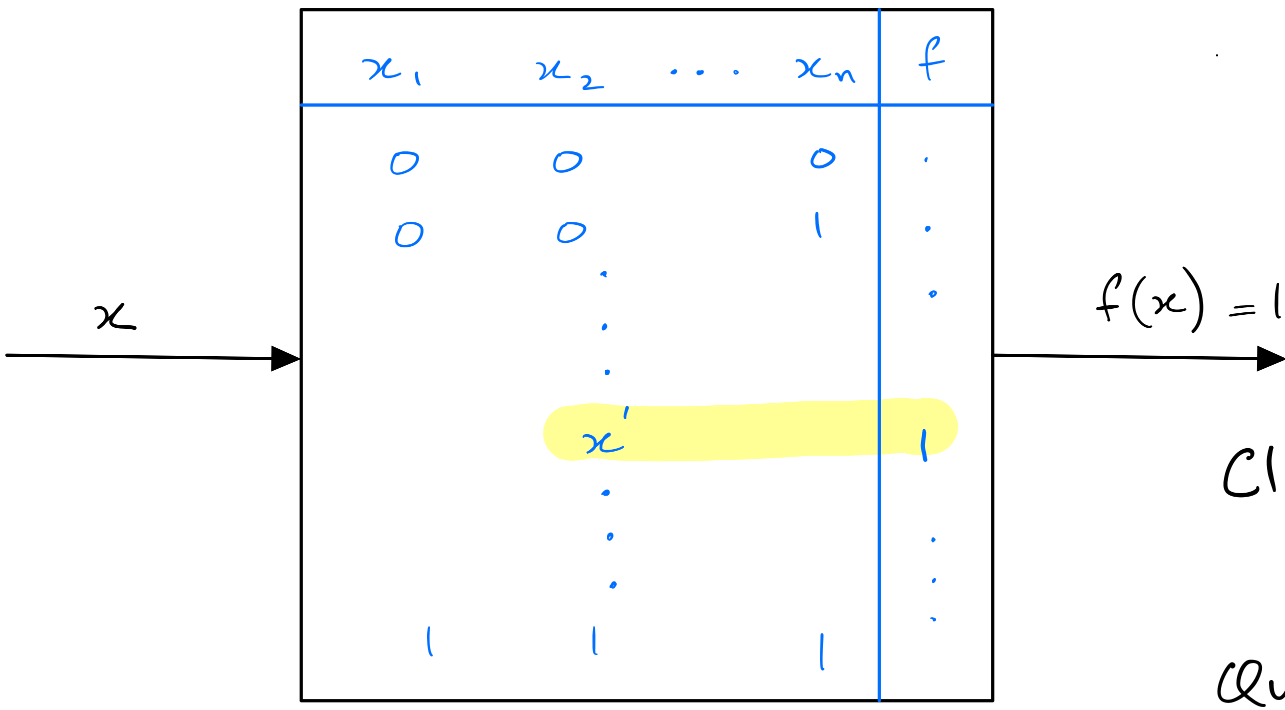
QWORLD

GROVER'S ALGORITHM

Jibran Rashid

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 $f(x)=1$.



$N = 2^n$

Classical $\Omega(2^n)$

Quantum $\Omega(\sqrt{2^n})$

Grover's Algorithm

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

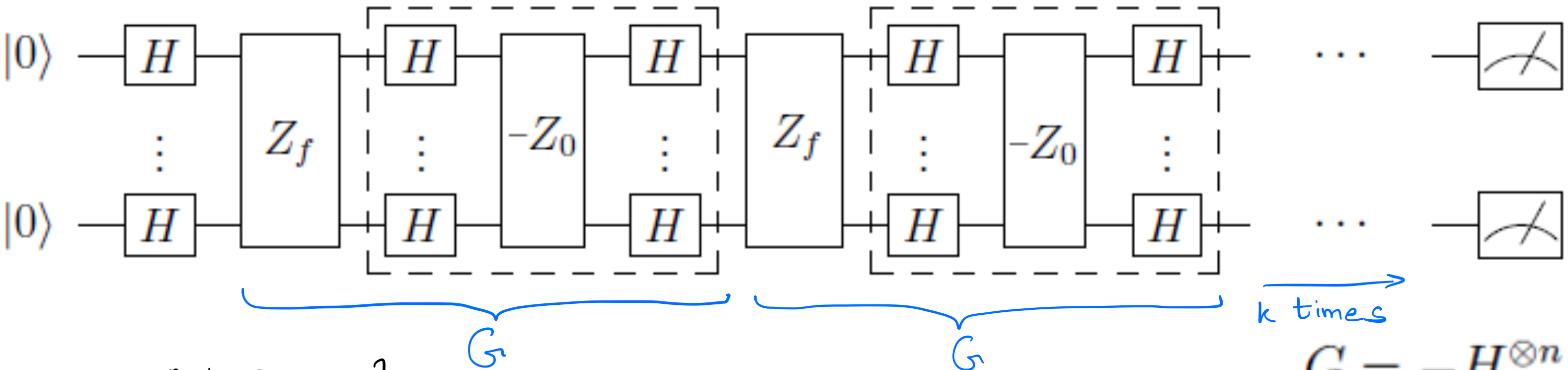
$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

