QWORLD

Quantum Search Algorithm: Grover

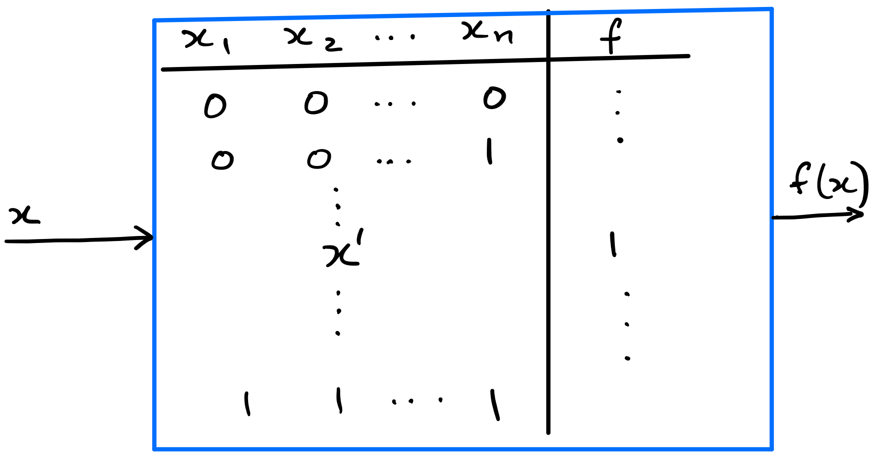
Jibran Rashid

Wednesday, July 20

WOMANIUM QUANTUM 2022

Unstructured Search

Given a Boolean function $f : \{0,1\}^n \longrightarrow \{0,1\}$ as a black-box find a string $x \in \{0,1\}^n$ such that $f(x) = 1$.



$N = 2^n$

<u>Query Complexity</u>

Number of times our algorithm uses the black box.

<u>Classical</u> $\Omega(2^n)$

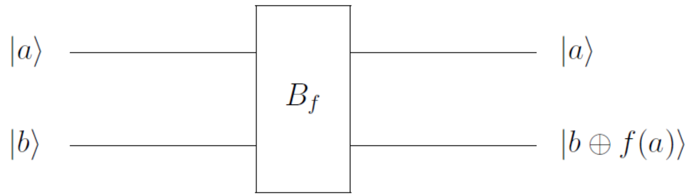
$2^n = N$ $\Omega(N)$

<u>Quantum</u>

$\Omega(\sqrt{N})$

$x_1 \vee x_2 \vee x_3 \wedge x_4 \vee$ - - - - - -

Classical Gates Via Unitaries



$$B_f : |a\rangle|b\rangle \longrightarrow |a\rangle|b \oplus f(a)\rangle$$

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

$$B_f : |a\rangle|-\rangle \longrightarrow (-1)^{f(a)}|a\rangle|-\rangle$$

Hadamard on n Qubits

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |+\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle$$

$$(H \otimes H)|00\rangle = |+\rangle \otimes |+\rangle$$

$$= \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

$$H^{\otimes n}|00\ldots0\rangle = |+\rangle \otimes |+\rangle \otimes \ldots \otimes |+\rangle$$

$$= \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

Quantum Unstructured Search

Grover's Algorithm

1. Let X be an n-qubit quantum register (i.e., a collection of n qubits to which we assign the name X). Let the starting state of X be $|0^n\rangle$ and perform $H^{\otimes n}$ on X.
2. Apply to the register X the transformation

