Grover's Algorithm.

A fast algorithm to find all x^* such that $f(x^*)=1$.
for given function $f(x) = \begin{cases} 1 & \text{if } x = x^* \\ 0 & \text{if } x \neq x^* \end{cases}$

Given $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \Sigma^n} |x\rangle$, our goal is to change this

uniform superpositioned qubit such that when we measure $|\psi\rangle$, it will have a probability of getting x^*.

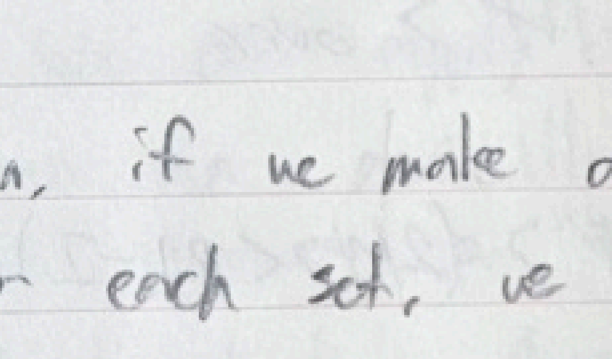
Let $A_0 = \{x \in \Sigma^n, f(x) = 1\}$: set of x^*
$A_1 = \{x \in \Sigma^n, f(x) = 0\}$: set of $\Sigma^n - x^*$

Then, if we make an uniform superpositioned qubit for each set, we can express them as the following

$$|A_0\rangle = \frac{1}{\sqrt{|A_0|}} \sum_{x \in A_0} |x\rangle, \quad |A_1\rangle = \frac{1}{\sqrt{|A_1|}} \sum_{x \in A_1} |x\rangle.$$

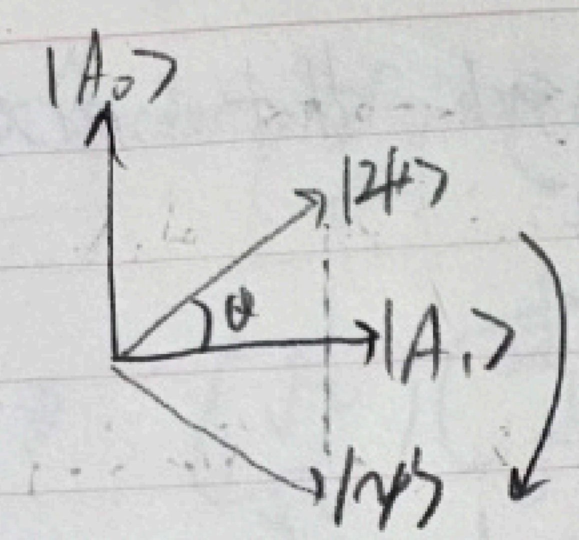
We know that these two vectors are orthonormal, and they can span to $|\psi\rangle$ such that

$$|\psi\rangle = \frac{\sqrt{|A_0|}}{\sqrt{N}} |A_0\rangle + \frac{\sqrt{|A_1|}}{\sqrt{N}} |A_1\rangle.$$



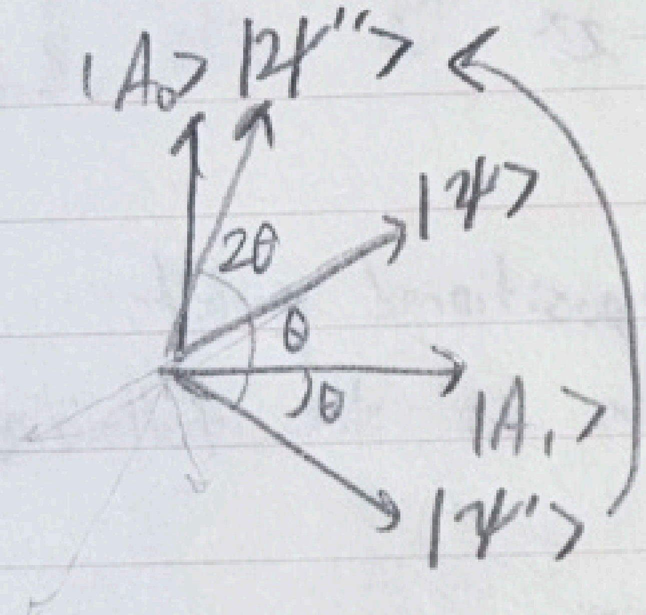
Geometrically, our goal is to modify $|\psi\rangle$ such that it gets closer to $|A_0\rangle$, which are the answer sets we would like to find.

