Lecture 13.

1) Introduction : search problems.

2) Grover's quantum search algorithm.

3) Optimality of Grover's algorithm.

4) Phase estimation & quantum counting algorithm.

1) Introduction : search problems.

Let us begin with the example of searching an item in a database. As a concrete example suppose that you are given a phonebook (the database) and a phonenumber "a" (the entry). Your problem is to find the person "x" corresponding to this entry. This is not easy because the phone numbers are not sorted out in any specified order. Of course the reverse problem where you are given a person's name (the entry) and you have to find its phonenumber is easy because the entries (the person names) are sorted out in alphabetical order. For initial problem, in the worst case, an exhaustive search would requires N queries of the phonebook database assuming there are N entries and N persons. One might think that a probabilistic search would improve the situation but this is not so. Indeed suppose we query the phonebook K times by picking randomly K values of "x" and checking whether they correspond to "a". Each time the probability of success is $\frac{1}{N}$ so after K queries the probability of success is less than $\frac{K}{N}$. Therefore it will always tend to zero unless $K = O(N)$. In fact this probability is precisely $\sum_{\ell=1}^{K} \binom{K}{\ell} \left(\frac{1}{N}\right)^{\ell} \left(1 - \frac{1}{N}\right)^{K-\ell}$

$= 1 - \left(1 - \frac{1}{N}\right)^{K} \simeq 1 - e^{-c}$ for $K = cN$; $0 < c < 1$. Thus a classical probabilistic search requires at least cN queries with $c = O(1)$.

Another example of search problems are decision problems. Take the example of 3-SAT. The we have a boolean function

$$f(x_1 \dots x_n) = \phi_1 \wedge \phi_2 \dots \wedge \phi_M$$

which is a conjunction of M clauses. Each clause is a disjunction of 3 litterals (boolean variables or bits) $\phi_i = x_{i_1} \vee \bar{x}_{i_2} \vee x_{i_3}$; $\phi_j = \bar{x}_{j_1} \vee x_{j_2} \vee \bar{x}_{j_3}$ ect... (Here $\bar{x} = 1 - x$). The 3-SAT decision problem is to decide wether there exist an assignement $(\bar{x}_1 \dots \bar{x}_n)$ to the n bits such that

$$f(\bar{x}_1 \dots \bar{x}_n) \text{ is SATISFIED i.e equals } 1.$$

The space of all possible assignements has $N = 2^n$ elements. Moreover this problem can be shown to be NP-complete and no polynomial (in $n = \log_2 N$) time method to solve it is known. Clasically we have to resort to exhaustive or probabilistic search which take a time $O(N) = O(2^n)$.

Remark 1: Given an "oracle" giving the solution of the decision problem for each n, we can find the solutions $\bar{x}_1 \dots \bar{x}_n$ in linear time $O(n)$. Indeed set $x_1 = 1$. Ask the oracle if the reduced formula has a solu. If yes continue with $x_2 = 1$ ect... If not set $x_1 = 0$ and continue. In this fashion we have a solution in linear time [given an oracle for all n].

Remark 2: Here we assume that f has no obvious or no "structure" as in the unsorted database problem.

Both the database and 3-SAT problem are special cases of the following class of problems. Let $f : \{0,1\}^n \to \{0,1\}$. We want to find a solution $\bar{x}_1 \dots \bar{x}_m$ such that

$$f(\bar{x}_1 \dots \bar{x}_m) = 1 . \qquad ; \; 2^n = N$$

The function f is assumed to be a "black box function" on which we know nothing special. We just assume that we have an oracle that we can query with an input $x_1 \dots x_m$ and which tells us wether $f(x_1 \dots x_m) = 0$ or 1.

Classicaly, as argued before, we need to query the oracle $O(N) = O(2^n)$ times to get a solution with finite probability.

We will now explain Grover's quantum algorithm which allows $O(\sqrt{N})$ queries in order to find a soln. This is not an exponential speedup but merely a quadratic one. In fact this speedup applies to all NP complete problems because the above problem contains 3-SAT and 3-SAT is NP complete [NP complete means that any problem in NP can be reduced to 3-SAT in poly time]. We will also show that it is optimal in some sense.

Remark that factoring allows for an exponential speedup because of the hidden structure behind the search problem: reduction to period finding!

Finaly we mention without proof that it is known that certain classical problem do not admit a speedup by using QM.

2) Grover's quantum search algorithm.

We are allowed to query a "quantum black box" and this counts as "one computational step". The quantum oracle is represented by a unitary operator U_f:

$$U_f |x\rangle |b\rangle = |x\rangle |b \oplus f(x)\rangle$$

where $|x\rangle \in \{|0\rangle, \ldots, |N-1\rangle\}$; $N = 2^n$

$|b\rangle = |0\rangle$ or $|1\rangle$ and $f(x) \in \{0, 1\}$.

We want to find a solution to $f(x_1 \ldots x_N) = 1$ in a minimal number of queries.

