Portland State University

S'20 CS410/510
Intro to quantum computing

Fang Song

Week 7

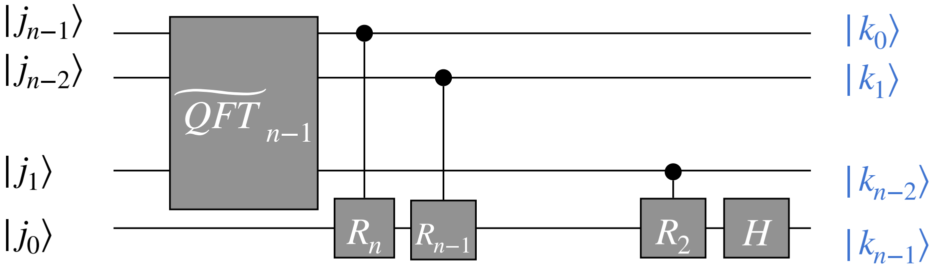
- QFT recap
- Grover's algorithm
- Optimality of Grover's alg.

Credit: based on slides by Richard Cleve

Review: QFT

$$QFT_n : |j_{n-1}j_{n-2}\ldots j_0\rangle \mapsto \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\omega_{2^n}^{jk}|k_{n-1}k_{n-2}\ldots k_0\rangle$$

$$\widetilde{QFT}_n : |j_{n-1}j_{n-2}\ldots j_0\rangle \mapsto \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}\omega_{2^n}^{jk}|k_0k_1\ldots k_{n-2}k_{n-1}\rangle$$



$cR_k |1\rangle|1\rangle$

$= |1\rangle\, \omega_{2^k} |1\rangle$

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \omega_{2^k} \end{pmatrix} \qquad \omega_{2^k} = e^{2\pi i/2^k}$$

x

Exercise

1. Let $\vec{x} = (\frac{1}{\sqrt{2}}, 0, 0, \frac{i}{\sqrt{2}})^T$. Compute $\vec{y} = F_4 \vec{x}$.

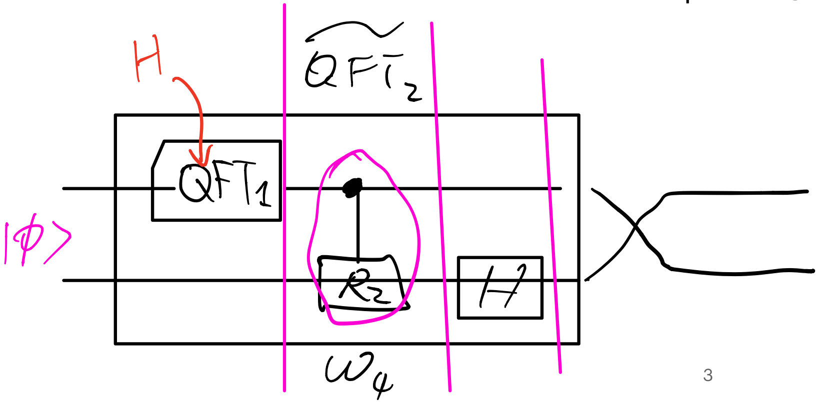
$$F_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_4 & \omega_4^2 & \omega_4^3 \\ 1 & \omega_4^2 & \omega_4^4 & \omega_4^6 \\ 1 & \omega_4^3 & \omega_4^6 & \omega_4^9 \end{pmatrix}$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1+i \\ 1+i\omega_4^3 \\ 1+i\omega_4^6 \\ 1+i\omega_4^9 \end{pmatrix}$$

$\omega_4^6 = \omega_4^2$

$\omega_4^9 = \omega_4$

2. Draw the QFT circuit implementing F_4 (i.e. QFT_2). How about $QFT_2^\dagger$?



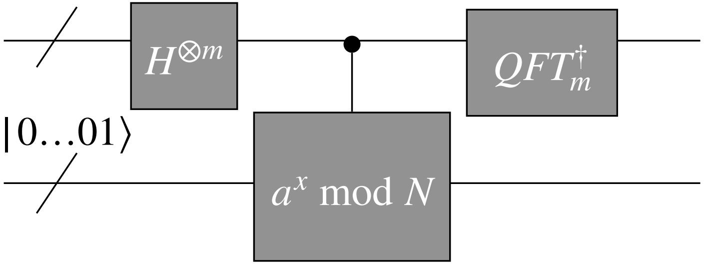
$$(\underbrace{I \otimes H}_{A}\ \underbrace{cR_2}_{B}\ \underbrace{H \otimes I}_{C})^\dagger = C^\dagger B^\dagger A^\dagger$$

$$(R_2)^\dagger = \begin{pmatrix} 1 & 0 \\ 0 & \overline{\omega_4} \end{pmatrix}$$