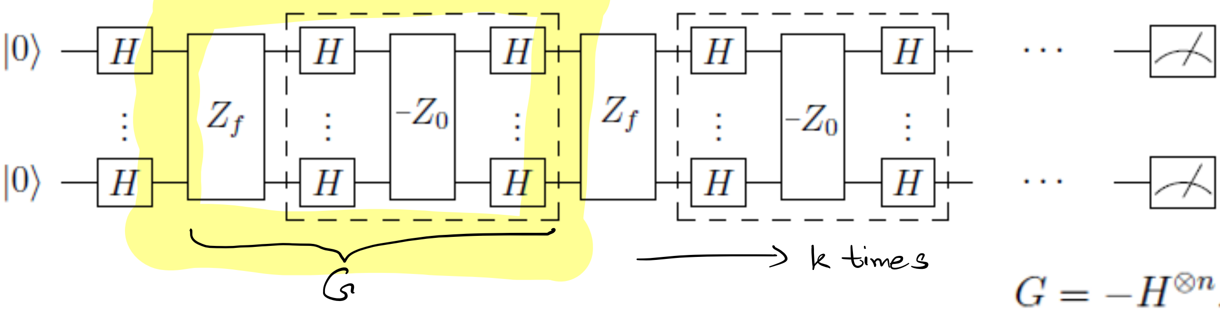
$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

   k times (where k will be specified later).
3. Measure X and output the result.

$$Z_f |x\rangle = (-1)^{f(x)} |x\rangle$$

$$Z_0 |x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

Quantum Unstructured Search



$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$A = \{ x \in \{0,1\}^n \mid f(x) = 1 \}$, $a = |A|$ # of good strings

$$Z_f |x\rangle = (-1)^{f(x)} |x\rangle$$

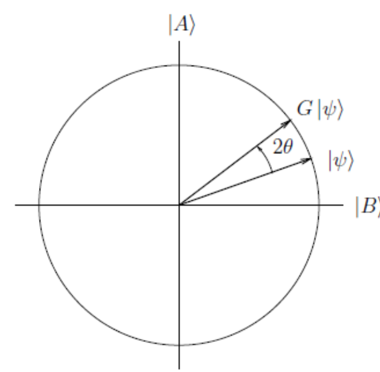
$B = \{ x \in \{0,1\}^n \mid f(x) = 0 \}$, $b = |B|$ # of bad strings

$$Z_0 |x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

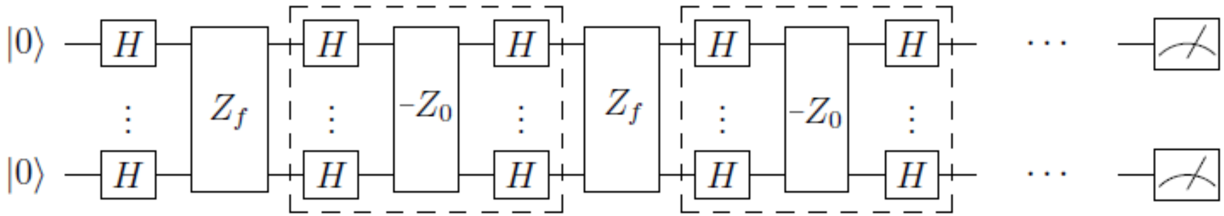
$$|A\rangle = \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle$$

$$|B\rangle = \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$$

$$\alpha |A\rangle + \beta |B\rangle, \quad \alpha, \beta \in \mathbb{R}$$



Quantum Unstructured Search



$$H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = |h\rangle$$

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$$|h\rangle = \sqrt{\frac{a}{N}}\,|A\rangle + \sqrt{\frac{b}{N}}\,|B\rangle$$

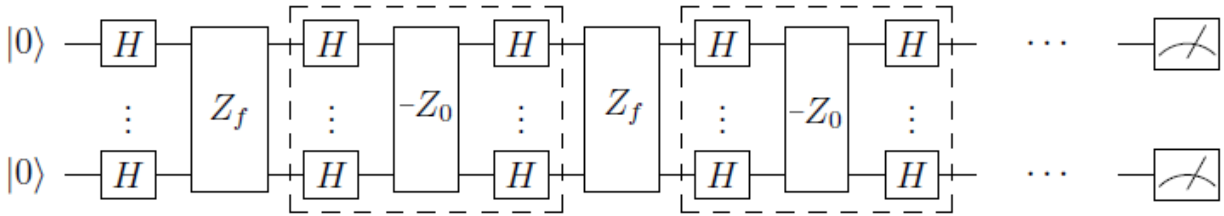
$$Z_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle$$

$$Z_0\,|x\rangle = \begin{cases} -\,|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

