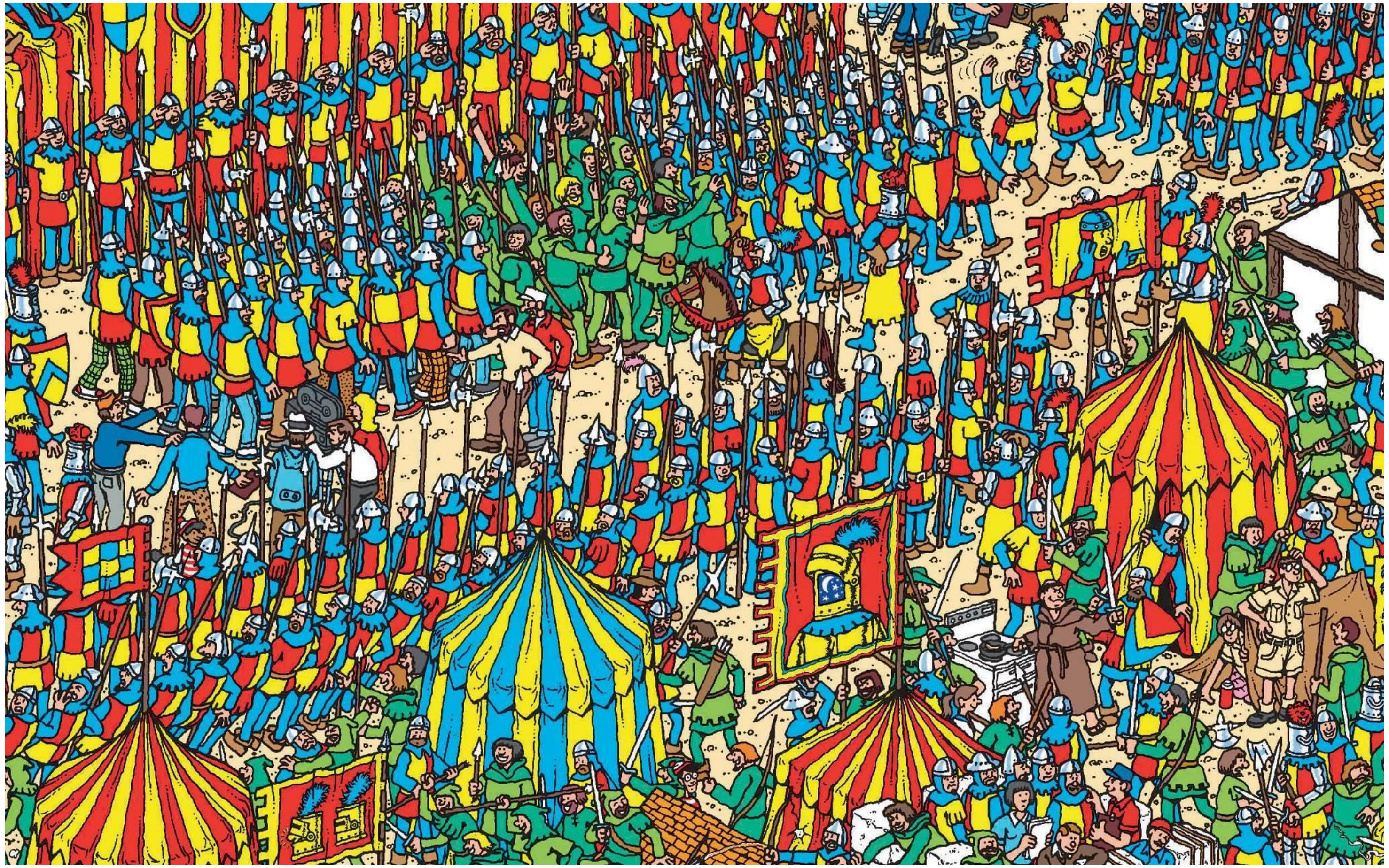


Quantum Computing: Grover's Algorithm

Luís Paulo Santos

Universidade do Minho

INESCTEC

April, 2019

Problem Statement: function inversion

- Let $f: \{0,1,..,2^n - 1\} \rightarrow \{0,1\}$, with $f(x) = \begin{cases} 0 \; if \; x \neq x^* \\ 1 \; if \; x = x^* \end{cases}$

- Grover's algorithm returns, with high probability, x^*: $f(x^*) = 1$

- On its simplest form requires that there is a single solution x^*

Problem Statement Example: Search

- Let *v* be a vector (array) with 2^n elements
- Grover's algortihm can be thought as searching for the index, x^*, of some unique key, y, within this vector:

$$f(x, y) = \begin{cases} 0 \; if \; v[x] \neq y \\ 1 \; if \; v[x] = y \end{cases}$$

Classical Problem Complexity

Given that:

- Nothing is known about $f(x)$ -- black box analogy

- The value of $f(x)$ for each x can only be known by evaluating $f(x)$

then a classical solution for finding $x^*: f(x^*) = 1$ requires, in the worst case, exhaustive search, i.e., evaluating all $N = 2^n$ values of x ;

- its complexity is $\mathcal{O}(N)$

Quantum Problem Definition: Oracle

- $f(x)$ becomes the operator $\hat{O}$, which is applied to an **uniform superposition** of all $N = 2^n$ states $|s\rangle = \hat{H}\,|0\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$

- The "Oracle", $\hat{O}$, negates state $|x^*\rangle$ sign:

$$\hat{O}\,|s\rangle = \frac{1}{\sqrt{N}}\sum_{x=0,x\neq x^*}^{N-1}|x\rangle - \frac{1}{\sqrt{N}}\,|x^*\rangle$$