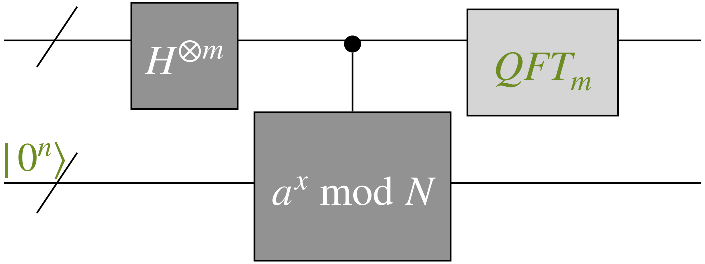
$\overline{\omega_4} = e^{-2\pi i/4}$

Quantum order finding/factorization

- Order finding à la phase estimation [Kitaev'95]



- Shor's algorithm à la quantum Fourier sampling [Shor'94]



Quantum speedup for "structured" problems

Problem	Deterministic	Randomized	Quantum
Deutsch	2	2	1
Deutsch-Josza	$2^n/2$	$O(n)$	1
Simon	$2^n/2$	$\sqrt{2^n}$	$O(n^2)$
Order-finding Factoring N	$2^{O((\log N)^{1/3}(\log\log N)^{2/3})}$		$(\log N)^3$

Oracle/Query model

- **Today. Generic quantum speedup for unstructured search.**

$a^r \equiv 1 \bmod N$

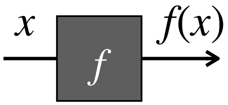
$N \mid (a^r - 1) = (a^{r/2} + 1)(a^{r/2} - 1)$

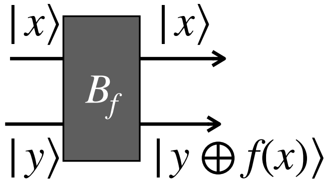
Grover's quantum search algorithm

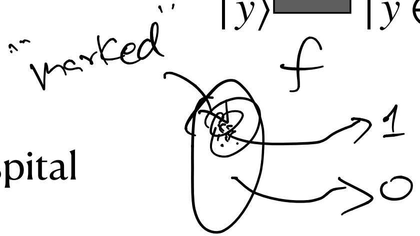
Unstructured search

Given: a black-box function $f : \{0,1\}^n \to \{0,1\}$

Goal: find x such that $f(x) = 1$ (if there is one).







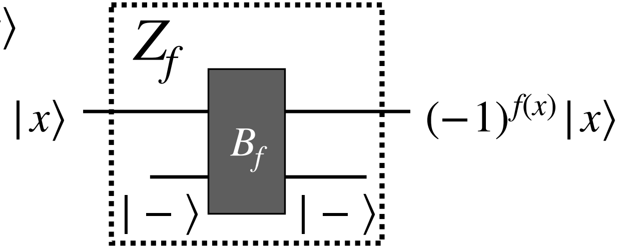
- **Example.**
  - $x \in \{0,1\}^n$ represents a record of a patient at a hospital
  - $f(x) = 1$ if x is tested positive for DIVOC-91
- **Classical algorithms: 2^n queries necessary**
- **Grover's quantum algorithm: $O(\sqrt{2^n})$ queries**

quadratic speedup

$2^{128} \longrightarrow 2^{64}$

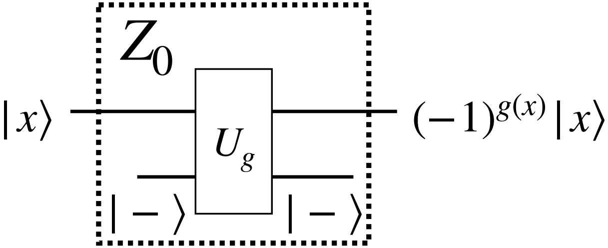
Grover's algorithm: basic operations

- $Z_f : |x\rangle \mapsto \begin{cases} -|x\rangle, & f(x) = 1 \\ \ \ |x\rangle, & f(x) = 0 \end{cases} \quad = (-1)^{f(x)}|x\rangle$



