Grover's Search Algorithm

Raul Garcia-Patron Sanchez

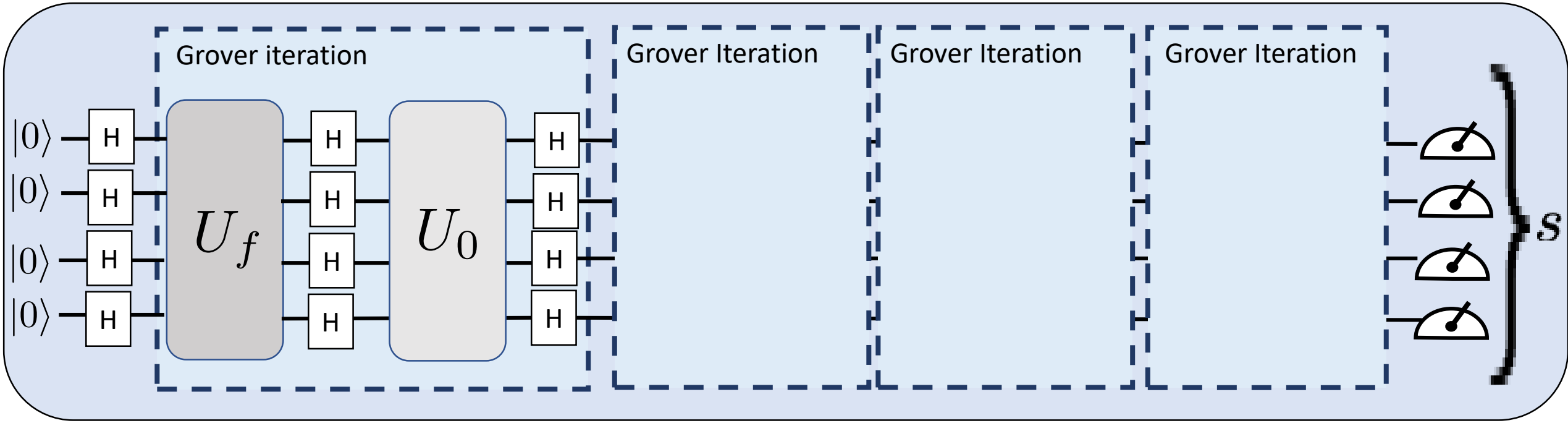
Search problems

Black-box access to a function: $f : \{0,1\}^n \to \{0,1\}$
Promise: $f(x) = 1$ if $x = s_i$, $f(x) = 0$ if $x \neq s_i$
Problem: find one s_i

- Examples:
  - Satisfiability problems: 3-SAT
  - Finding a cryptographic key by brute force
- Polynomial improvements only!
- Generalized to approximate counting of solutions

Unstructured Search

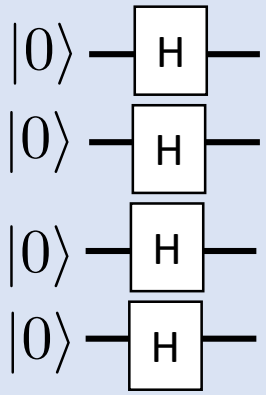
Black-box access to a function: $f : \{0,1\}^n \to \{0,1\}$
Promise: $f(x) = 1$ if $x = s$, $f(x) = 0$ if $x \neq s$
Problem: find s



- We need to implement $O(2^{n/2})$ Grover iterations
- Classically we need $O(2^n)$

Unstructured Search

Black-box access to a function: $f : \{0,1\}^n \to \{0,1\}$
Promise: $f(x) = 1$ if $x = s$, $f(x) = 0$ if $x \neq s$
Problem: find s

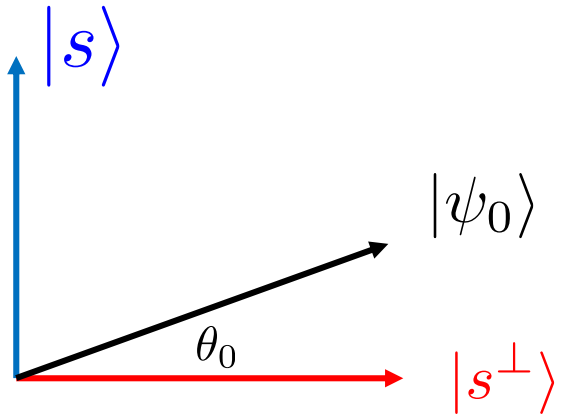


$$|0\rangle^n \xrightarrow{H^{\otimes n}} |\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle = \frac{1}{\sqrt{2^n}}|s\rangle + \sqrt{\frac{2^n-1}{2^n}} \left[\frac{1}{\sqrt{2^n-1}} \sum_{x\in\{0,1\}^n : x\neq s} |x\rangle\right]$$

$$= \frac{1}{\sqrt{2^n}}|s\rangle + \sqrt{1-\frac{1}{2^n}} \left[\frac{1}{\sqrt{2^n-1}} \sum_{x\in\{0,1\}^n : x\neq s} |x\rangle\right]$$

$$|\psi_0\rangle = \sin\theta_0 |s\rangle + \cos\theta_0 |s^\perp\rangle$$

$$\sin\theta_0 = \frac{1}{\sqrt{2^n}}$$



$|s^\perp\rangle \in$ subspace of unmarked elements

θ_0 angle between $|\psi_0\rangle$ and subspace of unmarked elements.

The intuition

$$|\psi_0\rangle = \sin\theta_0|s\rangle + \cos\theta_0|s^\perp\rangle \quad \Rightarrow \quad |s\rangle$$

$$\sin\theta_0 = \frac{1}{\sqrt{2^n}}$$

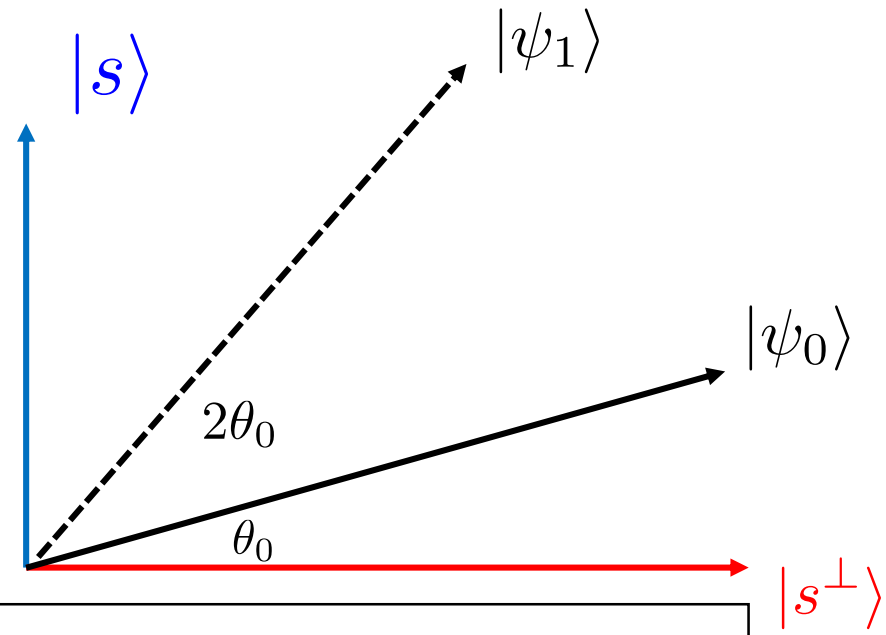
$$|s^\perp\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x\in\{0,1\}^n : x\neq s} |x\rangle$$