2a) Derivation of Algorithm with

In order to query all classical inputs simultaneously we first prepare a superposition state:

$$(H \otimes \ldots \otimes H)(\underbrace{|0\rangle \otimes \ldots \otimes |0\rangle}_{n\text{-qubits}}) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle .$$

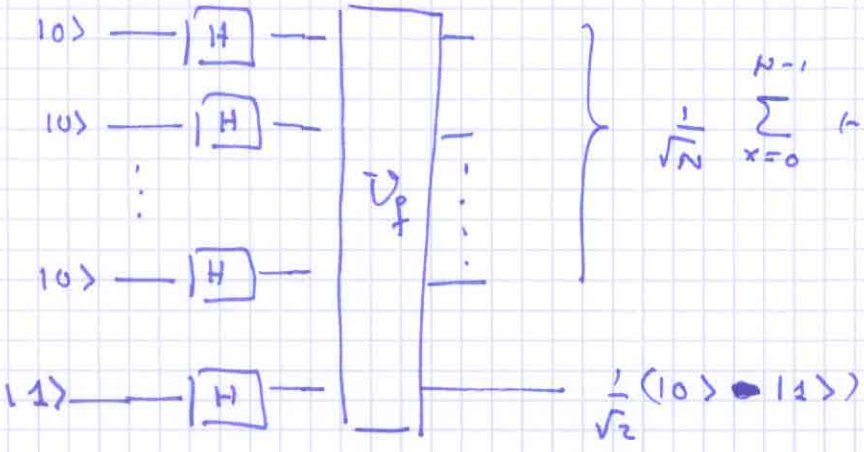
Note that
$$\begin{cases} U_f H^{\otimes n} \underbrace{|0 \ldots 0\rangle}_{n} \otimes |0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle \\ U_f H^{\otimes n} \underbrace{|0 \ldots 0\rangle}_{n} |1\rangle = \frac{1}{N} \sum_{x=0}^{N-1} |x\rangle |1 \oplus f(x)\rangle \end{cases}$$

and $$|f(x)\rangle - |1 \oplus f(x)\rangle = \begin{cases} |0\rangle - |1\rangle & \text{if } f(x)=0 \\ |1\rangle - |0\rangle & \text{if } f(x)=1 \end{cases}$$

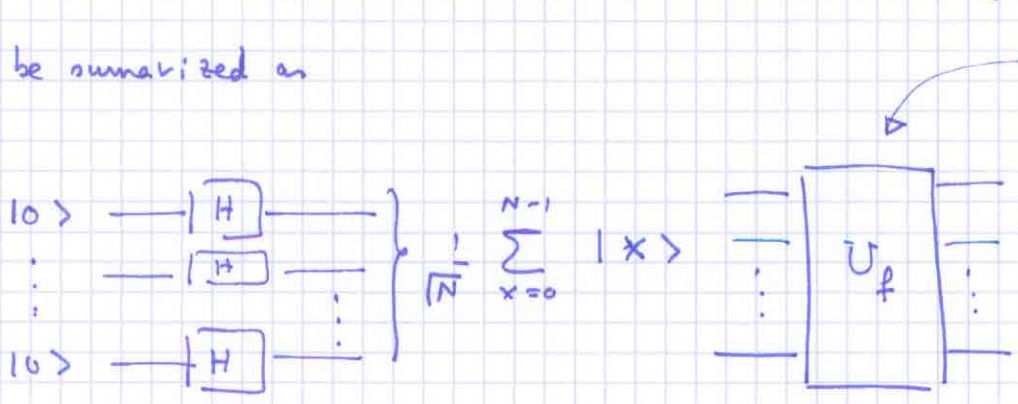
so $$|f(x)\rangle - |1 \oplus f(x)\rangle = (-1)^{f(x)} (|0\rangle - |1\rangle) .$$

$$\rightarrow \quad U_f \, H^{\otimes n} \, |0\ldots0\rangle \otimes \underbrace{H\,|1\rangle}_{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N} (-1)^{f(x)} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

The circuit representation of this last identity is



The extra bit $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ will play a trivial role in the sequel and it is customary to drop it. The action of the oracle can be summarized as



We may say that the oracle recognizes solutions $f(x) = 1$ and "marks them" with a phase (-1) while it leaves the phase $(+1)$ to non-solutions.

Now suppose there M solutions to $f(\vec{x}) = 1$. Define the normalized states:

$$\begin{cases} |S\rangle = \frac{1}{\sqrt{M}} \sum_{\vec{x}\ \text{solution}} |\vec{x}\rangle \\ \\ |M\rangle = \frac{1}{\sqrt{N-M}} \sum_{x\ \text{not a solution}} |x\rangle . \end{cases}$$

The input to the quantum oracle is

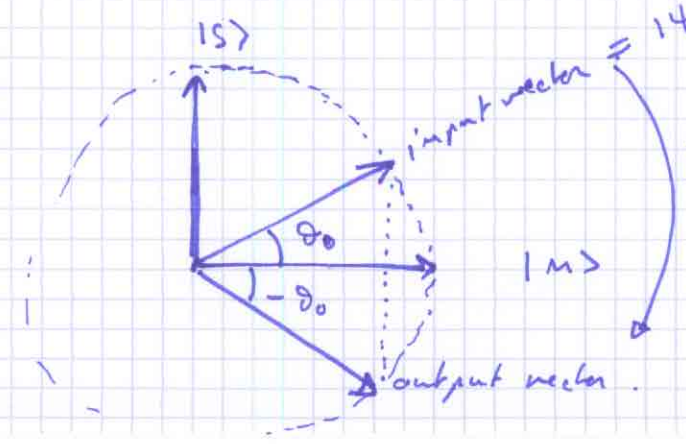
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{M}{N}}\, |S\rangle + \sqrt{\frac{N-M}{N}}\, |M\rangle .$$

