Quantum Computing

- Lectures 17 and 18 (July 9-10, 2025)

- 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.

- Running time: (Suppose that $|D| = 2^n$, namely, exponentially large)
  - The worst case: Brute-force, $\mathrm{O}(|D|)$
  - Good cases: D has some **structures**…

- Polynomial-time ($\mathrm{O}(\log |D|) = O(n)$) searching algorithms relying on specific data structures:
  - Binary search in *sorted lists*
  - Binary search in *some tree structures* (binary tree, AVL tree, red-black tree, …)
  - BFS/DFS in some *graph structures*
  - QFT (or Shor's algorithm) in functions *with periods*

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.

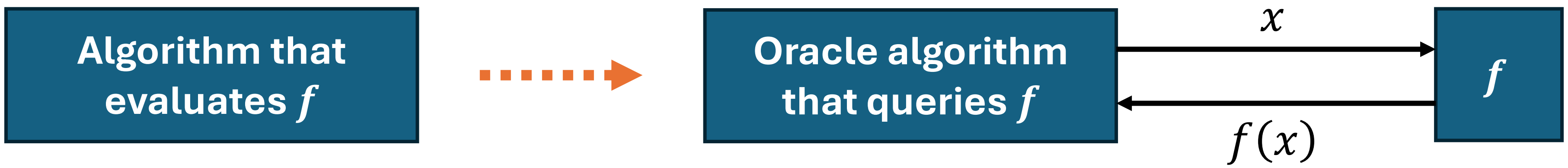
- Running time: (Suppose that $|D| = 2^n$, namely, exponentially large)
  - **The worst case: Brute-force, $\mathbf{O}(|\boldsymbol{D}|)$**
  - Good cases: D has some structures…

- For unstructured search problems, can quantum computing offer a better solution?
  - Grover's algorithm, $\mathbf{O}\left(\sqrt{|\boldsymbol{D}|}\right)$ **quantum** evaluations on f

Unstructured Search

- **Transform a “standard oracle” into a “phase oracle”**

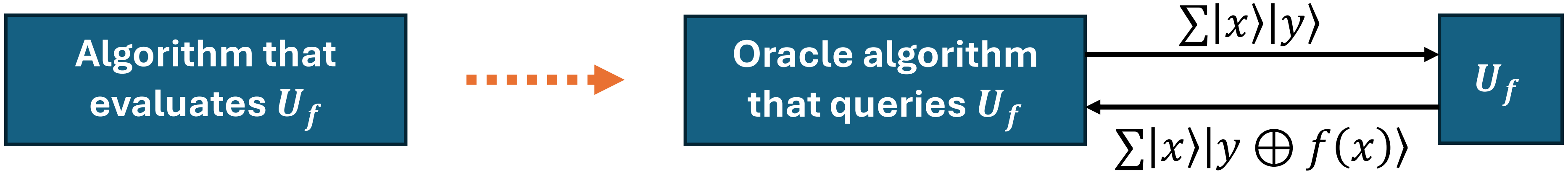
- Understand f as an oracle:
  - Reformulate a search algorithm as an oracle algorithm
  - Treat f as an oracle to reflect its black-box nature and the lack of structure
  - Evaluate f once = query the oracle f once



Unstructured Search

- **Transform a “standard oracle” into a “phase oracle”**

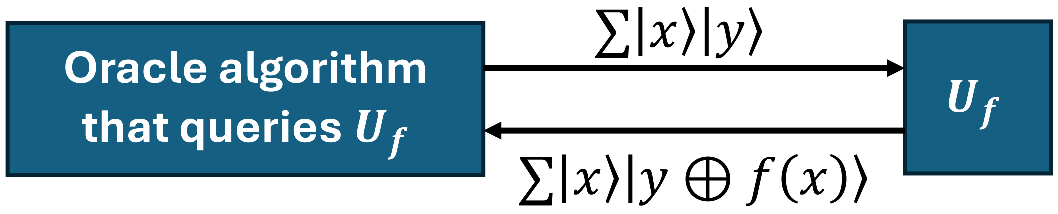
- Understand f as a *quantum-accessible* oracle:
  - …
  - Evaluate U_f once = query the oracle U_f once



Unstructured Search

- **Transform a "standard oracle" into a "phase oracle"**

- Understand f as a *quantum-accessible* oracle:

