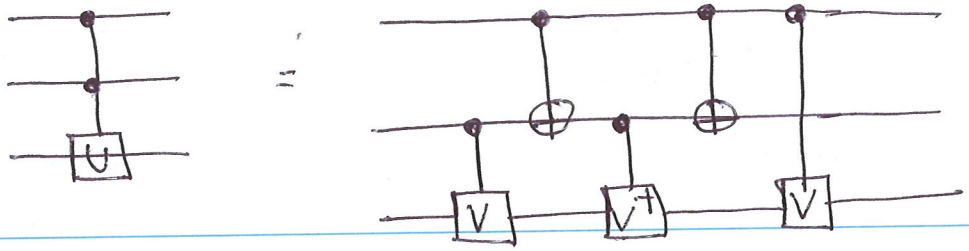
Lec7 Thm.

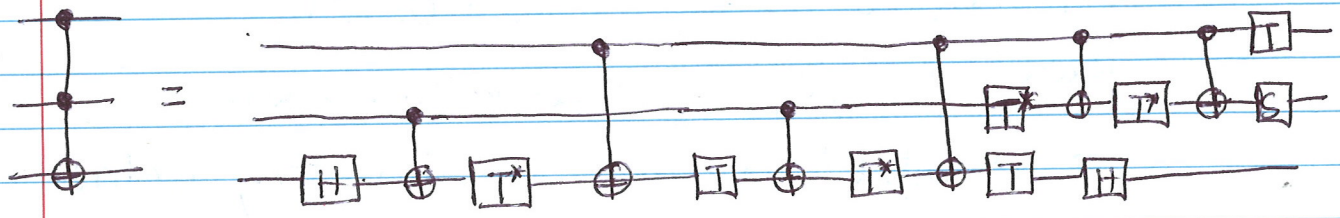


where.

