THE UNIVERSITY of EDINBURGH
informatics

Quantum Algorithms

Lecture 4: Grover’s Search Algorithm

Raul Garcia-Patron Sanchez

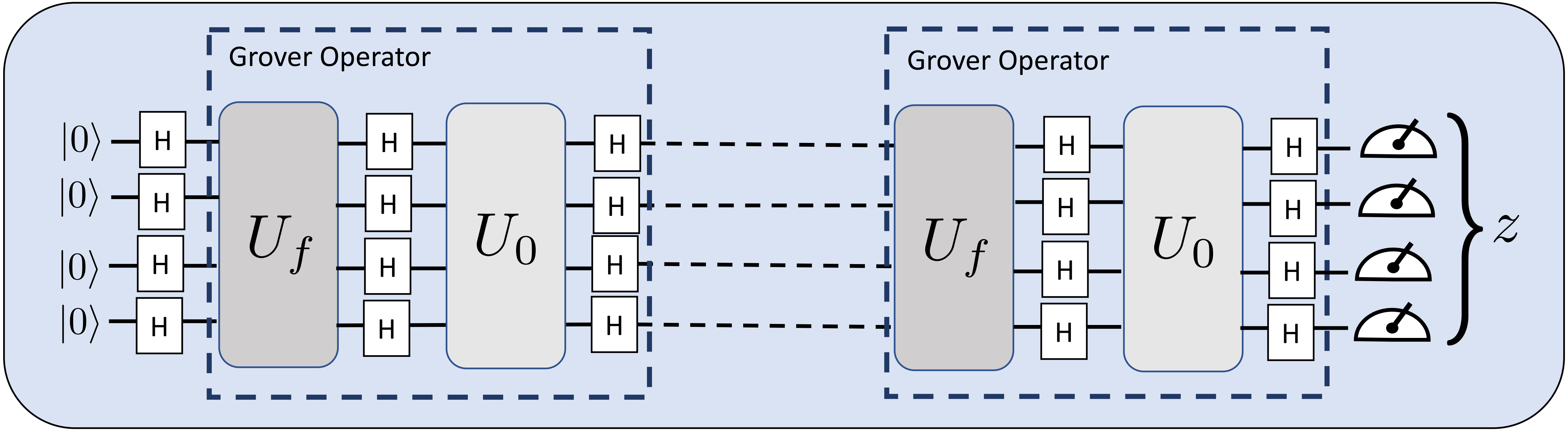
Search problems

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 s

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

Unstructured Search

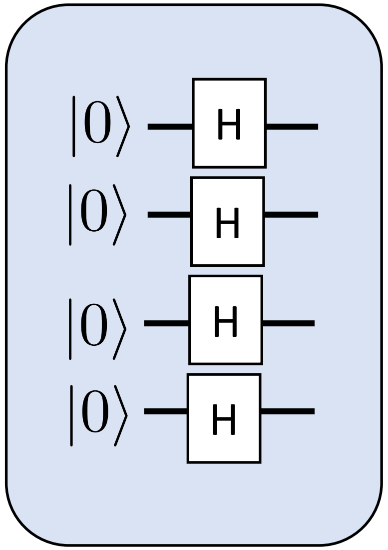
Black-box access to a function: $f : \{0,1\}^n \to \{0,1\}$
Promise: $f(x) = 1$ if $x = s$, $f(x) = 0$ if $x \neq s$
Problem: find s



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

Unstructured Search

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

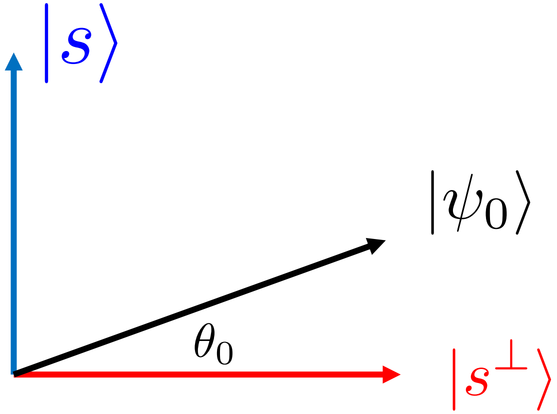


$$|0\rangle^n \xrightarrow{H^{\otimes n}} |\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle = \frac{1}{\sqrt{2^n}}|s\rangle + \sqrt{\frac{2^n - 1}{2^n}} \left[\frac{1}{\sqrt{2^n - 1}} \sum_{x \in \{0,1\}^n : x \neq s} |x\rangle \right]$$