and the output is

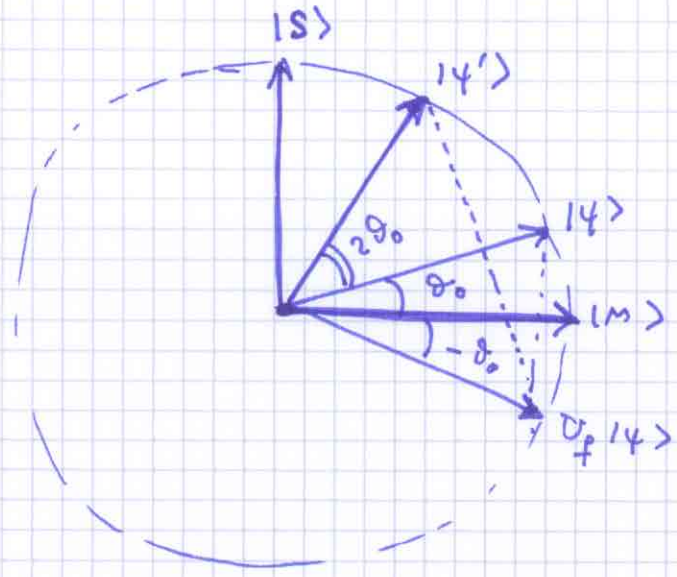
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} (-1)^{f(x)} |x\rangle = \sqrt{\frac{N-M}{N}}\, |M\rangle - \sqrt{\frac{M}{N}}\, |S\rangle .$$

Setting $\sin\vartheta_0 = \sqrt{\frac{M}{N}}$; $\cos\vartheta_0 = \sqrt{\frac{N-M}{N}}$

(note that $\sin^2\vartheta_0 + \cos^2\vartheta_0 = 1$) we see that the action of the oracle is the following reflection:



Let us now take the output vector and perform a reflection about the axis $\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \equiv |\psi\rangle$:



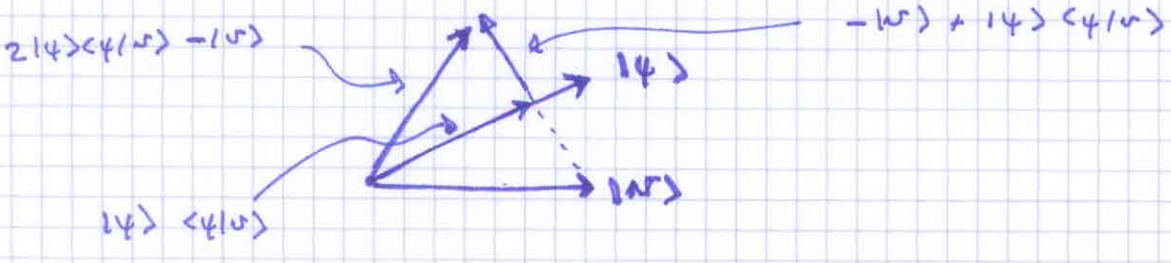
This second reflection yields

$$|\psi'\rangle = (\cos 3\theta_0)\,|m\rangle + (\sin 3\theta_0)\,|s\rangle .$$

Note that this vector is closer to $|s\rangle$ and this is the crucial point which makes Grover's algorithm work. The second reflection can be performed even though its axis $|\psi\rangle$ is not known (θ_0 is not known)!

Indeed a reflection about $|\psi\rangle$ is the unitary operation :

$$|v\rangle \longmapsto (2|\psi\rangle\langle\psi| - I)|v\rangle$$

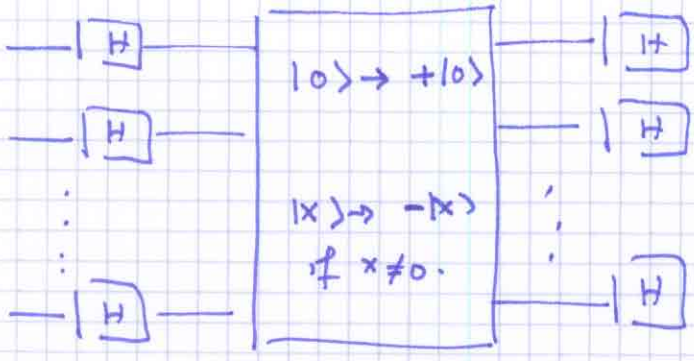


Now $2|\psi\rangle\langle\psi| - I = 2H^{\otimes n}|0\ldots0\rangle\langle 0\ldots0|H^{\otimes n} - I$

$= H^{\otimes n}\left(2|0\ldots0\rangle\langle 0\ldots0| - I\right)H^{\otimes n}$