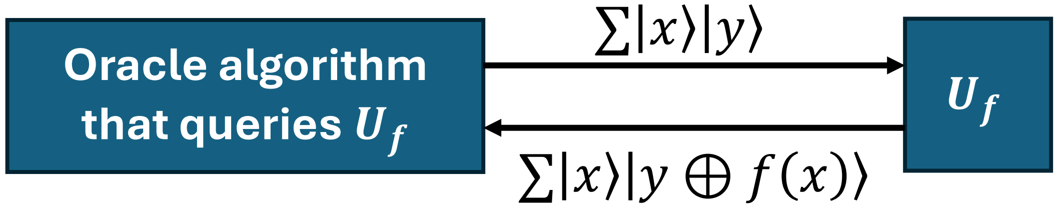


- Query $\boldsymbol{U_f}$ on $\sum|x\rangle|0\rangle$, then get $\sum|x\rangle|f(x)\rangle$
- Question: Query $\boldsymbol{U_f}$ on $\sum|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$, then get…

Unstructured Search

- **Transform a “standard oracle” into a “phase oracle”**

- Understand f as a *quantum-accessible* oracle:

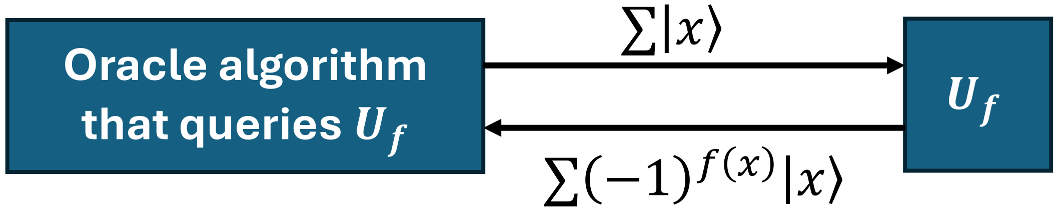


- Query U_f on $\sum|x\rangle|0\rangle$, then get $\sum|x\rangle|f(x)\rangle$
- Question: Query U_f on $\sum|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$, then get $\sum(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

Unstructured Search

- **Transform a “standard oracle” into a “phase oracle”**

- Phase oracle:



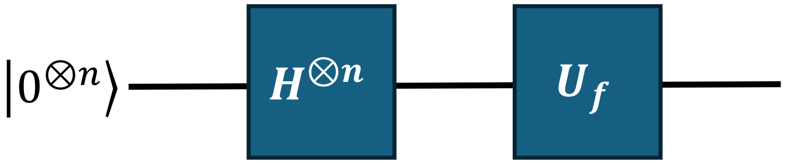
- Query $\boldsymbol{U_f}$ on $\sum|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$, then get $\sum(-1)^{f(x)}|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$
- Ignore the last qubit $\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$

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. $f(x_0) = 1$

Amplitude Amplification

- Reformulate unstructured search problems
- Given a domain D and a phase oracle $U_f\colon |x\rangle \mapsto (-1)^{f(x)}|x\rangle$, 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:

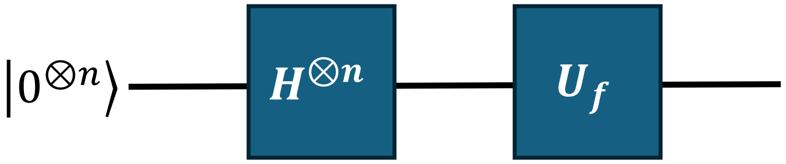


$$\sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{\sqrt{N}} |x\rangle$$

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:

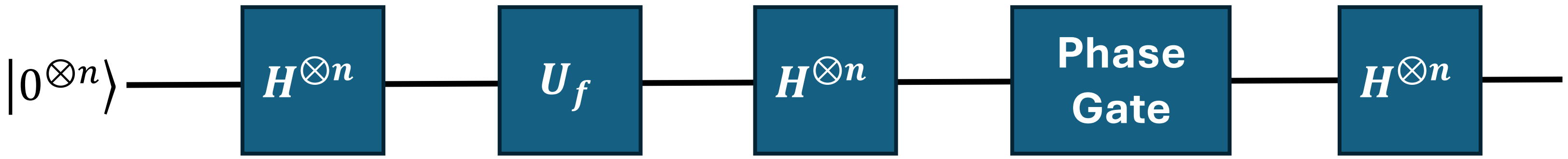


$$\sum_{x=0}^{N-1} \frac{(-1)^{f(x)}}{\sqrt{N}} |x\rangle = \sum_{\substack{x=0 \\ x \neq x_0}}^{N-1} \frac{1}{\sqrt{N}} |x\rangle + \frac{(-1)}{\sqrt{N}} |x_0\rangle$$