$V^2 = U$

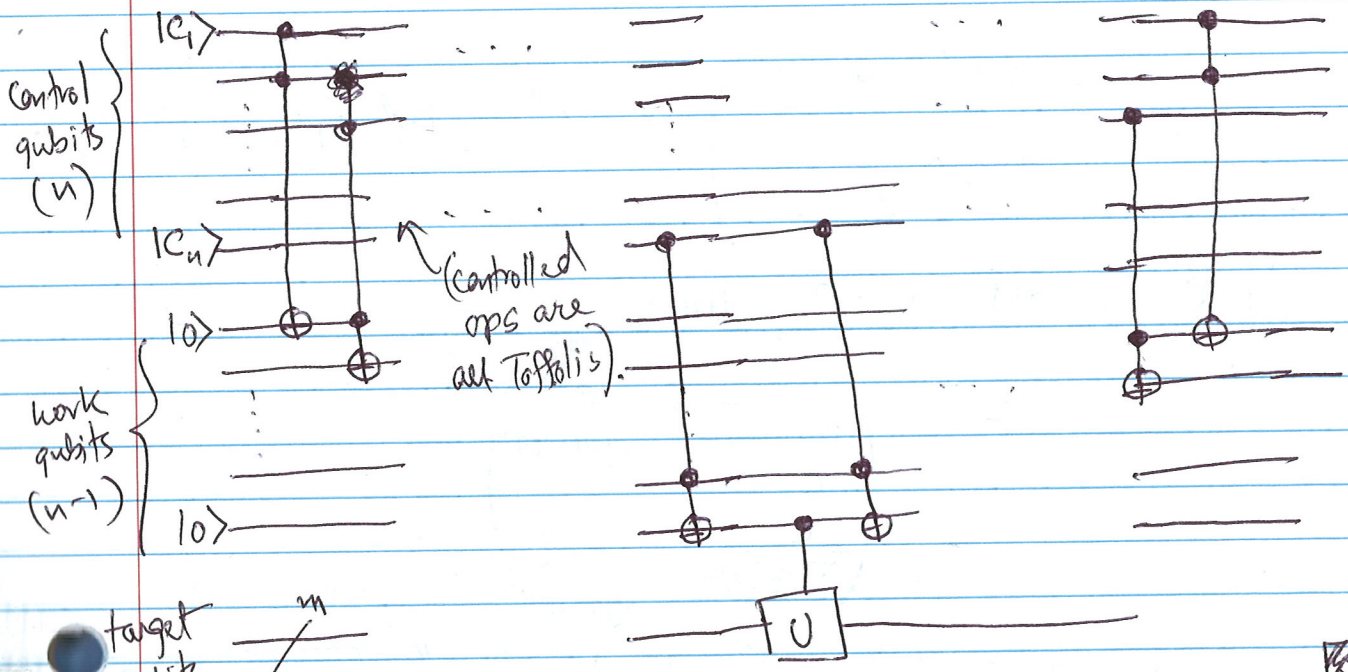
Pf: Check on basis states. ∎

Toffoli gate

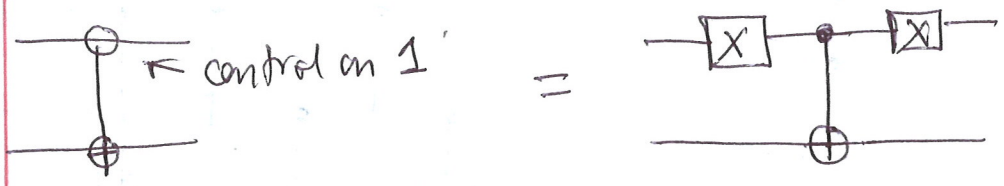


Pf: Check on basis states.

Q. What about general $C^n(U)$?



[Check on basis states]. ∎

Ex. 

>>>

Thm: Two level unitary gates are universal.

Pf. $\begin{pmatrix} a & d & g \\ b & e & h \\ c & f & j \end{pmatrix} = U$

Strategy: $U_3 U_2 U_1 U = I \Rightarrow U = U_3^\dagger U_2^\dagger U_1^\dagger$

where U_1, U_2, U_3 are 2-level unitary matrices

$\Rightarrow U_1^\dagger, U_2^\dagger, U_3^\dagger$ are also 2-level unitary matrices.

- if $a=b=0$ or $b=0$, set $U_1 = I$.
- else set $U_1 = \begin{pmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$

$$U_1 U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f & j \end{pmatrix}, \quad a' = \sqrt{|a|^2+|b|^2} \in \mathbb{R}$$

- if $c=0$, set $U_2 = I$,
- else set $U_2 = \begin{pmatrix} \frac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{pmatrix}$

$$U_2 U_1 U = \begin{pmatrix} a'' & d'' & g'' \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix}, \quad a'' = \sqrt{|a'|^2+|c'|^2} \in \mathbb{R}$$

But U_2U_1U is unitary.

$\Rightarrow a'' = 1, \quad d'' = g'' = 0.$

$$\therefore \quad U_2U_1U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix}$$

- now both $e'', f'' \neq 0$.

so choose. $U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{e''^*}{\sqrt{|e''|^2+|f''|^2}} & \frac{f''^*}{\sqrt{|e''|^2+|f''|^2}} \\ 0 & \frac{f''}{\sqrt{|e''|^2+|f''|^2}} & \frac{-e''}{\sqrt{|e''|^2+|f''|^2}} \end{pmatrix}$

So $U_3U_2U_1U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & j''' \end{pmatrix}$

- Set $U_3' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & j'''^* \end{pmatrix}$

- So $(U_3'U_3)U_2U_1U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.$

But $U_3'U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix} \rightarrow U_3$

- $U_3U_2U_1U = I.$

This procedure can be performed for any $n \times n$ unitary matrix. ∎

Q. For a general $n \times n$ unitary, how many 2-level unitaries needed?

A. $(n-1) + (n-2) + \cdots + 1 = \frac{n(n-1)}{2}$.

$\Rightarrow$ For n-qubit system, # of 2-level unitaries required

$= \boxed{2^{n-1}\left(2^{n-1}-1\right)}$ (**).

[Ex: Prove that $\forall$ $d \times d$ unitary matrix U which cannot be decomposed as a product of fewer than $d-1$ 2-level unitaries].

— Follows by studying sparsity patterns.

>>> Single qubit & CNOT gates are universal.