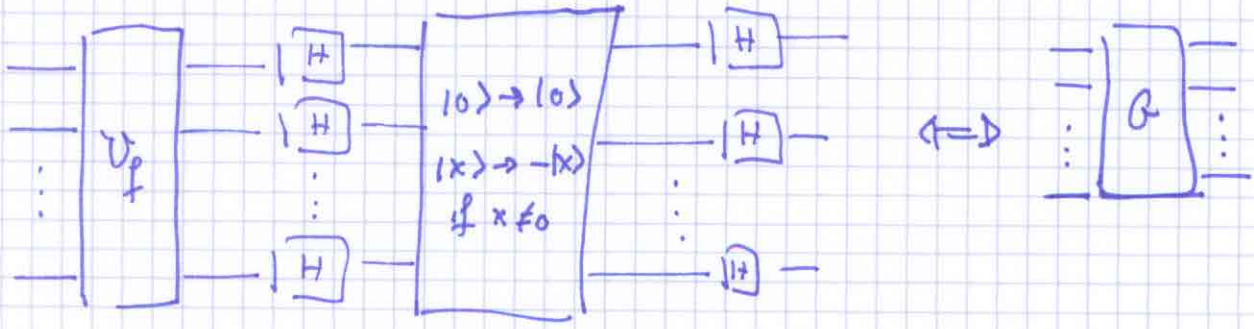
and $\left(2|0\ldots0\rangle\langle 0\ldots0| - I\right)|\nu\rangle = \begin{cases} -|\nu\rangle & \text{if } \nu \neq 0\ldots0 \\ +|0\ldots0\rangle & \text{if } \nu = 0\ldots0 \end{cases}$.

So the circuit for the second reflection about $|\psi\rangle$ is:



The box can be represented by $O(n)$ elementary gates (exercise) [For this use a classical circuit, then make it reversible if needed and you have a quantum circuit].

The combination of the two reflections is defined as the "Grover operator" G



We have by the preceding discussion

$$G\left(\cos\vartheta_0\,|m\rangle + \sin\vartheta_0\,|s\rangle\right) = (\cos 3\vartheta_0)\,|m\rangle + (\sin 2\vartheta_0)\,|s\rangle.$$

So the Grover operator is a rotation in the subspace $\{|m\rangle, |s\rangle\}$ by an angle $2\vartheta_0$.

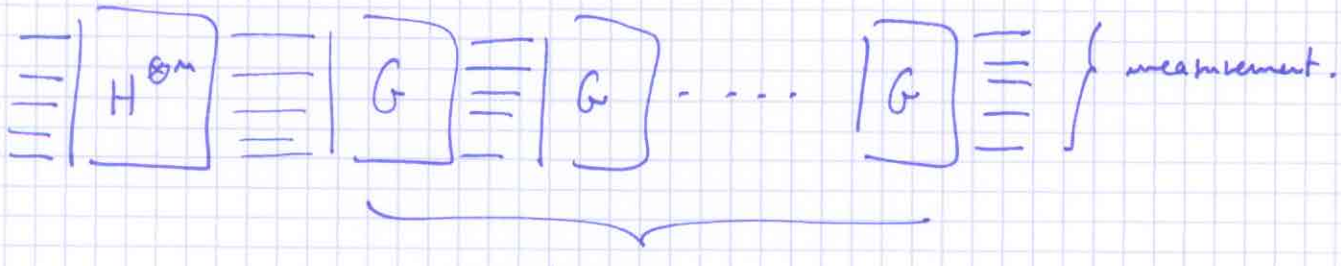
The basic idea of the Grover algorithm is then to iterate this rotation

$$G^K\left(\cos\vartheta_0\,|m\rangle + \sin\vartheta_0\,|s\rangle\right) = (\cos(2k+1)\vartheta_0)\,|m\rangle + (\sin(2k+1)\vartheta_0)\,|s\rangle.$$

in such a way that $\sin^2(2k+1)\vartheta_0 \approx 1$ and $\cos^2(2k+1)\vartheta_0 \approx 0$.

Then a measurement will yield some state belonging to $|s\rangle = \frac{1}{\sqrt{M}} \sum_{x \text{ is a sol.}} |x\rangle$ with a prob equal to one.

The quantum circuit for Grover's algorithm is



The size of this circuit is $O(n) + O(K) = O(\ell_{s_2} N) + O(K)$.

We will now see that in order to have $\sin^2(2k+1)\vartheta_0 \approx O(1)$ we must take $K = O(\sqrt{N})$.

2b). Analysis of success probability. M assumed to be known.

- Let first $M = 1$ ("hardest case"). Then $\sin\vartheta_0 = \frac{1}{\sqrt{N}}$ so $\vartheta_0 \approx \frac{1}{\sqrt{N}}$. Since we want $\sin^2((2k+1)\vartheta_0) = O(1)$ we must iterate $K \approx \frac{\pi}{4}\sqrt{N}$ times. We take the integer part: $K = \left\lfloor \frac{\pi}{4\vartheta_0} \right\rfloor$. Then

$$(2k+1)\vartheta_0 = \left(2\left\lfloor \frac{\pi}{4\vartheta_0} \right\rfloor + 1\right)\vartheta_0$$

$$= \frac{\pi}{2} + 2\delta\vartheta_0 .$$

where we used $\left\lfloor \frac{\pi}{4\vartheta_0} \right\rfloor = \frac{\pi}{4\vartheta_0} - \frac{1}{2} + \delta \quad ; \quad |\delta| < \frac{1}{2}$.