$G|A\rangle = \,?$ $\qquad$ $G|B\rangle = \,?$

Note $\quad Z_0 = \begin{pmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix} = \mathbb{1} - 2\,\underbrace{|0^n\rangle\langle 0^n|}_{\text{Outer Product}}$

Quantum Unstructured Search



$$G|A\rangle = \left(-H^{\otimes n} Z_0 H^{\otimes n} Z_f\right)|A\rangle$$

$$= \left(H^{\otimes n} Z_0 H^{\otimes n}\right)|A\rangle$$

$$-Z_f|A\rangle = |A\rangle$$

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$$Z_f|x\rangle = (-1)^{f(x)}|x\rangle$$

$$Z_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

$$\underline{H^{\otimes n} Z_0 H^{\otimes n}} = H^{\otimes n}\left(\mathbb{1} - 2|0^n\rangle\langle 0^n|\right)H^{\otimes n}$$

$$= \underbrace{H^{\otimes n} H^{\otimes n}}_{\mathbb{1}} - 2 H^{\otimes n}|0^n\rangle\langle 0^n| H^{\otimes n}$$

$$= \underline{\mathbb{1} - 2|h\rangle\langle h|}$$

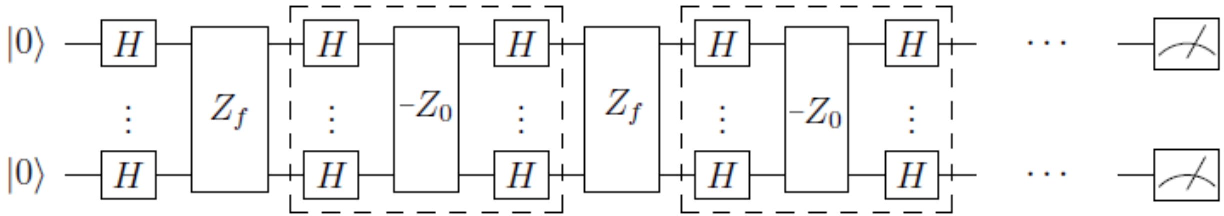
$$|A\rangle = \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle$$

$$|B\rangle = \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$$

$$|h\rangle = \frac{1}{\sqrt{N}} \sum_{x} |x\rangle$$

$x \in \{0,1\}^n$

Quantum Unstructured Search



$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$$Z_f |x\rangle = (-1)^{f(x)} |x\rangle$$

$$Z_0 |x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

$$|h\rangle = \sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle$$

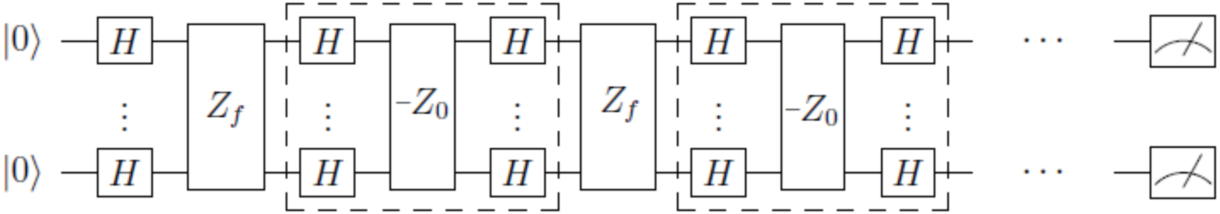
$$G|A\rangle = (\mathbb{1} - 2|h\rangle\langle h|)|A\rangle$$

$$= |A\rangle - 2|h\rangle\langle h|A\rangle$$

$$= |A\rangle - 2\sqrt{\frac{a}{N}}\left(\sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle\right)$$

$$= \left(1 - \frac{2a}{N}\right)|A\rangle - \frac{2\sqrt{ab}}{N}|B\rangle$$

Quantum Unstructured Search



$$G|A\rangle = \left(1-\frac{2a}{N}\right)|A\rangle + \frac{2\sqrt{ab}}{N}|B\rangle$$

