Lectures 10 - 11

QUANTUM SEARCH ALGORITHM (Grover's search)

(pages 248-255, 256 of the textbook)

Suppose that you have N possible routes to get from one place to another and you would like to find the shortest routes.

Solution: check through all the routes and find the shortest one.
Classical computer requires O(N) operations to find the shortest way.
Quantum computer requires only $\sqrt{N}$ operations using Grover's search algorithm.

Problem: we search through the space of N elements. Let's deal with the index of the elements: 0, 1, … N-1. We assume for convenience that $N=2^n$, i.e. that index can be stored in n bits. Our search problem has M solutions: $1 \le M \le N$.

We define a function f(x):

f(x)=1 if x=0..N-1 is a solution to our problem
f(x)=0 if x is not a solution.

Now we introduce a **quantum oracle**. It is a black box that can recognize the solutions to the search problem defined above. We will discuss what circuit can be in the black box for a particular example of the search problem later. For now, it is only important what the quantum oracle does.

$$|x\rangle|q\rangle \xrightarrow[\text{oracle}]{O} |x\rangle\underbrace{|q\oplus f(x)\rangle}$$

oracle qubit

q is flipped if f(x)=1 and left unchanged if f(x)=0

Value of x that we want to check (solution or not?). It is an integer register 0 ... N-1 which labels all possible elements.

How to check the solution?

$$|x\rangle|0\rangle \xrightarrow{O} \begin{cases} |x\rangle|0\rangle \\ \text{or} \\ |x\rangle|1\rangle \end{cases}$$

$\leftarrow$ Index x corresponds to the element which is a solution to the problem.

Let's change it so the oracle qubit itself does not change.

$$|x\rangle\left[\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right] \xrightarrow{O} \begin{cases} \text{not solution} \\ |x\rangle\left[\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right] \\ \text{solution} \\ |x\rangle\left[\frac{1}{\sqrt{2}}(|1\rangle-|0\rangle)\right] \end{cases}$$

$$\underbrace{|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)} \xrightarrow{O} (-1)^{f(x)}\, |x\rangle \underbrace{\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)}_{\text{oracle qubit}}$$

Remember, $f(x)=1$ if x is a solution and $f(x)=0$ if x is not a solution

Oracle qubit is always unchanged now so we can omit it from the discussion.

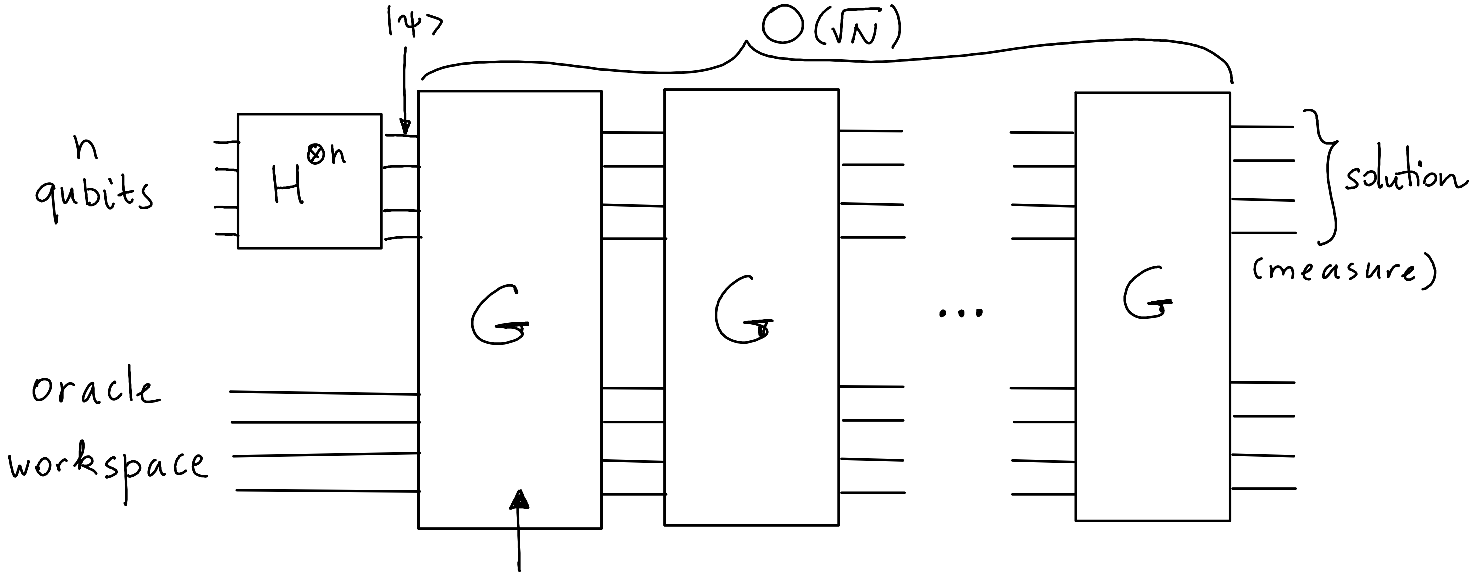
Oracle marks the solution $\quad |x\rangle \xrightarrow{O} (-1)^{f(x)}\,|x\rangle$

Example: we can factor number m by checking through all prime numbers from x=2 to $\sqrt{m}$. Oracle will calculate m/x to check if x is a factor and flip the oracle qubit if it is so. Note: this is not an efficient way to factor.