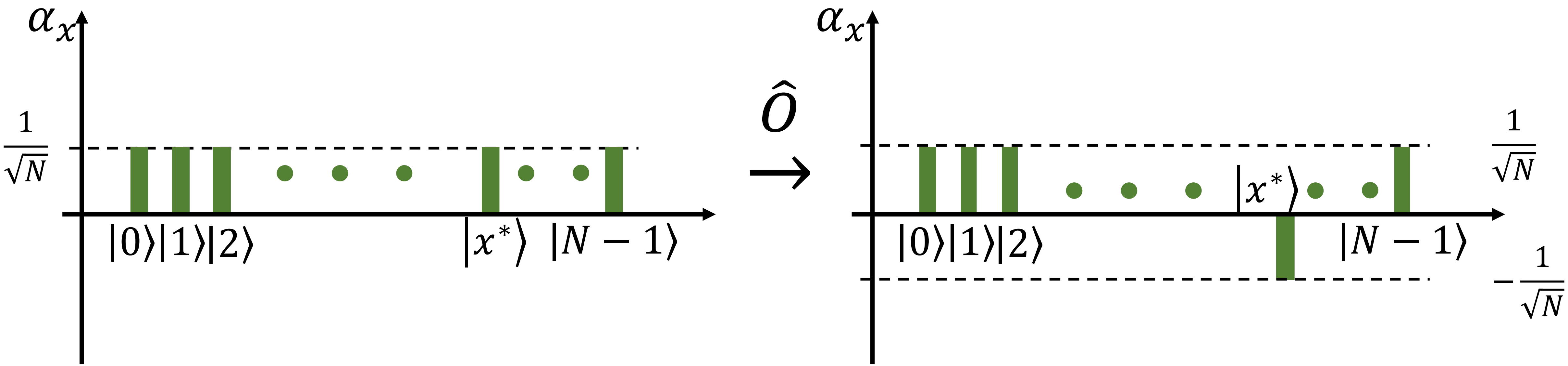
- $\hat{O}$ is often denoted as the reflection operator $\hat{S}_f$, conditionally changing the signal of the good state:

$$\hat{S}_f\,|x\rangle = \begin{cases} |x\rangle & \text{if } f(|x\rangle) = 0 \\ -|x\rangle & \text{if } f(|x\rangle) = 1 \end{cases}$$

Oracle Graphical Interpretation

- The oracle negates the sign of the desired state $|x^*\rangle$:

$$\hat{O}\ |s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0, x\neq x^*}^{N-1} |x\rangle - \frac{1}{\sqrt{N}} |x^*\rangle$$



The probability of measuring each state doesn't change: $P(x) = |\alpha_x|^2$

Grover's Diffusion Operator

- Grover's diffusion operator, $\widehat{D}$, amplifies the magnitude of $\left|x^*\right\rangle$
- It reflects the coefficients over their mean:

$$\sum_{x=0}^{N-1} \alpha_x |x\rangle \overset{\widehat{D}}{\rightarrow} \sum_{x=0}^{N-1} (2\mu - \alpha_x)|x\rangle, \text{ with } \mu = \frac{1}{N}\sum_{x=0}^{N-1} \alpha_x$$

- After the oracle $\hat{O}$ the mean is

$$\mu = \frac{1}{N}\left(\frac{N-1}{\sqrt{N}} - \frac{1}{\sqrt{N}}\right) = \frac{N-2}{N\sqrt{N}} = \frac{1}{\sqrt{N}} - \epsilon, \qquad \epsilon = \frac{2}{N\sqrt{N}} \approx 0$$

Grover's Diffusion operator

- Given:

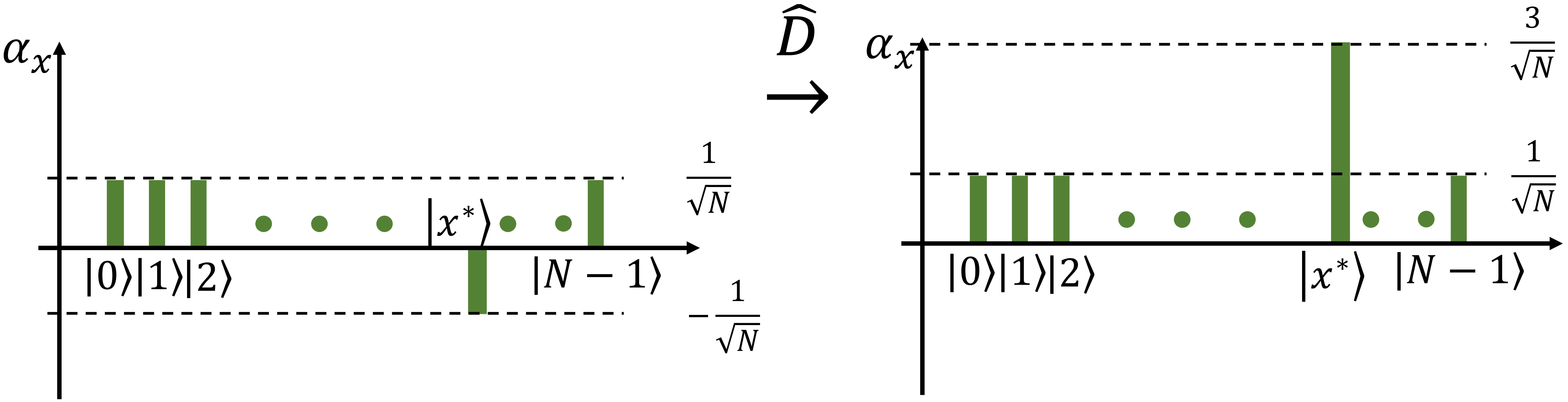
$$\sum_{x=0}^{N-1} \alpha_x |x\rangle \xrightarrow{\widehat{D}} \sum_{x=0}^{N-1} (2\mu - \alpha_x)|x\rangle, \text{ with } \mu \approx \frac{1}{\sqrt{N}}$$

- Applying $\widehat{D}$ to the oracle's output yields:

$$\begin{cases} \alpha_{x,x\neq x^*} = \dfrac{1}{\sqrt{N}} \xrightarrow{\widehat{D}} \alpha_{x,x\neq x^*} = (2\mu - \alpha_x) \approx \dfrac{2}{\sqrt{N}} - \dfrac{1}{\sqrt{N}} = \dfrac{1}{\sqrt{N}} \\ \alpha_{x^*} = -\dfrac{1}{\sqrt{N}} \xrightarrow{\widehat{D}} \alpha_{x^*} = (2\mu - \alpha_{x^*}) \approx \dfrac{2}{\sqrt{N}} + \dfrac{1}{\sqrt{N}} = \dfrac{3}{\sqrt{N}} \end{cases}$$