   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



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

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

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

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

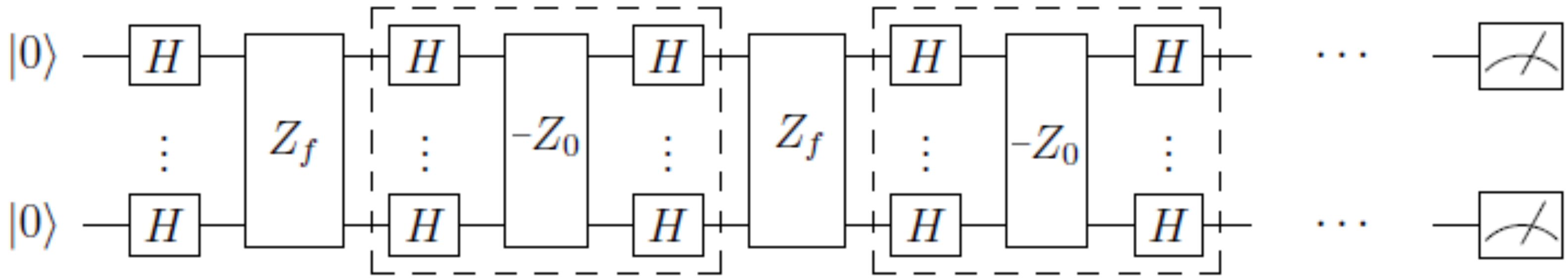
$B = \{x \in \{0,1\}^n \mid f(x) = 0\}$, $b = |B|$ # of bad strings

$$|A\rangle = \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle, \qquad |B\rangle = \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$$

at any given time in the state's evolution during the algorithm, we can write it as

$$\alpha\,|A\rangle + \beta\,|B\rangle$$

Quantum Unstructured Search



$$H^{\otimes n}|0^{\otimes n}\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle = |h\rangle \, , \qquad N = 2^n$$

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

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

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

$$|0^n\rangle = \overbrace{|0\rangle\otimes|0\rangle\cdots\otimes|0\rangle}^{n \text{ qubits}}$$

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

$$Z_0 = \begin{pmatrix} -1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix} = \mathbb{1} - 2\underbrace{|0^n\rangle\langle 0^n|}_{\text{outer product}}$$

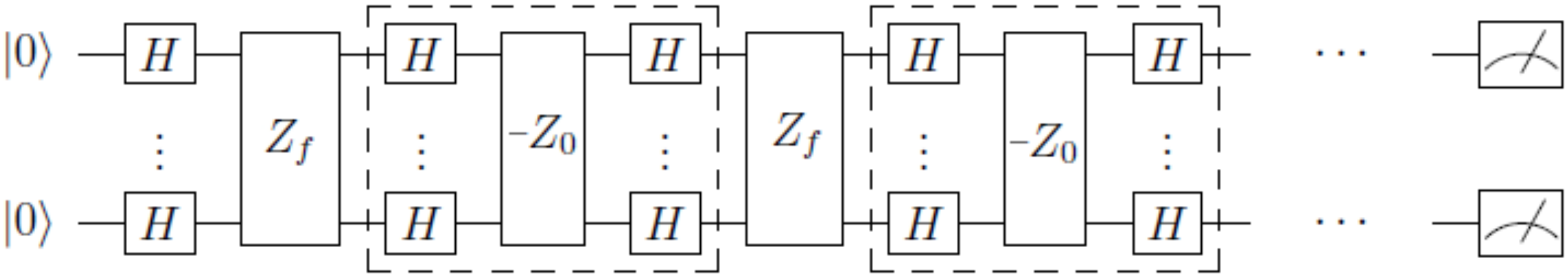
$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ & 0 & \\ 0 & & \ddots\; 0 \end{pmatrix}$$

