Approximate Counting - page 1

Monday, November 26, 2018 10:53 AM

We now combine the algorithm for phase estimation and Grover Search to approximate the number of $x \in \{0,1\}^n$ such that $f(x) = 1$ for some function f to which we have black-box access.

Let G correspond to the unitary transformation which is one iteration of Grover's algorithm:

G = one rotation about $|e\rangle$ followed by a rotation about $|\psi\rangle$.

Define $S_f = \{x \mid f(x) = 1\}$ $|S_f| = M$.

$$|\phi_0\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \notin S_f} |x\rangle \qquad |\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \{0,1\}^n} |x\rangle$$

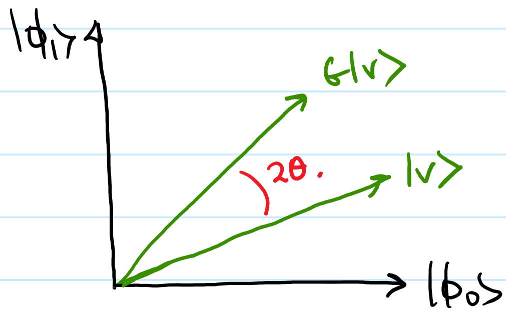
$$|\phi_1\rangle = \frac{1}{\sqrt{M}} \sum_{x \in S_f} |x\rangle \qquad |\psi\rangle = \sqrt{\frac{N-M}{N}}\, |\phi_0\rangle + \sqrt{\frac{M}{N}}\, |\phi_1\rangle$$

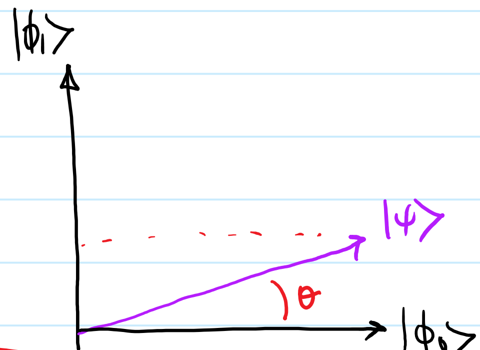
Approximate Counting - page 2

Monday, November 26, 2018 10:53 AM

For any state inside the 2-dimensional subspace spanned by $|e\rangle$ and $|a\rangle$, G is a counter-clockwise rotation by 2θ where θ is the angle between $|\psi\rangle$ and $|e\rangle$

→ with real coefficients.

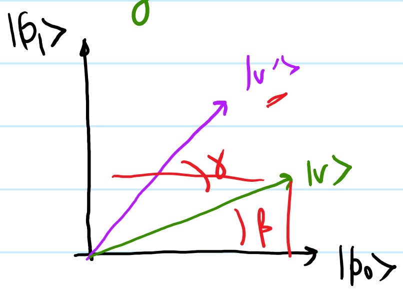




$\cos\theta = |\langle\psi|\phi_0\rangle| = \sqrt{\frac{N-M}{N}}$

$\sin\theta = |\langle\phi_1|\psi_0\rangle| = \sqrt{\frac{M}{N}}$

In general rotation by γ in 2-d space spanned by orthonormal basis $|e\rangle$ and $|a\rangle$:



$$\begin{bmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{bmatrix}$$

Input $|v\rangle = \cos\beta\,|e\rangle + \sin\beta\,|a\rangle$

$$\begin{bmatrix} \cos\gamma & -\sin\gamma \\ \sin\gamma & \cos\gamma \end{bmatrix} \begin{bmatrix} \cos\beta \\ \sin\beta \end{bmatrix} = \begin{bmatrix} \cos(\gamma+\beta) \\ \sin(\gamma+\beta) \end{bmatrix}$$

→ Uses angle sum identities.

Approximate Counting - page 3

$e^{2\pi i \varphi}$ $e^{2i\theta}$

Monday, November 26, 2018 10:53 AM

If we express G restricted to the 2-dimensional subspace spanned by $|e\rangle$ and $|a\rangle$ we get:

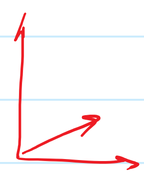
$$\begin{bmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix}$$

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

Eigenvalues of this matrix are $e^{i2\theta}$ and $e^{-i2\theta}$

eigenvalues of matrix A are roots of $\det(A - xI) = 0$.