Grover's Diffusion Operator

Grover's diffusion operator $\hat{D}$ reflects the coefficients over their mean

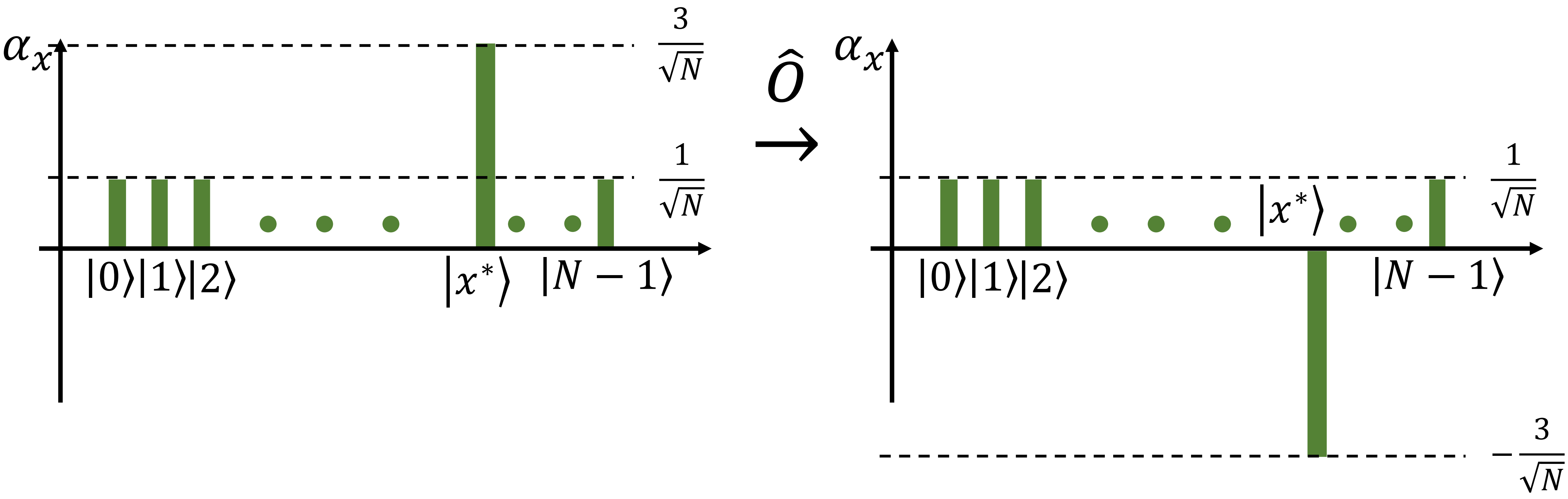


The probability of measuring state $|x^*\rangle$ is amplified $\mathrm{P}(|x^*\rangle) = \frac{9}{N}$

Grover's Iterations

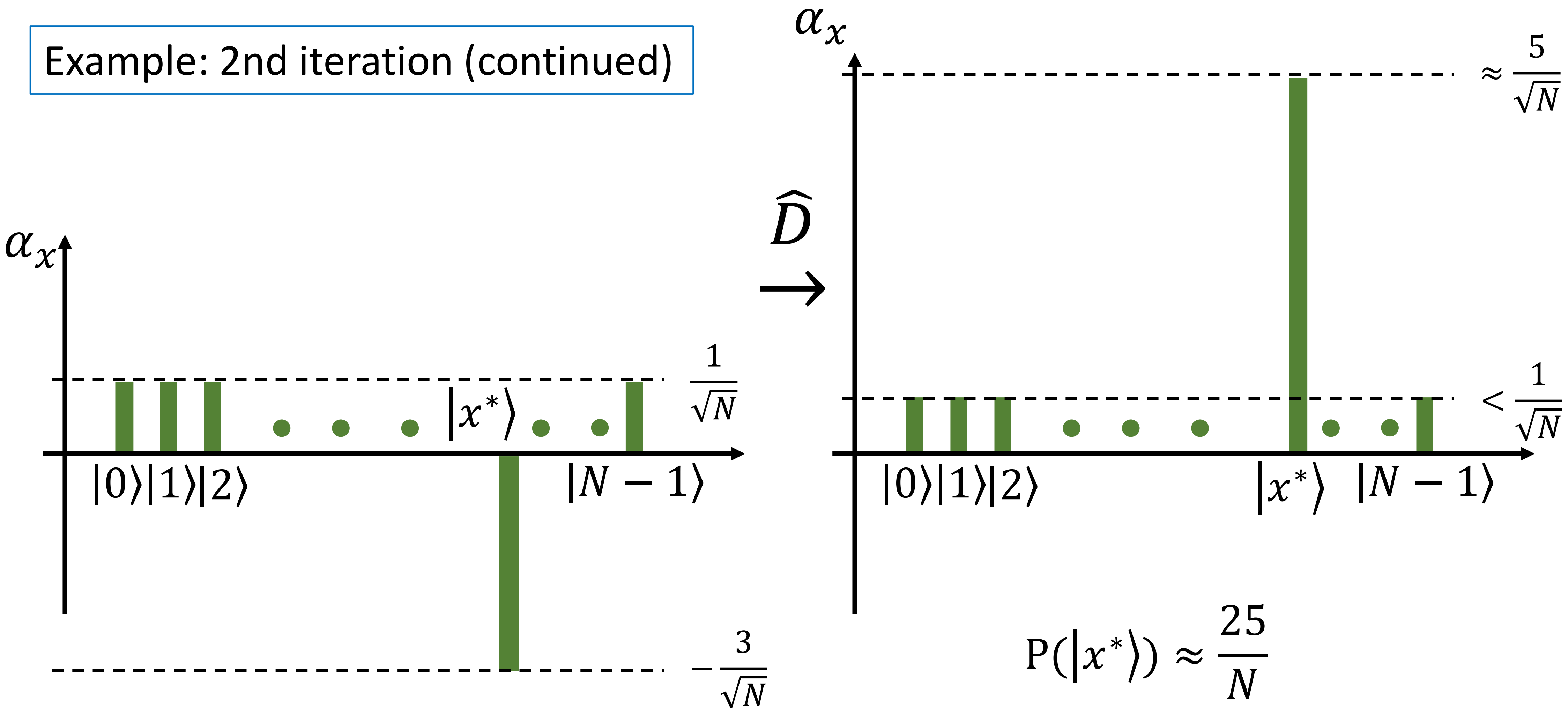
- The operators $\hat{D}\hat{O}$ are iteratively applied r times: $\left|\Psi^{(r)}\right\rangle = \left(\hat{D}\hat{O}\right)^{(r)}|s\rangle$