$$G|\psi_0\rangle = \sin(3\theta)|s\rangle + \cos(3\theta)|s^\perp\rangle$$

$$\theta_1 = (2+1)\theta_0 = 3\theta_0$$

$$G^t|\psi_0\rangle = \sin\theta_t|s\rangle + \cos\theta_t|s^\perp\rangle$$

$$\theta_t = (2t+1)\theta_0$$

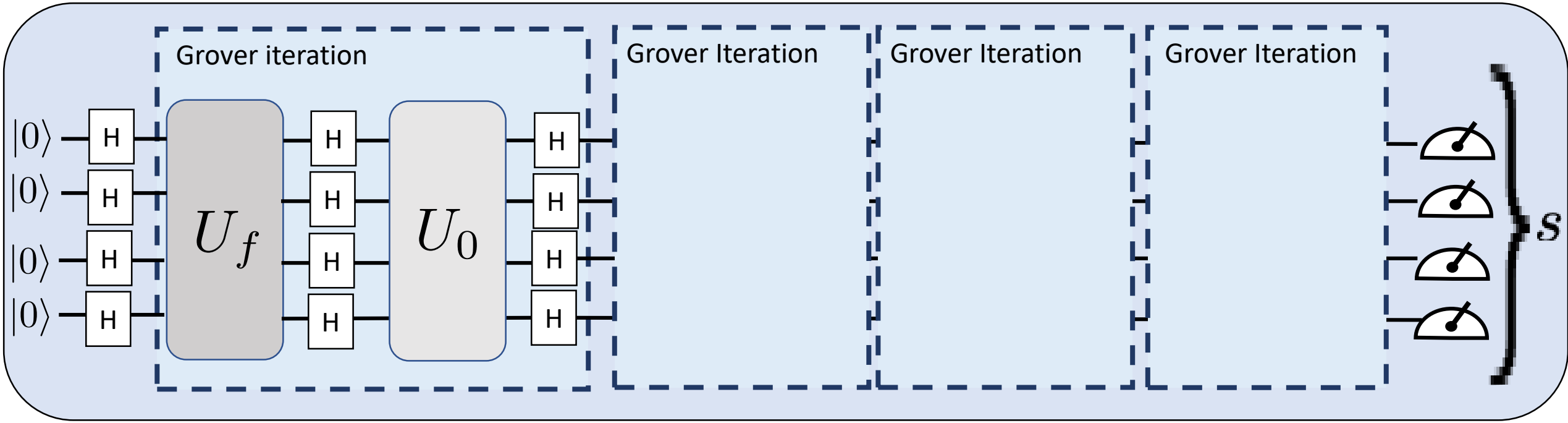


$$\theta_T \approx \frac{\pi}{2} \quad \Rightarrow \quad T \approx \frac{\pi}{4\theta_0} \approx \frac{\pi}{4}\frac{1}{\sin\theta_0} \approx \frac{\pi}{4}\sqrt{2^n}$$

$$T >> 1 : \theta_T \approx 2T\theta_0$$

Unstructured Search

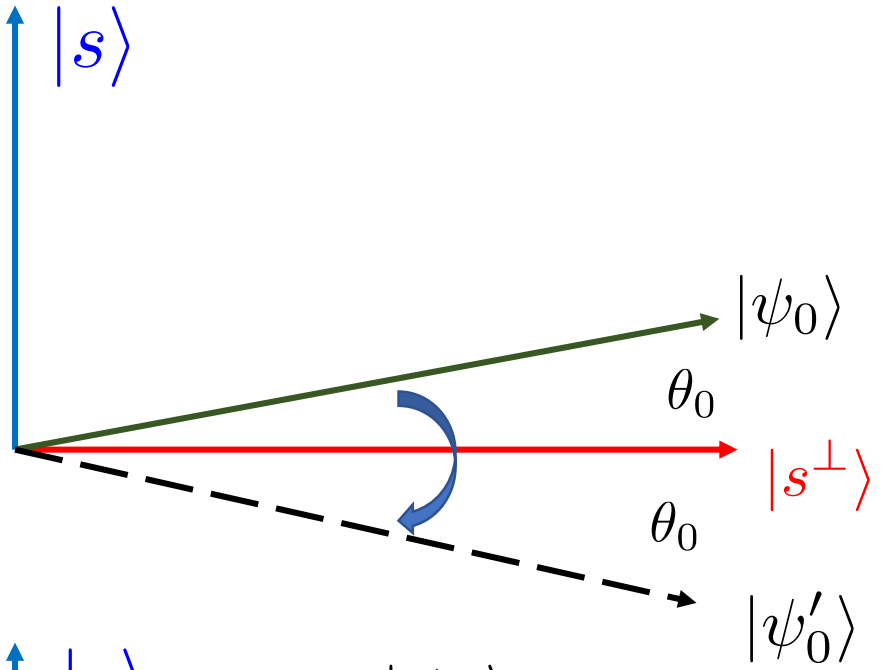
Black-box access to a function: $f : \{0,1\}^n \to \{0,1\}$
Promise: $f(x) = 1$ if $x = s$, $f(x) = 0$ if $x \neq s$
Problem: find s



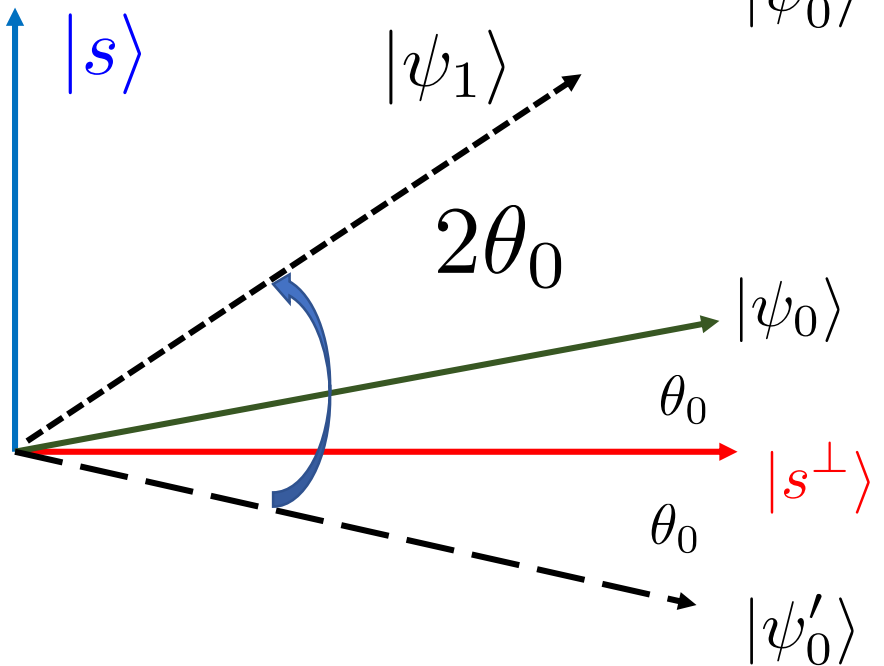
- We need to implement $O(2^{n/2})$ Grover iterations
- Classically we need $O(2^n)$

