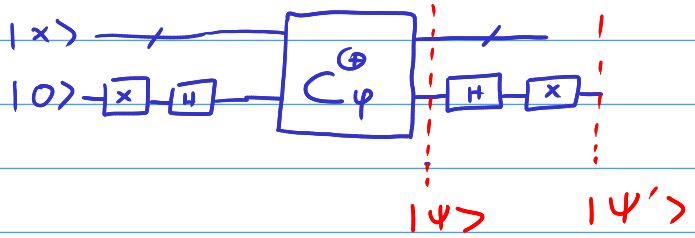
I - Homework

1. Via the construction seen in class, it is easy, given a formula φ to construct a circuit C_φ (with ancillas) such that $C_\varphi^{\oplus} |x\rangle|b\rangle = |x\rangle|\varphi(x)\oplus b\rangle$

We can then construct $C_\varphi^{\text{phase}} |x\rangle = (-1)^{\varphi(x)} |x\rangle$ (with ancillas) by



$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|x\rangle|0\oplus\varphi(x)\rangle - |x\rangle|1\oplus\varphi(x)\rangle \right)$$
$$= \frac{1}{\sqrt{2}} |x\rangle \left((-1)^{\varphi(x)} |-\rangle \right)$$

So $|\psi'\rangle = (-1)^{\varphi(x)} |x\rangle|0\rangle$ □

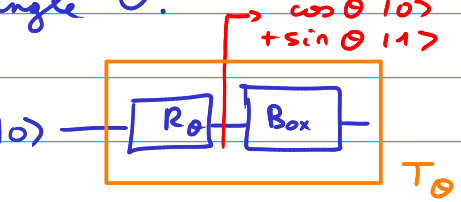
We then use Grover with $Z_g = C_\varphi^{\text{phase}}$, then if $\varphi \in SAT$, Grover returns x / $\varphi(x)=1$ in $O(\sqrt{N})$ queries
else, Grover fails in $O(\sqrt{N})$ "

Each query uses $O(|\varphi|)$ - gates, so in total:
$O(2^{n/2}|\varphi|)$ in size.

2. The Bomb:

Let R_θ = rotation of angle θ.

Take a look at the circuit



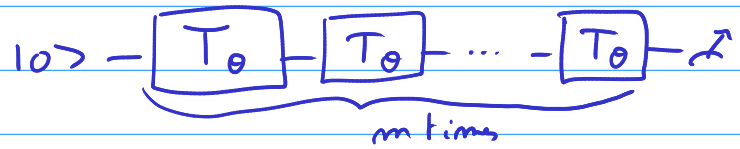
If NO BOMB, $\equiv$ $|0\rangle - R_\theta - \cos\theta|0\rangle + \sin\theta|1\rangle$

If BOMB, with probability $(\sin\theta)^2$, explosion
else, output $|0\rangle$

Let $\varepsilon > 0$ be the probability with which we want to win (and live).

Let $m \in \mathbb{Z}$ such that $\varepsilon \geq \frac{\pi^2}{4m}$. Let $\theta = \frac{\pi}{2m}$

We are going to apply T_θ m times:



If NO BOMB, then $T_\theta \equiv R_{\frac{\pi}{2m}}$

and hence

$$(T_\theta)^m = R_{\pi/2}$$

So $T_\theta^m |0\rangle = |1\rangle$, we measure 1 w.p. 1

If BOMB, then at each application of T_θ we explode with probability $(\sin\theta)^2 \leq \theta^2 = \frac{\pi^2}{4m^2}$

We then never explode with probability

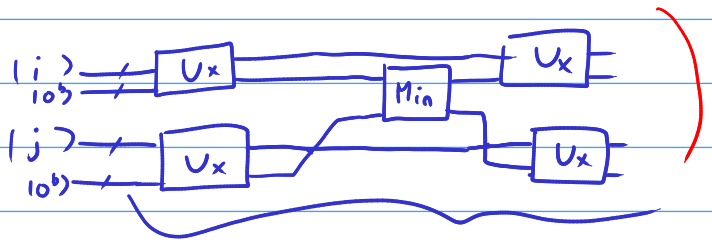
$$\leq m \cdot \theta^2 = \frac{\pi^2}{4m} \leq \varepsilon$$

In that case, $T_\theta = I$ so we measure 0 w.p. 1.