- $Z_0 : |x\rangle \mapsto \begin{cases} -|x\rangle, & x = 0^n \\ \ \ |x\rangle, & x \neq 0^n \end{cases} \quad = (-1)^{g(x)}|x\rangle$

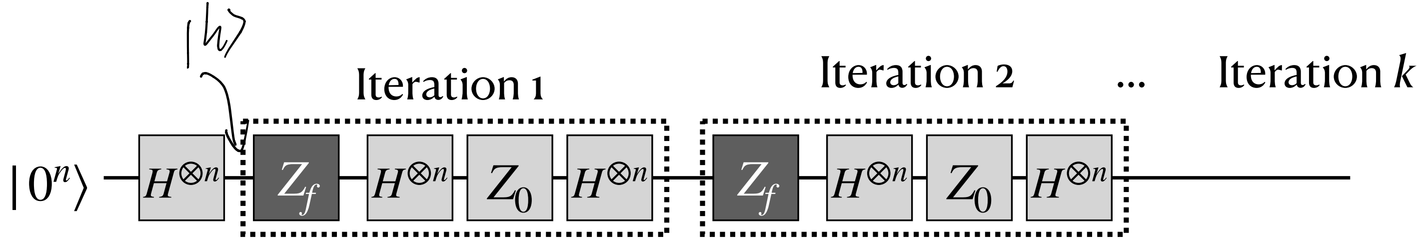
- $g(x) = 1$ **iff.** $x = 0^n$.



$x = x_1 x_2 \cdots x_n$

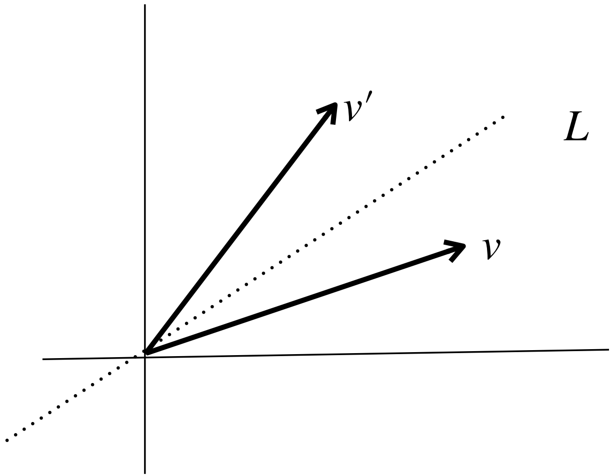
$g(x) = \neg x_1 \wedge \neg x_2 \wedge \cdots \wedge \neg x_3$

Grover's algorithm

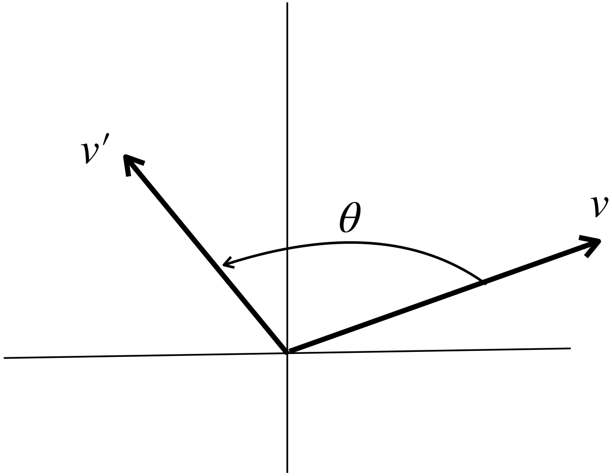


- **Prepare** $|h\rangle := H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle.$
- **Repeat** k **times:** $(HZ_0H)Z_f$.
- **Measure and get** x, **check if** $f(x) = 1$.