Example: 2nd iteration



Grover's Iterations

Example: 2nd iteration (continued)

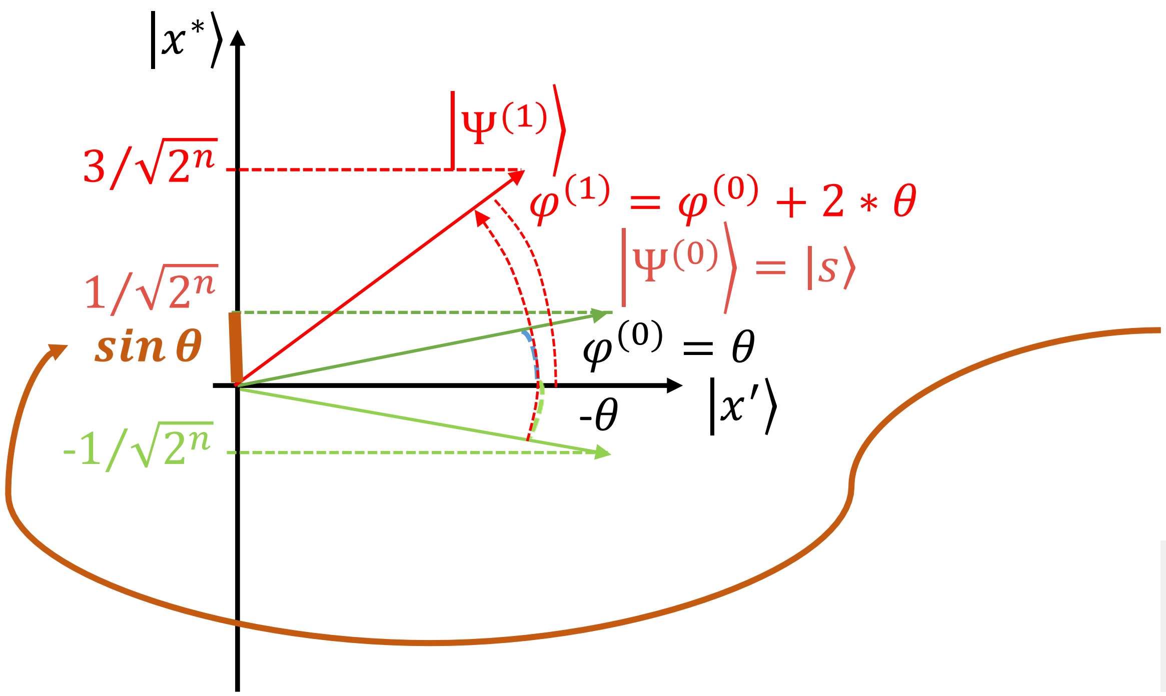


$$P(|x^*\rangle) \approx \frac{25}{N}$$

Grover's Iterations

To diffusion slide

- Goal: compute $\left|\Psi^{(r)}\right\rangle = \left(\hat{D}\hat{O}\right)^{(r)}|s\rangle$, such that $P(|x^*\rangle) \approx 1$
- What is the number of iterations r?



$\hat{O}$ - oracle

$\hat{D}$ - diffusion

$$\varphi^{(r)} = (2r+1)\theta \approx \pi/2$$

$$\sin\theta = 1/\sqrt{2^n}\,; n \gg 1 \Rightarrow \theta \approx 1/\sqrt{2^n}$$

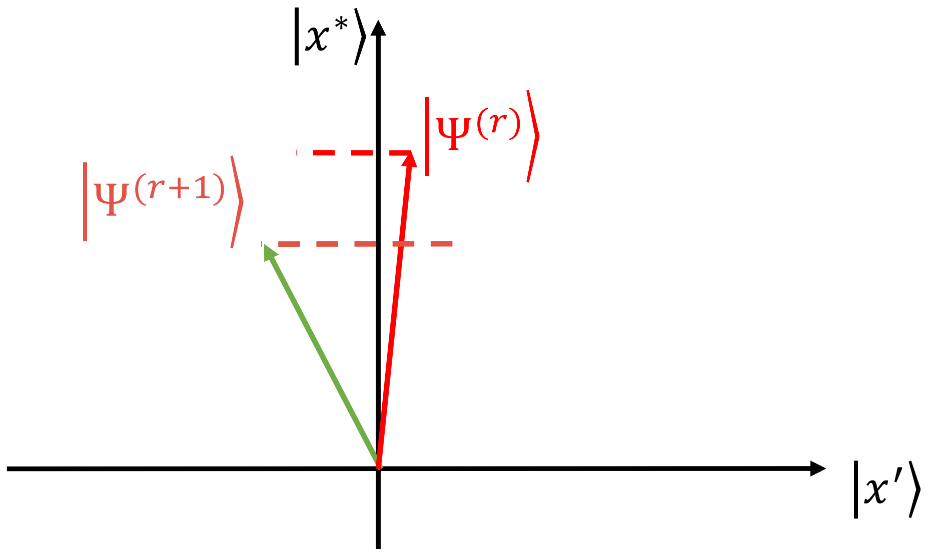
$$\frac{2r+1}{\sqrt{2^n}} \approx \pi/2 \Leftrightarrow 2r \approx \frac{\pi}{2}\sqrt{2^n} - 1 \Rightarrow$$

$$\Rightarrow r = \frac{\pi}{4}\sqrt{2^n} - \frac{1}{2} \approx \left\lceil\sqrt{2^n}\right\rceil, n \gg 1$$