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

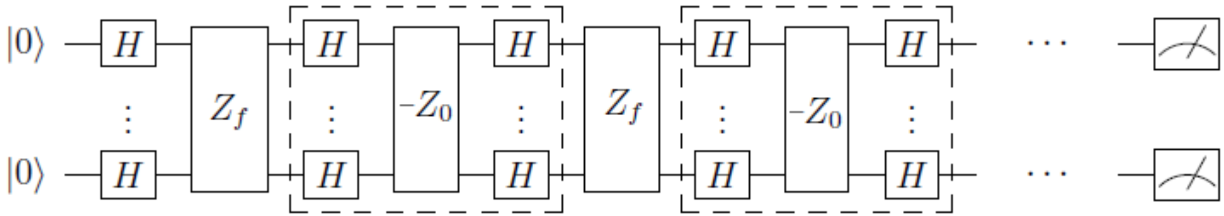
Similarly, $G|B\rangle = \frac{2\sqrt{ab}}{N}|A\rangle - \left(1-\frac{2b}{N}\right)|B\rangle$

$$Z_f|x\rangle = (-1)^{f(x)}|x\rangle$$

$$Z_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

$$M = \begin{array}{c} \\ |B\rangle \\ \\ |A\rangle \end{array} \begin{array}{c} \begin{array}{cc} |B\rangle & \qquad |A\rangle \end{array} \\ \begin{pmatrix} -\left(1-\frac{2b}{N}\right) & -\frac{2\sqrt{ab}}{N} \\ \frac{2\sqrt{ab}}{N} & \left(1-\frac{2a}{N}\right) \end{pmatrix} \end{array} = \begin{pmatrix} \sqrt{\frac{b}{N}} & -\sqrt{\frac{a}{N}} \\ \sqrt{\frac{a}{N}} & \sqrt{\frac{b}{N}} \end{pmatrix}^2$$

Quantum Unstructured Search



Let $\sin\theta = \sqrt{\frac{a}{N}}$, $\cos\theta = \sqrt{\frac{b}{N}}$

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$$|h\rangle = \underline{\cos\theta\,|B\rangle + \sin\theta\,|A\rangle}$$

$$Z_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle$$

After k applications of G, the state is given by

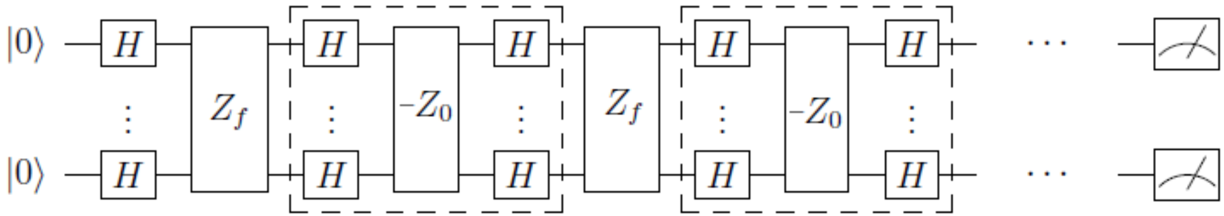
$$Z_0\,|x\rangle = \begin{cases} -\,|x\rangle & \text{if } x = 0^n \\ \ \ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

$$\cos(\underline{2k}+1)\theta\,|B\rangle + \underline{\sin(2k+1)\theta\,|A\rangle}$$