The first Grover Iteration: Geometric picture

- First step: a reflection over $|s^{\perp}\rangle$

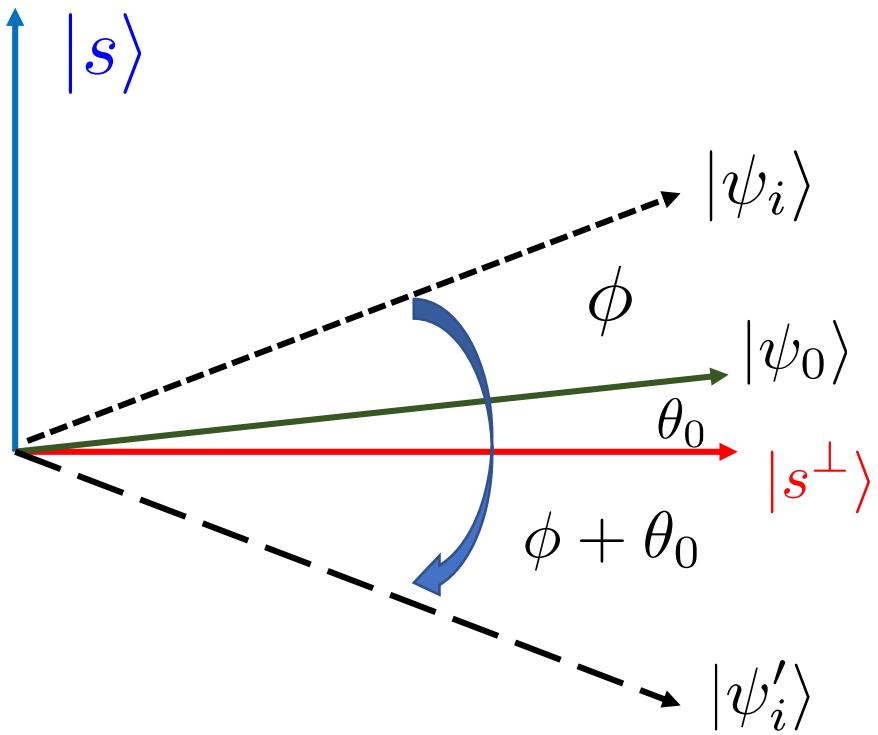


- Second step: a reflection over $|\psi_0\rangle$



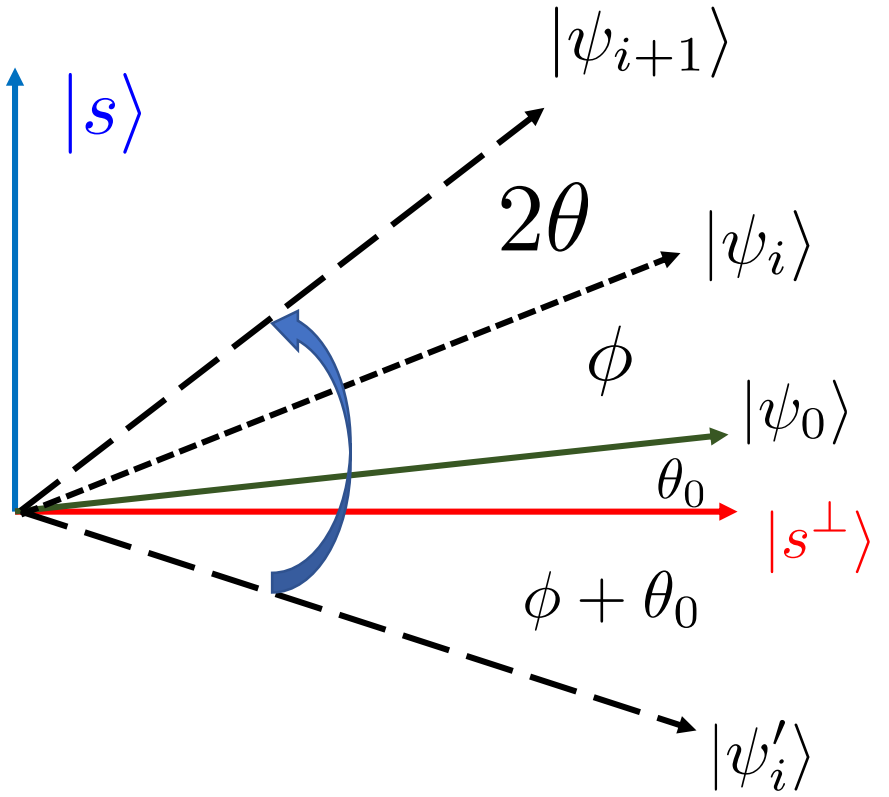
A general Grover Iteration: Geometric picture I

- First step: a reflection over $|s^{\perp}\rangle$



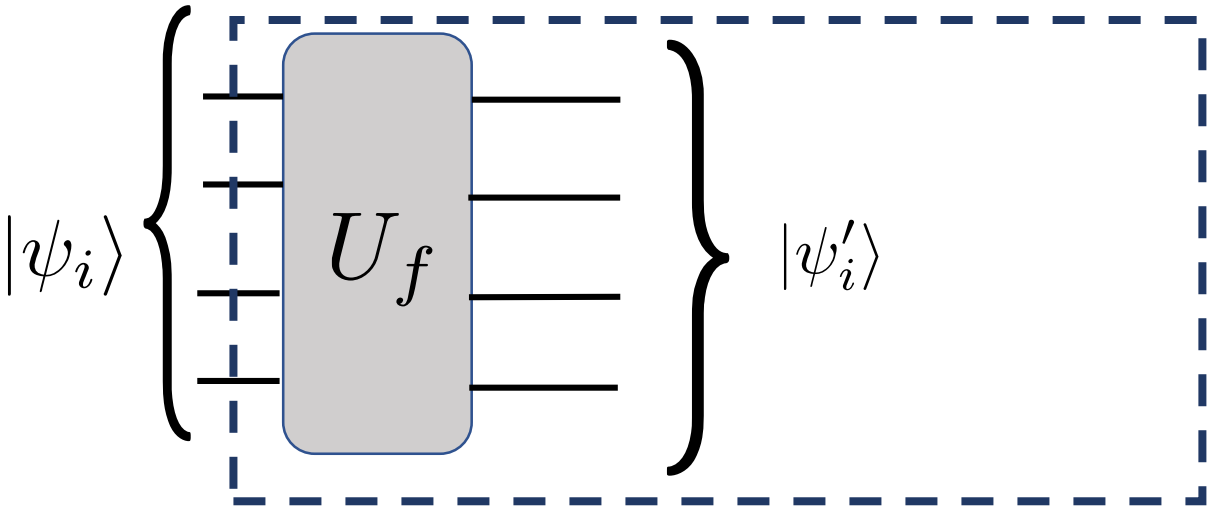
A general Grover Iteration: Geometric picture II