Suppose U is a 2-level unitary that acts non-trivially on computational basis states $|s\rangle$ and $|t\rangle$ on n-qubits, given by:

$s = s_1 \cdots s_n$, $t = t_1 \cdots t_n$.

— Basic construction: Construct a gray code connecting $|s\rangle$ and $|t\rangle$.

- $g_1, \ldots, g_m$ is Gray code connecting s and t.

  So $g_1 = s$, $g_m = t$

- g_i, g_{i+1} differ in only 1-bit.

— $m+1 = \text{Ham}(s,t)$ ← Hamming dist.

Next implement the following unitaries.

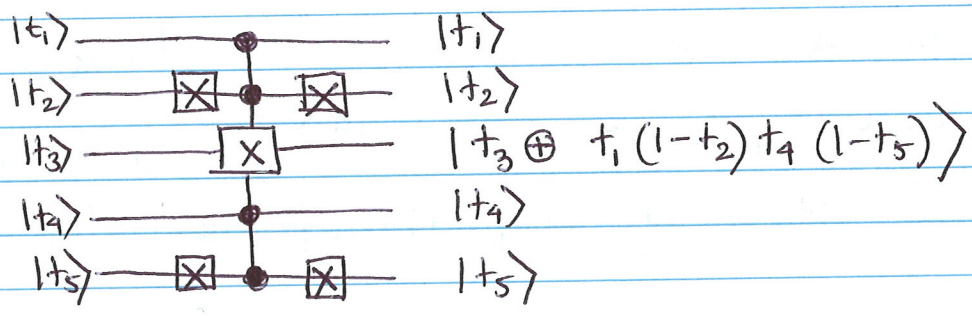
- Controlled SWAP operations (Phase 1)

$|g_1\rangle \rightarrow |g_2\rangle \rightarrow \cdots \rightarrow |g_{m-1}\rangle$

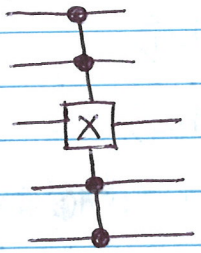
- During each swap, for e.g. $|g_i\rangle \rightarrow |g_{i+1}\rangle$ if g_i, g_{i+1} differ in q^{th} bit, then swap is achieved by a controlled NOT (CNOT) of q^{th} qubit, conditional on other qubits having the values in g_i, g_{i+1}.

e.g. Let $n=5$.

$|g_1\rangle = |1\,0\,0\,1\,0\rangle$, $|g_2\rangle = |1\,0\,1\,1\,0\rangle$



- We saw before how to perform operations such as



- End result after 1st stage of swaps.

$|g_1\rangle \rightarrow |g_{m-1}\rangle$
$|g_2\rangle \rightarrow |g_1\rangle$
$|g_3\rangle \rightarrow |g_2\rangle$, other basis states left unchanged.
$\vdots$
$|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle$.

- Now perform controlled $\tilde{U}$, where $\tilde{U}$ is 2×2 submatrix of 2-level unitary U, that is non-trivial.
  - if g_{m-1}, g_m differ in j^{th} bit, we do controlled-$\tilde{U}$ on j^{th} qubit, conditioned on other qubits being in same values as in g_{m-1}, g_m.
- Specifically if $\tilde{U} = \begin{array}{c|cc} & g_{m-1} & g_m \\ \hline g_{m-1} & a & b \\ g_m & c & d \end{array}$ (Phase 2)
  then we want,

$$|g_{m-1}\rangle \rightarrow a|g_{m-1}\rangle + b|g_m\rangle$$
$$|g_m\rangle \rightarrow c|g_{m-1}\rangle + d|g_m\rangle$$

  - all other basis states unchanged.

- Now fix the swaps. (Phase 3)
  $|g_{m-1}\rangle \rightarrow |g_{m-2}\rangle \rightarrow \cdots \rightarrow |g_1\rangle$, by reversing the first stage of swap circuit basically.

- End result

$$|g_1\rangle \rightarrow a|g_1\rangle + b|g_m\rangle$$
$$|g_m\rangle \rightarrow c|g_1\rangle + d|g_m\rangle$$

all other basis states left unchanged.

- Phase 2 can be performed by a controlled $\tilde{U}$ op. using single qubit & CNOT gates.

