Grover's algorithm.

Suppose we are given a boolean function $f: \mathbb{B}^n \to \mathbb{B}$ and would like to find $x \in \mathbb{B}^n$ with $f(x) = 1$. We will assume that the quantum circuit Q_f, implementing f is given. The fastest classical algorithm can solve the problem in $\theta(2^n)$ steps. We will discuss a quantum algorithm due to L. Grover, which works in $\theta(\sqrt{2^n})$ steps.

As usual, we start with the state $|0^n\rangle$ and put it in a generic superposition via application of $H^{\otimes n}$:

$$H^{\otimes n}(|0^n\rangle) = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \quad (N = 2^n)$$

Suppose there are $1 \leq t \leq N$ elements $x \in \mathbb{B}^n$ with $f(x) = 1$, then we can write

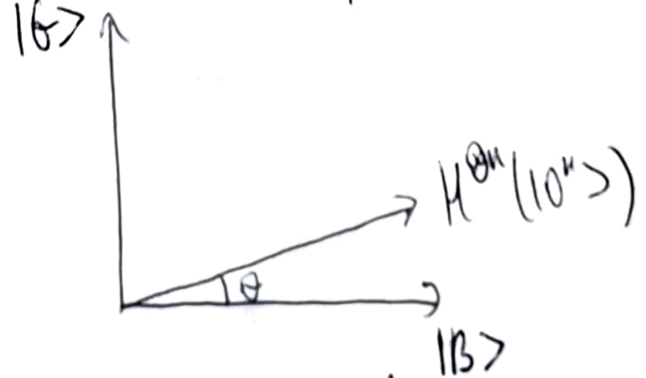
$$H^{\otimes n}(|0^n\rangle) = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle = \sqrt{\frac{N}{t}} \sum_{s, f(i_s)=1}^{t-1} |i_s\rangle + \sqrt{\frac{N-t}{N}} \sum_{\ell, f(i_\ell)=0} |i_\ell\rangle$$

$$\underset{(\text{good})}{\frac{1}{\sqrt{t}} \sum_{s, f(s)=1}^{t-1} |i_s\rangle =: |G\rangle} \Big\} \underset{(\text{bad})}{\frac{1}{\sqrt{N-t}} \sum_{\ell, f(i_\ell)=0} |i_\ell\rangle =: |B\rangle}$$

Notice that setting $\theta := \arcsin(\sqrt{t/N})$ allows to write

$$H^{\otimes n}(|0^n\rangle) = \sin(\theta)|G\rangle + \cos(\theta)|B\rangle$$

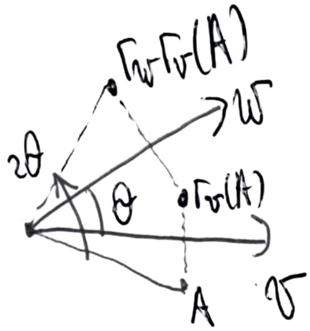
There is a nice geometric picture 'behind' the current state. Let's take a look. First, notice that the vectors $|G\rangle$, $|B\rangle$ and $H^{\otimes n}(|0^n\rangle)$ lie in a 2-dimensional real vector space spanned by the vectors $|G\rangle$ and $|B\rangle$. Moreover, $|G\rangle$ and $|B\rangle$ are orthogonal (since if $|G\rangle = \frac{1}{\sqrt{t}}(a_1, a_2, \dots, a_N)$, then $|B\rangle = \frac{1}{\sqrt{N-t}}(1-a_1, 1-a_2, \dots, 1-a_N)$ with $a_j \in \{0,1\}$) and $H^{\otimes n}(|0^n\rangle)$ forms angle θ with $|B\rangle$. It is reasonable to assume that $t \ll N$ (otherwise, we can find a solution reasonably fast by trying out a few random $x \in \mathbb{B}^n$), so $\theta = \arcsin(\sqrt{t/N})$ is small.



The main idea of the algorithm is to realize a counter-clockwise rotation of $H^{\otimes n}(|0^n\rangle)$ by 2θ in the $(|G\rangle, |B\rangle)$-plane. It is called 'Grover iteration' and, being applied $m = \lfloor \frac{\pi}{4\theta} \rfloor$ times, produces a vector very close to $|G\rangle$.

