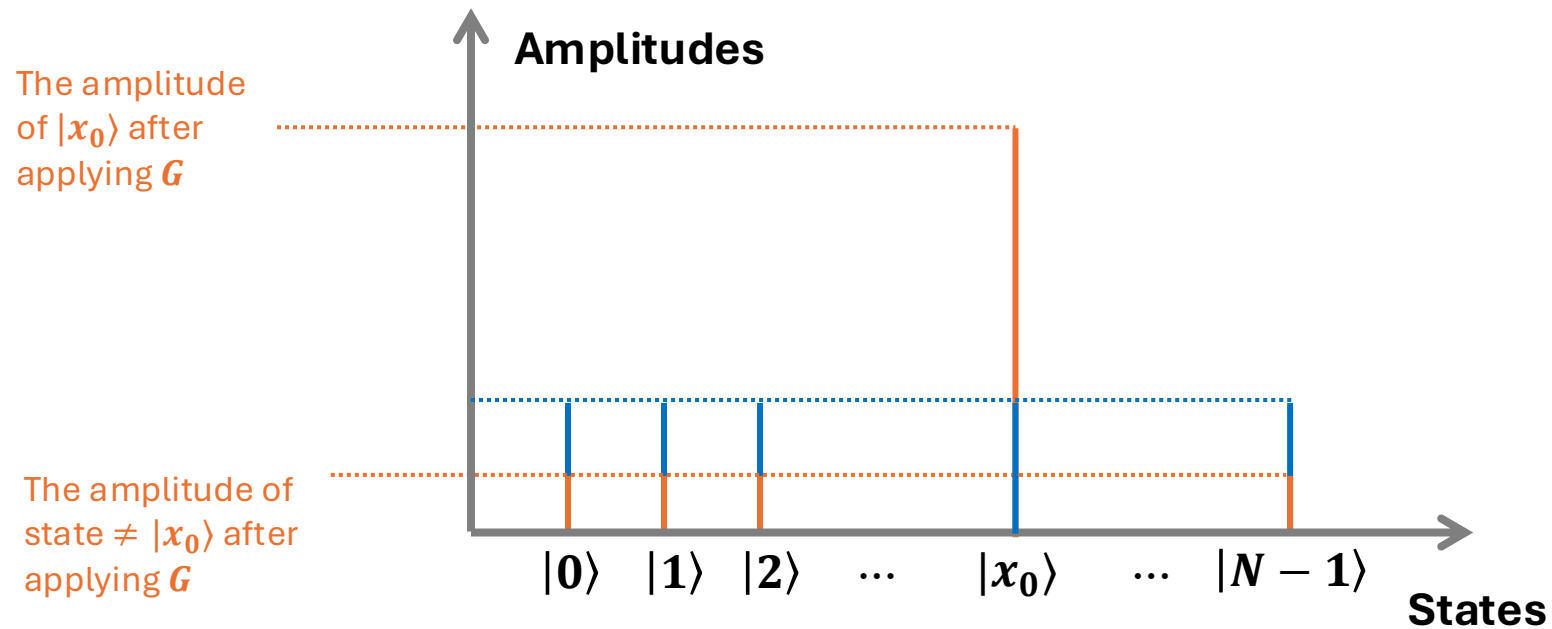
- Two ways to understand the process of amplitude amplification: $(2|\psi_\$ \rangle \langle \psi_\$ | - I)U_f|\psi_\$ \rangle$



Grover Search Algorithm

- Two ways to understand the process of amplitude amplification:

$$G|\psi\rangle$$



Reference

- **[NC00]:** Chapter 6
- **[KLM07]:** Chapter 8