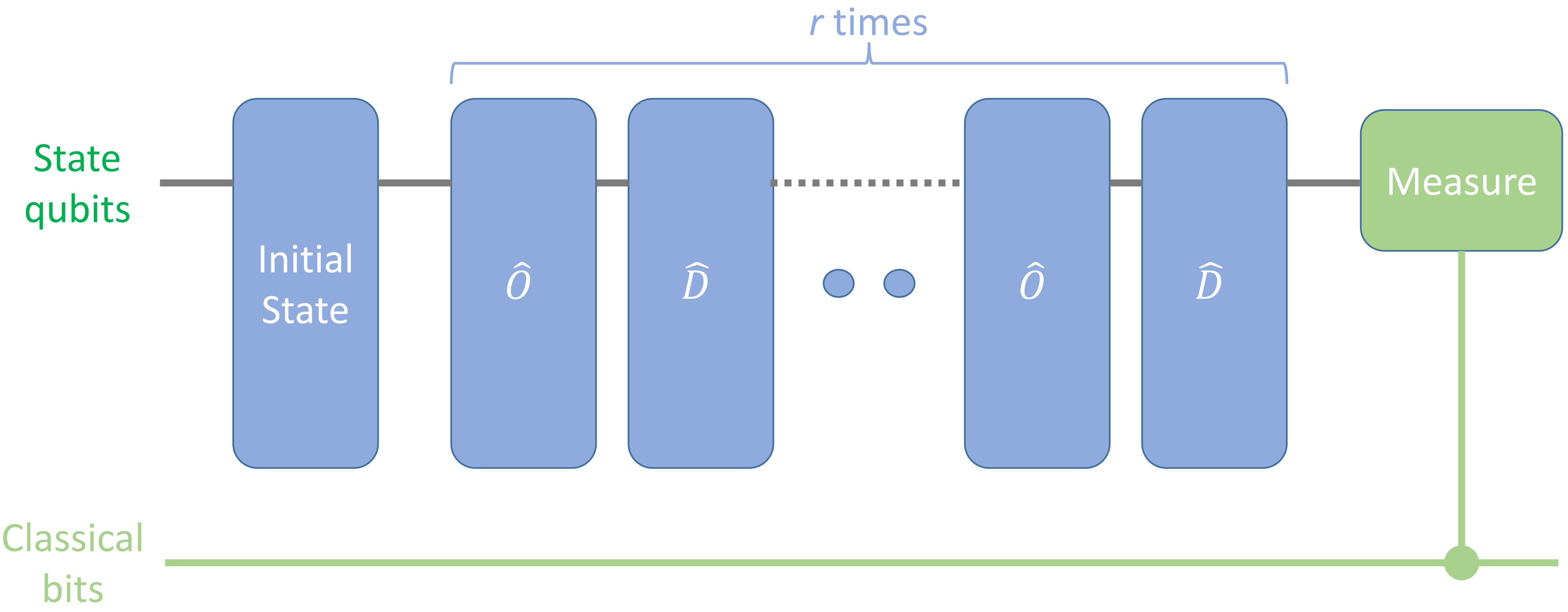
Grover's Iterations

- $r = \lceil \sqrt{2^n} \rceil$, meaning the oracle is evaluated $\mathcal{O}(\sqrt{2^n})$ times, representing a quadratic advantage over classical ($\mathcal{O}(2^n)$)

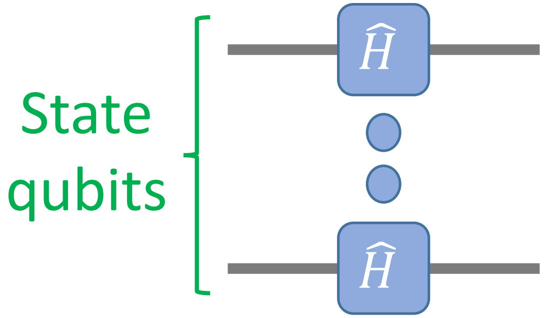
- Note that iterating more than r times reduces the probability of measuring $|x^*\rangle$



Grover's Implementation



Grover’s Implementation: Initial State



The state qubits are set onto an uniform superposition:

$$|x\rangle = \hat{H}^{(n)}\,|0\rangle$$

$$\hat{H}^{(1)} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix};\qquad \hat{H}^{(n)} = \hat{H}^{(1)\otimes(n)} = \frac{1}{\sqrt{2^n}}\Bigg(\underbrace{\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\otimes\cdots\otimes\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}}_{n\ times}\Bigg)$$

- Example for 2 qubits: $|x\rangle = \hat{H}|0\rangle = \frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \begin{bmatrix}1/2\\1/2\\1/2\\1/2\end{bmatrix}$

Grover's cZ Implementation: Oracle

$$\sum_{x=0,}^{N-1} \alpha_x |x\rangle = \overset{\hat{O}}{\rightarrow} \sum_{x=0, x\neq x^*}^{N-1} \alpha_x |x\rangle - \alpha_{x^*} \left| x^* \right\rangle$$

Z gate:

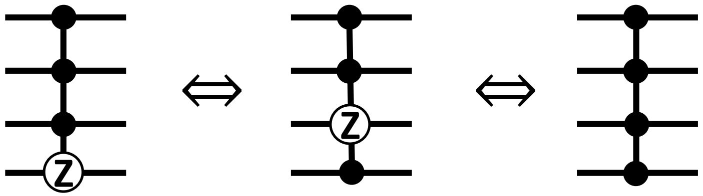
flips the signal of the $|1\rangle$ basis state coefficient:

$$\hat{Z}\,|\Psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ -\alpha_1 \end{bmatrix}$$

c^mZ gate:

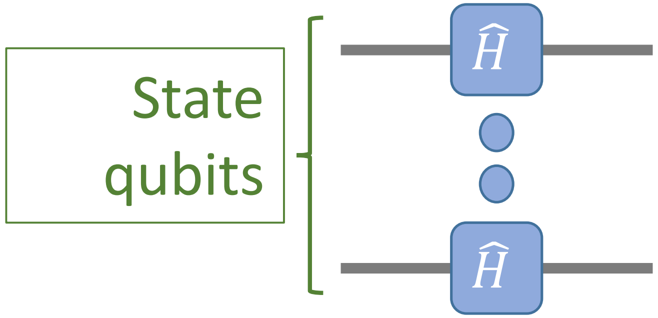
flips the signal of the $|1\rangle^{\otimes(m+1)} = |\mathbf{1}\rangle$ basis state coefficient:

