Grover's algorithm ['96] - unstructured search

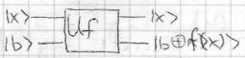
Problem: Given $f_w: \{0,1\}^n \to \{0,1\}$, such that $f_w(x) = 1 \iff x = w$. (otherwise, $f_w(x) = 0$)

Output w.

Classically, in the worst case, we would require $\overset{N-1 = \Omega(N)}{2^n - 1}$ queries of f. In the average case, we would also require $\Omega(N)$ queries, around 2^{n-1}.

Quantumly we will require $O(\sqrt{N})$ queries of f.

Example: $n=2$, $N=4$. Classically 3 queries. We'll use:



Using Hadamard gates, as in Simon's algorithm, we'll transform the black box into: $|x\rangle$ $\boxed{S_f}$ $(-1)^{f(x)}|x\rangle$

$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

$w = |00\rangle$ $\frac{1}{2}(-|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

$w = |01\rangle$ $\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)$ → ~~all~~ 4 such states are orthogonal

We have 1 out of 4 possible orthogonal states $\frac{1}{2}\begin{pmatrix}-1\\1\\1\\1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\-1\\1\\1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\1\\-1\\1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\1\\1\\-1\end{pmatrix}$.

So we need to find a unitary that changes those states into $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

First consider the <u>phase gate</u>: P: $|00\rangle \to |00\rangle$, $|01\rangle \to -|01\rangle$
$|10\rangle \to -|10\rangle$
$|11\rangle \to -|11\rangle$.

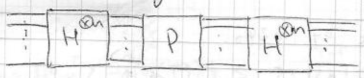
After applying it, we get one of the four: $\frac{1}{2}\begin{pmatrix}1\\-1\\-1\\-1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \frac{1}{2}\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}$

Then apply $H \otimes H$, and swap the two lines. (Check that output is exactly $|w\rangle$)

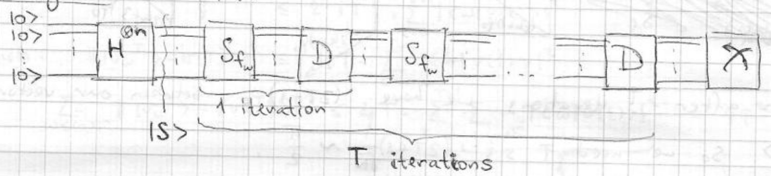
So, quantumly, we get one query.

We will use a gate $P: |00\ldots0\rangle \to |00\ldots0\rangle$
$|y\rangle \to -|y\rangle$, $y \in \{0,1\}^n - \{0\}^n$

Then call the following circuit. D: (<u>diffusion operator</u>)



<u>Grover's algorithm on $\{0,1\}^n$:</u>



<u>Analysis:</u>

$$|s\rangle = \frac{1}{N} \sum_{x \in \{0,1\}^n} |x\rangle$$

<u>Statement</u>: The circuit laves invariant the plane spanned by $|s\rangle$ and $|w\rangle$.

<u>Proof:</u> $S_{f_w}|w\rangle = -|w\rangle$. $S_{f_w} = \mathbb{1} - 2 \cdot \begin{pmatrix} 0 & & 0 \\ & 1 & \\ 0 & & 0 \end{pmatrix} = \mathbb{1} - 2 \cdot \begin{pmatrix} 0\\ \vdots \\ 1 \\ \vdots \\ 0\end{pmatrix} \cdot (00\ldots1\ldots0)$ (wth)

Hence: $S_{f_w} = \mathbb{1} - |w\rangle\langle w|$.

$$S_{f_w}|s\rangle = (\mathbb{1} - |w\rangle\langle w|)|s\rangle = |s\rangle - 2|w\rangle \cdot \langle w|s\rangle = |s\rangle - \frac{2}{\sqrt{N}}|w\rangle \quad \in \text{Span}(|s\rangle, |w\rangle)$$

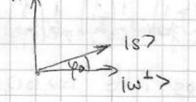
$$P = -\mathbb{1} + 2 \cdot |00\ldots0\rangle\langle 00\ldots0|.$$

$$D = H^{\otimes n} P H^{\otimes n} = -H^{\otimes n} \mathbb{1} H^{\otimes n} + 2 \cdot \underbrace{H^{\otimes n}|00\ldots0\rangle}_{|s\rangle}\langle 00\ldots0| H^{\otimes n} =$$
$$= -\mathbb{1} + 2 \cdot |s\rangle\langle s|$$

So $D|s\rangle = (-\mathbb{1} + 2 \cdot |s\rangle\langle s|) \cdot |s\rangle = -|s\rangle + 2 \cdot |s\rangle \cdot \langle s|s\rangle = |s\rangle \quad \in \text{Span}(|s\rangle, |w\rangle)$

And $D|w\rangle = (-\mathbb{1} + 2 \cdot |s\rangle \cdot \langle s|)|w\rangle = -|w\rangle + 2 \cdot |s\rangle \cdot \langle s|w\rangle = -|w\rangle + \frac{2}{\sqrt{N}} \cdot |s\rangle \in \text{Span}(|s\rangle, w\rangle)$.