We can take $m = \left\lceil \frac{\pi^2}{4\varepsilon} \right\rceil$ □

IV LIST MIN

1. There is a classical algo that on input x, y returns "$x < y$", we can then use the quantum gate



$$|i\rangle|j\rangle|0^?\rangle = (-1)^{\quad} |i\rangle|j\rangle|0^?\rangle$$

Then Grover using the above circuit with fixed i.
If rank $(x_i) = r$, there are $r-1$ elements j s.t. $x_j < x_i$ so Grover runs in time

$O\left(\sqrt{\frac{N}{r-1}}\right)$ calls to Comp

so $O\left(\sqrt{\frac{N}{r}}\right)$ calls to U_x

2. a) Worst case, $x_{i_0} > x_{i_1} > \cdots > x_{i_{N-1}} = \min$

$$\Rightarrow O\left(\sum_{i=1}^{N} \sqrt{\frac{N}{i}}\right) = O\left(\sqrt{N} \sum_{i=1}^{N} \frac{1}{\sqrt{i}}\right)$$

$$= O\left(\sqrt{N} \cdot \sqrt{N}\right) = O(N)$$

$\sum_{i=1}^{N} \frac{1}{\sqrt{i}} = O(\sqrt{N})$ can be proven by Sum / Integral comparison.

b) $p(r, N) = \mathbb{P}$(rank r is picked when there are N elements looked into)

Clearly, $p(r, 1) = \begin{cases} 0 \text{ if } r > 1 \\ 1 \text{ if } r = 1 \end{cases}$

Now assume that $\forall r \in \mathbb{N} \quad p(r, N) = \frac{1}{r}$

$$p(r, N+1) = \mathbb{P}(r \text{ picked on the random choice}) + \mathbb{P}(r \text{ picked after})$$

$$= \frac{1}{N+1} + \sum_{i=1}^{N+1} \mathbb{P}(r \text{ picked after} / i \text{ is chosen}) \cdot \frac{1}{N+1}$$

$$= \frac{1}{N+1} + \sum_{i=1}^{N+1} \frac{1}{N+1} p(r, N-i)$$

$$= \frac{1}{N+1} + \sum_{i=r+1}^{N+1} \frac{1}{N+1} \cdot \frac{1}{r} = \frac{1}{N+1}\left(1 + \frac{N+1-r}{r}\right)$$

$$= \frac{1}{N+1} \cdot \frac{N+1}{r} = \frac{1}{r}$$

□

c. Expected number of query Q :

$$\mathbb{E}(Q) \leq \sum_{r=1}^{N} p(r, N) \cdot C \cdot \sqrt{\frac{N}{r}}$$

$$= C \cdot \sqrt{N} \cdot \left(\sum_{r=1}^{N} \frac{1}{r\sqrt{r}}\right) \quad cv = O(1)$$

$$= O(\sqrt{N})$$

□

d. Markov $\quad \mathbb{P}(Q \geq t \cdot \mathbb{E}(Q)) \leq \frac{1}{t}$

So take Alg. 1 & stop it after runtime of $3 \cdot \sqrt{N} \cdot C$, w.p. $\leq 1/3$ it fails
w.p. $\geq 2/3$ it has already finished

□

2. Unitary Approximation

1. • $\|\lambda A\| = |\lambda| \|A\|$ because $\|\lambda|\psi\rangle\|_2 = |\lambda| \||\psi\rangle\|_2$

• $\|0\| = \|0\|_2 = 0$

• $\|A+B\| = \sup_{|\psi\rangle \neq 0} \frac{\|(A+B)|\psi\rangle\|_2}{\||\psi\rangle\|_2}$

$\leq \sup_{|\psi\rangle \neq 0} \left(\frac{\|A|\psi\rangle\|_2}{\||\psi\rangle\|_2} + \frac{\|B|\psi\rangle\|_2}{\||\psi\rangle\|_2} \right)$

$\leq \sup_{|\psi\rangle \neq 0} \frac{A\||\psi\rangle\|_2}{\||\psi\rangle\|_2} + \sup_{|\psi\rangle \neq 0} \frac{\|B|\psi\rangle\|_2}{\||\psi\rangle\|_2}$

$= \|A\| + \|B\|$

• $\|AB\| = \sup_{|\psi\rangle \neq 0} \frac{\|AB|\psi\rangle\|_2}{\||\psi\rangle\|_2} = \sup_{|\psi\rangle \neq 0} \frac{\|A(B|\psi\rangle)\|_2}{\|B|\psi\rangle\|_2} \frac{\|B|\psi\rangle\|_2}{\||\psi\rangle\|_2}$

$\leq \sup_{|\psi\rangle \neq 0} \frac{\|A(B|\psi\rangle)\|_2}{\|B|\psi\rangle\|_2} \times \sup_{|\psi\rangle \neq 0} \frac{\|B|\psi\rangle\|_2}{\||\psi\rangle\|_2}$