Thus we have proved that single qubit & CNOT gates are universal ∎ (**).

E.g. Suppose we want to implement the following 2-level unitary ($n=3$).

$|000\rangle \rightarrow a|000\rangle + b|111\rangle$

$|111\rangle \rightarrow c|000\rangle + d|111\rangle$

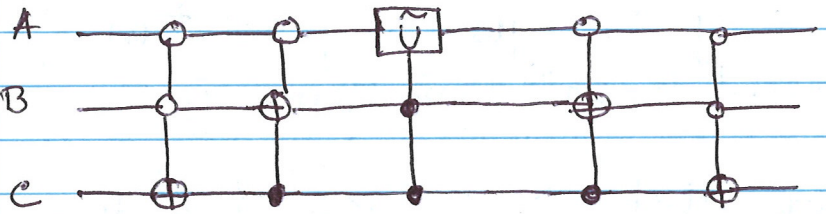
other basis states unchanged.

$\tilde{U} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

Gray code:

A	B	C	
0	0	0	$\|g_1\rangle$
0	0	1	$\|g_2\rangle$
0	1	1	$\|g_3\rangle$
1	1	1	$\|g_4\rangle$.

Circuit:



Resource Estimates

- Each swap ~ $O(n)$ quantum gates
- Controlled-$\tilde{U}$ ~ $O(n)$ quantum gates
- $2(n-1)$ swaps at most $\Rightarrow O(n^2)$ quantum gates to implement a 2-level unitary.
- For general U, $O(4^{n-1})$ 2-level unitaries.

$\Rightarrow O(n^2 4^n)$ CNOT & single qubit gates.

What we achieved so for?

- Any unitary U can be implement using $O(n^2 4^n)$ CNOT & single qubit quantum gates.
- We see how CNOT gate entered the discussion
- Only thing remaining to do: how to implement single qubit quantum gates.

Next time ▸ $H + \frac{\pi}{8}$ gates are universal in $SU(2)$
▸ Solovay-Kitaev theorem.

Thm: Consider rotation $R_{\hat{n}}(\theta)$, where θ is an irrational multiple of 2π. Then any rotation $R_{\hat{n}}(\delta)$ can be approximated to arbitrary accuracy.

Pf. Suffices to show that $\{k\theta : k \in \mathbb{Z}\}$ is dense in $[0, 2\pi)$.

(Proof of claim) Because then $\exists\ \theta_i \to \delta$.

So, $$R_{\hat{n}}(\theta_i) - R_{\hat{n}}(\delta) = \left(\cos\frac{\theta_i}{2} - \cos\frac{\delta}{2}\right) I - i\left(\sin\frac{\theta_i}{2} - \sin\frac{\delta}{2}\right)(\hat{n}\cdot\vec{\sigma})$$

$$\Rightarrow \| R_{\hat{n}}(\theta_i) - R_{\hat{n}}(\delta) \| \leq \left|\left(\cos\frac{\theta_i}{2} - \cos\frac{\delta}{2}\right)\right| \|I\| + \left|\left(\sin\frac{\theta_i}{2} - \sin\frac{\delta}{2}\right)\right| \|\hat{n}\cdot\vec{\sigma}\|$$

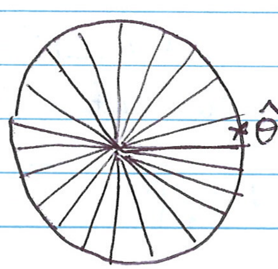
As $\sin\theta$, $\cos\theta$ are continuous,

$$\cos\frac{\theta_i}{2} \to \cos\frac{\delta}{2}, \quad \sin\frac{\theta_i}{2} \to \sin\frac{\delta}{2}$$

$\Rightarrow R_{\hat{n}}(\theta_i) \rightarrow R_{\hat{n}}(\delta)$.

Proof that $\{k\theta : k \in \mathbb{Z}\}$ is dense in $[0, 2\pi)$.

[Give some intuition of this process to the class].



— Divide 2π into N intervals s.t $\frac{2\pi}{N} \leq \delta$, (for δ chosen & fixed).