□

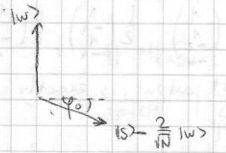


φ_0 = angle between $|s\rangle, |w^\perp\rangle$.

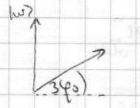
$\langle s|w\rangle = \frac{1}{\sqrt{N}}$, so $|s\rangle$ is close to $|w^\perp\rangle$ and $\sin\varphi_0 = \frac{1}{\sqrt{N}}$.

$\Rightarrow \varphi_0 \approx \frac{1}{\sqrt{N}}$

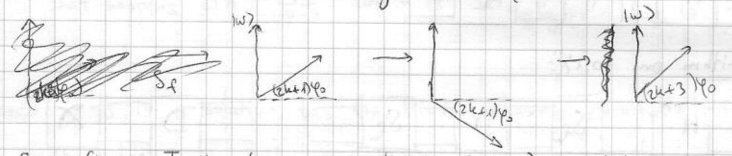
~~After~~ We start with the $|s\rangle$ vector. After the 1^{st} S_f we get:



After the first D gate - completing the 1^{st} iteration, we get:

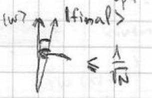


Each iteration increases the angle by $+2\varphi_0$.



So after T iterations, we have $(2T+1)\varphi_0$ between our vector and $|w^\perp\rangle$. So we need T s.t: $(2T+1)\frac{1}{\sqrt{N}} \sim \frac{\pi}{2}$.

Then $T_{opt} = \lfloor \frac{\pi}{4}\sqrt{N} - \frac{1}{2} \rceil$ (rounded), gives a precision of at least $\frac{1}{\sqrt{N}}$



or: ~~$\langle$~~ $\langle w^\perp | final\rangle \leq \frac{1}{\sqrt{N}}$. Also, we know:

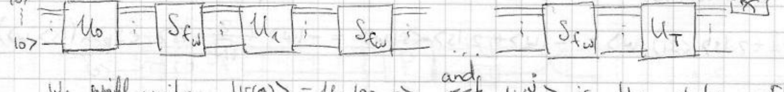
$$\langle w|final\rangle^2 + \langle w^\perp|final\rangle^2 = 1 \Rightarrow \langle w|final\rangle^2 \geq 1 - \frac{1}{N}$$

$\langle w|final\rangle^2$ is also the probability we will measure w. Then check is f(measured) = 1. If not, repeat. (with high probability, we will find correct w).

We'll now ~~show~~ show lower bounds for some problems.

Hybrid lower bound

The most general algorithm for the unstructed serch problems is:



We ~~will~~ write $|v(0)\rangle = U_0|00\ldots0\rangle$, and ~~and~~ $|v_w^j\rangle$ is the state after U_j.

Let $|v(1)\rangle = U_1|v(0)\rangle$, $|v(2)\rangle = U_2U_1|v(0)\rangle$, ..., $|v(T)\rangle = U_T \cdots U_1|v(0)\rangle$.

Notice that $|v(j)\rangle$ don't contain information ~~of~~ on w, since we never apply S_f.

Study: $\| |v_w^{t+1}\rangle - |v(t+1)\rangle \|$.

Note $\| |\alpha\rangle \| = \| U|\alpha\rangle \|$, where U is unitary.

$$\| |v_w^{t+1}\rangle - |v(t+1)\rangle \| = \| U_{t+1}S_{f_w}U_t \cdots S_{f_w}|v(0)\rangle - U_{t+1}U_t \cdots U_1|v(0)\rangle \| = \quad (U_{t+1} \text{ is unitary})$$

$$= \| S_{f_w}U_t S_{f_w} \cdots U_1 S_{f_w}|v(0)\rangle - U_t \cdots U_1|v(0)\rangle \| =$$

$$= \| S_{f_w}|v_w^t\rangle - |v(t)\rangle \| =$$

$$= \| S_{f_w}(|v_w^t\rangle - |v(t)\rangle) + (S_{f_w} - \mathbb{1})|v(t)\rangle \| \le \quad (\text{Triangle ineq.})$$

$$\le \| S_{f_w}(|v_w^t\rangle - |v(t)\rangle) \| + \| \underbrace{2|w\rangle\langle w|}_{S_{f_w}-\mathbb{1}}v(t)\rangle \| = \quad (S_{f_w} \text{ is unitary})$$

$$= \| |v_w^t\rangle - |v(t)\rangle \| + 2\cdot|\langle w|v(t)\rangle|$$

Therefore: $$\| |v_w^T\rangle - |v(T)\rangle \| \le 2\cdot\sum_{t=0}^{T-1} |\langle w|v(t)\rangle| \le \quad (\text{Cauchy-Schwarz ineq.})$$