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

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

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



The intuition

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

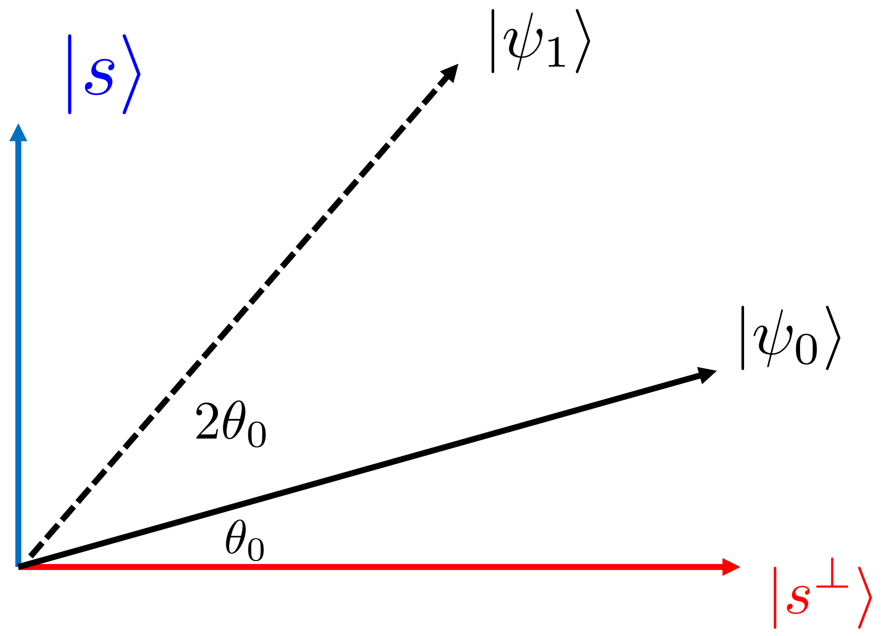
$$|\psi_0\rangle = \sin\theta_0 |s\rangle + \cos\theta_0 |s^\perp\rangle \Rightarrow |s\rangle$$

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

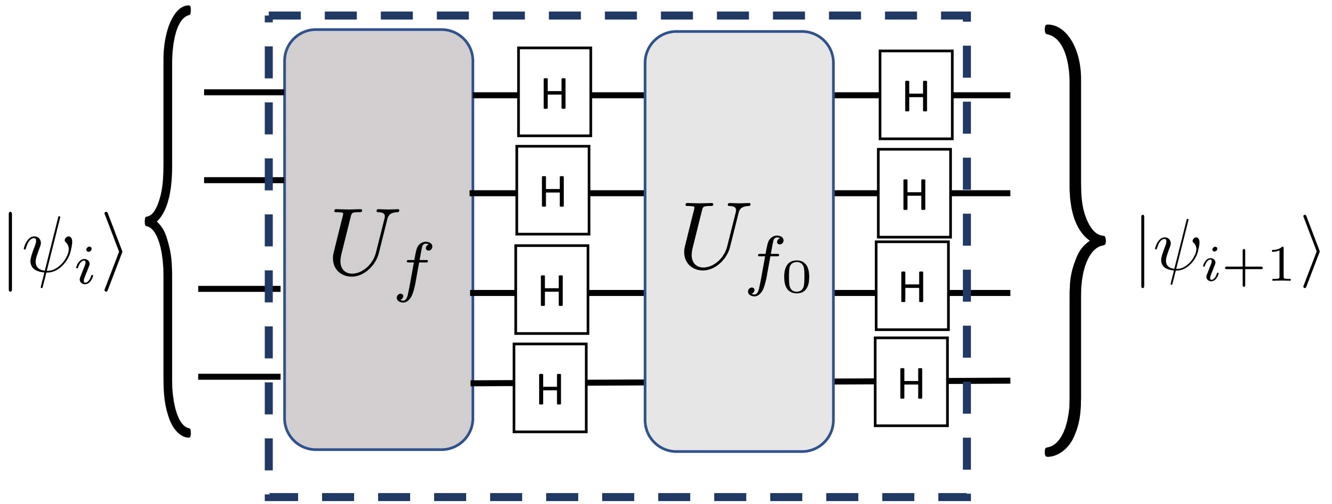
$$G^T|\psi_0\rangle = \sin\theta_T |s\rangle + \cos\theta_T |s^\perp\rangle$$