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

Amplitude Amplification

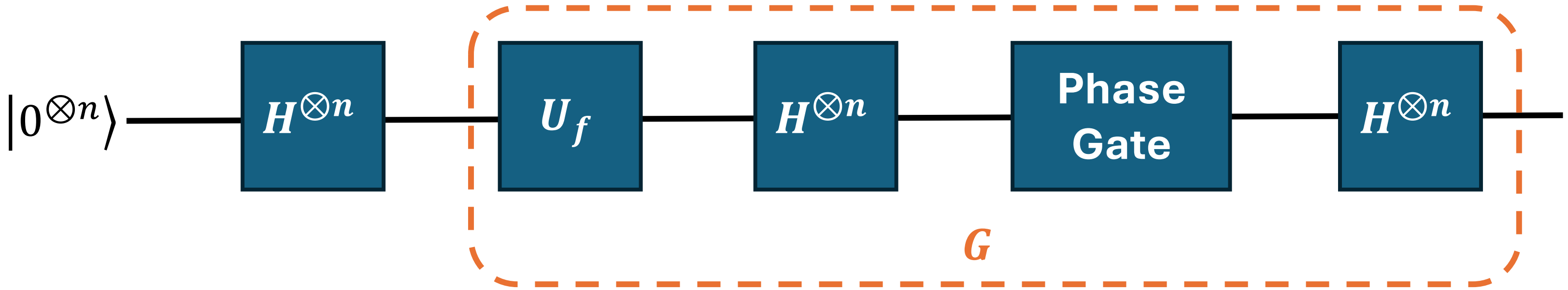
- Consider the following quantum circuit:



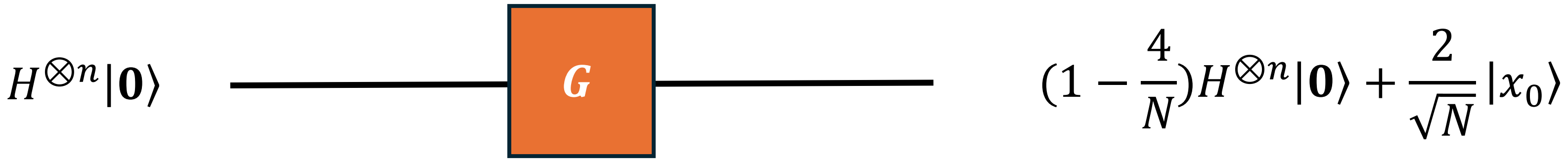
- The phase gate: $|x\rangle \mapsto (-1)^x|x\rangle$

Amplitude Amplification

- Consider the following quantum circuit:

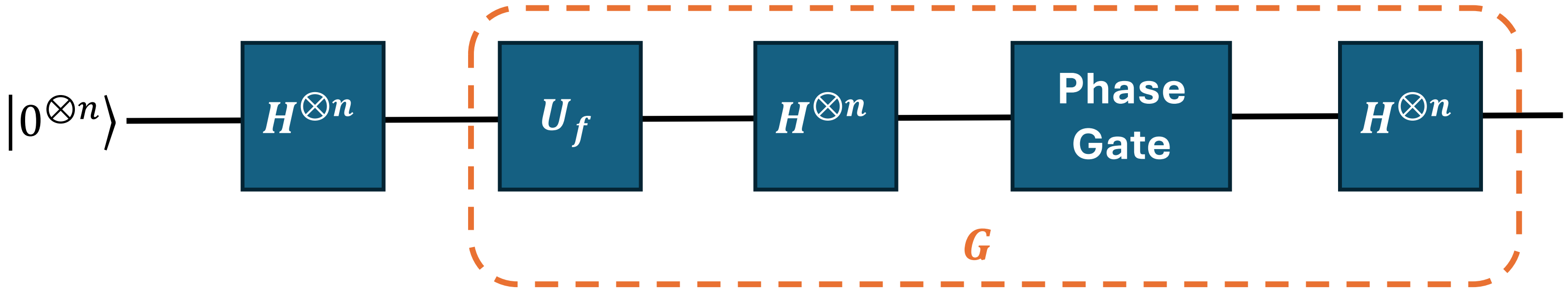


- The phase gate: $|x\rangle \mapsto (-1)^x|x\rangle$



Amplitude Amplification

- Consider the following quantum circuit:



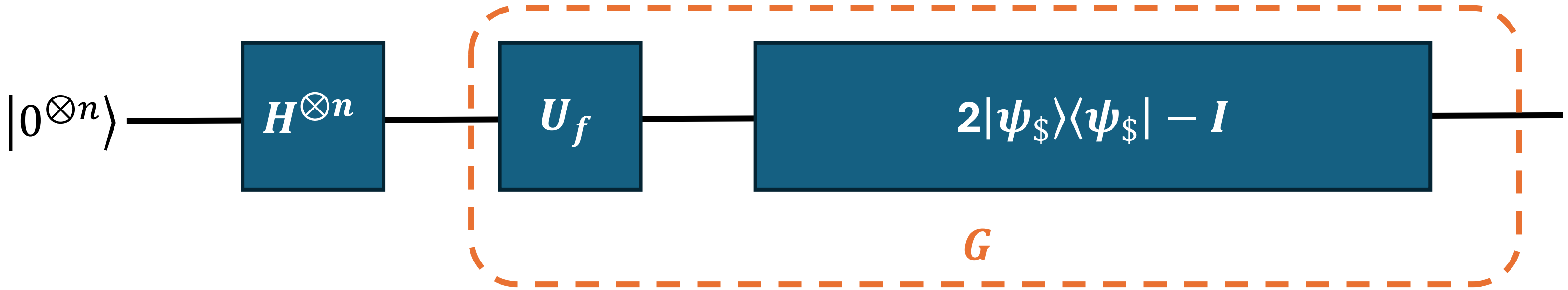
- The phase gate: $|x\rangle \mapsto (-1)^x |x\rangle$
- Let $\left|x_0^\perp\right\rangle \coloneqq \sum_{x \neq x_0} \frac{1}{\sqrt{N-1}} |x\rangle$

$$H^{\otimes n}|\mathbf{0}\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}\left|x_0^\perp\right\rangle + \frac{1}{\sqrt{N}}|x_0\rangle$$

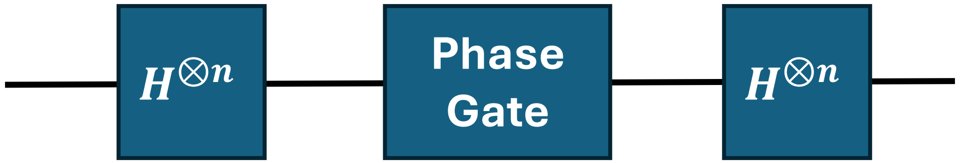
$$\left(1 - \frac{4}{N}\right) H^{\otimes n}|\mathbf{0}\rangle + \frac{2}{\sqrt{N}}|x_0\rangle = \left(1 - \frac{4}{N}\right)\frac{\sqrt{N-1}}{\sqrt{N}}\left|x_0^\perp\right\rangle + \left(3 - \frac{4}{N}\right)\frac{1}{\sqrt{N}}|x_0\rangle$$

Amplitude Amplification

- Consider the following quantum circuit:



- Observation:



$$= H^{\otimes n}|0\rangle\langle 0|H^{\otimes n} - I$$
$$:= 2|\psi_\$\rangle\langle\psi_\$| - I$$

Amplitude Amplification

- Change the view:

$$H^{\otimes n}|\mathbf{0}\rangle = \frac{\sqrt{N-1}}{\sqrt{N}}|x_0^{\perp}\rangle + \frac{1}{\sqrt{N}}|x_0\rangle$$

Amplitude Amplification

- Change the view:

$$H^{\otimes n}|\mathbf{0}\rangle = \cos(\theta)\left|x_0^{\perp}\right\rangle + \sin\theta\,|x_0\rangle$$

$$\boldsymbol{G} = (2|\boldsymbol{\psi}_{\$}\rangle\langle\boldsymbol{\psi}_{\$}| - \boldsymbol{I})\boldsymbol{U}_{\boldsymbol{f}}$$