— Consider $\{k\theta : \theta = 1, \ldots, N+1\}$ (mod 2π)

— By pigeon-hole principle, atleast 1 interval contains two points $k_1\theta, k_2\theta$, let $k_2 > k_1$

— Then $(k_2 - k_1)\theta \pmod{2\pi} < \delta$.

$$\underset{\hat{\theta}}{\overset{\|}{(k_2 - k_1)\theta}}$$

— $\hat{\theta}$ is a multiple of θ

— By taking multiples of $\hat{\theta}$ each interval contains a point which is a multiple of $\hat{\theta}$ (hence θ).

— As δ was arbitrary, this completes the proof. ∎

>>> Approximating arbitrary unitary gates is ~~arbitrary~~ hard.

> Q. How many gates does it take to generate an arbitrary state of n-qubits.

— Suppose we have g different gates,

— f different inputs for each gate.

$\therefore$ for each gate there are $\left(\frac{n!}{(n-f)!}\right)^g$ ways to connect the qubits.

$\sim O(n^{fg})$.

- f, g fixed by computing hardware.
- If m gates in quantum circuit, then we can create at most $O(n^{fgm})$ distinct unitaries.

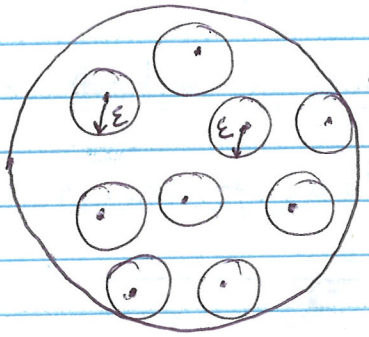
Basic idea:

Consider the set of all unitaries that take $|0\rangle \to |x\rangle$ where $|x\rangle$ is all possible states: call this set Q.

Fact: for each $|x\rangle$ such a unitary exist (prove in class).

- We will prove a lower bound on m for Q, which will imply at lower bound for all unitaries.
- measure error in 2-norm.
- Using $m(f,g,m)$ we can reach at most $O(n^{fgm})$ distinct points $|x\rangle$.
- $|x\rangle \in \mathbb{S}^{2^{n+1}-1}$ (because of normalization)

ε-net construction



- ε-balls around each point reached.
- These balls must cover the sphere.

Because, for $U \in Q$, if $\tilde{U}$ is an approx of U s.t. $\|U - \tilde{U}\|_2 \leq \varepsilon \Rightarrow \|U|0\rangle - \tilde{U}|0\rangle\|_2 \leq \varepsilon$.

$\stackrel{\text{def}}{=} \max_{|x\rangle} \|(U-\tilde{U})|x\rangle\|_2$

- Vol. of K-sphere: $V_K(r) = \frac{2\pi^{(K+1)/2} r^{K+1}}{(K+1)\Gamma\left(\frac{K+1}{2}\right)}$

- surface area of K-sphere: $S_K(r) = \frac{2\pi^{(K+1)/2} r^K}{\Gamma\left(\frac{K+1}{2}\right)}$.

- Area covered by balls of radius $\varepsilon \approx V_{2^{n+1}-2}(\varepsilon)$. (when ε is small).

- To cover the sphere need:

$$\frac{S_{2^{n+1}-1}(1)}{V_{2^{n+1}-2}(\varepsilon)} \geq c(n)\left(\frac{1}{\varepsilon^{2^{n+1}-1}}\right)$$

points.

$$O(n^t g^m) \geq \Omega\left(\frac{1}{\varepsilon^{2^{n+1}-1}}\right)$$

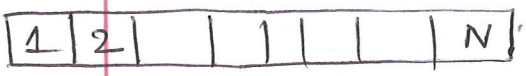
$$\Rightarrow m = \Omega\left(\frac{2^n \log(1/\varepsilon)}{\log n}\right).$$

This is a lower bound on gate complexity.

Grover's Search

$N = 2^n$ elements in an unstructured database.

- classically need $O(N)$ reads into database to find an element
- If database search can be done using quantum memory, search can be performed using $O(\sqrt{N})$ oracle calls.