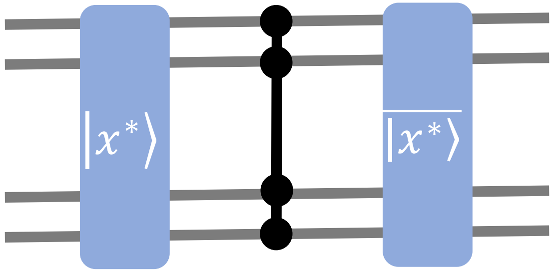
$$c\hat{Z}\,|\Psi\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{bmatrix} = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ -\alpha_3 \end{bmatrix}$$



symmetric on the position of Z

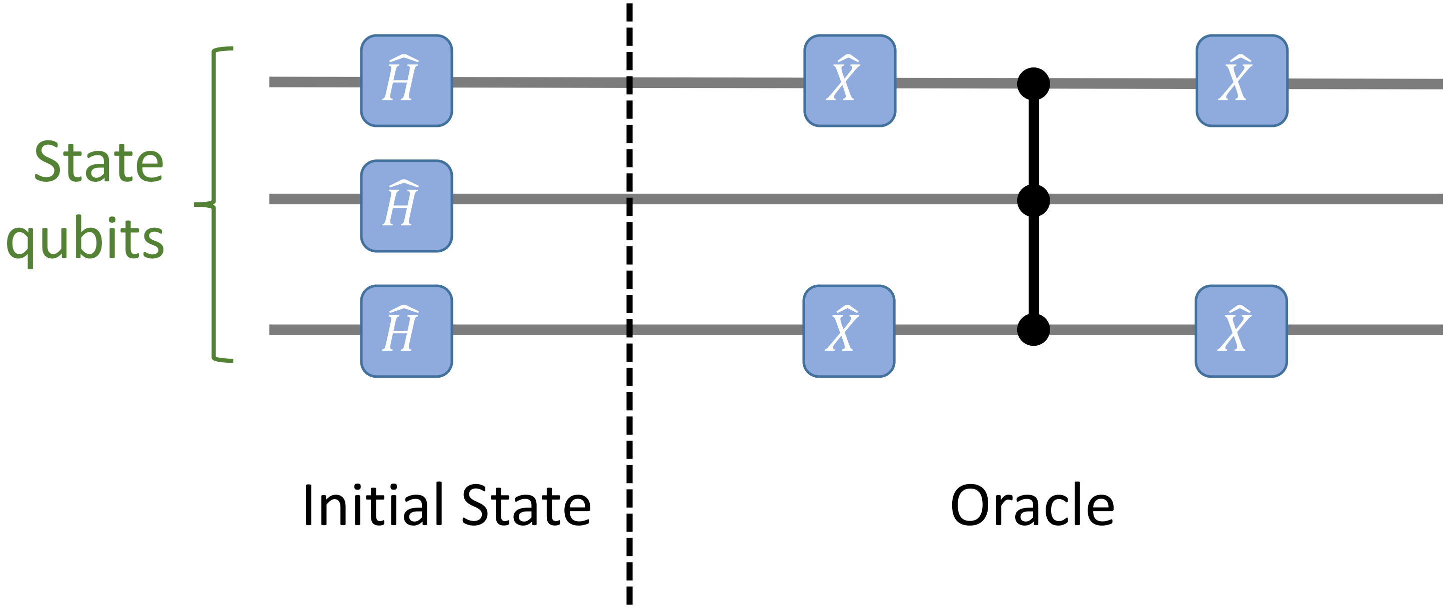
Grover’s cZ Implementation: Oracle





Grover's cZ Implementation: Oracle

Example circuit for 3 qubits and $|x^*\rangle = |010\rangle$



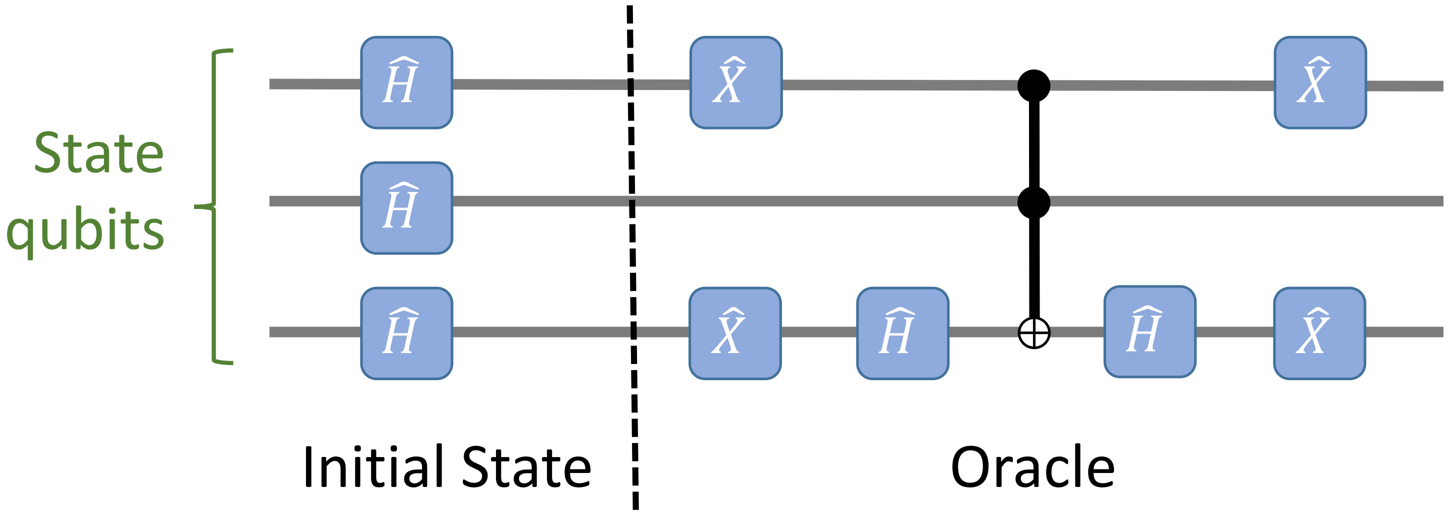
Grover's cZ Implementation: Oracle

Example circuit for 3 qubits and $|x^*\rangle = |010\rangle$

$c^m Z$ gates are equivalent to:

1. applying Hadamard to the target qubit
2. then a c^mNOT gate
3. then Hadamard again

(since the Hadamard transform rotates the X axis to Z and Z to X, and cNOT is a cX)