- We have: $\boldsymbol{G}\left(\cos(\theta)\left|x_0^{\perp}\right\rangle + \sin\theta\,|x_0\rangle\right) = (|\boldsymbol{\psi}_{\$}\rangle\langle\boldsymbol{\psi}_{\$}| - \boldsymbol{I})\boldsymbol{U}_{\boldsymbol{f}}\left(\cos(\theta)\left|x_0^{\perp}\right\rangle + \sin\theta\,|x_0\rangle\right)$

$$= \cos(3\theta)\left|x_0^{\perp}\right\rangle + \sin(3\theta)\,|x_0\rangle$$

Amplitude Amplification

- Change the view:

$$H^{\otimes n}|\mathbf{0}\rangle = \cos(\theta)\,|x_0^{\perp}\rangle + \sin\theta\,|x_0\rangle$$

$$\boldsymbol{G} = (2|\boldsymbol{\psi}_{\$}\rangle\langle\boldsymbol{\psi}_{\$}| - \boldsymbol{I})\boldsymbol{U}_{\boldsymbol{f}}$$

- More generally:

$$\boldsymbol{G}^{\boldsymbol{k}}\left(\cos(\theta)\,|x_0^{\perp}\rangle + \sin\theta\,|x_0\rangle\right) = \cos\left((1+2k)\theta\right)|x_0^{\perp}\rangle + \sin\left((1+2k)\theta\right)|x_0\rangle$$

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

Amplitude Amplification

- Change the view:

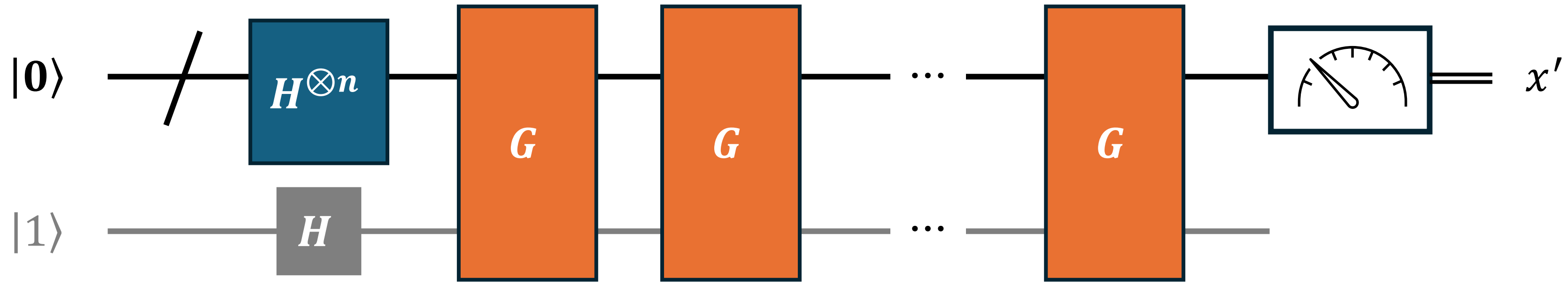
$$H^{\otimes n}|\mathbf{0}\rangle = \cos(\theta)\left|x_0^{\perp}\right\rangle + \sin\theta\,|x_0\rangle \qquad \boldsymbol{G = (2|\psi_{\$}\rangle\langle\psi_{\$}| - I)U_f}$$

- More generally:

$$G^k\left(\cos(\theta)\left|x_0^{\perp}\right\rangle + \sin\theta\,|x_0\rangle\right) = \cos\big((1+2k)\theta\big)\left|x_0^{\perp}\right\rangle + \sin\big((1+2k)\theta\big)\,|x_0\rangle$$