- N items
- M are marked.

$$f(x) = \begin{cases} 1 & \text{if } x \text{ is marked} \\ 0 & \text{if } x \text{ is unmarked.} \end{cases}$$

Oracle

$$|x\rangle |q\rangle \xrightarrow{O} |x\rangle |q \oplus f(x)\rangle$$

← unitary operation.

$|x\rangle$: n-qubits; $|q\rangle$: 1-qubit

bit is flipped if $f(x)$ is a marked item.

One way to realize this is by:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{O} (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right).$$

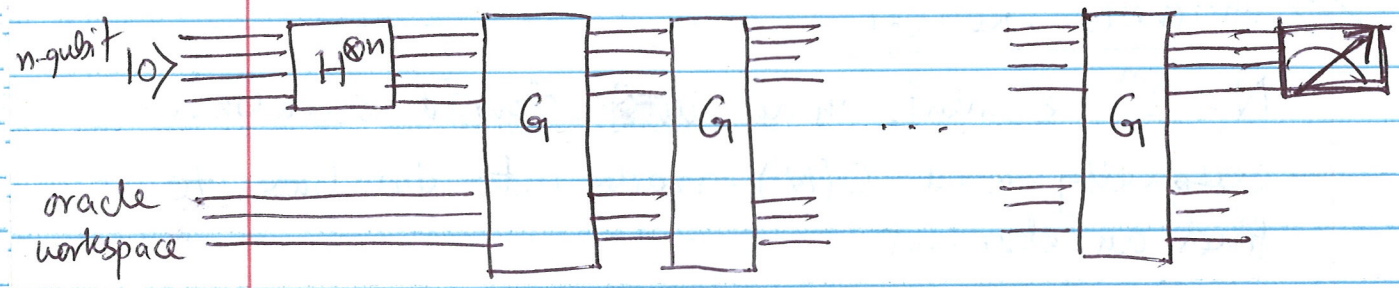
↑ unitary operation.

Then can ignore the qubit $|q\rangle$ as it doesn't change in the process.

Thus, simplified working of the oracle is

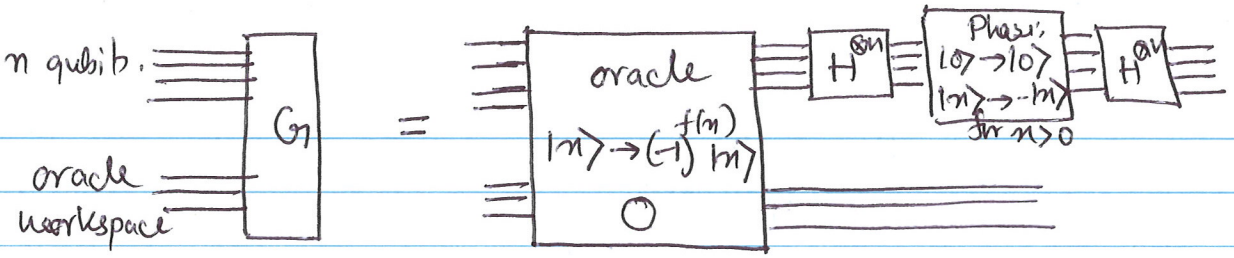
$$\boxed{|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle}$$

Grover Search Circuit



$O(\sqrt{N/M})$ Grover oracle calls.

Grover iteration



- Apply oracle
- Apply $H^{\otimes n}$
- Conditional phase shift (all states except $|0\rangle$ picking up phase of -1)
- Apply $H^{\otimes n}$.

▶ Phase: $|0\rangle \to |0\rangle$, $|x\rangle \to -|x\rangle$ for $x>0$ $= 2|0\rangle\langle 0| - I$

▶ $H^{\otimes n}\left(2|0\rangle\langle 0| - I\right)H^{\otimes n} = 2\left(H^{\otimes n}|0\rangle\right)\left(\langle 0|H^{\otimes n}\right) - I$

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

$\equiv |\psi\rangle$

So, $H^{\otimes n}\left(2|0\rangle\langle 0| - I\right)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$.

▶ $G = \left(2|\psi\rangle\langle\psi| - I\right)O$ ← O is oracle.