The two eigenvectors of G live inside the subspace spanned by $|e\rangle$ and $|a\rangle$
Call them $|v_1\rangle$ and $|v_2\rangle$



We don't need to know what $|v_1\rangle$ and $|v_2\rangle$ are other than that they are an alternate basis to $|\phi_0\rangle$ and $|\phi_1\rangle$.

Since $|\psi\rangle$ is also in this subspace:

$$|\psi\rangle = \alpha_1 |v_1\rangle + \alpha_2 |v_2\rangle$$

eigenvalue $e^{-i2\theta}$

$$|\psi\rangle = \alpha_1 \underbrace{|v_1\rangle}_{\text{eigenvalue } e^{i2\theta}} + \alpha_2 \underbrace{|v_2\rangle}_{\text{eigenvalue } e^{-i2\theta} = e^{i(2\pi - 2\theta)}}$$

Approximate Counting - page 4

Monday, November 26, 2018 1:10 PM

$|\psi\rangle = \alpha_1|v_1\rangle + \alpha_2|v_2\rangle$

<u>Idea</u>: run the phase estimation algorithm to estimate the phase of an eigenvalue of G. The input will be $|\psi\rangle$.

$|v_1\rangle$ λ_1 $e^{2\theta i}$

$|v_2\rangle$ λ_2 $e^{-2\theta i}$

$|\psi\rangle$ is the superposition of the two eigenstates $|v_1\rangle$ and $|v_2\rangle$

If the Phase Estimation algorithm is successful (no errors) we estimate

2θ with probability $|\alpha_1|^2$

$2\pi - 2\theta$ with probability $|\alpha_2|^2$

It doesn't matter what the probabilities are as long as we can distinguish between the two.

Recall that $\sin\theta = \sqrt{M/N}$.

So if $M \le N/2$ then $\sin\theta \le 1/\sqrt{2}$

$\Rightarrow \theta \le \pi/4 \rightarrow 2\theta \le \pi/2$

In this case, we can easily distinguish between

$\underset{\le \pi/2}{2\theta}$ and $\underset{\ge 3\pi/2}{2\pi - 2\theta}$.

Monday, November 26, 2018 1:26 PM

We can artificially ensure that $M \leq N/2$ by adding an extra bit y to the input and using f':

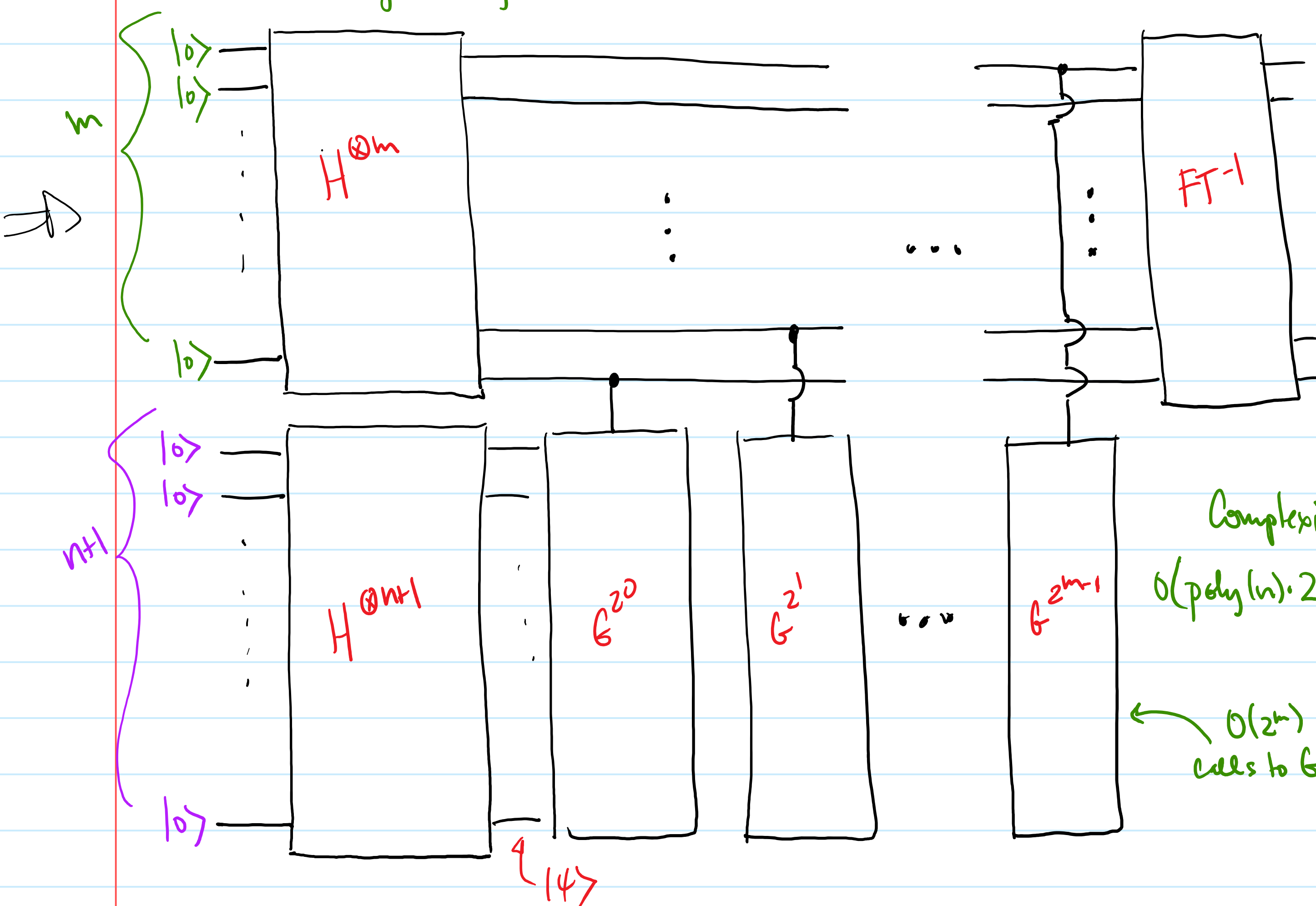
$$f'(\underbrace{x}_{n \text{ bits}}, \underbrace{y}_{1 \text{ bit.}}) = f(x) \wedge y$$