Reflections and rotations



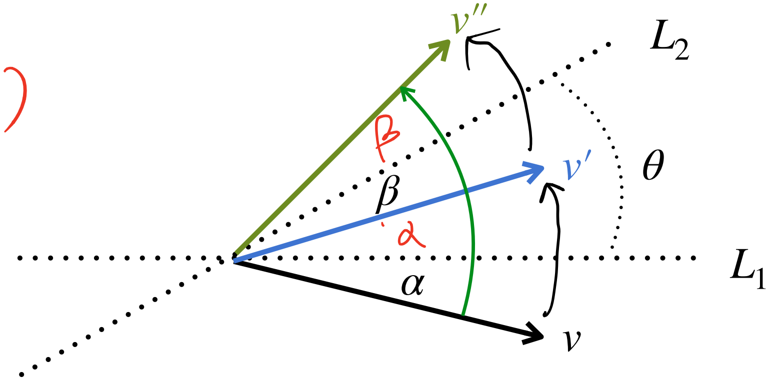
Reflection



Rotation

2 reflections = 1 rotation

$2(\alpha+\beta)$
$\parallel$
2θ

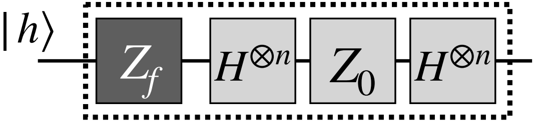


$(L_1, L_2) = \theta$

Reflection about L_1 and L_2 $\equiv$ Rotation by 2θ

Grover's algorithm: analysis

Grover Iteration

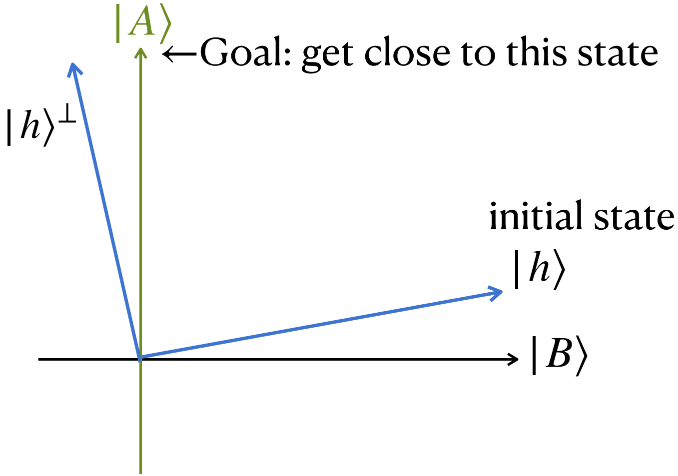


Notations

- $A := \{x \in \{0,1\}^n : f(x) = 1\}$
- $B := \{x \in \{0,1\}^n : f(x) = 0\} = \{0,1\}^n \backslash A$
- $N = 2^n, a = |A|, b = |B|$

A fundamental 2D-plane

- $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle, |B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n} |0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$
- $|h\rangle^\perp$: orthogonal to $|h\rangle$ on span$\{|A\rangle, |B\rangle\}$



Exercise

Notations

- $A := \{x \in \{0,1\}^n : f(x) = 1\}$
- $B := \{x \in \{0,1\}^n : f(x) = 0\} = \{0,1\}^n \backslash A$
- $N = 2^n, a = |A|, b = |B|. (a << N)$

A fundamental 2D-plane

- $|A\rangle := \frac{1}{\sqrt{a}} \sum_{x \in A} |x\rangle, |B\rangle := \frac{1}{\sqrt{b}} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n} |0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$
- $|h\rangle^\perp$: orthogonal to $|h\rangle$ on span$\{|A\rangle, |B\rangle\}$

1. Show that $\langle B | A \rangle = 0.$ ✓

$A \cap B = \emptyset$

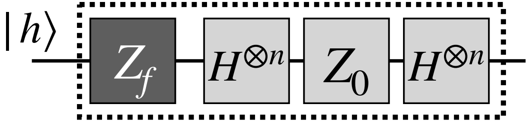
2. Find α and β so that $|h\rangle = \alpha |A\rangle + \beta |B\rangle$

$\alpha := \sqrt{\frac{a}{N}} \quad \left(|A\rangle = \frac{1}{\sqrt{N}} \sum_{x \in A} |x\rangle \right)$