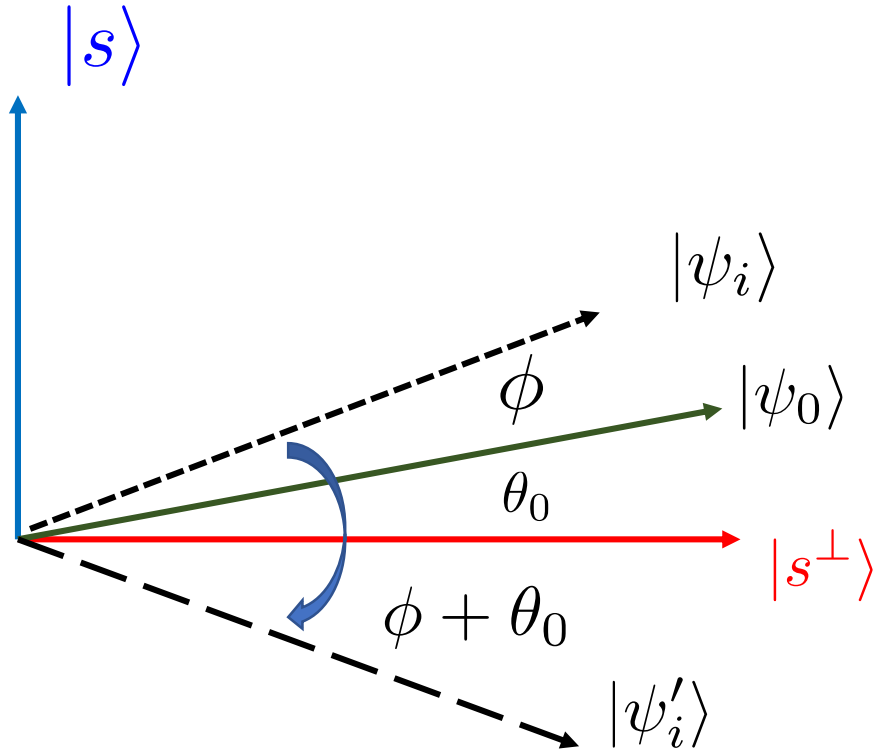
- Second step: a reflection over $|\psi_0\rangle$



The Grover Iteration: 1st Reflection via Phase Kickback

- Promise: $f(x) = 1$ if $x = s$, $f(x) = 0$ if $x \neq s$





Phase Kickback

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

$f(x) = 1$ if $x = s, 0$ otherwise: U_f $U_f(a|s\rangle + b|s^\perp\rangle) = -a|s\rangle + b|s^\perp\rangle$

- U_f implements a reflection over $|s^\perp\rangle$

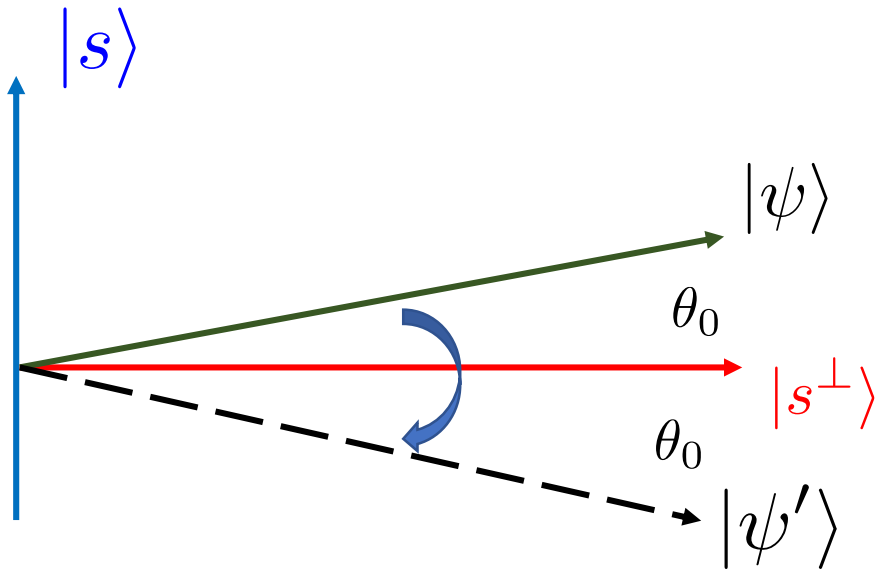
The Grover Iteration: 1st Reflection via Phase Kickback

Phase Kickback

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

$f(x) = 1$ if $x = s, 0$ otherwise:

$$U_f(a|s\rangle + b|s^\perp\rangle) = -a|s\rangle + b|s^\perp\rangle \qquad U_f$$



$$U_f = I - 2|s\rangle\langle s|$$

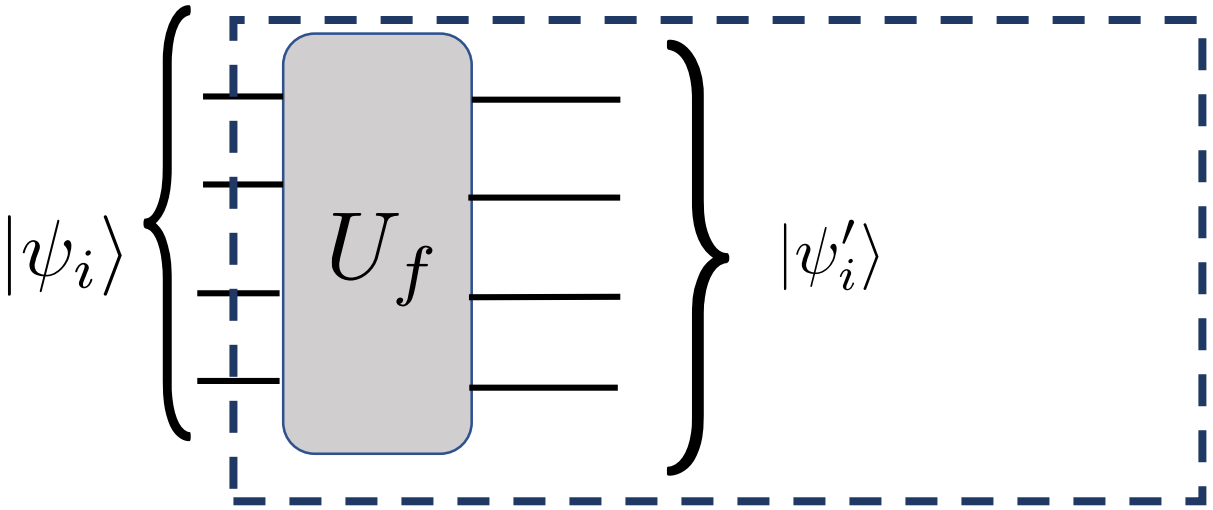
$$(|s\rangle\langle s|)|\psi\rangle = |s\rangle \underbrace{\langle s|\psi\rangle}_{\in\mathbb{C}} = \langle s|\psi\rangle|s\rangle = a|s\rangle$$