Note $f'(x, 0) = 0 \quad \forall x.$

$N' = 2^{n+1}$

$M' \leq 2^n$

An oracle for f can be transformed into an oracle for f'.



Complexity: $O(\text{poly}(n) \cdot 2^m)$

Approximate Counting - page 6

Wednesday, November 28, 2018 9:17 AM

The eigenvalue of G is $e^{i2\theta} = e^{2\pi i \varphi}$.

We estimate φ to within $\pm 2^{-(m+1)}$ $\quad \theta = \pi\varphi$.

And then use the following to determine M:

phase est.

$$\Rightarrow \frac{M}{N} = \sin^2\theta = \sin^2(\pi\varphi)$$

$$M = N \cdot \sin^2(\pi\varphi)$$

We will show that the error in M is: $\frac{1}{\sqrt{N}}$,

$$\Delta M \le \left(2\sqrt{M\cancel{N}} + \frac{\cancel{N}}{\cancel{2^m}}\pi\right) 2^{-m}\pi$$

$\sqrt{N}$ $\quad \sqrt{N}$. $\quad \sqrt{N}$

$2^{\frac{\log N}{2}} = (N)^{1/2}$

If $m = \frac{\log N}{2}$ $\quad 2^m = \sqrt{N}$. $\Rightarrow \Delta M$ is $O(\sqrt{M})$

(Remember the complexity of the algorithm was
poly $(\log N) \cdot 2^m$ $\quad$ poly $(\log N) \cdot \sqrt{N}$.)

Approximate Counting - page 7

Wednesday, November 28, 2018 9:17 AM

How do we use this for search?

After c iterations of Grover, the algorithm is at an angle $(2c+1)\theta$.

The error from Grover Search is $\cos^2((2c+1)\theta)$

We want to use our estimate for φ (call it $\tilde{\varphi}$) to select a c to minimize this error.

$\sin(\pi\varphi) = \sqrt{\frac{M}{N}}$

$\varphi - 2^{-(m+1)} \le \tilde{\varphi} \le \varphi + 2^{-(m+1)}$

Also $1 \le M \le N/2$

$\frac{1}{\sqrt{N}} \le \sin(\pi\varphi) \le 1/\sqrt{2}$

$\frac{1}{\sqrt{N}} \le \pi\varphi \le \pi/4$

$\frac{1}{\pi\sqrt{N}} \le \varphi \le 1/4$

Select integer c to the the best approximation of $\frac{1}{4\tilde{\varphi}} - \frac{1}{2}$.