$\leq \|A\|$ (since $\|A\|$ is the sup) $\times \|B\|$ (since $\|B\|$ is the sup)

$\leq \|A\| \times \|B\|$

2. $\|\tilde{U}^{-1} - U^{-1}\| = \|\tilde{U}^{-1}(U - \tilde{U})U^{-1}\|$

$\leq \|\tilde{U}^{-1}\| \, \|\tilde{U} - U\| \, \|U^{-1}\|$ since $\tilde{U}^{-1}$ and U^{-1} unitary, so $\|U\| = 1$

$\leq 1 \cdot \delta \cdot 1$

$\leq \delta$

3. Enough to show this for $L = 2$:

$\|\tilde{U}_2\tilde{U}_1 - U_2U_1\| = \|\tilde{U}_2(\tilde{U}_1 - U_1) + (\tilde{U}_2 - U_2)U_1\|$

$\leq \|\tilde{U}_2\| \, \|\tilde{U}_1 - U_1\| + \|\tilde{U}_2 - U_2\| \, \|U_1\|$

$\leq \delta_1 + \delta_2$ ∎

4. We have that $|\langle F(x)|U|x\rangle|^2 = |\langle x|U^\dagger |F(x)\rangle\langle F(x)|U|x\rangle|$

Let us call $\Pi_{|x\rangle} = |F(x)\rangle\langle F(x)|$

$$\text{Diff} = |\langle x|\tilde{U}^\dagger \Pi_x \tilde{U}|x\rangle - \langle x|U^\dagger \Pi_x U|x\rangle|$$

$$= |\langle x|(\tilde{U}^\dagger - U^\dagger)\Pi_x \tilde{U}|x\rangle + \langle x|U^\dagger \Pi_x (\tilde{U}-U)|x\rangle|$$

$$\leq |\text{———————}| + |\text{———————}|$$

$$\leq \|(\tilde{U}^\dagger - U)\Pi_x \tilde{U}\| + \|U^\dagger \Pi_x (\tilde{U}-U)\| \quad \text{by the inq } |\langle x|A|x\rangle| \leq \|A\|$$

$$\leq \|\tilde{U}^\dagger - U\| \|\Pi_x\| \|\tilde{U}\| + \|U^\dagger\| \|\Pi_x\| \|\tilde{U}-U\|$$

$$\leq \delta \quad = 1 \quad = 1 \quad = 1 \quad = 1 \quad \leq \delta$$

$$\leq 2\delta$$

So $|\langle x|\tilde{U}^\dagger \Pi_x \tilde{U}|x\rangle| \leq |\langle x|U^\dagger \Pi_x U|x\rangle| - \text{Diff}$

$$\leq 1 - \varepsilon - 2\delta$$

QED

NB $|\langle x|A|x\rangle| = |\langle x|BB|x\rangle|$ for some square root B of A

$$= \|B|x\rangle\|_2^2 \qquad \text{(exists since } A^\dagger = A\text{)}$$

$$\leq \|B\|^2 \|\,|x\rangle\|_2^2$$

$$\leq \|B\|^2 = \|BB\| = \|A\|$$

↑ true for some B

3. Amplitude Amplification

1. The number of times you need to repeat in order to have a good output is given by $G(p)$, a geometric law of parameter p

$$\mathbb{P}(G(p)=k) = p(1-p)^{k-1}$$

Its mean is $\boxed{\frac{1}{p}}$.

2. $\mathcal{A} = \underbrace{U_1 \dots U_p}_{\text{circuit with 2-qubit gates}}$ then $\mathcal{A}^{-1} = \underbrace{U_p^{-1} \dots U_1^{-1}}_{\text{circuit with 2-qubit gates}} = U_p^{\dagger} \dots U_1^{\dagger}$

3. When we measure $|U\rangle = \mathcal{A}|0^n\rangle$, we know by hypothesis that $\mathbb{P}(\text{output} = i \in \beta^{-1}(1)) = p$

so $\mathbb{P}(\text{output} = i \underbrace{\notin \beta^{-1}(1)}_{\text{same as } i \in \beta^{-1}(0)}) = 1-p$

$$|U\rangle = \sum_{i=0}^{n} u_i |i\rangle = \sum_{i \in \beta^{-1}(1)} u_i |i\rangle + \sum_{j \in \beta^{-1}(0)} u_j |j\rangle$$

$$= \sqrt{\sum_{i \in \beta^{-1}(1)} |u_i|^2}\ |G\rangle + \sqrt{\sum_{j \in \beta^{-1}(0)} |u_j|^2}\ |B\rangle$$