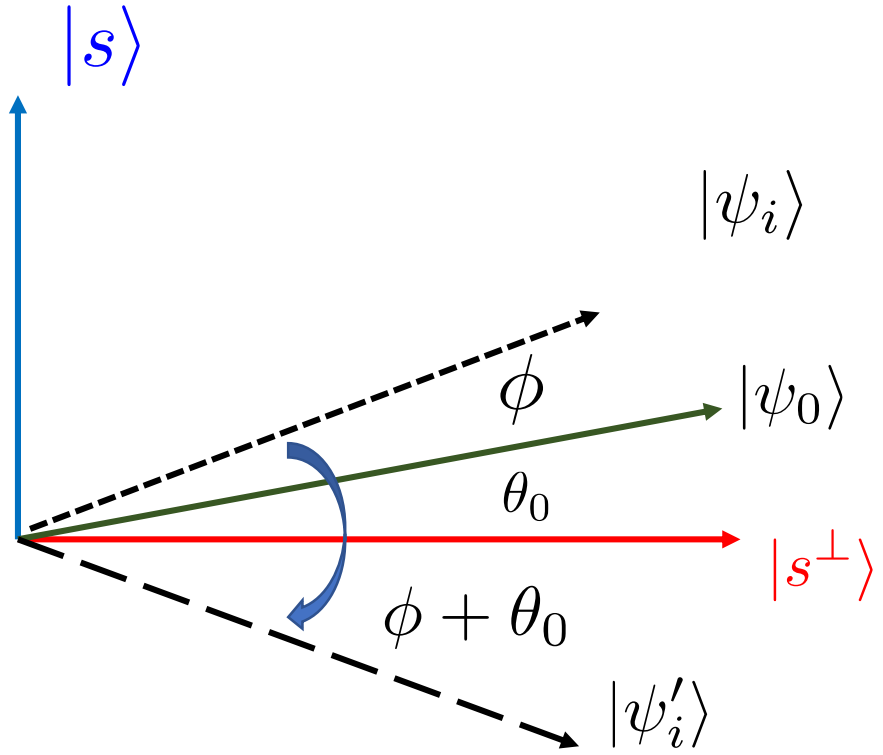
$$I|\psi\rangle = a|s\rangle + b|s^\perp\rangle$$

$$U_f = \sum_{x\in\{0,1\}^n} |x\rangle\langle x| - 2|s\rangle\langle s| = \sum_{x\in\{0,1\}^n \neq s} |x\rangle\langle x| - |s\rangle\langle s| \quad \text{Reflection over } |s^\perp\rangle$$

The Grover Iteration: 1st Reflection via Phase Kickback

- Promise: $f(x) = 1$ if $x = s$, $f(x) = 0$ if $x \neq s$





Phase Kickback

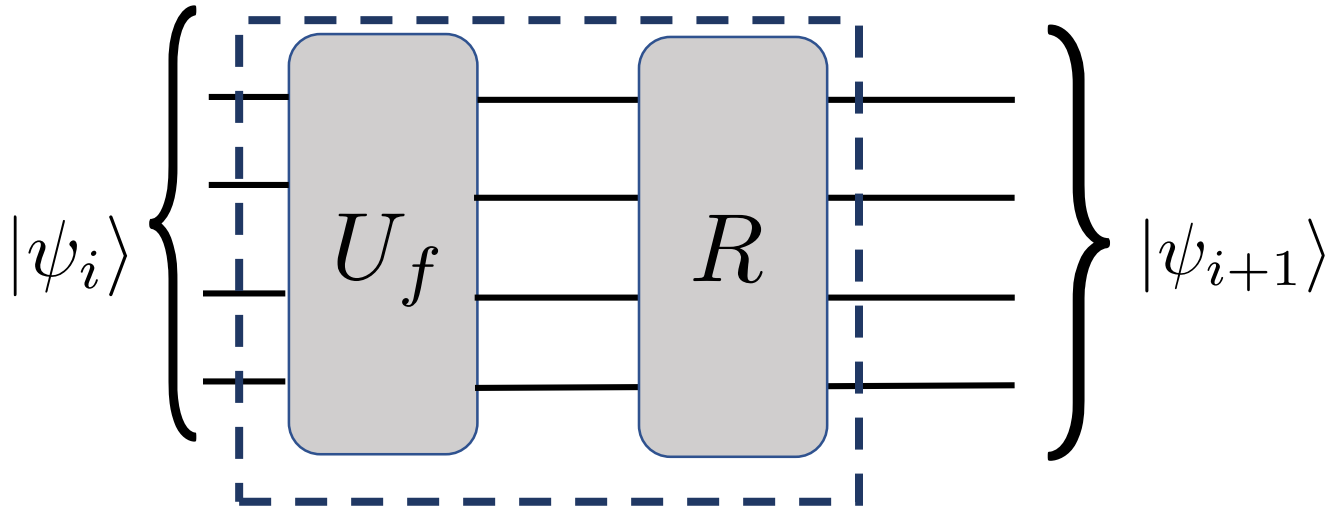
$U_f : |x\rangle \rightarrow (-1)^{f(x)}|x\rangle$ U_f

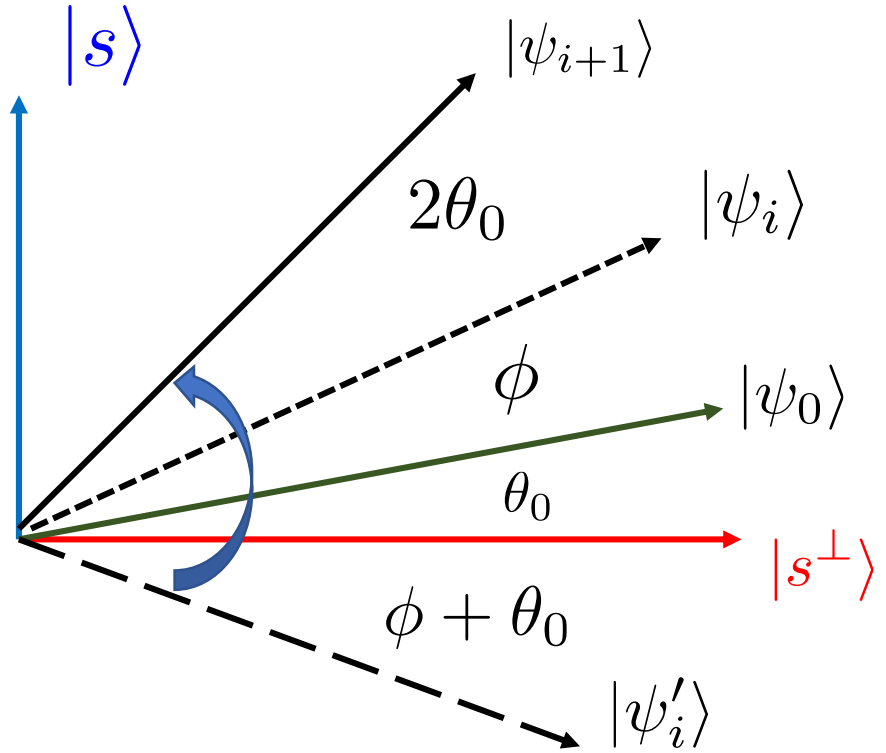
$f(x) = 1$ if $x = s, 0$ otherwise:

$U_f = I - 2|s\rangle\langle s|$ U_f $U_f(a|s\rangle + b|s^\perp\rangle) = -a|s\rangle + b|s^\perp\rangle$

- U_f implements a reflection over $|s^\perp\rangle$

The Grover Iteration: 2nd Reflection





$f(x) = 1$ if $x = s, 0$ otherwise:

$$U_f = I - 2|s\rangle\langle s|$$

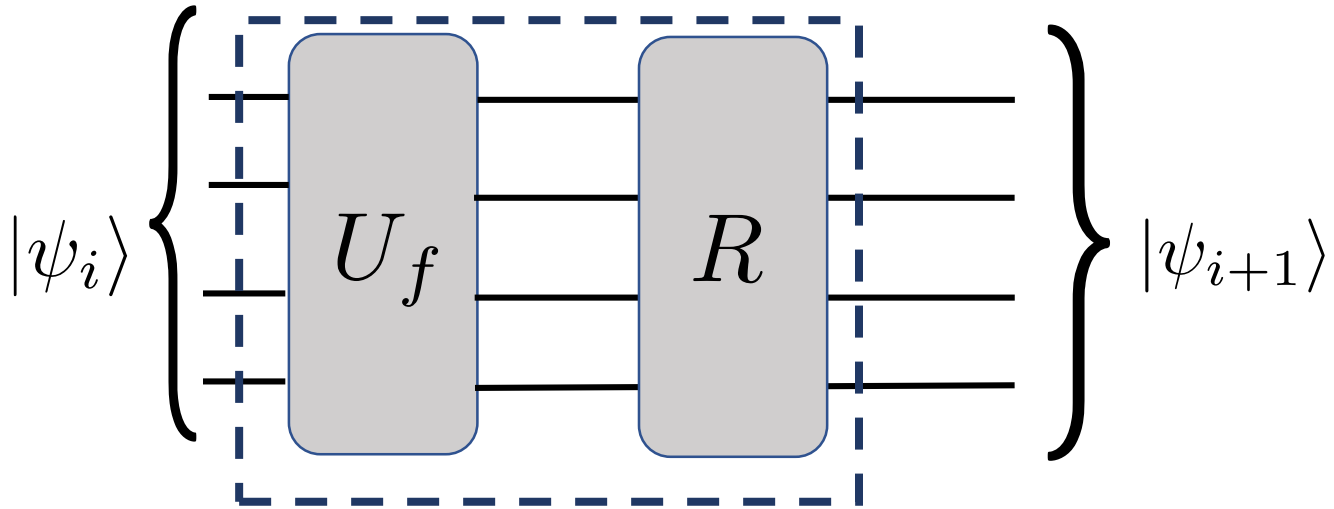
U_f

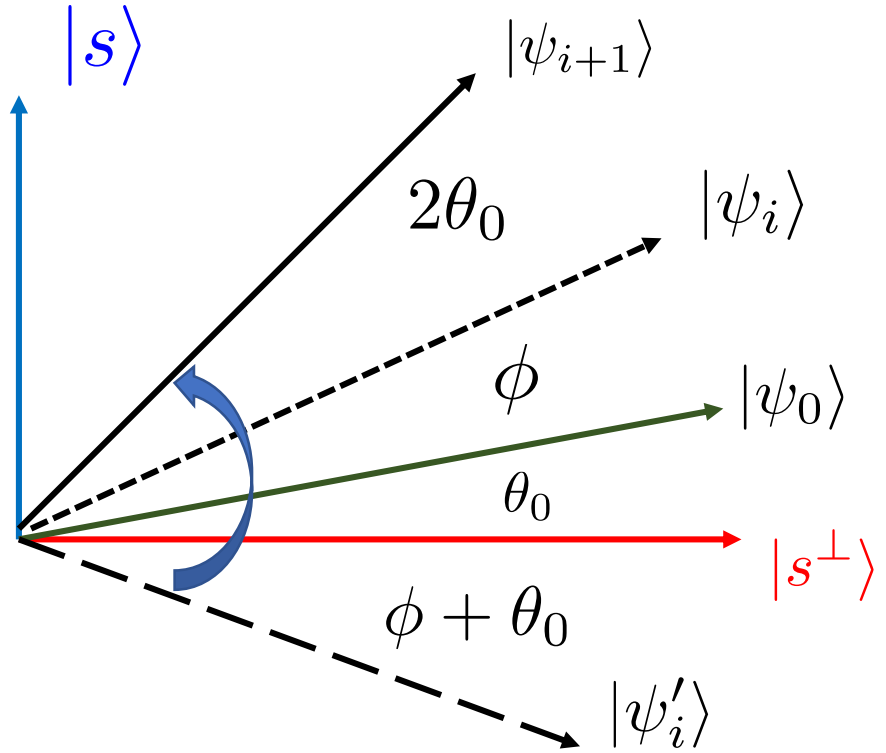
$$U_f(a|s\rangle + b|s^\perp\rangle) = -a|s\rangle + b|s^\perp\rangle$$

R

$$R(a|\psi_0\rangle + b|\psi_0^\perp\rangle) = a|\psi_0\rangle - b|\psi_0^\perp\rangle$$

The Grover Iteration: 2nd Reflection





$f(x) = 1$ if $x = s, 0$ otherwise:

$$U_f = I - 2|s\rangle\langle s|$$

U_f

$$U_f(a|s\rangle + b|s^\perp\rangle) = -a|s\rangle + b|s^\perp\rangle$$

$$R = 2|\psi_0\rangle\langle\psi_0| - I$$

R

$$R(a|\psi_0\rangle + b|\psi_0^\perp\rangle) = a|\psi_0\rangle - b|\psi_0^\perp\rangle$$