$\beta := \sqrt{\frac{b}{N}} \quad \left(|B\rangle = \frac{1}{\sqrt{N}} \sum_{x \in B} |x\rangle \right)$

Grover's algorithm: analysis

Grover Iteration



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

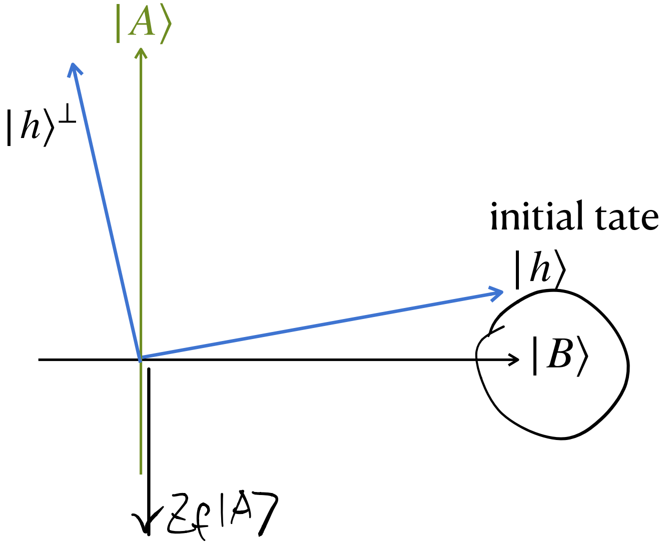
A fundamental 2D-plane

- $|A\rangle := 1/\sqrt{a} \sum_{x \in A} |x\rangle$, $|B\rangle := 1/\sqrt{b} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n} |0^n\rangle$, $|h\rangle^\perp \perp |h\rangle$

◉ **Obs. 1.** Z_f is a reflection about $|B\rangle$

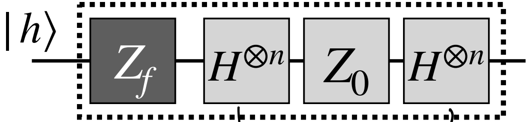
Pf: $Z_f|B\rangle = |B\rangle$

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



Grover's algorithm: analysis

Grover Iteration

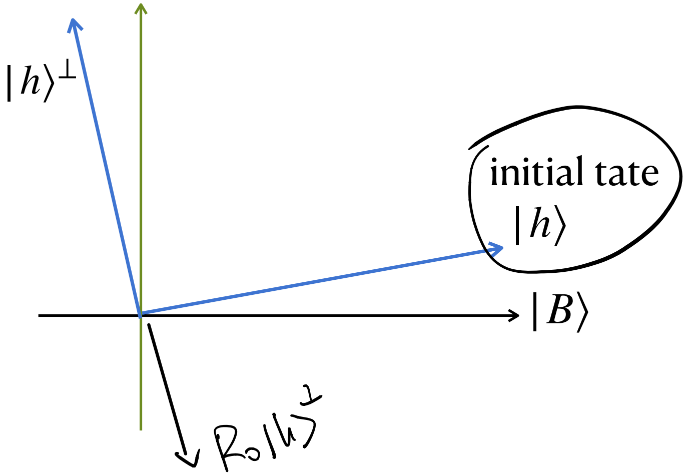


$Z_0 : |x\rangle \mapsto (-1)^{g(x)} |x\rangle$

$g(x) = 1$ iff. $x = 0^n$

A fundamental 2D-plane

- $|A\rangle := 1/\sqrt{a} \sum_{x \in A} |x\rangle$, $|B\rangle := 1/\sqrt{b} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n} |0^n\rangle$, $|h\rangle^{\perp} \perp |h\rangle$



◉ **Obs 2:** $-HZ_0H$ **is a** **reflection** **about** $|h\rangle$.