$$|h\rangle = \sqrt{\frac{a}{N}}\,|A\rangle + \sqrt{\frac{b}{N}}\,|B\rangle$$

$$\sin(2k+1)\theta \approx 1$$

Quantum Unstructured Search



Want $\sin(2k+1)\theta \approx 1 \Rightarrow (2k+1)\theta \approx \frac{\pi}{2}$

$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

$k \approx \frac{\pi}{4\pi} - \frac{1}{2} \rightarrow k = \left\lfloor \frac{\pi\sqrt{N}}{4} \right\rfloor$

$$Z_f\,|x\rangle = (-1)^{f(x)}\,|x\rangle$$

$$Z_0\,|x\rangle = \begin{cases} -\,|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

$\theta = \sin^{-1}\sqrt{\frac{a}{N}} = \sin^{-1}\sqrt{\frac{1}{N}} \,.\; \theta \approx \sqrt{\frac{1}{N}}$

Grover's Algorithm is $O(\sqrt{N})$

Inversion Around the Mean

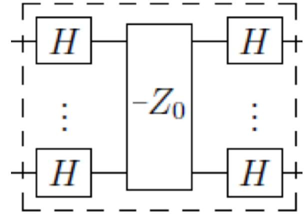
$$U = -H^{\otimes n} Z_0 H^{\otimes n} = 2|h\rangle\langle h| - \mathbb{1}, \quad G = U Z_f$$

$$= \frac{2}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} - \mathbb{1}$$

$$U\left(\sum_x \alpha_x |x\rangle \right) = \sum_x \alpha_x U|x\rangle$$

$$= \sum_x \alpha_x \left(\frac{2}{N}\begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix} - \mathbb{1} \right) |x\rangle$$

$$= \sum_x \left(2\mu - \alpha_x \right) |x\rangle, \quad \mu = \frac{1}{N} \sum_x \alpha_x$$

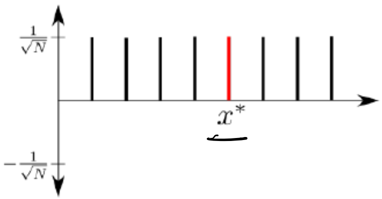


Diffusion Operator

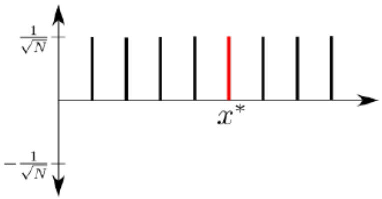
$$|h\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