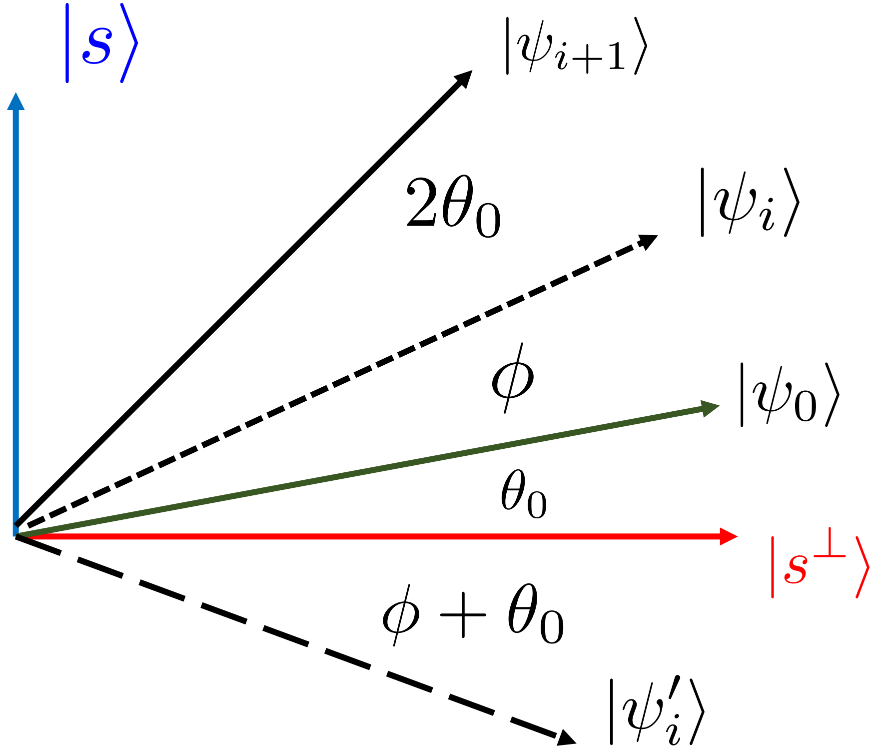
$$\theta_T = (2T+1)\theta_0$$

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



The Grover Iteration





Phase Kickback

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

U_f

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

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

U_f

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

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

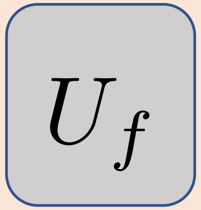
R

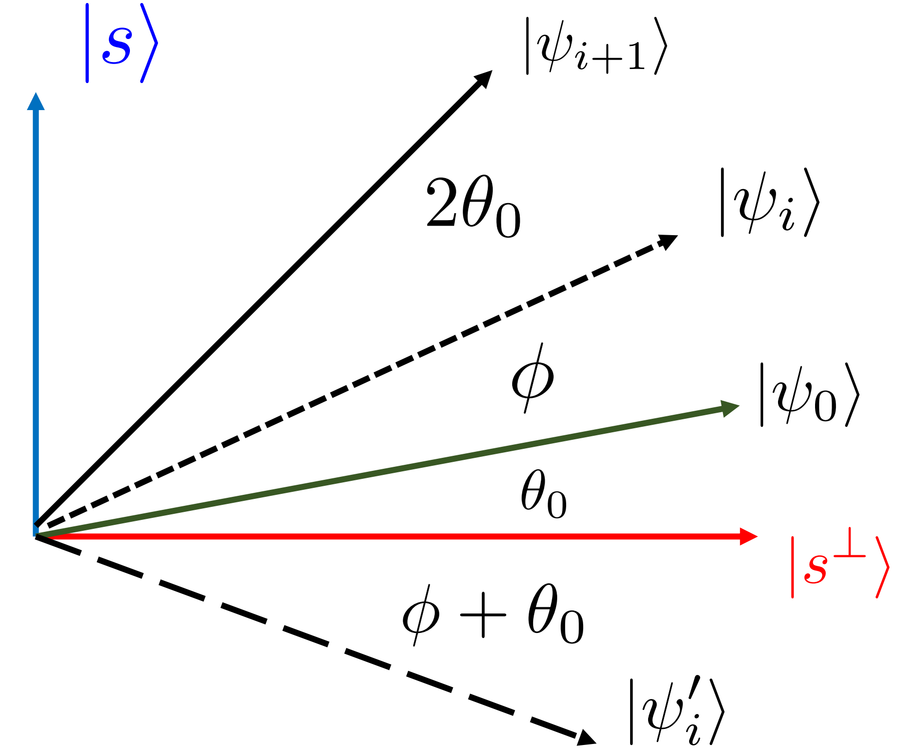
$$R(a|\psi_0\rangle + b|\psi_0^\perp\rangle) = a|\psi_0\rangle - b|\psi_0^\perp\rangle$$