Grover's Implementation: Diffusion Operator

- Geometric analysis of $\widehat{D}$ -> reflection over the uniform sobreposition (see slide again):

$$\widehat{D} = 2\,|s\rangle\langle s| - \hat{I}$$

- By using the Hadamard transform this can be made into a reflection over $|0\rangle$
  (remember that $|s\rangle = \widehat{H}|0\rangle$ and $\widehat{H}$ is its own inverse):

$$\widehat{D} = 2\,\widehat{H}\,|0\rangle\langle 0|\,\widehat{H} - \hat{I}$$

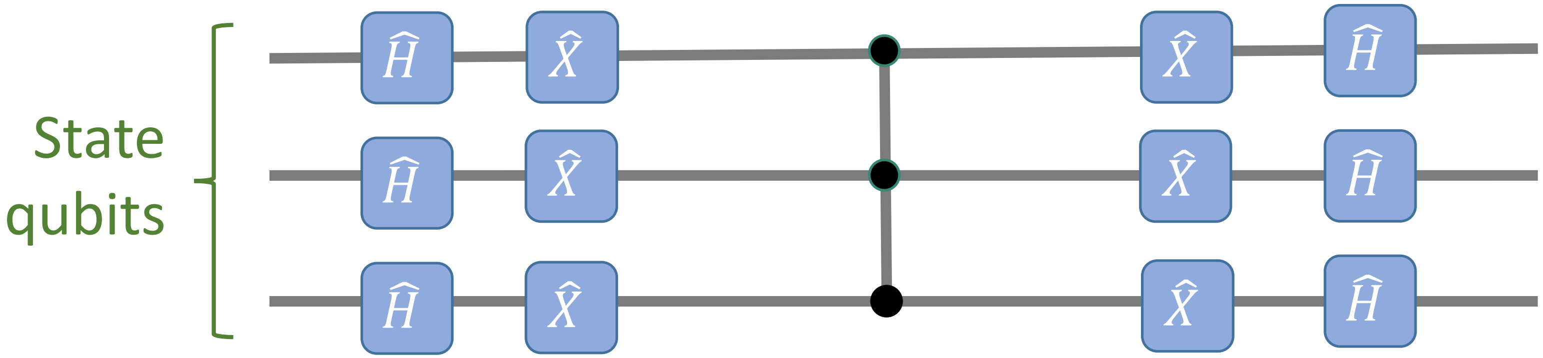
- Let $-\hat{S}_0$ be the negated reflector over $|0\rangle$: changes the sign of state $|0\rangle$

$$-\hat{S}_0\,|x\rangle = \begin{cases} |x\rangle\ if\,|x\rangle \neq |0\rangle \\ -|0\rangle\ if\,|x\rangle = |0\rangle \end{cases}$$

- Then $-\widehat{D}\,|x\rangle = -\widehat{H}\hat{S}_0\,\widehat{H}\,|x\rangle$
  (the sign is not relevant, since the probability is given by the squared amplitude)

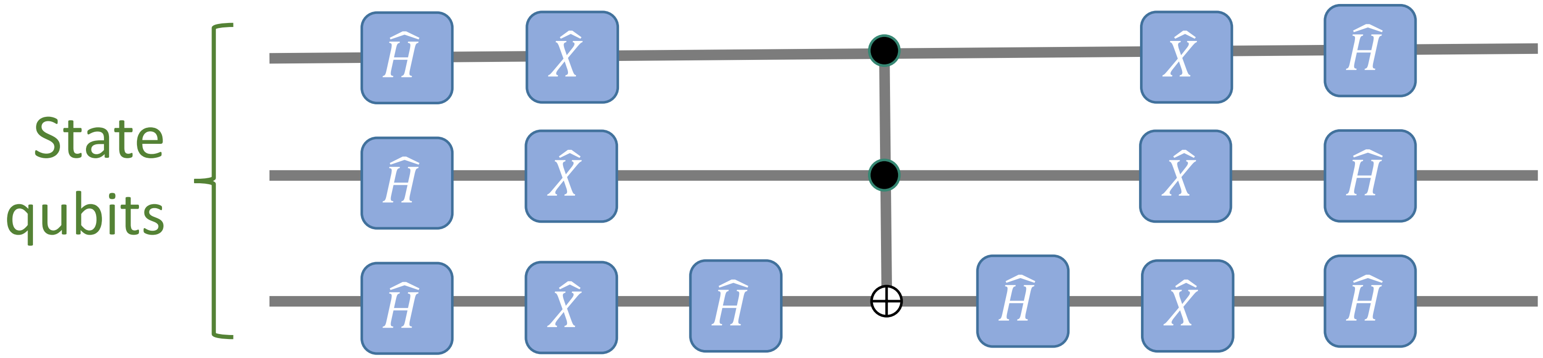
Grover's implementation: DIFFUSION OPERATOR

$-\widehat{D} = -\widehat{H}\hat{S}_0\,\widehat{H}$ - Example circuit for 3 qubits (ccZ gate):