Since $2\delta\vartheta_0 \approx \frac{2\delta}{\sqrt{N}} < \frac{2}{\sqrt{N}}$ we have $(2k+1)\vartheta_0 \approx \frac{\pi}{2} + O\left(\frac{1}{\sqrt{N}}\right)$

$\Rightarrow$ The success probability is $\sin^2((2k+1)\vartheta_0) = \sin^2\left(\frac{\pi}{2} + O\left(\frac{1}{\sqrt{N}}\right)\right)$

$$= 1 - O\left(\frac{1}{N}\right) .$$

- Let then $M = \frac{N}{4}$ ("easiest" (quantum mechanically) case).

$$\sin\vartheta_0 = \sqrt{\frac{M}{N}} = \frac{1}{2} \Rightarrow \vartheta_0 = \frac{\pi}{6} .$$

choose $k = 1$ one iterate $\underbrace{\sin^2\frac{3\pi}{6}}_{\text{success probability}} = \sin^2\frac{\pi}{2} = 1$!

With one iteration we find a solution! (remarquable).

- Let M be general.

* **If $M < \frac{3}{4}N$** then $\sin\vartheta_0 < \sqrt{\frac{3}{4}} = \frac{\sqrt{3}}{2} \Rightarrow \vartheta_0 < \frac{\pi}{3}$.

iterate $K = \left\lfloor \frac{\pi}{4\vartheta_0} \right\rfloor$ times (which is at most $O(\sqrt{N})$ if $M \geq 1$).

Then $(2K+1)\vartheta_0 = \left(2\left\lfloor \frac{\pi}{4\vartheta_0} \right\rfloor + 1\right)\vartheta_0 = \frac{\pi}{2} + 2\delta\vartheta_0$ where we used

again $\left\lfloor \frac{\pi}{4\vartheta_0} \right\rfloor = \frac{\pi}{4\vartheta_0} - \frac{1}{2} + \delta$ for some $|\delta| < \frac{1}{2}$.

Now $2|\delta|\vartheta_0 < \frac{\pi}{3}$ so the success probability is

$$\sin^2(2K+1)\vartheta_0 = \sin^2\left(\frac{\pi}{2} + 2\delta\vartheta_0\right) \geq \sin^2\left(\frac{\pi}{2} - \frac{\pi}{3}\right) = \sin^2\frac{\pi}{6} = \left(\frac{1}{2}\right)^2 = \frac{1}{4}.$$

So for $M < \frac{3}{4}N$ the success probability is $\frac{1}{4}$ which is enough because we can iterate the whole process to make it as close to 1 as we wish.

* **If $M \geq \frac{3}{4}N$** then forget about the quantum algorithm and pick $x \in \{0 \ldots N-1\}$ randomly uniformly. The success probability is at least $\frac{3}{4}$.

2c) Case where M is unknown.

In this case we can use the following version of Grover's algorithm.

1). Pick x at random. If $f(x) = 1$ output x and stop.

2). Otherwise let $\tilde{M} = \sqrt{N} + 1$. Choose $R \in \{0, 1, \ldots, \tilde{M}-1\}$ at random uniformly.

3) Apply Grover's algorithm with R iterations.

4) Measure the output to get some $x \in \{0 \ldots N-1\}$.

The claim is that the success probability is at least $1/4$.

Proof of claim:

Let M be the unknown number of solns. If $M \geq \frac{3}{5}N$ we succeed with probability $\frac{3}{5}$ in the first step. If $M < \frac{3}{5}N$ we may not succeed and then we go to the second step. Then given R the success probability is $\sin^2(2R+1)\theta_0$ where $\sin\theta_0 = \sqrt{\frac{M}{N}}$. As before $\theta_0 < \frac{\pi}{3}$. Since R is chosen uniformly at random in $\{0 \ldots \tilde{M}-1\}$ the succ prob is

$$\text{prob success} = \frac{1}{\tilde{M}} \sum_{R=0}^{\tilde{M}-1} \sin^2(2R+1)\theta_0$$

$$= \frac{1}{2\tilde{M}} \sum_{R=0}^{\tilde{M}-1} \left(1 - \cos((2R+1)2\theta_0)\right)$$

$$= \frac{1}{2} - \frac{\sin 4\tilde{M}\theta_0}{4\tilde{M}\sin 2\theta_0}$$

Now we have $\sin \tilde{4} \theta_0 < 1$ and

$$\sin 2\theta_0 = 2 \sin\theta_0 \cos\theta_0 = 2 \sqrt{\frac{M}{N}} \sqrt{\frac{N-M}{M}} = 2 \sqrt{\frac{N-M}{N}} \geq \frac{1}{\sqrt{N}} > \frac{1}{\tilde{M}}.$$

Thus prob success $\geq \frac{1}{2} - \frac{1}{4} = \frac{1}{4}$. ∎

3) Optimality of Grover's search algorithm.

