Physics 4481-7681/cs4812
Lec 19, 2 Nov 2021

\[ f(x) = \begin{cases} 0 & x \neq a \\ 1 & x = a \end{cases} \]

\[ U_f |x\rangle_n |y\rangle = |x\rangle |y \oplus f(x)\rangle_n \]

\[ a = 10110 \]

\[ U_f |x\rangle \begin{cases} \times \text{ at output} \\ \text{for} \quad x = a \end{cases} \]

\[ V_f = 1 - 2 |a\rangle \langle a | \text{ embodies } f \]

\[ W = 2 |\psi\rangle \langle \psi | - 1 \quad |\psi\rangle = H^{|n|} |10\rangle \]
work in 2d space generated by $|a\rangle, |\psi\rangle$

\[ \langle a | \psi \rangle = \cos \left( \frac{\pi}{2} - \theta \right) = \sin \theta = \frac{1}{2^{n/2}} \]

\[ \sim \theta \sim \frac{1}{\sqrt{n}} \]

$WV$ is a rotation (by what angle?) by $2\theta$

$(\text{or } V = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, W = R_\theta VR_{-\theta})$

$WV = R_\theta VR_{-\theta}$

$V = R_{2\theta}$
Apply \((WV)^\ell\) \(\Theta = \frac{1}{2^{n/2}}\) with \((2\ell+1)\frac{1}{2^{n/2}} = \frac{\pi}{2}\) gives close as possible to \(|a\rangle\)

\[l \approx \frac{\pi}{4} 2^{n/2} = \frac{\pi}{4} \sqrt{N}\]

\[p(a) = |\langle a| (WV)^\ell |\phi\rangle|^2 = \sin^2 (2\ell+1)\Theta = \sin^2 \left(\frac{2\ell+1}{2^{n/2}}\right)\]
Deutsch ’92 (p.44), factor of 2 speedup to determine whether or not 1bit→1bit function $f(x)$ is constant

Bernstein–Vazirani ’93 (p.52), $f(x) = a \cdot x \equiv \oplus_i a_i x_i$, factor of $n$ speedup to determine $a$

Simon ’94 (p.56), $f(x) = f(x \oplus a)$, measured $y$ has $a \cdot y = 0$ (equivalently $\sum_i a_i y_i = 0 \mod 2$), exponential speedup ($2^{n/2} \rightarrow O(n)$) to determine $a$

Shor ’94 (p.70), $f(x) = f(x + r)$, resulting $y$ is measured with probability $p(y) = \frac{1}{2^{n/2}} \left| \sum_{k=0}^{m-1} e^{2\pi i ky/2^n} \right|^2$, gives $|y - 2^n/r| < 1/2$ with $p > .4$, sufficient to determine period $r$ via partial fraction expansion, exponential speedup ($n2^n$, exp($n^{1/3}$) $\rightarrow O(n^3)$).

(Note: replaces $H^\otimes n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{0\leq y < 2^n} e^{i\pi x \cdot y} |y\rangle$ with $U_{FT} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{0\leq y < 2^n} e^{2\pi i x y/2^n} |y\rangle$.) Practical application is $f(x) \equiv b^x \mod N$, where $b \equiv a^c \mod N$ is an encrypted message, from which $d'$, satisfying $cd' \equiv 1 \mod r$, can be calculated, and $d'$ recovers unencrypted message $a \equiv b^{-d'} \mod N$ (in contrast to using $d$, with $cd = 1 \mod (p-1)(q-1)$, where $N = pq$ and $r$ divides $(p-1)(q-1) = |G_{pq}|$.

Grover ’96 (p.90), $f(x) = 1$ only for $(m)$ marked value(s) $x = a$, uses “phase kickback” to express $U_f$ in terms of $V = 1 - 2|a\rangle\langle a|$, and $W = 2|\phi\rangle\langle\phi| - 1 = H^\otimes n (2|0\rangle\langle0| - 1)H^\otimes n$ is easily constructed. Applying $\ell \approx \frac{\pi}{4} \frac{2^n}{\sqrt{m}}$ times gives probability $p(a) \approx 1 - O(m/2^n)$, for square-root speedup ($2^n/m \rightarrow \sqrt{2^n/m}$).
Figure 22.1: The initial amplitudes of the system, an even superposition state.

Figure 22.2: The amplitudes following the first application of the phase oracle. Note that the amplitude of the marked item has had its sign flipped.

Figure 22.3: The average amplitude $\bar{\alpha}$ has been explicitly drawn in.

Figure 22.4: The amplitudes following the first Grover diffusion operator.