Final angle is $\left[2\left(\overbrace{\frac{1}{4\tilde{\varphi}} - \frac{1}{2} \pm \frac{1}{2}}^{c}\right) + 1\right]\varphi\pi$

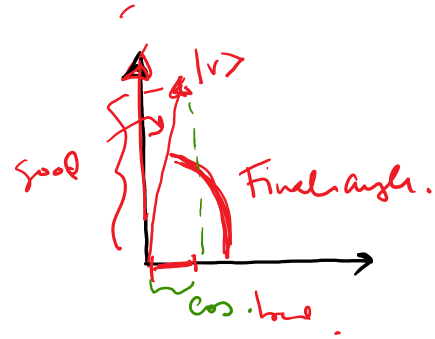
$= \left[\frac{1}{2\tilde{\varphi}} \pm 1\right]\varphi\pi = \frac{1}{2}\left[\frac{1}{\tilde{\varphi}} \pm 2\right]\varphi\pi$

$\ge \frac{1}{\varphi + 2^{-(m+1)}} - 2$

$\le \frac{1}{\varphi - 2^{-(m+1)}} + 2.$

Approximate Counting - page 8

Wednesday, November 28, 2018 10:31 AM



Worst case final angle is:

$$\frac{1}{2}\left[\frac{1}{\varphi+2^{-m-1}}-2\right]\varphi\pi$$

$$= \frac{\pi}{2}\left[\frac{\varphi}{\varphi+2^{-m-1}}-2\varphi\right] = \frac{\pi}{2}\left[1-\frac{2^{-m-1}}{\varphi+2^{-m-1}}-2\varphi\right]$$

Worst Case Error is:

$$\cos^2\left(\frac{\pi}{2}-\frac{\pi}{2}\left(\frac{2^{-m-1}}{\varphi+2^{-m-1}}+2\varphi\right)\right) = \sin^2\left(\frac{\pi}{2}\left(\underbrace{\frac{2^{-m-1}}{\varphi+2^{-m-1}}+2\varphi}_{\le 5/6}\right)\right)$$

for $0 \le \theta \le \pi/2$, $\cos(\theta) = \sin(\pi/2-\theta)$

Want to upperbound

$$\Rightarrow \underbrace{\frac{2^{-m-1}}{\varphi+2^{-m-1}}}_{\le 1/3} + \underbrace{2\varphi}_{\le 1/2}$$

$$\frac{1}{\pi\sqrt{N}} \le \varphi \le \frac{1}{4}$$

Select $m = \left\lceil \frac{\log N}{2} \right\rceil + 2$

$2^{m+1} \ge 8\sqrt{N}$.

$$\le \frac{\frac{1}{8\sqrt{N}}}{\frac{1}{\pi\sqrt{N}}+\frac{1}{8\sqrt{N}}} = \frac{1}{1+8/\pi} \le \frac{1}{3}.$$

$$\text{Error} \le \sin^2\left(\frac{\pi}{2}\cdot\frac{5}{6}\right) \le .94$$

Approximate Counting - page 9

Wednesday, November 28, 2018 11:18 AM

$\theta = \pi\varphi.$

The eigenvalue of G is $e^{i2\theta} = e^{2\pi i \varphi}.$

We estimate φ to within 2^{-m} $\quad \varphi - 2^{-(m+1)} \le \tilde{\varphi} \le \varphi + 2^{-(m+1)}$

And then use the following to determine M:

$$\frac{M}{N} = \sin^2\theta = \sin^2(\pi\varphi)$$

We will show that the error in M is:

$$\Delta M \le \left(2\sqrt{MN} + \frac{N}{2^m}\pi\right)2^{-m}\pi$$

$$\frac{\Delta M}{N} = \left| \sin^2(\pi(\varphi + 2^{-m})) - \sin^2(\pi\varphi) \right|$$

Will use $\sin(\alpha + \Delta\alpha) \le \sin\alpha + \Delta\alpha$
for small $\Delta\alpha$.

$$x^2 - y^2 = (x+y)(x-y)$$

$$= \Big[\underbrace{\sin(\pi(\varphi + 2^{-m}))}_{\le \sin(\pi\varphi) + \pi 2^{-m}} + \sin(\pi\varphi)\Big]\Big[\underbrace{\sin(\pi(\varphi + 2^{-m}))}_{\le \sin(\varphi\pi) + \pi 2^{-m}.} - \sin(\pi\varphi)\Big]$$

$$\le \Big(2\underbrace{\sin(\pi\varphi)}_{\sqrt{M/N}} + \pi 2^{-m}\Big)\pi 2^{-m} = \left(2\sqrt{\frac{M}{N}} + \pi 2^{-m}\right)\pi 2^{-m}$$

$$\Delta M \le \left(2\sqrt{MN} + \frac{N}{2^m}\pi\right)\pi 2^{-m}.$$