Approximate Counting (à la phase estimation & Grover)

Note Title 5/3/2012

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

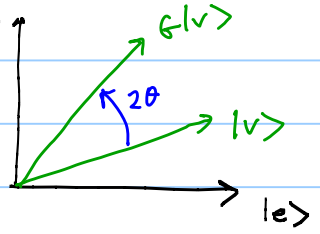
Let G correspond to the unitary transformation which is one iteration of Grover's algorithm.

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

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

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

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 $|e\rangle$ $\quad (\cos\theta = \sqrt{N-M}/N)$



If we express G restricted to this 2-dimensional subspace it is

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

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

The two eigenvectors of G live inside the subspace spanned by $|e\rangle$ and $|a\rangle$. Call them $|\phi_1\rangle$ and $|\phi_2\rangle$. We don't really need to know what they are besides the fact that they are an alternative orthonormal basis for the subspace spanned by $|e\rangle$ & $|a\rangle$. Since $|4\rangle$ also lives inside this subspace, we can write $|4\rangle = \alpha_1 |\phi_1\rangle + \alpha_2 |\phi_2\rangle$

$|\phi_1\rangle$: eigenvalue $e^{i2\theta}$ — $|\phi_2\rangle$: eigenvalue $e^{-i2\theta} = e^{i(2\pi - 2\theta)}$

The plan is to run the phase estimation algorithm to estimate the phase of an eigenvalue of G. The input to the phase estimation algorithm will be $|4\rangle$. Although $|4\rangle$ is not itself an eigenstate of G, it is the superposition of two eigenstates. Assuming that the phase estimation algorithm is successful (i.e no errors), we estimate 2θ with probability $|\alpha_1|^2$ and $2\pi - 2\theta$ with probability $|\alpha_2|^2$. It doesn't matter what these probabilities are as long as we can distinguish between the two and recover θ.

Note that if $M < N/2$ then $\theta < \pi/4$ (recall $\sin\theta = \sqrt{\frac{M}{N}}$)
This means that $2\theta < \pi/2$ and we will not confuse 2θ with $2\pi - 2\theta$.

2θ: upper-right quadrant. $2\pi - 2\theta$: lower right quadrant.

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

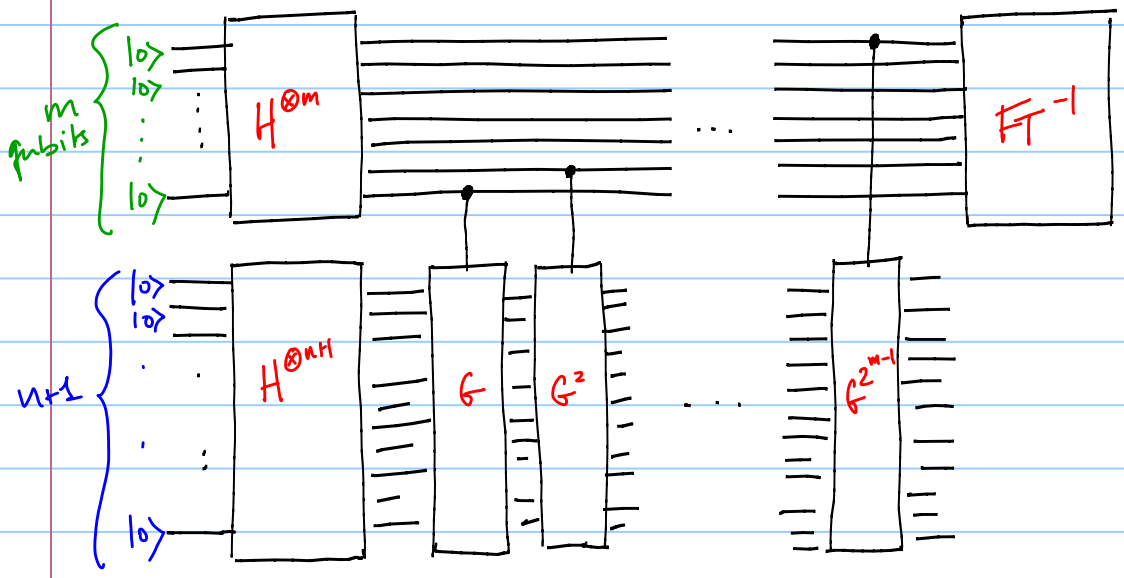
$$f'(x\,y) = f(x) \wedge y$$

x: n-bit input. y: extra bit.

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

What kind of accuracy do we get?

Suppose we use m-bits in Register 1 for phase estimation:



Complexity is $O(\text{poly}(n)\, 2^m)$

↳ # Grover iterations $= 2^{m-1} + 2^{m-2} + \cdots + 1 = 2^m - 1$

eigenvalue is $e^{i2\theta} = e^{2\pi i \varphi}$ and we approximate φ to within error 2^{-m}. ↳ $\theta = \pi\varphi$

We use the following relation to determine M: $\frac{M}{N} = \sin^2\theta = \sin^2(\pi\varphi)$

So the error in M, ΔM is:

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

will use: $\sin^2(\theta + \Delta\theta) - \sin^2\theta \leq \Delta\theta$

$\sin(\theta + \Delta\theta) \leq \sin\theta + \Delta\theta$

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

$$= \left(\sin\left(\pi\left(\varphi + 2^{-m}\right)\right) + \sin(\pi\varphi)\right)\left(\sin\left(\pi\left(\varphi + 2^{-m}\right)\right) - \sin(\pi\varphi)\right)$$

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

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

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

if $m = \log N/2 \Rightarrow \Delta M$ is $O(\sqrt{M})$

How do we use this estimate for search?

We have $\theta = \pi\varphi$ and we have an estimate $\tilde{\varphi}$ for φ to within 2^{-m}. $\varphi \leq \tilde{\varphi} \leq \varphi + 2^{-m}$

Recall that $\sin(\pi\varphi) = \sqrt{M/N}$. $1 \leq M \leq N/2 \Rightarrow \frac{1}{\pi\sqrt{N}} \leq \varphi \leq \frac{1}{4}$

After c Grover iterations, the algorithm is at an angle $(2c+1)\theta$. The error is $\cos^2\left((2c+1)\theta\right)$.

The algorithm knows $\tilde{\varphi}$ the approximation of φ and selects c to be the best integer approximation of $\frac{1}{4\tilde{\varphi}} - \frac{1}{2}$

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

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

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

Error is $\cos^2(\gamma) = \sin^2\left[\left(\frac{2^{-m}}{\varphi + 2^{-m}} + 2\varphi\right)\frac{\pi}{2}\right]$

Want to upper bound $\underbrace{\frac{2^{-m}}{\varphi + 2^{-m}}}_{\leq \frac{1}{3}} + \underbrace{2\varphi}_{\leq 1/2}$.

Know: $\frac{1}{\pi\sqrt{N}} \leq \varphi \leq \frac{1}{4}$

pick: $m = \lceil \log N/2 \rceil + 3$

$\Rightarrow 2^{-m} \leq \varphi/2$.

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