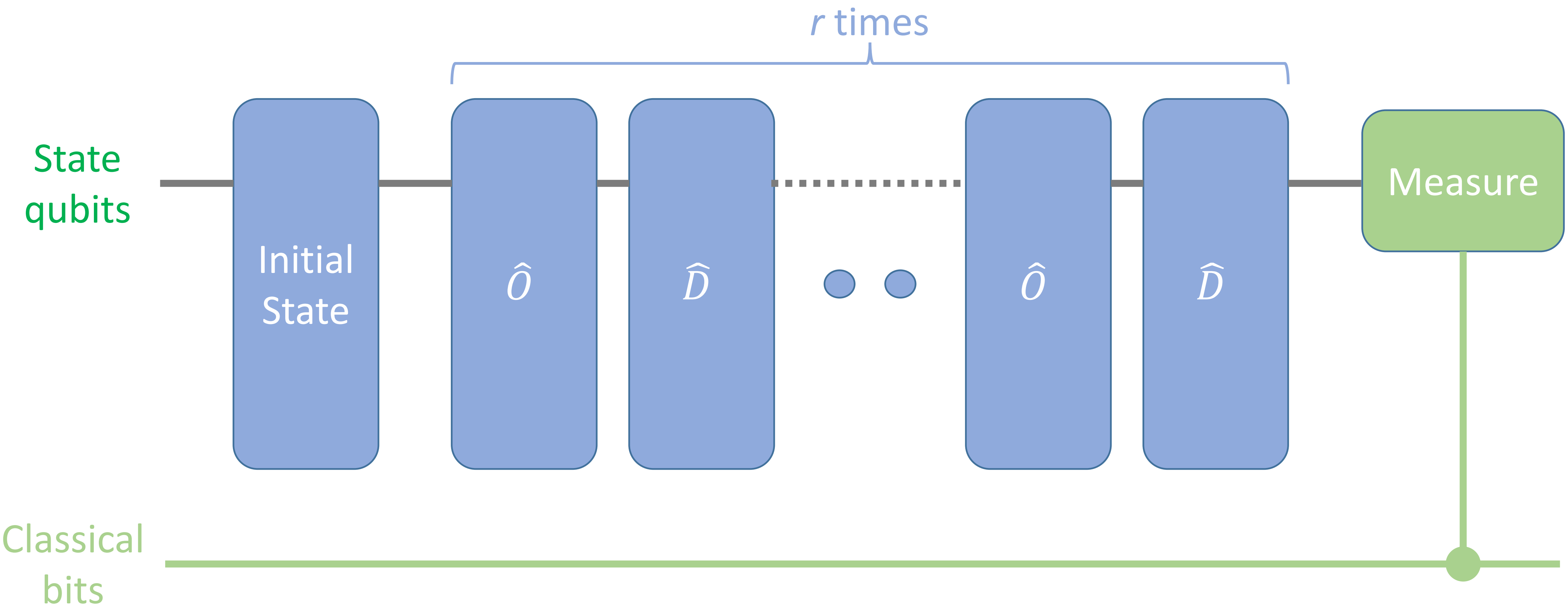


Grover’s implementation: DIFFUSION OPERATOR

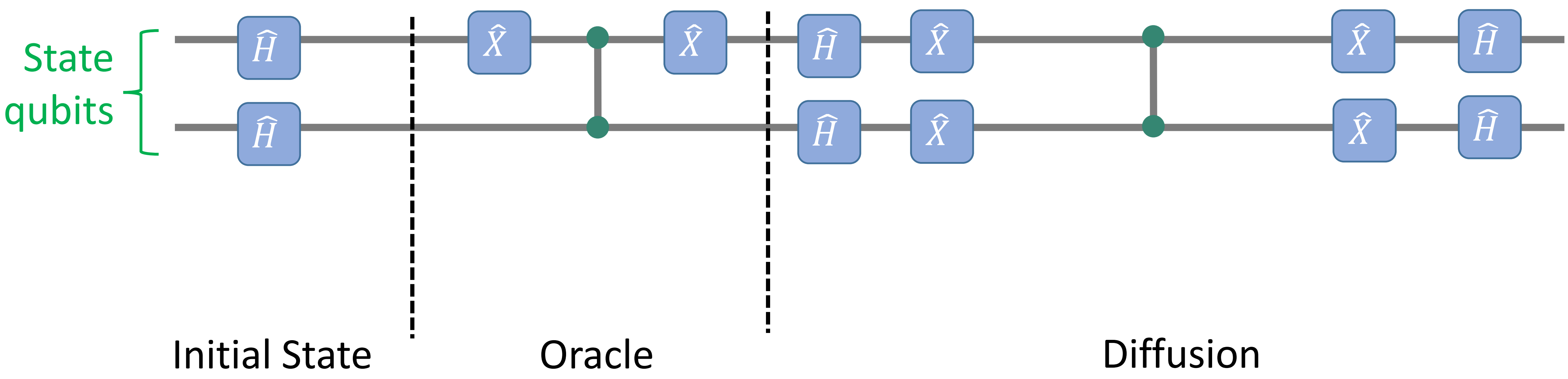
Example circuit for 3 qubits (which as seen here can be designed with ccX gates):



Grover's Implementation



Grover's Circuit: 2 qubits and $|x^*\rangle = |01\rangle$



Grover: multiple solutions

- If there are $M < N$ $(N = 2^n)$ solutions, then the number of iterations *r* to search for 1 solution is

$$r \approx \sqrt{N/M}$$

- *r* can not exceed the ideal number of iterations, therefore the above applies for *M* known
- If the number of solutions, M, is unknown then [Brassard2000] use either :
  - a probabilistic algorithm
  - an approximate counting algorithm to estimate N/M, using an approach similar to Shor's algorithm (period finding via Quantum Fourier Transform)

Brassard, Gilles; Hoyer, Peter; Mosca, Michele;Tapp, Alain; "*Quantum Amplitude Amplification and Estimation*", May 2000

Grover multiple solutions: probabilistic Qsearch [Brassard2000]

1. $l = 0\,; 1 < c < 2$
2. $l = l + 1\,; S = \lceil c^l \rceil$
3. $|s\rangle = \hat{H}\,|0\rangle\,; x =$ measure $(|s\rangle)$; if $f(x) == 1$ then **stop**
4. $|s\rangle = \hat{H}\,|0\rangle$
5. $j =$ random_integer $(1..S)$
6. $|\psi\rangle = (\hat{D}\,\hat{O})^j |s\rangle$
7. $x =$ measure $(|s\rangle)$; if $f(x) == 1$ then **stop**
8. goto 2

Exponential searching: S, the search space, increases exponentially

$\mathcal{O}(\sqrt{N/M})$

Grover: arbitrary initial state [Brassard2000]

- Generalized: initial state $|\psi\rangle$ different from uniform sobreposition $|s\rangle$ [Brassard2000]
  - Grover: $|s\rangle = \hat{H}\ |0\rangle\ ;\ \hat{O} = \hat{S}_f\ ;\ \hat{D} = -\hat{H}\ \hat{S}_0\ \hat{H}$
  - Generalized: $|\psi\rangle = \mathcal{A}\ |0\rangle\ ;\ \hat{O} = \hat{S}_f\ ;\ \hat{D} = -\mathcal{A}\ \hat{S}_0\ \mathcal{A}^{-1}$

    number of iterations $r \approx \frac{1}{\sqrt{a}}\ ;\ a = P(|x^*\rangle)$

Grover: finding the minimum

1. Select initial minimum threshold index

$$y = \text{random\_integer}(0..N-1)$$

2. Run the QSearch algorithm
3. If $v(x) < v(y)$ then $y = x$
4. If $timeSteps < 22.5\sqrt{N} + 1.4\, log_2 N$ goto 2
5. Output y