$$\le 2\cdot\sqrt{T}\cdot\sqrt{\sum_{t=0}^{T-1}|\langle w|v(t)\rangle|^2}$$

And then: $$\| |v_w^T\rangle - |v(T)\rangle \|^2 \le 4T\cdot\sum_{t=0}^{T-1}|\langle w|v(t)\rangle|^2$$

$$\sum_{w\in\{0,1\}^n} \| |v_w^T\rangle - |v(T)\rangle \|^2 \le 4T\cdot\sum_{t=0}^{T-1}\underbrace{\sum_{w\in\{0,1\}^n}|\langle w|v(t)\rangle|^2}_{1} = 4T^2$$

Note: $\| |a\rangle - |b\rangle \|^2 = \langle a|a\rangle + \langle b|b\rangle - \langle a|b\rangle - \langle b|a\rangle = 2 - 2\,\mathrm{Re}\,\langle a|b\rangle$.

So: $$\sum_w \| |v_w^T\rangle - |v(T)\rangle \|^2 = \sum_w (2 - 2\,\mathrm{Re}\,\langle v_w^T|v(T)\rangle) = 2N - 2\cdot\sum_w \mathrm{Re}\,\langle v_w^T|v(T)\rangle \ge$$

$$\ge 2N - 2\cdot\sum_w |\langle v_w^T|v(T)\rangle| \ge \quad (\text{Cauchy-Schwartz ineq})$$

$$\ge 2N - 2\cdot\sqrt{N}\cdot\sqrt{\sum_w |\langle v_w^T|v(T)\rangle|^2}$$

If all v_w^T (for different w) are orthogonal, the expression becomes $2N - 2\sqrt{N}$.

Hence: $2N - 2\sqrt{N} \le 4T^2$, $T = \Omega(\sqrt{N})$

<u>Remark</u>: In the algorithm we can have more than n wires, and therefore apply $S_f \otimes \mathbb{1}$ instead of S_f. Notice that the <u>upper</u> bound on $\sum_{w\in\{0,1\}^n} \| |v_w^T\rangle - |v(T)\rangle \|^2$ doesn't change.

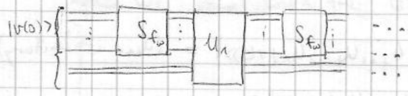
<u>Claim</u>: Even for not orthogonal v_w^T, we can assume $\sum_w |\langle v_w^T|v(T)\rangle|^2 \le 0.99N$

<u>Proof</u>: If not, at least half of the w's : $|\langle v_w^T|v(T)\rangle|^2 \ge 0.98$ (Markov)

The for 2 such w's, w_1, w_2 $\langle v_{w_1}^T|v_{w_2}^T\rangle \ge 0.9$.

So the measurement of $v_{\omega_1}^T$ and $v_{\omega_2}^T$ is the same with high probability.
But we need to achieve different measurements for $v_{\omega_1}^T$ and $v_{\omega_2}^T$. $\square$

<u>Second method</u>



(General algorithm, as in 1st method)

Define $y_j = f(j)$, $j \in \{0,1\}^n$, $y_j \in \{0,1\}$.

It is obvious that computing $OR(y_1, y_2, \dots, y_N)$ is simpler than solving the unstructured search.

$S_f : |x\rangle \to (-1)^{f(x)}|x\rangle = (1-2y_x)|x\rangle$

Assume: $|v(0)\rangle = \sum\limits_{x \in \{0,1\}^n} \alpha_x |x\rangle$.

Then $|v(0)\rangle \xrightarrow{S_f} \sum\limits_x \underbrace{\alpha_x (1-2y_x)}_{\alpha_x^1(y_1,\dots,y_N)} |x\rangle$

$\alpha_x^1(y_1,\dots,y_N) \to$ polynomial in $y_1,\dots,y_N$ of degree 1.

After U_1 we get a superposition of $|x\rangle$, with coefficients $\alpha_x(\alpha_1,\dots,\alpha_N)$ - polynomial of degree 1 - U_1 acting on a superposition is a linear combination.

So after T steps, $|final\rangle = \sum\limits_x \alpha_x^f |x\rangle$, where $\alpha_x^f(y_1,\dots,y_N)$ is a polynomial of degree T.

If we measure only the first bit the probability to get 1 is

$pr(\text{"}1\text{"}) = \sum\limits_{x \in \{1\} \times \{0,1\}^{n-1}} |\alpha_x|^2$ - is a polynomial of degree $2T$.

If $OR(y_1,\dots,y_N) = 1$, we want to achieve $Pr(\text{"}1\text{"}) \geq 0.9$, otherwise $Pr(\text{"}0\text{"}) \leq 0.1$.

$OR(y_1,\dots,y_N)$ is a polynomial of degree N. (in $y_1,\dots,y_N$)