The 2nd Reflection

$$R = 2|\psi_0\rangle\langle\psi_0| - I$$

R

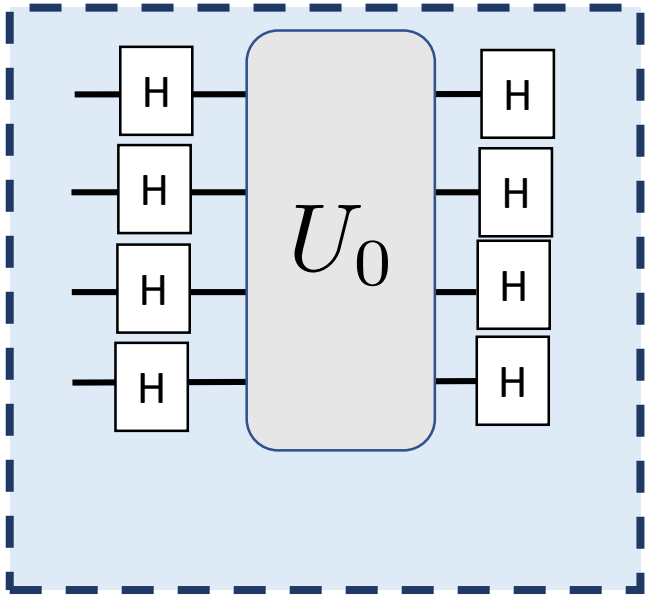
$$R(a|\psi_0\rangle + b|\psi_0^{\perp}\rangle) = a|\psi_0\rangle - b|\psi_0^{\perp}\rangle$$

U_0

$f(x) = 0$ if $x = 0^n$, 1 otherwise:

$$U_{f_0} = 2|0^n\rangle\langle 0^n| - I$$

$$H^{\otimes n} U_0 H^{\otimes n} = H^{\otimes n}(2|0^n\rangle\langle 0^n| - I)H^{\otimes n} = 2|\psi_0\rangle\langle\psi_0| - I$$



Both U_0 and U_f are phase-kickbacks but:

- We do not know f(x) so we need to call the oracle O_f
- U_0 is associate to an easy function, we can implement the circuit ourselves.

The 2nd Reflection

$$R = 2|\psi_0\rangle\langle\psi_0| - I$$

R

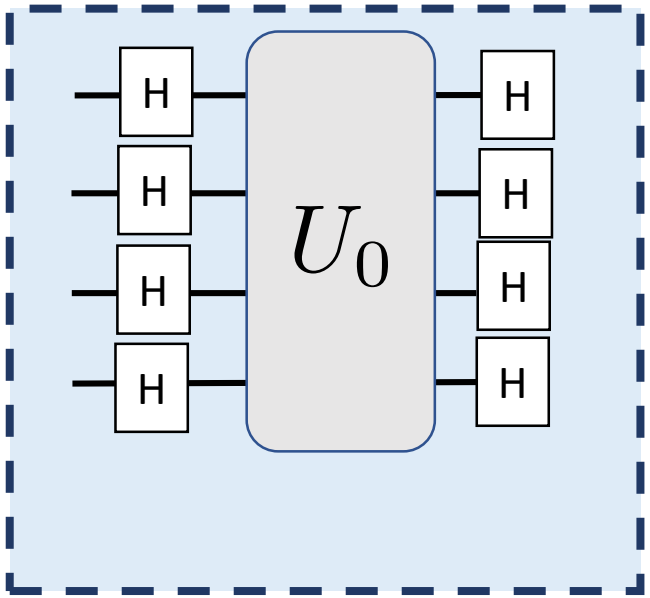
$$R(a|\psi_0\rangle + b|\psi_0^{\perp}\rangle) = a|\psi_0\rangle - b|\psi_0^{\perp}\rangle$$

U_0

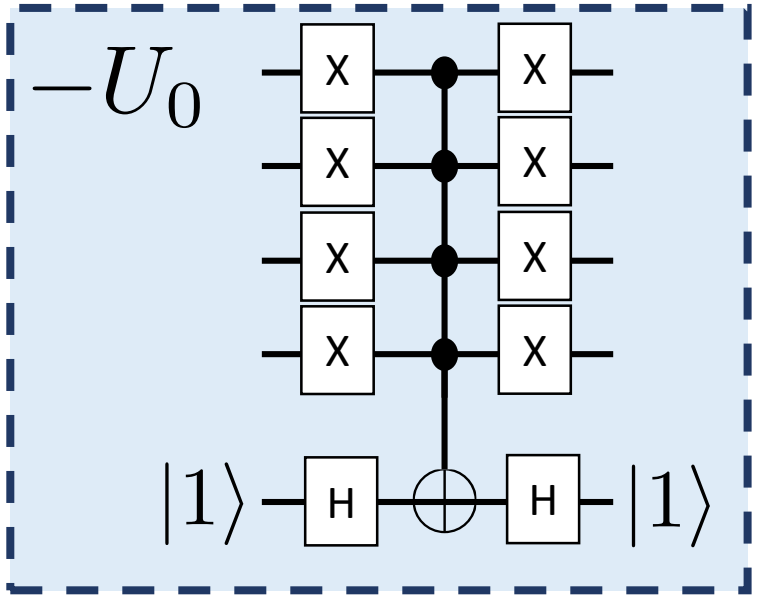
$f(x) = 0$ if $x = 0, 1$ otherwise:

$$U_{f_0} = 2|0^n\rangle\langle 0^n| - I$$

$$H^{\otimes n} U_0 H^{\otimes n} = 2|\psi_0\rangle\langle\psi_0| - I$$

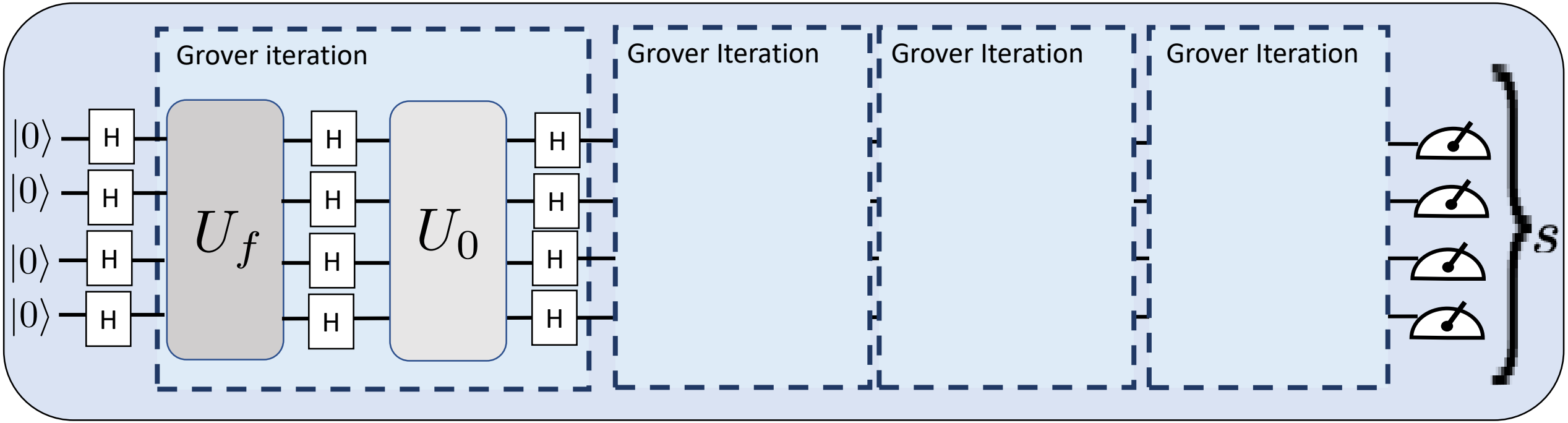


U_0 can be obtained from the Following circuit, up to a global phase -1.