Quick digression: rotation as a product of reflections.

Let $v, w \in \mathbb{R}^2$ be two vectors and r_v, r_w reflections with respect to those vectors. Then $r_w r_v$ is rotation by 2θ from v to w (here $\theta = \arccos\left(\frac{(v,w)}{|v|\cdot|w|}\right)$ is the angle between v and w).



Rmk. By reflection with respect to v we understand the linear map that leaves v in place and maps any vector orthogonal to v to its negative:
$r_v(v) = v$, $r_v(h) = -h$ for h with $(h, v) = 0$.

It will be a HW exercise to verify that the composition of two such reflections is rotation by twice the angle between the corresponding vectors (see the picture above).

Luckily, we already have reflection with respect to $|B\rangle$!
Let's take a look at the oracle $\mathcal{O}_f$:

$$\mathcal{O}_f(|i\rangle|-\rangle) = (-1)^{f(i)}|i\rangle|-\rangle, \text{ hence,}$$

$$\mathcal{O}_f(|B\rangle|-\rangle) = |B\rangle|-\rangle \quad \left(\text{as } |B\rangle = \left(\sum_{\underline{i_e, f(i_e)=0}} |i_e\rangle\right) \cdot \frac{1}{\sqrt{N-t}}\right).$$

On the other hand, $\langle B|v\rangle = 0$ for a vector $|v\rangle = \sum_{i=0}^{N-1} \alpha_i |i\rangle$ implies $\sum_{i_e, f(i_e)=0} \alpha_{i_e} = 0$ forcing $\mathcal{O}_f(|v\rangle|-\rangle) = |v\rangle|-\rangle$ ONLY if all $\alpha_{i_e} = 0$!

To summarize:

- $\mathcal{O}_f$ restricted to the 2-dimensional plane $\mathbb{R}^2 = \mathbb{R}\langle |G\rangle, |B\rangle\rangle$ is a reflection with respect to $|B\rangle$ ($r_{|B\rangle}$) (exactly what we need!)
- $\mathcal{O}_f$ acts as a reflection with respect to the $(N-t)$-dim-l plane spanned by $|i\rangle|-\rangle$ with $f(|i\rangle) = 0$ on the ambient N-dim-l space (we won't need that).

Next we need an operator (circuit) for reflection with respect to $H^{\otimes n}(|0^n\rangle)$. First, let's see what an operator of reflection with respect to a vector is.

Let $(V, (\cdot,\cdot))$ be a finite-dimensional vector space and $v \in V$ a vector. Then $r_v : V \to V$, $r_v(w) = \frac{2(v,w)}{(v,v)} v - w$ or

$r_v(\cdot) = \frac{2(v,\cdot)}{(v,v)} v - Id$ is the linear operator representing reflection with respect to v. Indeed, we check that

- $r_v(v) = \frac{2(v,v)}{(v,v)} v - v = 2v - v = v$
- $r_v(w) = \frac{2(w,v)}{(v,v)} v - w = -w$ for $w \in V$, $(w,v) = 0$.

Notice that as any state vector has norm, the formula above simplifies to $r_{|v\rangle}(\cdot) = 2\langle v|\cdot\rangle|v\rangle - Id$. That looks cumbersome and is written (in Dirac's notation) as

$r_{|v\rangle} = 2|v\rangle\langle v| - Id$. Hence, the operator we need is

$2|H^{\otimes n}(|0^n\rangle)\rangle\langle H^{\otimes n}(|0^n\rangle)| - Id$, which can be written as

$$H^{\otimes n}(2|0^n\rangle\langle 0^n| - Id)H^{\otimes n}.$$

There is a 'line of linear algebra' to verify the last equality, which can be summarized as

reflect with respect to Av (some lin. operator A)	=	map Av to v (using A^{-1}), reflect with respect to v, map back to the original (using A).

In our case $A = A^{-1} = H^{\otimes n}$.