with $|G\rangle = \frac{1}{\sqrt{\sum_{i \in \beta^{-1}(1)} |u_i|^2}} \sum_{i \in \beta^{-1}(1)} u_i |i\rangle$ is a unit vector in $\operatorname{span}\{|i\rangle : i \in \beta^{-1}(1)\}$

and $|B\rangle = \frac{1}{\sqrt{\sum_{j \in \beta^{-1}(0)} |u_j|^2}} \sum_{j \in \beta^{-1}(0)} u_j |j\rangle$ in $\operatorname{span}\{|i\rangle : i \in \beta^{-1}(0)\}$

BUT since $\mathbb{P}(\text{output} \in \beta^{-1}(1)) = p = \sum_{i \in \beta^{-1}(1)} \mathbb{P}(\text{output} = i) = \sum_{i \in \beta^{-1}(1)} |u_i|^2$

We get $|U\rangle = \sqrt{p}\,|G\rangle + \sqrt{1-p}\,|B\rangle$

4. Z_β is the reflexion through $|B\rangle$ in that plane

Indeed $Z_\beta |B\rangle = |B\rangle$ since $|B\rangle \in \text{span}\{|i\rangle : i \in \beta^{-1}(0)\}$

$Z_\beta |G\rangle = -|G\rangle$ — $|G\rangle \in \text{span}\{|i\rangle : i \in \beta^{-1}(1)\}$

(Z_β stabilizes indeed that plane as proved first)

× $A R A^{-1}$ is the reflexion through $|U\rangle$ in that plane

First $|V\rangle = \sqrt{1-p}\,|G\rangle - \sqrt{p}\,|B\rangle$ is an orthogonal state of $|U\rangle$ in that plan

We have . $A R A^{-1} |U\rangle = A R |0^n\rangle = A |0^n\rangle = |U\rangle$

. $A R A^{-1} |V\rangle$:

Since A unitary : $|0^n\rangle \mapsto |U\rangle$

thus $|x\rangle \mapsto |\Psi_x\rangle \in (|U\rangle)^\perp$ (preserve of the basis)

$x \neq 0^n$

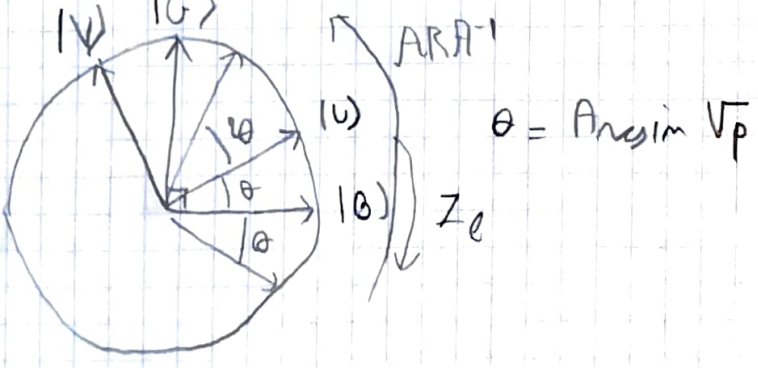
Thus $A^{-1}|V\rangle \in \text{span}\{|x\rangle : x \neq 0^n\}$

so $R A^{-1} |V\rangle = -A^{-1}|V\rangle$

Thus $\boxed{A R A^{-1} |V\rangle = -|V\rangle}$

(and $A R A^{-1}$ stabilizes the plane):

So:



$\theta = \arcsin \sqrt{p}$

5. After k steps, we have:

$$|\psi\rangle = \sin(\theta(2k+1))\,|G\rangle + \cos(\theta(2q+1))\,|B\rangle$$

We want $\sin(\theta(2k+1)) \simeq 1$

So we want $\theta(2k+1) \simeq \frac{\pi}{2}$

ie $k \simeq \frac{\pi}{4\theta} - \frac{1}{2} = \frac{\pi}{4\arcsin(\sqrt{p})} - \frac{1}{2}$

$$\simeq \frac{\pi}{4\sqrt{p}} - \frac{1}{2} = O\left(\frac{1}{\sqrt{p}}\right)$$

(for small p)

$\Rightarrow O\left(\frac{1}{\sqrt{p}}\right)$ vs classically $O\left(\frac{1}{p}\right)$

6. To get back gone, take $A = H = A^{-1}$

and $Z_f = Z_0$: $|0^n\rangle \mapsto |0^n\rangle$

$|x\rangle \mapsto -|x\rangle$ otherwise