The Grover Iteration

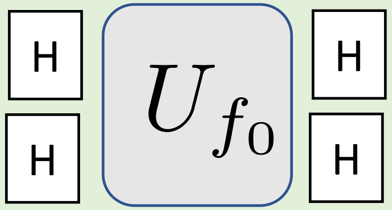
Phase Kickback

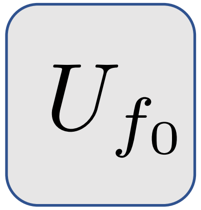
$$U_f : |x\rangle \to (-1)^{f(x)}|x\rangle$$





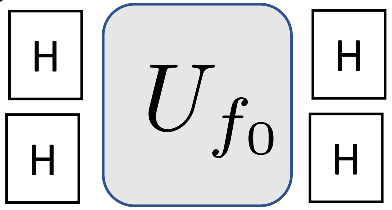
$$R = 2|\psi_0\rangle\langle\psi_0| - I$$





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

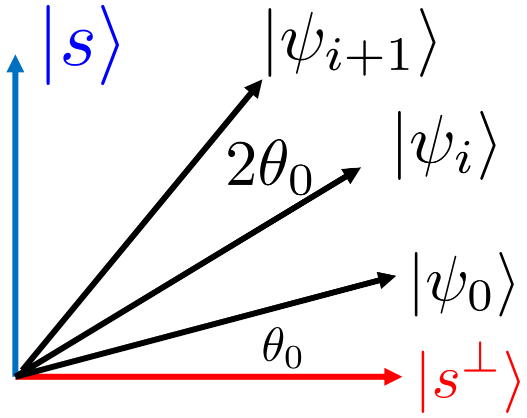
$$U_{f_0} = 2|0\rangle\langle 0| - I$$

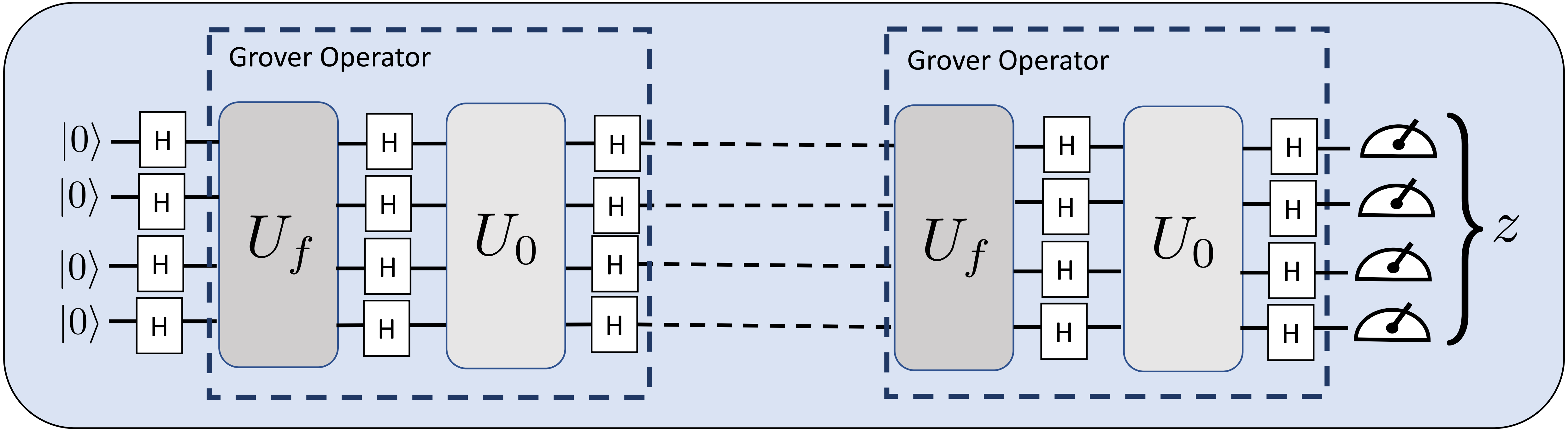


$$H^{\otimes n} U_{f_0} H^{\otimes n} = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi_0\rangle\langle\psi_0| - I$$

Summary

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





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

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

References

1. Lov K. Grover, *A fast quantum mechanical algorithm for database search,* Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), pages 212-219 (1996).
2. Michael Nielsen and Isaac Chuang, Quantum Computing and Quantum Information Cambridge University Press (2010) [Chapter 6: section 6.1]
3. Ronal de Wolf, *Quantum Computing: Lecture Notes*, arXiv:1907.09415v1 (2019) [Chapter 7].
4. Sevag Gharibian, *Introduction to Quantum Computation* [Chapter 11] Website link