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

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

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

Quantum Unstructured Search



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

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

$$\left(\mathbb{1} - 2|h\rangle\langle h|\right)|A\rangle$$

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

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

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

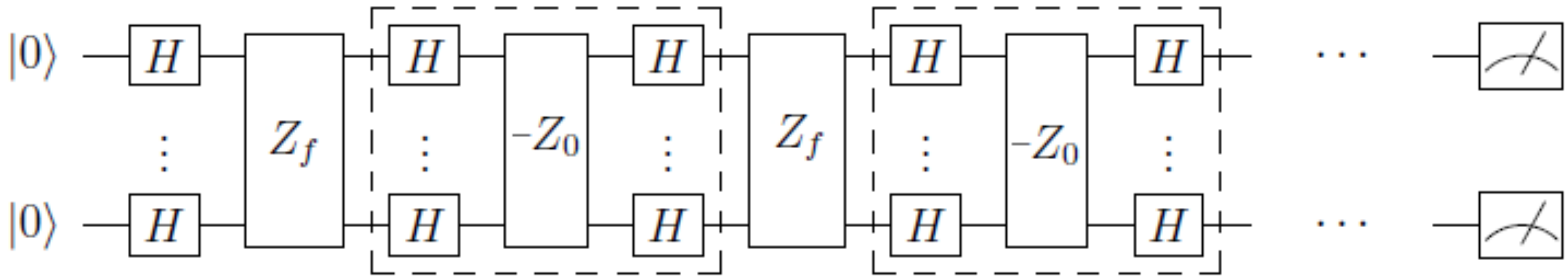
$$Z_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

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

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

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

Quantum Unstructured Search



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

$$= |A\rangle - 2|h\rangle \underbrace{\langle h|A\rangle}_{\substack{\text{inner product} \\ \sqrt{\frac{a}{N}}}}$$

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

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

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

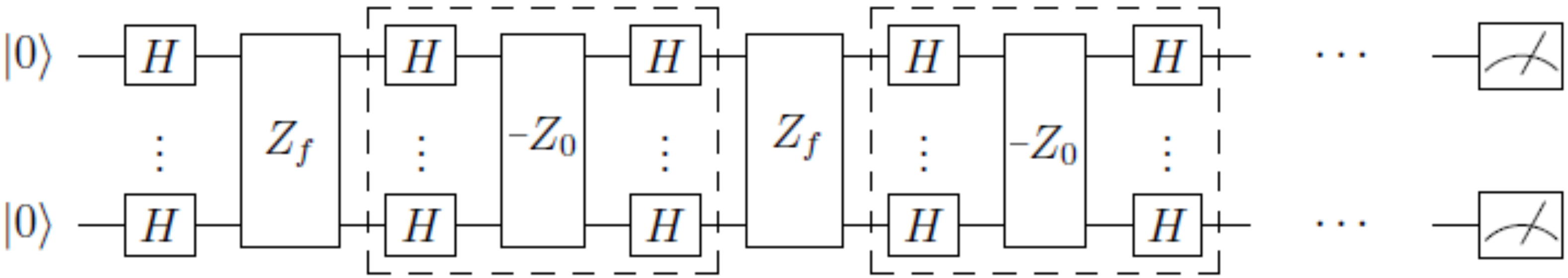
$$Z_f|x\rangle = (-1)^{f(x)}|x\rangle$$

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

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

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

Quantum Unstructured Search



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

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

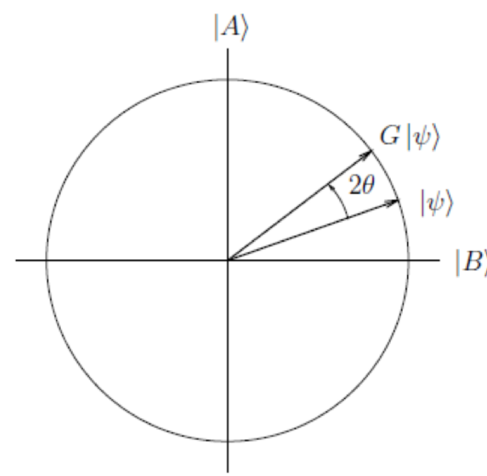
$$G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$$