To do this, we flip the qubits.

① 

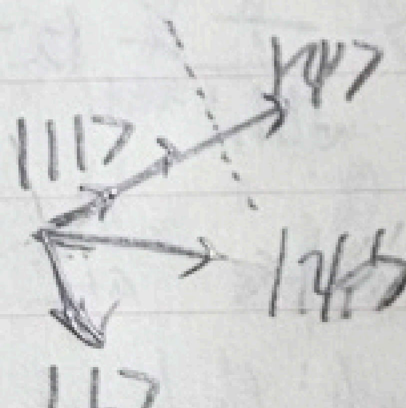
We first flip $|\psi\rangle$ such that

$$|\psi'\rangle = -\frac{\sqrt{|A_0|}}{\sqrt{N}}|A_0\rangle + \frac{\sqrt{|A_1|}}{\sqrt{N}}|A_1\rangle$$

② 

Then we flip $|\psi'\rangle$ over $|\psi\rangle$

such that $|\psi''\rangle = (2|\psi\rangle\langle\psi| - I)|\psi'\rangle$



$|\psi'\rangle = |\perp\rangle + |\parallel\rangle$ parallel to $|\psi\rangle$

$|\perp\rangle - |\parallel\rangle$

$$|\parallel\rangle = \underbrace{\langle\psi|\psi'\rangle}_{\text{inner product}}|\psi\rangle$$

$$|\perp\rangle = |\psi'\rangle - |\parallel\rangle$$

$$\Rightarrow |\psi''\rangle = |\parallel\rangle - |\perp\rangle$$
$$= |\parallel\rangle + |\parallel\rangle - |\psi'\rangle$$
$$= 2|\parallel\rangle - |\psi'\rangle$$
$$= 2\langle\psi|\psi'\rangle|\psi\rangle - |\psi'\rangle$$
$$= 2|\psi\rangle\langle\psi|\psi'\rangle - |\psi'\rangle = (2|\psi\rangle\langle\psi| - I)|\psi'\rangle$$

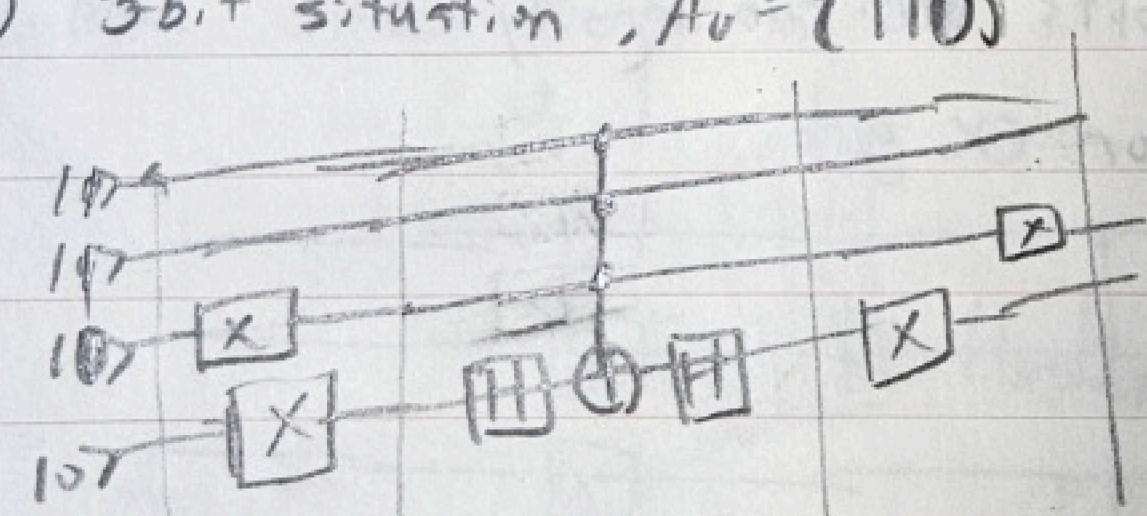
By repetitively doing these two flipping operations, we can make $|\psi\rangle$ become closer to $|A_0\rangle$.