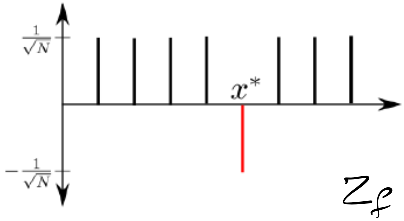
Inversion Around the Mean

$|h\rangle$



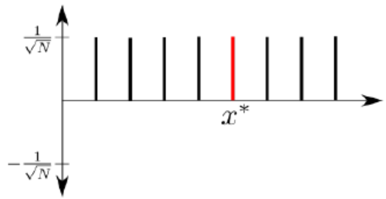
Inversion Around the Mean

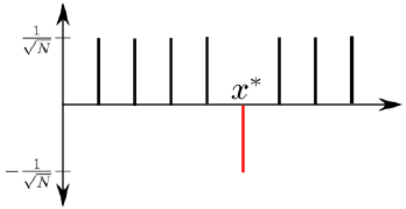


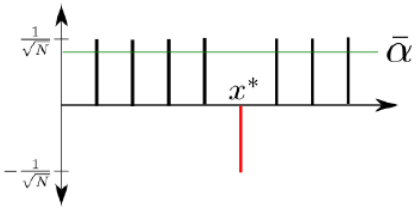


$$Z_f |x\rangle = (-1)^{f(x)} |x\rangle$$

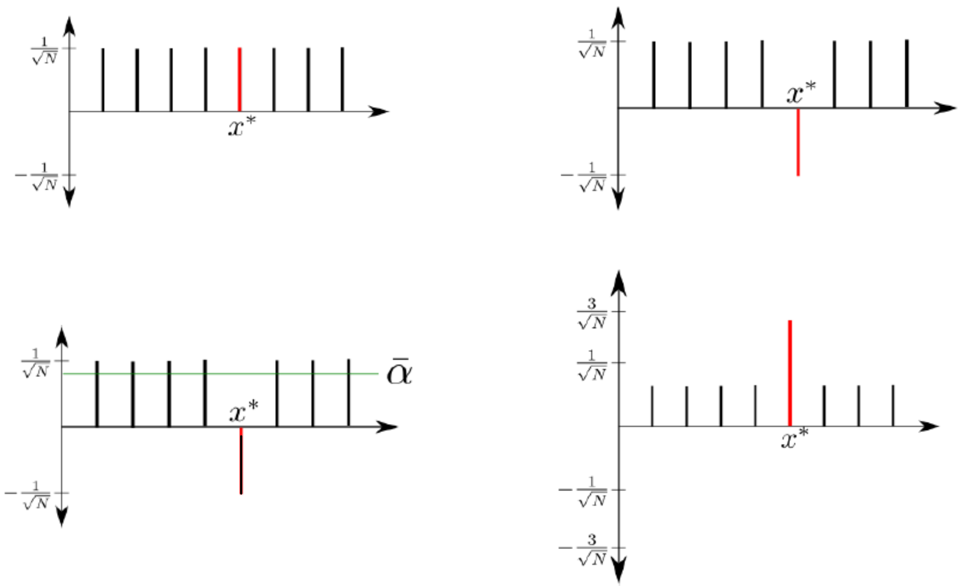
Inversion Around the Mean







Inversion Around the Mean

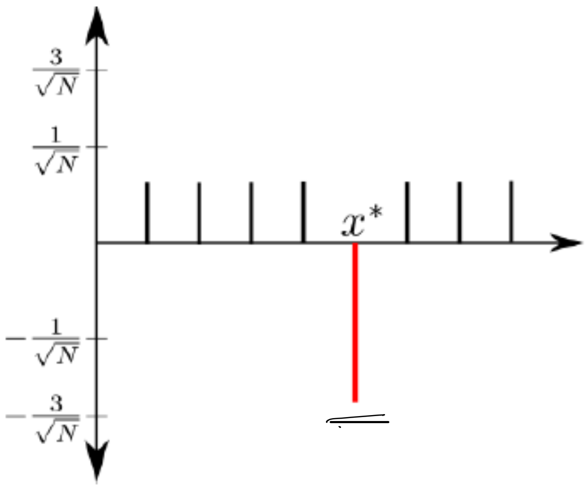


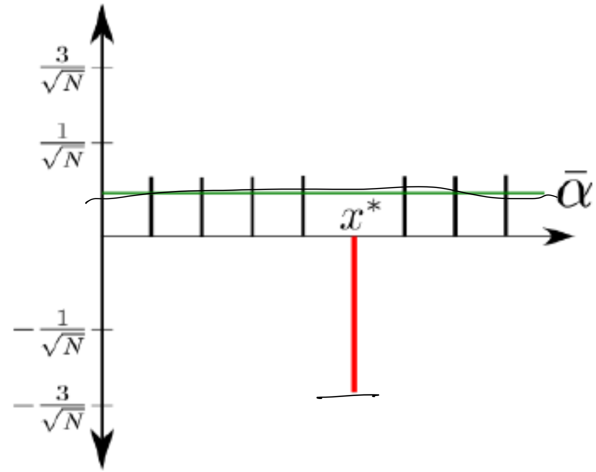
$$2\mu - \alpha_x$$

$$2\left(\frac{1}{\sqrt{N}}\right) - \left(-\frac{1}{\sqrt{N}}\right)$$

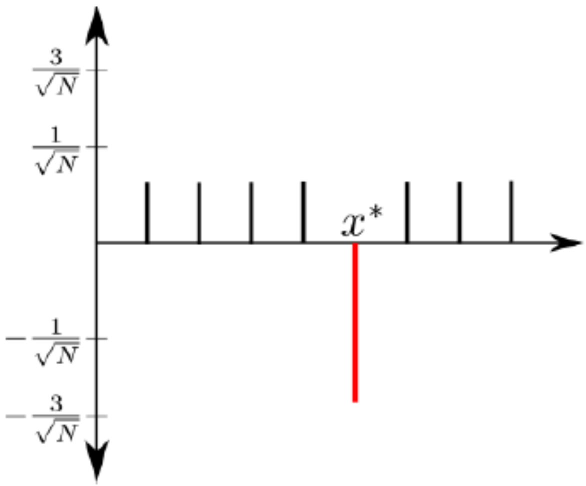
$$= \frac{3}{\sqrt{N}}$$

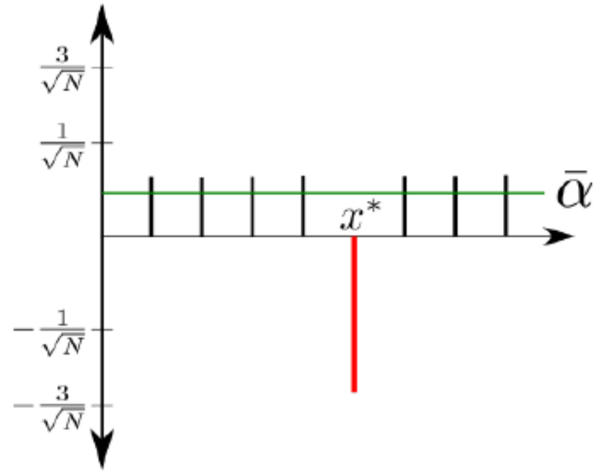
Second Round Inversion

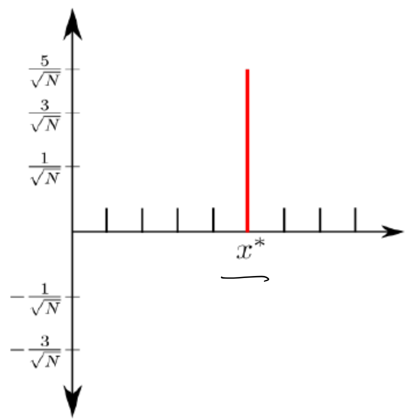




Second Round Inversion







$\frac{5}{\sqrt{N}}$

Unstructured Search

Suppose we run Grover's Algorithm on a function $f : \{0,1\}^n \mapsto \{0,1\}$ that satisfies

$$|\{x \in \{0,1\}^n : f(x) = 1\}| = 2^{n-1}.$$

What is the probability that the algorithm outputs a string $x \in \{0,1\}^n$ satisfying $f(x) = 1$ when $k = 1$. Justify your answer.

Unstructured Search

Suppose we run Grover's Algorithm on a function $f : \{0,1\}^n \mapsto \{0,1\}$ that satisfies

$$|\{x \in \{0,1\}^n : f(x) = 1\}| = 2^{n-1}.$$

What is the probability that the algorithm outputs a string $x \in \{0,1\}^n$ satisfying $f(x) = 1$ when $k = 1$. Justify your answer.

For the same function f, describe how Grover's algorithm f could be modified so that an element $x \in \{0,1\}^n$ satisfying $f(x) = 1$ can be found with certainty using only one query to a black box for f (implemented as a unitary transformation Z_f in the usual way).

What is Your Favourite Super Power?

MANIPULATE PROBABILITY!!!