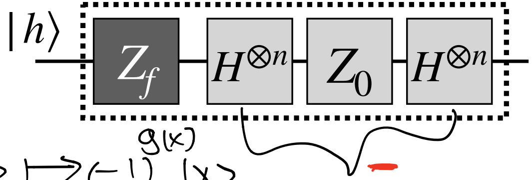
Pf: $R_0'' := -HZ_0H$

- $R_0|h\rangle = -HZ_0H|h\rangle = -HZ_0|0^n\rangle$
  $= +H|0^n\rangle$
  $= +|h\rangle$

- $R_0|h\rangle^{\perp} = -|h\rangle^{\perp}$

Grover's algorithm: analysis

Grover Iteration



$Z_0 : |x\rangle \mapsto (-1)^{g(x)} |x\rangle$

$g(x) = 1$ iff. $x = 0^n$

A fundamental 2D-plane

- $|A\rangle := 1/\sqrt{a} \sum_{x \in A} |x\rangle$, $|B\rangle := 1/\sqrt{b} \sum_{x \in B} |x\rangle$
- $|h\rangle := H^{\otimes n} |0^n\rangle$, $|h\rangle^\perp \perp |h\rangle$

◉ **Obs 2:** HZ_0H is a reflection about $|h\rangle$.

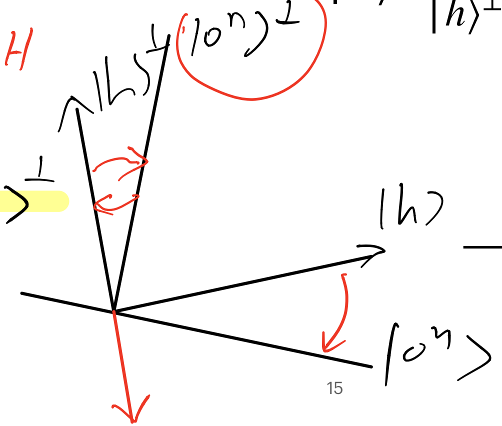
$R_0 := -HZ_0H$

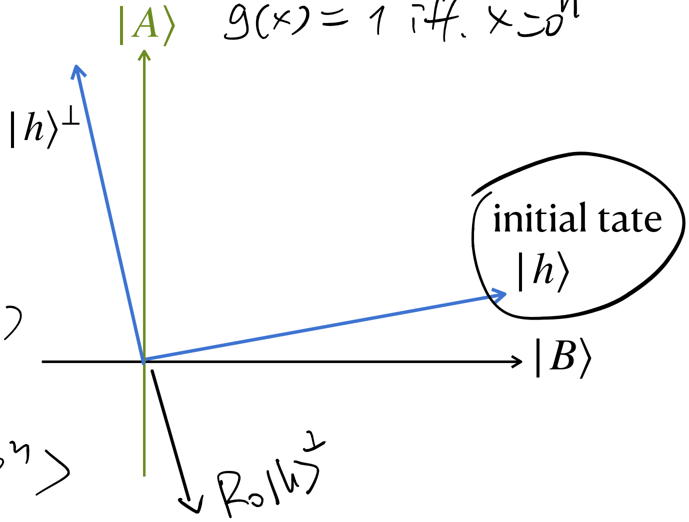
Pf:

· $R_0|h\rangle = +|h\rangle$

· $R_0|h\rangle^\perp = -|h\rangle^\perp$

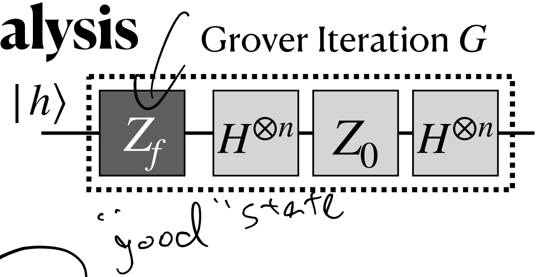
$-HZ_0H|h\rangle^\perp$

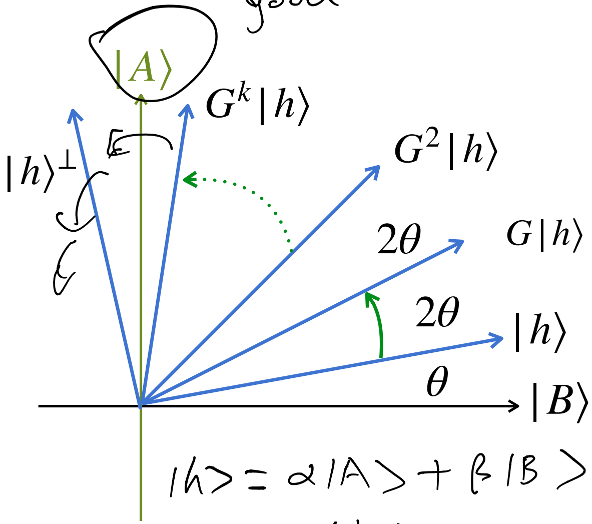




Grover's algorithm: analysis

- **Obs**. Each Grover iteration is a rotation of $2\theta, \theta = sin^{-1}\left(\sqrt{a/N}\right)$. $a \ll N$
- **Goal**: $(2k+1)\theta \approx \pi/2$
- **Theorem**. $k = \Omega(\sqrt{N/a})$ suffice for $\Omega(1)$ success prob.





$$(2k+1)\theta \approx \pi/2$$

$$k \approx \frac{\pi}{4\theta} - \frac{1}{2}$$

$$\approx \frac{\pi}{4} \cdot \sqrt{N/a}$$

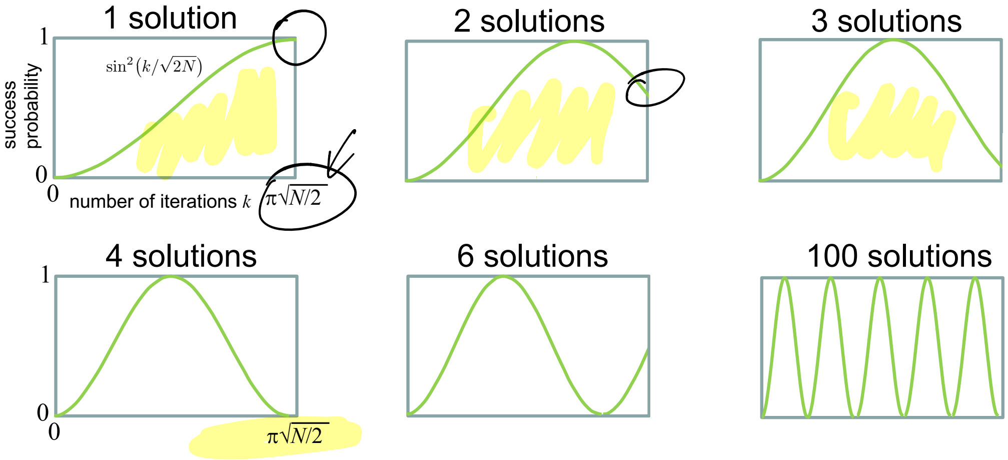
$$\theta \approx \sin\theta = \sqrt{\frac{a}{N}}$$

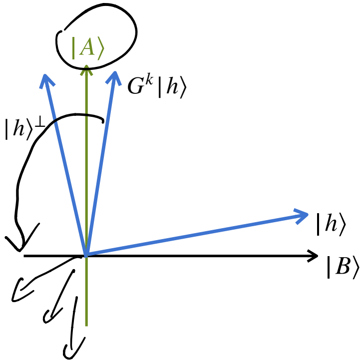
$a = 1$ $\sqrt{N}$

$$|h\rangle = \alpha|A\rangle + \beta|B\rangle$$

$$\sin\theta = \langle h|A\rangle = \alpha = \sqrt{\frac{a}{N}}$$

Unknown number of solutions





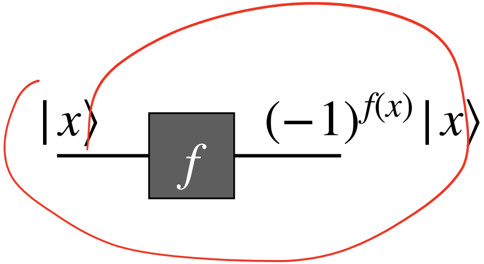
- **One approach: if random k, then success prob. is the area under the curve**
  - ... It turns out to be always > 0.4
- **Read more if interested https://arxiv.org/abs/1709.01236**

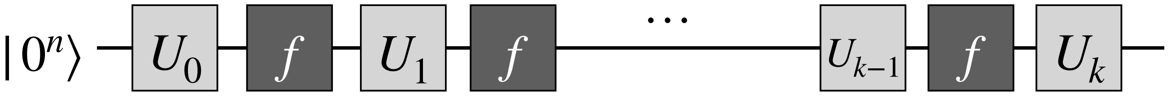
Optimality of Grover's algorithm

An unfortunate news ...