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

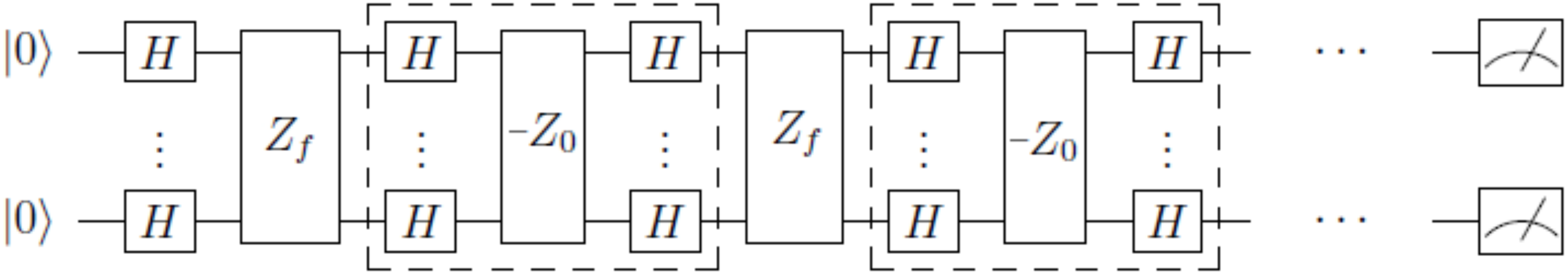
$$Z_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$$

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

$$M := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^2$$



Quantum Unstructured Search



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

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

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

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

After applying G k times

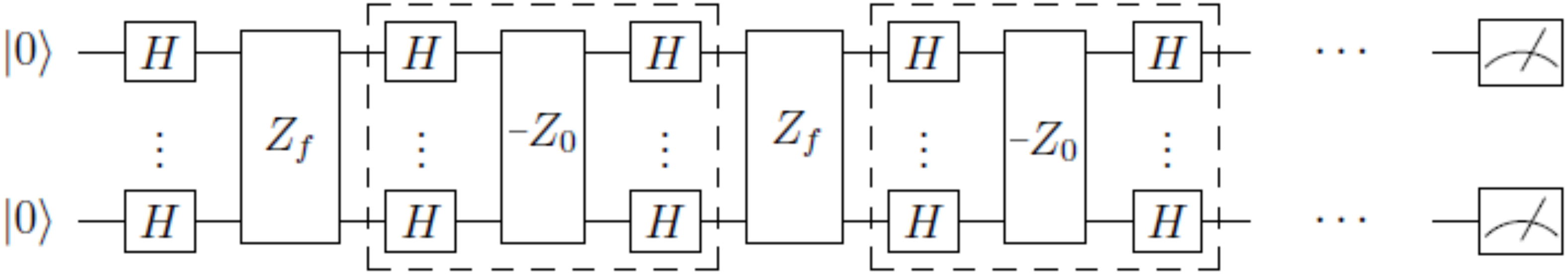
$$G^k|h\rangle = \cos(2k+1)\theta\,|B\rangle + \sin(2k+1)\theta\,|A\rangle$$

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

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

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

Quantum Unstructured Search



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

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

$$k = \frac{\pi}{4\theta} - \frac{1}{2} \longrightarrow k \approx \frac{\pi\sqrt{N}}{4}$$

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

$$\sin\theta = \sqrt{\frac{a}{N}}$$

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

$$\theta = \sin^{-1}\sqrt{\frac{a}{N}}$$

assume $a=1 \Rightarrow \theta \approx \sqrt{\frac{1}{N}}$

i.e., one marked item

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.

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

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

Inversion Around the Mean

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

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

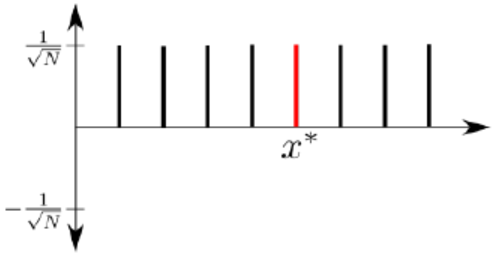
$$U\left(\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle\right) = \sum_x \alpha_x U|x\rangle$$