Unstructured Search

Black-box access to a function: $f : \{0,1\}^n \to \{0,1\}$
Promise: $f(x) = 1$ if $x = s$, $f(x) = 0$ if $x \neq s$
Problem: find s



$$\theta_T \approx \frac{\pi}{2} \quad \Rightarrow \quad T \approx \frac{\pi}{4\theta_0} \approx \frac{\pi}{4}\frac{1}{\sin\theta_0} \approx \frac{\pi}{4}\sqrt{2^n}$$

- From $O(2^n)$ to $O(2^{n/2})$

General Reflection

$$R = 2|\psi\rangle\langle\psi| - I$$

R_ψ

$$R(a|\psi_0\rangle + b|\psi_0^\perp\rangle) = a|\psi_0\rangle - b|\psi_0^\perp\rangle$$

U_0

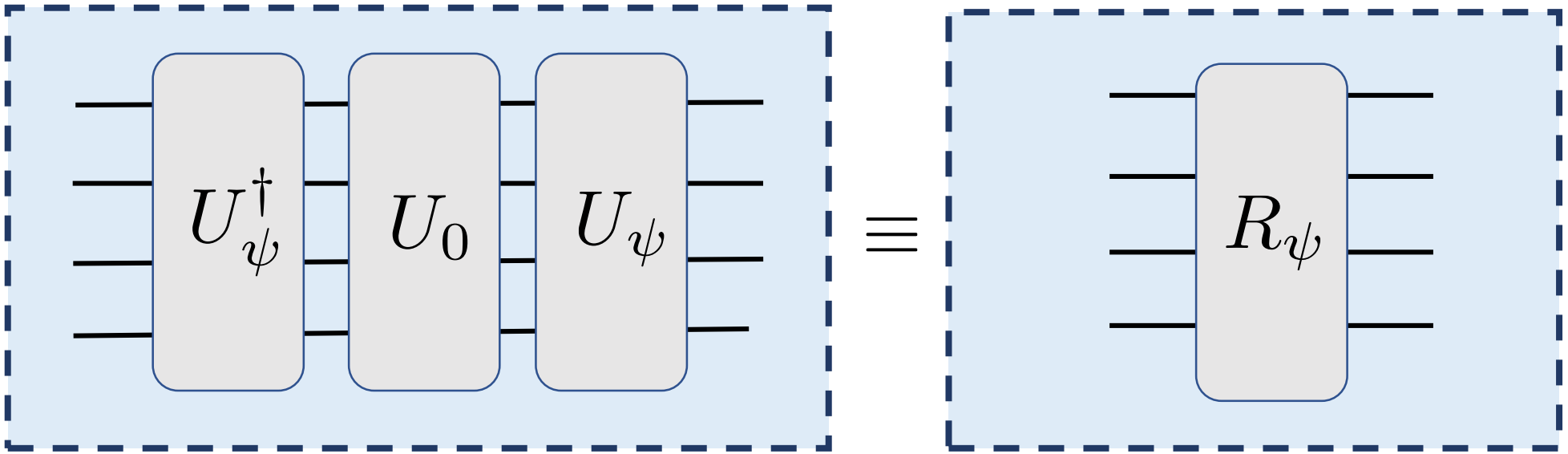
$f(x) = 0$ if $x = 0^n, 1$ otherwise:

$$U_{f_0} = 2|0^n\rangle\langle 0^n| - I$$

U_ψ

Choose U_ψ s.t.: $U_\psi|0^n\rangle = |\psi\rangle$

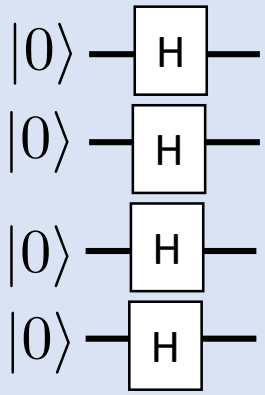
If you can do U_ψ you can also do $U_\psi^\dagger$



$$U_\psi U_0 U_\psi^\dagger = U_\psi(2|0^n\rangle\langle 0^n| - I)U_\psi^\dagger = 2|\psi\rangle\langle\psi| - U_\psi U_\psi^\dagger = 2|\psi\rangle\langle\psi| - I$$

Multiple marked elements

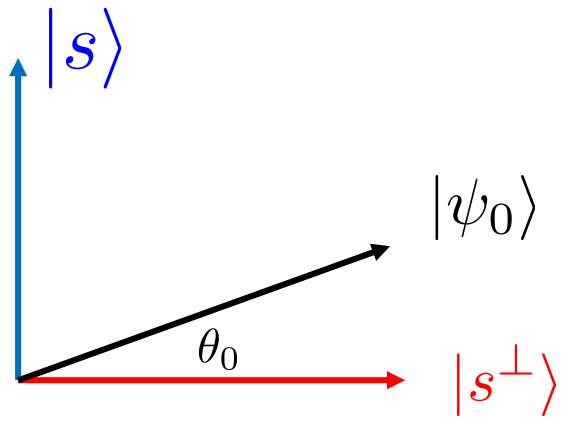
Black-box access to a function: $f : \{0,1\}^n \to \{0,1\}$
Promise: $f(x) = 1$ if $x = s$, $f(x) = 0$ if $x \neq s$
Problem: find s belonging to set S of size D.



$$|0\rangle^n \xrightarrow{H^{\otimes n}} |\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle = \sqrt{\frac{D}{2^n}} \left[\frac{1}{\sqrt{D}} \sum_{x\in S} |s\rangle\right] + \sqrt{\frac{2^n - D}{2^n}} \left[\frac{1}{\sqrt{2^n - D}} \sum_{x\in\{0,1\}^n : x\notin S} |x\rangle\right]$$

$$|\psi_0\rangle = \sin\tilde{\theta}_0 |s\rangle + \cos\tilde{\theta}_0 |s^\perp\rangle$$

$$\sin\tilde{\theta}_0 = \sqrt{\frac{D}{2^n}}$$



$$T \approx \frac{\pi}{4\tilde{\theta}_0} \approx \frac{\pi}{4} \frac{1}{\sin\tilde{\theta}_0} \approx \frac{\pi}{4} \frac{2^{n/2}}{\sqrt{D}}$$

References

Reading references

1. Bernstein-Vazirani NC 1.4.3 RdW 2.4.2 and G 7.5
2. Grover: NC 6.1 RdW 7.1-7.2 and G 11.1-11.2

NC ≣ Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information Cambridge University Press (2010)
RdW ≣ Quantum Computing Lecture Notes, Ronald de Wolf, https://arxiv.org/abs/1907.09415
G ≣ Introduction to Quantum Computation, Sevag Gharibian, Lectures notes