We got a formula for Grover's iterate:

$$G = H^{\otimes n}(2|0^n\rangle\langle 0^n| - Id)H^{\otimes n} O_f.$$

Notice that our generic state ($H^{\otimes n}(|0^n\rangle)$) forms angle θ with state vector $|B\rangle$, so after m aplications of Grover's iterate G, the angle will become $(2m+1)\theta$. Our goal is to get $(2m+1)\theta$ close to $\frac{\pi}{2}$ (as the angle between $|B\rangle$ and $|G\rangle$ is $\pi/2$). Therefore, we need to apply G

$m = \lfloor \frac{\pi}{4\theta} \rfloor \approx \lfloor \frac{\pi}{4} \cdot \sqrt{\frac{N}{t}} \rfloor$ ($\sin\theta \sim \theta$ for small values of θ).

The algorithm can be summarized as follows.

1. Start (initiate) with the generic state $H^{\otimes n}(|0^n\rangle|-\rangle) = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle|-\rangle$.
2. Apply Grover's iterate G for m times (G and m given above).
3. Measure and check that the resulting state $|j\rangle$ has $f(j) = 1$.

Example. Jane wants to throw a party. She invites Alice, Carol and Steve. However, certain conditions have to be met.

- Alice joins the party only together with Carol and if Steve doesn't show up.
- Steve participates only if so does Carol, but Carol doesn't want his company (she doesn't join if he does).

We see that there are two arrangements of participants satisfying the aforementioned conditions:

(1) noone comes to the party $\rightsquigarrow$ state $|0\rangle = |000\rangle$

(2) Alice and Carol come to the party $\rightsquigarrow$ state $|6\rangle = |110\rangle$

Let's see how the application of Grover's algorithm gives these answers. Notice that $N = 8 = 2^3$ and $t = 2$, so $t/N = \frac{1}{4}$ and $\theta = \arcsin(\sqrt{t/N}) = \frac{\pi}{6}$ giving $2m+1 = \frac{\pi}{2\theta} = 3$. Thus Grover's iterate G should be applied $m = 1$ time and will produce the state $|G\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |\underset{\text{Alice}}{1}\underset{\text{Carol}}{1}0\rangle)$.

As $\theta = \frac{\pi}{6}$, we get $H^{\otimes 3}(|0^3\rangle)|-\rangle = (\frac{1}{2}|G\rangle + \frac{\sqrt{3}}{2}|B\rangle)|-\rangle$.

The state transforms as follows:

$$\left(\frac{1}{2}|G\rangle + \frac{\sqrt{3}}{2}|B\rangle\right)|-\rangle \xrightarrow{O_f} \left(-\frac{1}{2}|G\rangle + \frac{\sqrt{3}}{2}|B\rangle\right)|-\rangle =$$

$$= \left(-\frac{1}{2\sqrt{2}}(|000\rangle + |110\rangle) + \frac{\sqrt{3}}{2}\cdot\frac{1}{\sqrt{6}}(|001\rangle + |010\rangle + |100\rangle + |101\rangle + |011\rangle + |111\rangle)\right)|-\rangle$$

$$\xrightarrow{H^{\otimes 3}} \left(-\frac{1}{2\sqrt{2}}\left(|{+}{+}{+}\rangle + |{-}{-}{+}\rangle\right) + \frac{1}{2\sqrt{2}}\left(|{+}{+}{-}\rangle + |{+}{-}{+}\rangle + |{-}{+}{+}\rangle + |{-}{+}{-}\rangle + |{+}{-}{-}\rangle + |{-}{-}{-}\rangle\right)\right)|{-}\rangle$$

$$\xrightarrow{2|0^3\rangle\langle 0^3| - Id} \frac{1}{2\sqrt{2}}\left(-\left(\frac{4}{\sqrt{8}}|0^3\rangle - |{+}{+}{+}\rangle - |{-}{-}{+}\rangle\right) + \left(\frac{12}{\sqrt{8}}|0^3\rangle - |{+}{+}{-}\rangle - |{+}{-}{+}\rangle - |{-}{+}{+}\rangle - |{-}{+}{-}\rangle - |{+}{-}{-}\rangle - |{-}{-}{-}\rangle\right)\right)|{-}\rangle = \frac{1}{2\sqrt{2}}\left(\frac{|000\rangle}{\sqrt{8}} + |{+}{+}{+}\rangle + |{-}{-}{+}\rangle - |{+}{+}{-}\rangle - |{+}{-}{+}\rangle - |{-}{+}{+}\rangle - |{-}{+}{-}\rangle - |{+}{-}{-}\rangle - |{-}{-}{-}\rangle\right)|{-}\rangle$$