How to implement Grover's Algorithm in a Quantum Circuit

As explained before, it is divided in 2 steps. ①, ②
We will call ① as the "Oracle," and ② as "Diffusion",

① Oracle. : In order to make an oracle, we need the answer set A_0 and flip the answer sets into -1.
We can apply -1 by either using the Z gate on an anicilla bit

ex) 3bit situation, $A_0 = \{110\}$



$|1100\rangle$ $|1111\rangle$ $-|1111\rangle$ $-|1100\rangle$

② Diffusion : The diffusion operation is $2|\psi\rangle\langle\psi| - I$.
But this is hard to express directly on the circuit so we use Hadamard gates such that

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

Hermitian Conjugate Operator.
$|\phi\rangle = A|\psi\rangle$ if and only if $\langle\phi| = \langle\psi|A^{+}$

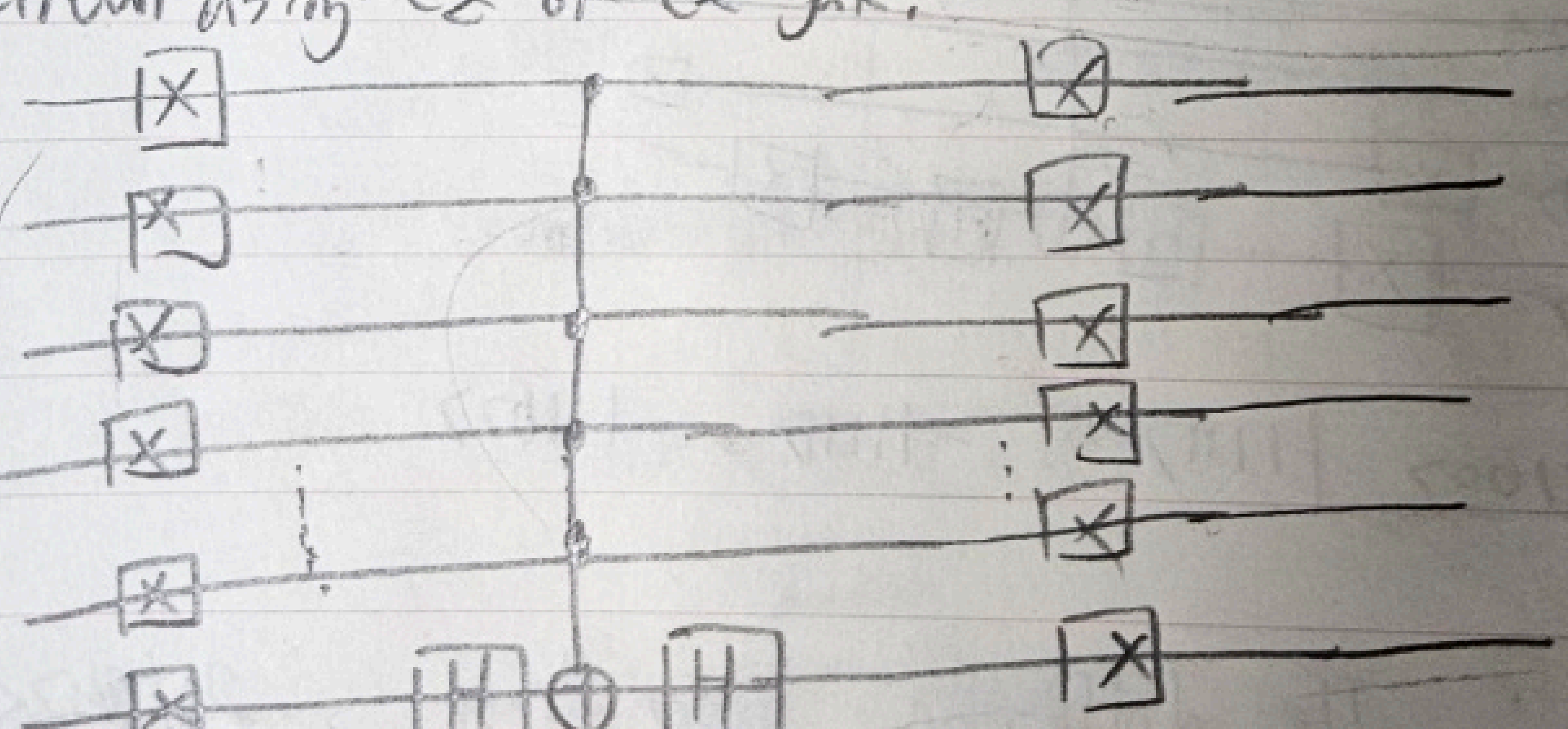
The Hadamard gates can be easily applied to the circuit.