Figure 22.5: Amplitudes following the second application of the phase oracle. Note that the amplitude of the marked item has had its sign flipped again.

Figure 22.6: Amplitudes following the second application of the phase oracle with the new average amplitude $\bar{\alpha}$ explicitly drawn in.

Figure 22.7: Amplitudes following the second Grover diffusion operator.
$m$ marked states

$$f(x) = \begin{cases} 
1 & x \in Y \\
0 & x \notin Y
\end{cases}$$

$Y =$ set of marked states

$|Y| = m$

$$|\psi\rangle = \frac{1}{2^n} \sum_{x\in 0^n} |x\rangle = \cos \theta |\text{no}\rangle + \sin \theta |\text{yes}\rangle$$

$|\text{yes}\rangle = \frac{1}{\sqrt{m}} \sum_{x \mid f(x) = 1} |x\rangle$

$|\text{no}\rangle = \frac{1}{\sqrt{2^n-m}} \sum_{x \mid f(x) = 0} |x\rangle$

$\sin \theta = \langle \text{yes} | \psi \rangle = \sqrt{\frac{m}{2^n}}$

$\cos \theta = \langle \text{no} | \psi \rangle = \sqrt{1 - \frac{m}{2^n}}$
\[ V = 1 - 2 \left| \text{yes} \right\rangle \left\langle \text{yes} \right| \]

\[ W = 2 \left| \phi \right\rangle \left\langle \phi \right| - 1 \]

\[ \left| \text{yes} \right\rangle \]

\[ \left| \psi \right\rangle \]

WV rotates by 2θ

\[ (2l+1)\theta \approx \pi/2 \]

\[ \theta \approx \sqrt{\frac{m}{2^l n}} = \sqrt{\frac{m}{n}} \]

\[ l \approx \frac{\pi}{4} \sqrt{\frac{N}{m}} \]
\[ \langle \text{yes} | (wv)^{l+1} | \psi \rangle \text{ is periodic} \]
\[ = \sin 2\theta \quad \text{in } l \pm \pi/\theta \]
so period = \( \frac{\pi 2^{n/2}}{\sqrt{m}} \).

Run QFT to get period, gives \( m \)
then Grover \( \frac{\pi}{4} \sqrt{N/m} \) times

A special case: \( m = 1 \), \( n = 2 \) (\( N = 4 \))
\[ \sin \theta = \langle a | \psi \rangle = \frac{1}{2^{n/2}} = \frac{1}{2} \quad \theta = \frac{\pi}{6} \]

\[ WV \text{ rotates by } \frac{\pi}{3} \]

Single \( WV \) exactly \( a \rangle \)

QM: \( 1 \) \quad \text{Classically: } \quad \frac{1}{4} \cdot 1 + \frac{3}{4} \cdot \frac{1}{3} \cdot 2 + \frac{1}{2} \cdot \frac{1}{3} \]
\[ = 2 \frac{1}{4} \]
Just choose $N/m$ states

$N = 200$, $m = 10$, pick $\frac{200}{10} = 20$

$\operatorname{prob} f \text{ at least one}$

$1 - \left( \frac{19}{20} \right)^{20} \approx 1 - e^{-1}$

$\operatorname{prob} f \text{ exactly one} \approx e^{-1}$ (Poisson)

Then run ordinary Grover

$\sqrt{\frac{N}{m}}$
How to implement $W$

$W = 1 - 2\left| y \right\rangle\left\langle y \right|$}

$= H^{\otimes n} \left( 1 - 2 \left| 0 \right\rangle\left\langle 0 \right| \right) H^{\otimes n}$

$X^{\otimes n} c^{-1} e^{X} X^{\otimes n}$

$n = 2$

$1 - 2\left| 111 \right\rangle\left\langle 111 \right| = \begin{array}{c}
\text{Diagram 1}
\end{array}$

$1 - 2\left| 00 \right\rangle\left\langle 00 \right| = \begin{array}{c}
\text{Diagram 2}
\end{array}$

$n$
One way to construct multiple $c^{n-1} Z$ and $W$

For n-fold $c^{n-1} Z$, needs n-3 ancillary initialized to $|0\rangle$
Now the ancillaries can have any states (or even be entangled with other qubits)

If any of the upper four (of $s|x$) are $10$, then reduces to identity (pairwise cancellation)
If the upper five (of six) are all on, becomes the above.

Then use \[ \begin{array}{ccc}
\text{upper five} & = & \text{lower five}
\end{array} \]

(twice) to reduce to \[ \begin{array}{ccc}
\text{lower five}
\end{array} \]
Above a construction where the ancillaries of some can be the control bits of others.