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

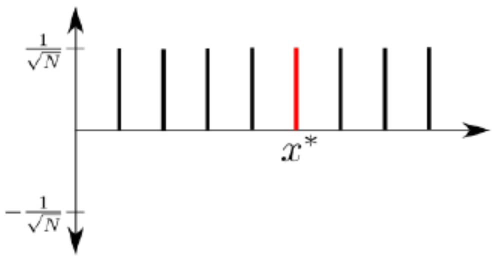
$$= \sum_x (2\mu - \alpha_x)|x\rangle$$

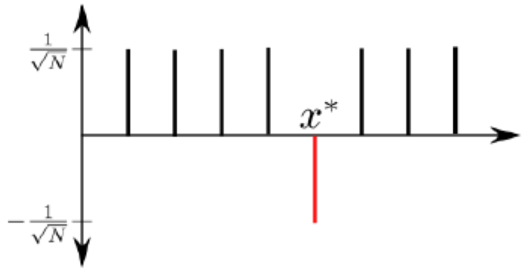
Mean $\mu = \frac{1}{N}\sum_x \alpha_x$

Inversion Around the Mean



Inversion Around the Mean

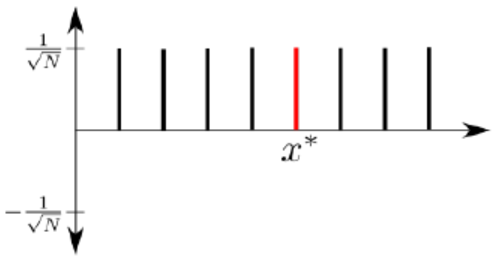


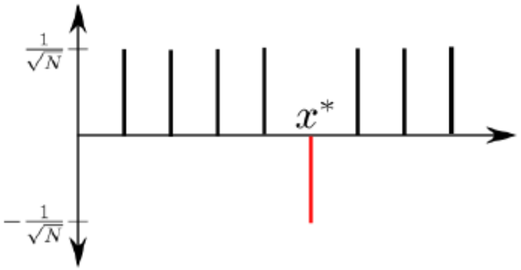


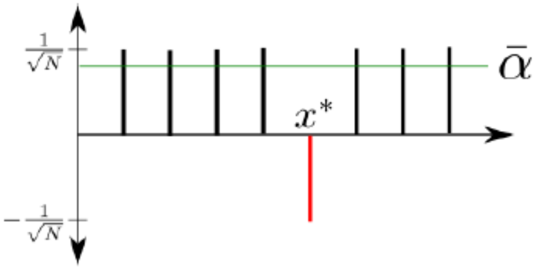
$f(x^*) = 1$

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

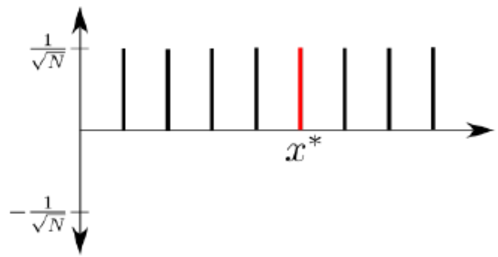
Inversion Around the Mean

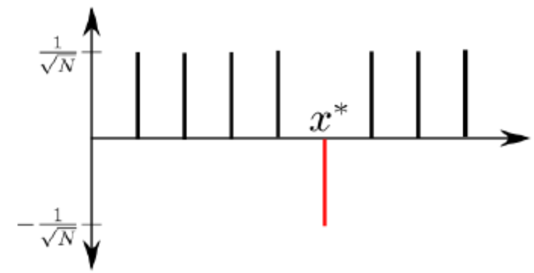


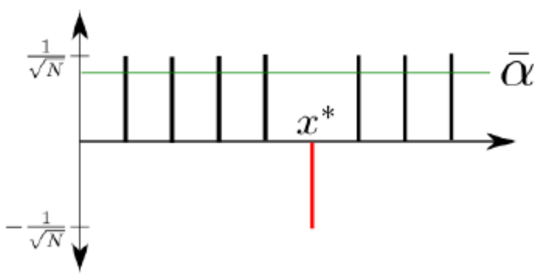


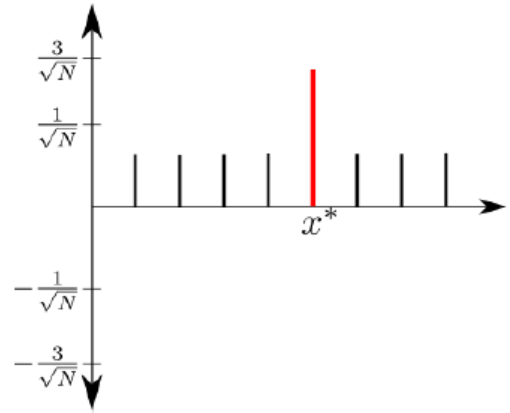


Inversion Around the Mean









$$2\mu - \alpha_{x^*}$$

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

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