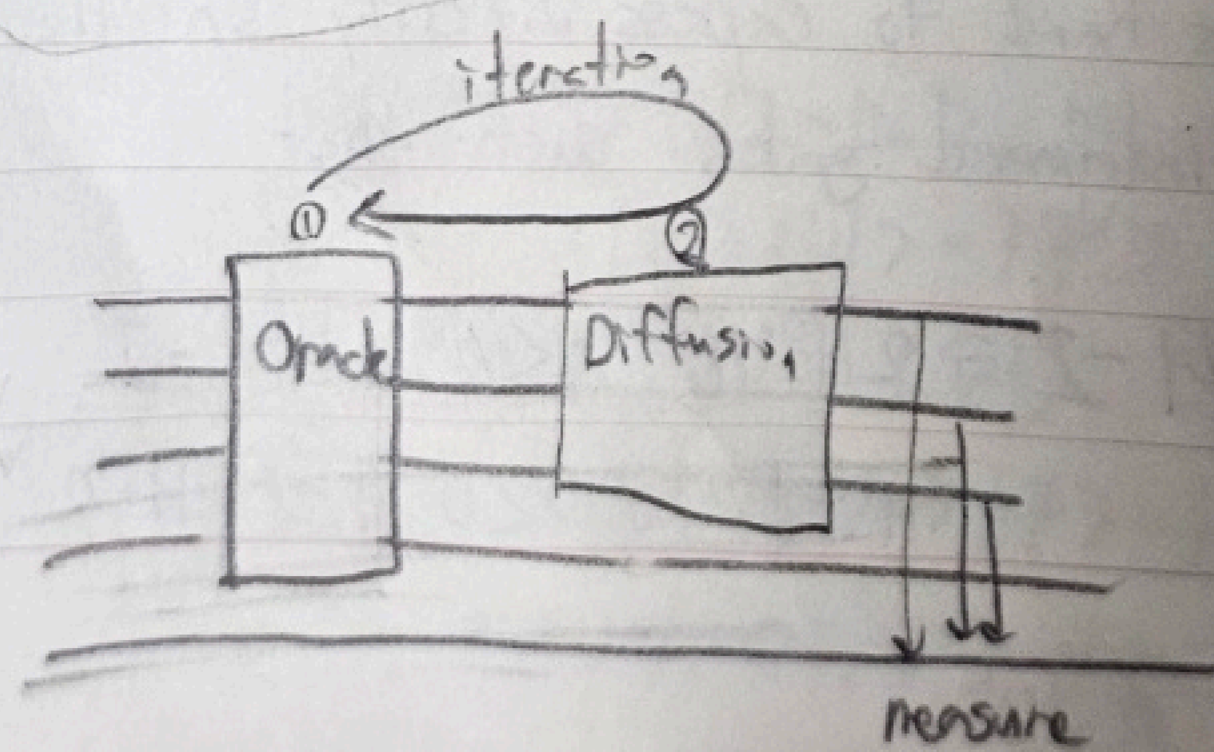
$2|0^{\otimes n}\rangle\langle 0^{\otimes n}| - I$ can be represented as a matrix with the standard basis of $\begin{bmatrix}1\\0\\\vdots\end{bmatrix}\begin{bmatrix}0\\1\\0\\\vdots\end{bmatrix}\begin{bmatrix}0\\0\\1\\0\\\vdots\end{bmatrix}$ ...... $\begin{bmatrix}0\\0\\\vdots\\0\\1\end{bmatrix}$

$$\begin{bmatrix}2&0&0&\cdots\\0&0&&\\\vdots&&\ddots&\\&&&\end{bmatrix} - \begin{bmatrix}1&0&\cdots&\\0&1&0&\cdots\\\vdots&&1&\\&&&\ddots\end{bmatrix}$$

$$= \begin{bmatrix}1&0&0&\cdots\\0&-1&&\\&&-1&\\\vdots&&&\ddots\\&&&&-1\end{bmatrix}. \qquad \begin{bmatrix}-1&&&\\&1&&\\&&1&\\&&&1\end{bmatrix}$$

This operation matrix means that if the input is not $|0^{\otimes n}\rangle$, it will -inverse the qubits. We can easily make such circuit using the CZ or CX gate.





①+②