- **Theorem**. Any quantum algorithm must make $\Omega(\sqrt{2^n})$ queries to f (assuming a single marked item).

- A k-query quantum algorithm if of the form below
  - $f = Z_f : |x\rangle \mapsto (-1)^{f(x)}|x\rangle$
  - $U_0, U_1, \ldots, U_k$ are arbitrary unitary operations

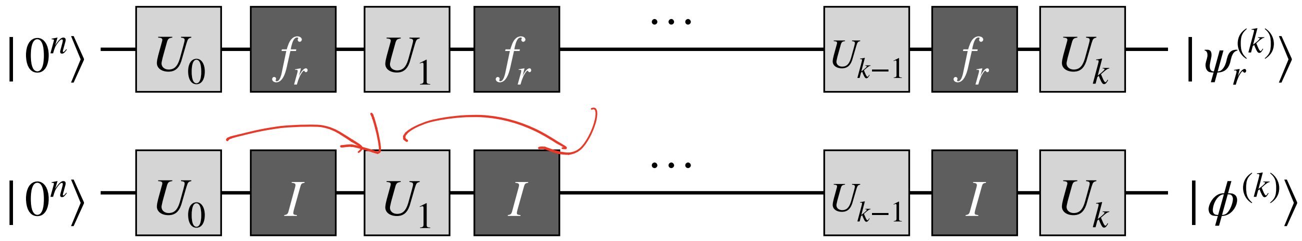




$H^{\otimes n}$

Optimality of Grover's algorithm: proof sketch

- For every $r \in \{0,1\}^n$, let $f_r : \{0,1\}^n \to \{0,1\}$ be such that $f_r(x) = 1$ iff. $x = r$.



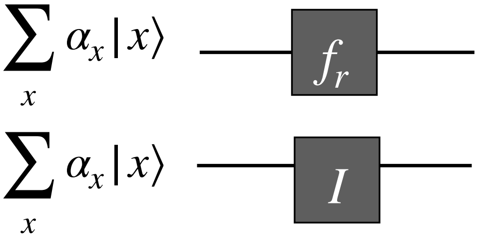
$\frac{1}{2} \leq$

- Averaging over $r \in \{0,1\}^n$, $\| |\psi_r^{(k)}\rangle - |\phi^{(k)}\rangle \| \leq 2k/\sqrt{2^n}$ $\Rightarrow k \geq \sqrt{2^n}/4$
  - each query only drifts the states apart by a tiny bit

Exercise

1. Show that $\| |\psi\rangle - |\phi\rangle \| \leq 2|\alpha_r|$

$f_r(x) = 1$ iff. $x = r$.



$$|\psi\rangle = f_r\Big(\sum_{x \neq r} \alpha_x |x\rangle\Big) + f_r\, \alpha_r |r\rangle = \sum_{x \neq r} \alpha_x |x\rangle - \alpha_r |r\rangle$$

$$|\phi\rangle = \mathbb{1}\big(\quad\big) = \sum_{x \neq r} \alpha_x |x\rangle + \alpha_r |r\rangle$$

$$\Rightarrow \quad \| |\psi\rangle - |\phi\rangle \|$$

$$= \| -\alpha_r |r\rangle - \alpha_r |r\rangle \|$$

$$= 2|\alpha_r|$$

Logistics

- **HW5 due Sunday**
  - One more to go! Keep up the good work
- **Project [Sign up on google spreadsheet]**
  - Week8. Progress check-up
    - Office hour + after Friday's lecture: mandatory meetings. Sign up ASAP.
  - Week10. Presentations
    - Office hour: voluntary meetings, sign up as you wish
    - Friday's lecture: presentations from you! Sign up a slot ASAP. Details to follow.

Discussion: quantum factoring experiments

- **[SSV13] Oversimplifying quantum factoring**
  - What are the main critique of prior experiments?

- **[MNM+16] Realization of a scalable Shor algorithm**
  - Does it address adequately the criticisms in the SSV13? Why and why not?

- **Recent estimate on quantum Factoring [hear more from a final presentation]**

Scratch