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

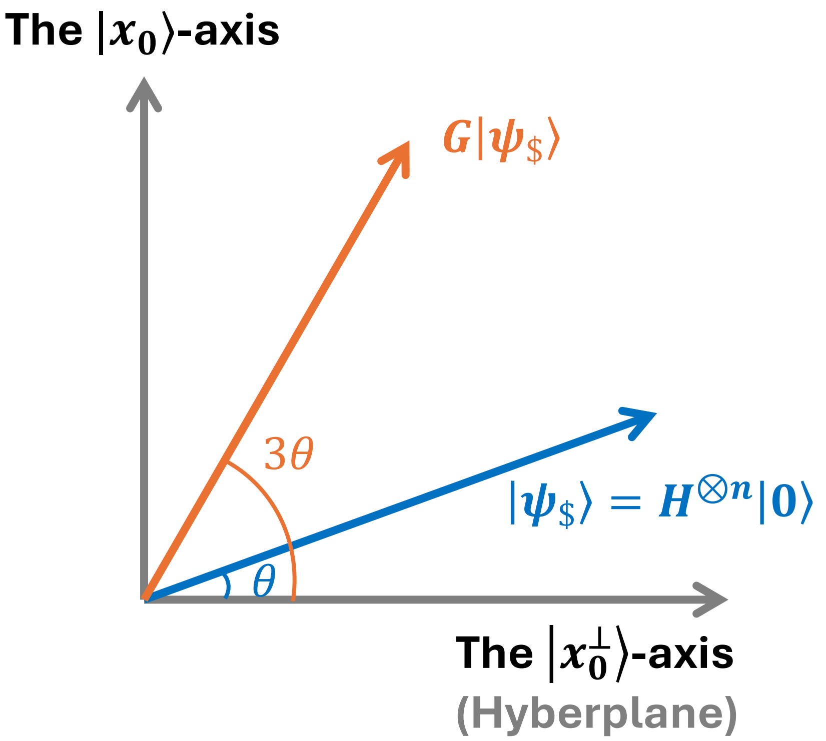
Grover Search Algorithm



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

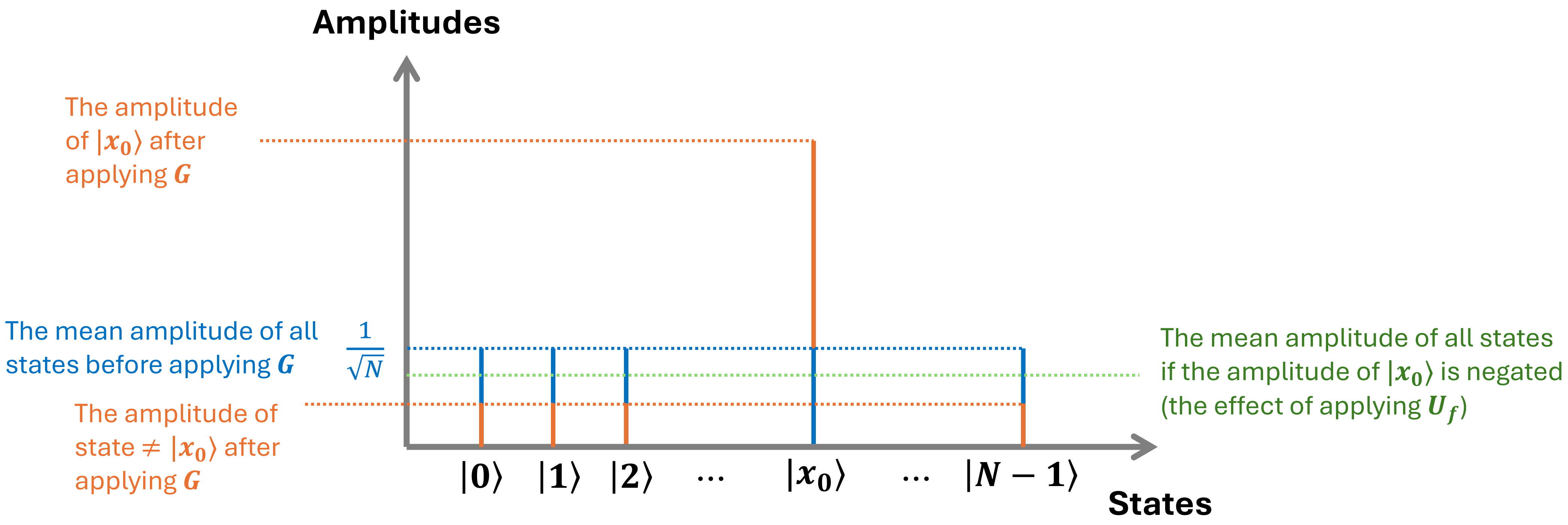
Grover Search Algorithm

- Two ways to understand the process of amplitude amplification:



Grover Search Algorithm

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



Reference

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