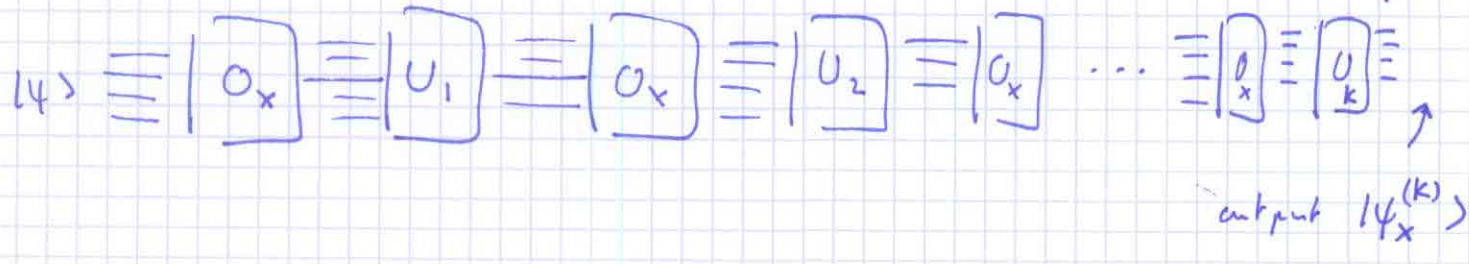
Consider the example of database search. Suppose that we have some "marked" state x that we search for using Grover's algorithm. We need at most $O(\sqrt{N})$ steps to achieve success with finite probability. But can we do better? The answer is no! In other words we need at least $\Omega(\sqrt{N})$ steps!

We suppose that we have oracles that recognize marked states x. Since they recognize these states the oracles can perform the unitary operations

$$O_x = I - 2|x\rangle\langle x|$$

which acts as $O_x |s\rangle = \begin{cases} |s\rangle & \text{if } s \neq x \\ -|s\rangle & \text{if } s = x. \end{cases}$

Furthermore we suppose that we have an arbitrary initial state $|\psi\rangle$ and that we query the oracle O_x K times as follows:



where $U_1 \dots U_k$ are arbitrary unitary operators making up the general search algorithm. The output of this algorithm is

$$|\psi_x^{(k)}\rangle = U_k O_x U_{k-1} \dots U_1 O_x |\psi\rangle .$$

In order to recognize any state x with finite probability $\varepsilon > 0$ we ask that this search procedure should satisfy

$$|\langle x | \psi_x^{(k)} \rangle|^2 \geq \varepsilon > 0 .$$

We will show that necessarily we must choose $k \geq c\sqrt{N}$ for some $c > 0$ (depending on ε).

Lemma 1: Set $D_k = \sum_{x=0}^{N-1} \| \psi_x^{(k)} - \psi_k \|^2$ where

$$|\psi_k\rangle = U_k U_{k-1} \dots U_1 |\psi\rangle .$$

Then $D_k \leq 4k^2$.

Lemma 2: We also have $D_k \geq cN$ for some c depending on ε.

Remark: Lemmas 1 & 2 imply $cN \leq 4k^2 \Rightarrow k = \Omega(\sqrt{N})$ so at least $c\sqrt{N}$ queries of the oracle O_x are needed.

Proof of lemma 2.

$|\langle x|\psi_x^{(k)}\rangle|^2 \geq \varepsilon > 0$.

This is a consequence of . We have

$$D_k = \sum_x \|(\psi_x^{(k)} - |x\rangle) - (\psi_k - |x\rangle)\|^2$$

$$\geq \sum_x \|\psi_x^{(k)} - |x\rangle\|^2 + \sum_x \|\psi_k - |x\rangle\|^2 - 2\sum_x \|\psi_x^k - |x\rangle\| \cdot \|\psi_k - |x\rangle\|$$

$$\geq \sum_x \|\psi_x^{(k)} - |x\rangle\|^2 + \sum_x \|\psi_k - |x\rangle\|^2 - 2\left(\sum_x \|\psi_x^{(k)} - |x\rangle\|^2\right)^{1/2}\left(\sum_x \|\psi_k - x\|^2\right)^{1/2}$$

$$= \left[\left(\sum_x \|\psi_x^{(k)} - x\|^2\right)^{1/2} - \left(\sum_x \|\psi_k - |x\rangle\|^2\right)^{1/2}\right]^2 \quad (*)$$

* Now $\|\psi_x^{(k)} - x\|^2 = 2 - \langle x|\psi_x^{(k)}\rangle - \langle\psi_x^{(k)}|x\rangle$

$$\leq 2 - 2\sqrt{\varepsilon}$$

$$\Rightarrow \left(\sum_x \|\psi_x^{(k)} - x\|^2\right)^{1/2} \leq \sqrt{2}\sqrt{N}\,(1 - \sqrt{\varepsilon})^{1/2}. \quad (**)$$

* Moreover $\|\psi_k - |x\rangle\|^2 = 2 - \langle\psi_k|x\rangle - \langle x|\psi_k\rangle$

$$\Rightarrow \sum_x \|\psi_k - x\|^2 = 2N - \sum_x \langle\psi_k|x\rangle - \sum_x \langle x|\psi_k\rangle$$

and $\left|\sum_x \langle\psi_k|x\rangle\right| \leq \left(\sum_x 1\right)^{1/2}\left(\sum_x |\langle\psi_k|x\rangle|^2\right)^{1/2}$

$= \sqrt{N} \cdot 1$. because $|x\rangle$ is a basis on which $|\psi_k\rangle$ can be expanded.

$$\Rightarrow \left(\sum_x \|\psi_k - x\|^2\right)^{1/2} \geq \sqrt{2N - 2\sqrt{N}}. \quad (***)$$

Combining (*), (**), (***) yields :

$$D_k \geq \left[\sqrt{2N}\,(1-\sqrt{\varepsilon})^{1/2} - \sqrt{2N}\,\left(1-\frac{1}{\sqrt{2N}}\right)^{1/2} \right]^2$$

$$D_k \geq 2N \left[\left(1-\frac{1}{\sqrt{2N}}\right)^{1/2} - (1-\sqrt{\varepsilon})^{1/2} \right]^2 .$$

■

Proof of Lemma 1.