[Ex: $\left(2|\psi\rangle\langle\psi| - I\right)\left(\sum_k \alpha_k |k\rangle\right) = \sum_k \left(-\alpha_k + 2\langle\alpha\rangle\right)|k\rangle$

where $\langle\alpha\rangle = \sum_k \alpha_k / N$]

**(Thus: $\left(2|\psi\rangle\langle\psi| - I\right)$ is also called "inversion about mean" operation).

Geometric Visualization

$$G = (2|\psi\rangle\langle\psi| - I)\,O$$

↑ Householder transformation

Define: $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x{}'' |x\rangle$ ← unmarked items

$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_x{}' |x\rangle$ ← marked items.

$\langle |\alpha\rangle, |\beta\rangle \rangle = 0.$

both are uniform superposition.

$$|\psi\rangle = \underbrace{\frac{\sqrt{N-M}}{\sqrt{N}}}_{p} |\alpha\rangle + \underbrace{\frac{\sqrt{M}}{\sqrt{N}}}_{q} |\beta\rangle \in \text{span}\{|\alpha\rangle, |\beta\rangle\}.$$

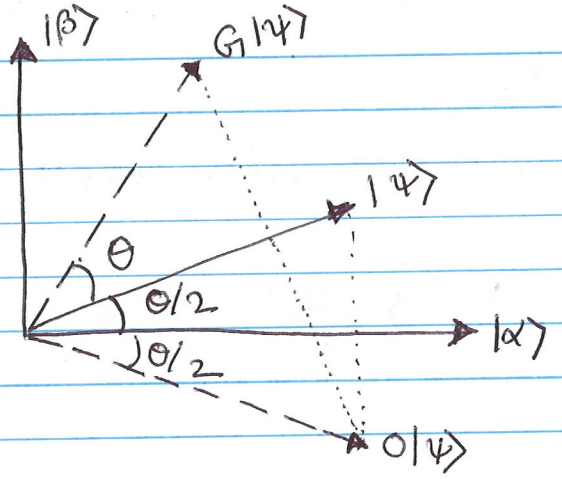
Fact: $G^k|\psi\rangle \in \text{span}\{|\alpha\rangle, |\beta\rangle\}$ for all k.

Pf: $|\phi\rangle = a|\alpha\rangle + b|\beta\rangle$

$O|\phi\rangle = a|\alpha\rangle - b|\beta\rangle \in \text{span}\{|\alpha\rangle, |\beta\rangle\}$

$$\begin{aligned}
&(2|\psi\rangle\langle\psi| - I)|\phi\rangle \\
&= (2|\psi\rangle\langle\psi| - I)(a|\alpha\rangle + \beta|\beta\rangle) \\
&= -|\phi\rangle + 2(p|\alpha\rangle + q|\beta\rangle)(p^*\langle\alpha| + q^*\langle\beta|) \\
&\qquad (a|\alpha\rangle + b|\beta\rangle) \\
&= -|\phi\rangle + 2(pa + qb)(p|\alpha\rangle + q|\beta\rangle) \\
&\in \text{span}\{|\alpha\rangle, |\beta\rangle\}.
\end{aligned}$$

- O is a reflection about $|\alpha\rangle$
- $(2|\psi\rangle\langle\psi| - I)$ is a reflection about $|\psi\rangle$.



Define: $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$, $\sin\frac{\theta}{2} = \sqrt{\frac{M}{N}}$

$= p$ $\quad = q$

Then, $|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$

$G|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle$

$$G^k|\psi\rangle = \cos\left(\left(\frac{2k+1}{2}\right)\theta\right)|\alpha\rangle + \sin\left(\left(\frac{2k+1}{2}\right)\theta\right)|\beta\rangle.$$

Case: $M = N/4$ is interesting!

$k=1$ needed $G^1|\psi\rangle = |\beta\rangle$. Measurement gives a marked item.

Prob. of getting a marked item: $\sin^2\left(\left(\frac{2k+1}{2}\right)\theta\right) \cdot \frac{M}{M}$

$= \sin^2\left(\left(\frac{2k+1}{2}\right)\theta\right)$.

Basic question: What should be k? } Next class (Easy analysis).

Ans: $O\left(\sqrt{\frac{N}{M}}\right)$