$$\xrightarrow{H^{\otimes 3}} \frac{1}{2\sqrt{2}}\left(\frac{|{+}{+}{+}\rangle}{\sqrt{8}} + |000\rangle + |110\rangle - |001\rangle - |010\rangle - |100\rangle - |101\rangle - |011\rangle - |111\rangle\right)|{-}\rangle =$$

$$= \frac{1}{2\sqrt{2}}\left(2|000\rangle + 2|110\rangle\right) = \frac{1}{\sqrt{2}}\left(|000\rangle + |110\rangle\right) = |\sigma\rangle.$$

Rmk (1) To make sure the transformation on the second line is clear, let's compute $(2|0^3\rangle\langle 0^3| - Id)(|{+}{+}{+}\rangle)$:

$$(2|0^3\rangle\langle 0^3| - Id)|{+}{+}{+}\rangle = (2|0^3\rangle\langle 0^3| - Id)\left(\frac{1}{\sqrt{8}}(|000\rangle + \ldots + |111\rangle)\right) =$$

$$= \frac{2}{\sqrt{8}}|000\rangle - |{+}{+}{+}\rangle.$$

(2) The function $f: \mathbb{B}^3 \to \mathbb{B}$ that we used was

x	$f(x)$
000	1
001	0
010	0
100	0
011	0
101	0
110	1
111	0.
ACS	

The three bits of the input were responsible for participation of corresponding person, while the value of f on a particular arrangement was 1 if the arrangement satisfied all of the requirements in the statement and 0 otherwise.

A few more words on Grover's algorithm.

Def-n. A <u>query</u> is a request for data or information from a database table.

Q.: how many queries does Grover's algorithm 'use'?

We found that Grover's iterate G should be applied $m = \frac{\pi}{4\theta} - \frac{1}{2}$ times (well, actually $\tilde{m}$, the closest integer to m, times). As $\theta = \arcsin\left(\sqrt{\frac{t}{N}}\right) \geq \sqrt{\frac{t}{N}}$, we get

$$m = \frac{\pi}{4\theta} - \frac{1}{2} \leq \frac{\pi}{4\sqrt{\frac{t}{N}}} - \frac{1}{2} \leq \sqrt{N}.$$

* Each application of G requires a single query (application of oracle O_f).

Rmk. As we do not know anything about f, any classical algorithm would require $O(N)$ queries.

Probability of error.

After $\tilde{m}$ iterations of G, the state becomes

$$\sin((2\tilde{m}+1)\theta)|G\rangle + \cos((2\tilde{m}+1)\theta)|B\rangle$$

and the error 'hides in the $|B\rangle$ part'.

$P(\text{error}) = P(\text{collapsing to one of states } |i\rangle \text{ with } f(i)=0) =$

$$= \cos^2((2\tilde{m}+1)\theta) \cdot \left(\frac{1}{\sqrt{N-t}}\right)^2 \cdot (N-t) = \cos^2((2\tilde{m}+1)\theta) = \cos^2((2m+1)\theta +$$
$$+ 2(\tilde{m}-m)\theta) = \cos^2\left(\frac{\pi}{2} + 2(\tilde{m}-m)\theta\right) =$$

$$= \sin^2(2(\tilde{m}-m)\theta) \underset{\substack{\uparrow \\ |\tilde{m}-m|\leq\frac{1}{2}}}{\leq} \sin^2(\theta) \leq \frac{t}{N}.$$

<u>Important rmk</u>. We assumed that t is known (as in Grover's version of the algorithm).

There is a modification (for unknown t), which 'works as fast' as the presented algorithm (see the paper on Canvas).