This is a consequence of $O_x = I - 2|x><x|$. We proceed by induction. For $k=0$; $D_0 = 0$. Suppose $D_k \leq 4k^2$. Compute D_{k+1} :

$$D_{k+1} = \sum_x \| O_x \varphi_x^{(k)} - \psi_k \|^2 \quad \text{because } U_{k+1} \text{ has norm 1.}$$

$$= \sum_x \| O_x(\varphi_x^{(k)} - \psi_k) - (O_x - I)\psi_k \|^2$$

$$\leq \sum_x \| \varphi_x^{(k)} - \psi_k \|^2 + \sum_x \| (O_x - I)\psi_k \|^2$$

$$+ 2 \sum_x \| \varphi_x^{(k)} - \psi_x \| \cdot \| O_x - I \| \qquad (*)$$

Now $(O_x - I)\psi_k = -2 <x|\psi_k>.|x>$

$$\Rightarrow \| (O_x - I)\psi_k \|^2 = 4 |<x|\psi_k>|^2$$

$$\Rightarrow \sum_x \| (O_x - I)\psi_k \|^2 = 4 \sum_x |<x|\psi_k>|^2 = 4 . \qquad (**)$$

From (*), (**) + Cauchy Schwarz on the last term we get

$$D_{k+1} \leq D_k + 4 + 4\sqrt{D_k} \leq 4k^2 + 4 + 8k = 4(k+1)^2$$

■

4) Phase estimation and quantum counting.

Suppose we want to count the number of solutions to a problem of the form $f(x_1 \dots x_N) = 1$, $N = 2^n$, $x_i \in \{0,1\}$. This could be for example the 3-SAT problem. Classically in the worst case this may require $\mathcal{O}(N)$ queries of an oracle computing f.

The "quantum counting" algorithm provides a way to count the number of solutions in $O(\sqrt{N})$ queries of the oracle.

This algorithm is a combination of our two more basic algorithms: the QFT & Grover. Here we wish to give a brief sketch of the main ideas involved and refer to the literature for a detailed analysis.

Looking back at Grover's algorithm we see that the number of solutions, say M, appears as an eigenvalue of the Grover rotation by an angle $2\theta_0$:

$$|\psi\rangle = \cos\theta_0 |m\rangle + \sin\theta_0 |s\rangle \to \cos 3\theta_0 |m\rangle + \sin 3\theta_0 |s\rangle .$$

where $\sin\theta_0 = \sqrt{\frac{M}{N}}$; $\cos\theta_0 = \sqrt{\frac{N-M}{N}}$.

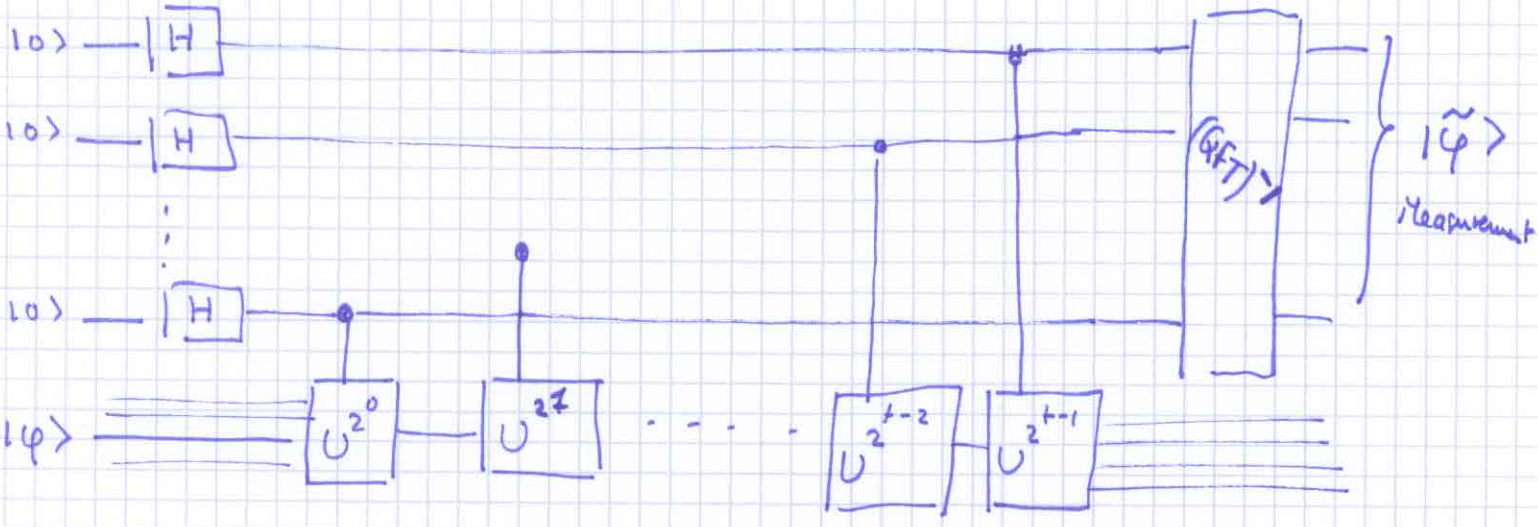
This rotation is a unitary operator with eigenvalues $e^{\pm i 2\theta_0}$ and corresponding eigenvectors $|2\theta_0\rangle$; $|-2\theta_0\rangle$:

$$G\,|\pm 2\theta_0\rangle = e^{\pm i 2\theta_0} |\pm 2\theta_0\rangle .$$

So counting the nb of solns M means estimating the phase of G.

4a) Phase estimation algorithm.

Estimating the phase of a unitary operator U is almost like finding the period of the modular exponential fct in Shor's algorithm. It should come as no surprise that we try out the following circuit:



Here $U|\varphi\rangle = e^{i2\pi\varphi}|\varphi\rangle$ and we want to estimate the phase φ. Let us show that the output $|\tilde{\varphi}\rangle$ is a good approximation to $|\varphi\rangle$.

For simplicity suppose $\varphi = 2^{-t}\varphi_t + \ldots + 2^{-2}\varphi_2 + 2^{-1}\varphi_1$; $\varphi_i \in \{0,1\}$.

[Note we define the phase as $0 \le \varphi < 1$]. The above circuit uses t - qbits $|0\rangle \otimes \ldots \otimes |0\rangle$ as input and t extra bit to input $|\varphi\rangle$. The action of all controlled unitary gates yields (just before $(QFT)^{-1}$)

$$\bigotimes_{\ell=0}^{t-1} \left(|0\rangle + e^{(2\pi i 2^{\ell}\varphi)} |1\rangle \right)$$

Since $\varphi = 2^{-t}\varphi_t + \cdots + 2^{-1}\varphi_1 = 2^{-t}\underbrace{\left(2^{t-1}\varphi_1 + \cdots + 2^{0}\varphi_t\right)}_{\cdot\,\tilde{\varphi}}$

$= 2^{-t}\cdot\tilde{\varphi}$

we have just before the $(QFT)^{-1}$ step :

$$\bigotimes_{\ell=0}^{t-1}\left(|0\rangle + e^{\frac{2\pi i\, 2^{\ell}}{2^t}\tilde{\varphi}}|1\rangle\right). \qquad (*)$$

But looking back at the QFT we have that this state is precisely

$$QFT\,|\tilde{\varphi}\rangle \quad \text{or} \quad QFT\,|\varphi_t \cdots \varphi_1\rangle .$$

So when $(QFT)^{-1}$ acts on $(*)$ we obtain $|\varphi_1 \cdots \varphi_t\rangle = |\varphi\rangle$.
Thus a measurement will yield the phase φ with probability equal to 1 !.

Of course in practice φ has more than t bits, but it can be shown that this circuit enables to estimate φ to t bits of accuracy with high probability. The error is basically

$$|\tilde{\varphi} - \varphi| < 2^{-t} .$$

Moreover in practice the eigenstate $|\varphi\rangle$ at the entry (page 18) is unknown. So one prepares a suitable superposition of eigenstates of U $|\psi\rangle = \sum_u c_u |\varphi_u\rangle$. Then at the output we will measure some φ_u with prob $|c_u|^2$.

When U has a small nb of eigenstates and eigenvalues this works pretty well since $\sum |c_u|^2 = 1$ so some of them have to be finite $O(1)$.

4b) Application to quantum counting.

In place of U we put G, the Grover operator, in the previous circuit.(*) Then we get an estimate of ϑ_0 to t bits of accuracy. We want to determine t.

$$\vartheta_0 \simeq \sqrt{\frac{M}{N}} \qquad \text{for} \qquad 1 \ll M \ll N$$

so $\delta\vartheta_0 \simeq \dfrac{\delta M}{\sqrt{MN}} \simeq \dfrac{\sqrt{M}}{\sqrt{MN}} = \dfrac{1}{\sqrt{N}}$ if $\delta M \sim \sqrt{M}$.

So to get an estimate of M with an error of $\sqrt{M}$ we need that $2^{-t} = \dfrac{1}{\sqrt{N}}$ i.e $\underline{t = \log_2 \sqrt{N} \text{ bits}}$.

How many times is the oracle queried ?.

In each box G^{2^ℓ} the Grover operator (and then the oracle) is queried 2^ℓ times. Then the total nb of queries is

$$2^0 + 2^1 + 2^2 + \cdots + 2^{t-1} = 2^t = 2^{\log_2 \sqrt{N}} = \sqrt{N}.$$

So we query the oracle $\sqrt{N}$ to estimate the nb of sols M to an accuracy of $\sqrt{M}$.

footnote :

(*) Note that the input $|\vartheta_0\rangle$ is not known but we can prepare the input

$$|\psi\rangle = \cos\vartheta_0 |u\rangle + \sin\vartheta_0 |s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = c_{\vartheta_0} |\vartheta_0\rangle + c_{-\vartheta_0} |-\vartheta_0\rangle .$$

At least one of the two coefficients is $> 1/\sqrt{2}$. Then we will surely obtain $|\vartheta_0\rangle$ or $|-\vartheta_0\rangle$ we finite probability.