Summary: oracle recognizes the solution.

Grover iteration & search procedure

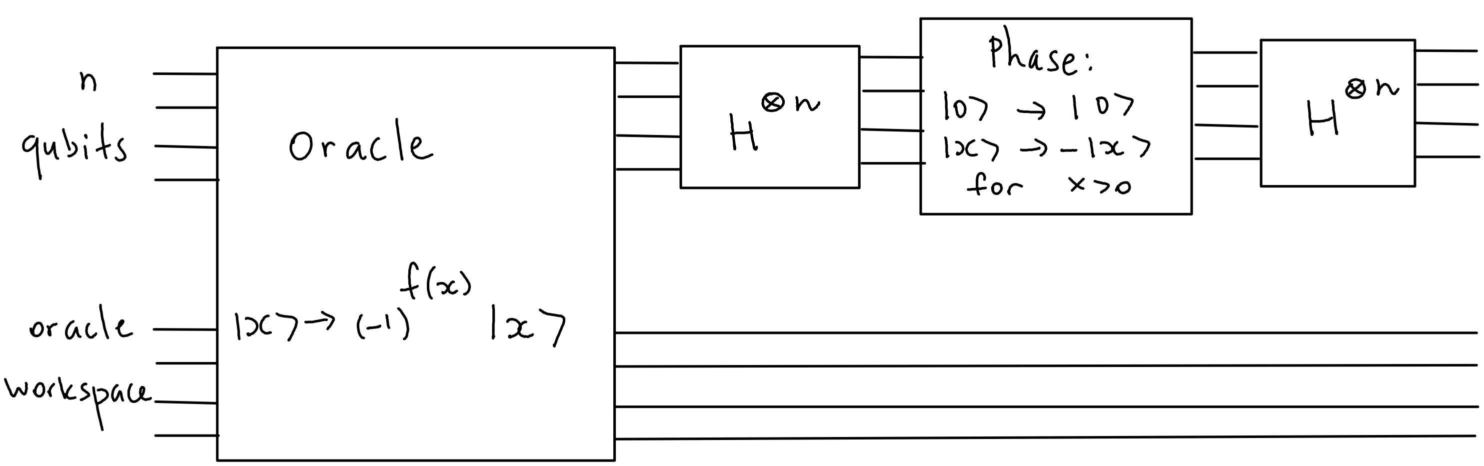
Goal: find a solution with least applications of the oracle.



Initial state of the N qubits : $|0\rangle^{\otimes n}$

After $H^{\otimes n}$: $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ (Register is randomized).

Grover's iteration circuit:



(1) Apply the oracle

(2) Apply the $H^{\otimes n}$

(3) Conditionally shift phase

(4) Apply the $H^{\otimes n}$ again

Let's consider step #3 (conditional phase shift) in more detail.
State $|0\rangle$ is the only state which phase is not shifted.

Operator for step 3 is: $S_3 = 2|0\rangle\langle 0| - I$

Why?

Check its action on $|x\rangle$:

If $|x\rangle \equiv |0\rangle \Rightarrow \quad S_3|0\rangle = (2|0\rangle\langle 0| - I)|0\rangle = |0\rangle$

If $|x\rangle \not\equiv |0\rangle \Rightarrow$

$S_3|x\rangle = (2|0\rangle\langle 0| - I)|x\rangle = -|x\rangle \Rightarrow$

S_3 operator shifts phase of $|x\rangle$ if $|x\rangle \not\equiv |0\rangle$

$S_2 S_3 S_4$ operator: $\quad H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} =$

$= 2|\psi\rangle\langle\psi| - I$

Remember that $\quad |\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$

Therefore, the result of Grover's iteration is:

oracle

$$\boxed{G = (2|\psi\rangle\langle\psi| - I)\,O}$$

What does the Grover iteration do?

We define (normalized) states

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x{}'' |x\rangle$$

number of elements (N); number of solutions (M)

$\sum''$ indicates sum over x which are <u>NOT</u> solutions to the problem

and

$$|\beta\rangle = \frac{1}{\sqrt{M}} \sum_x{}' |x\rangle$$

$\sum'$ indicates sum over solutions.

Initial state $|\psi\rangle$:

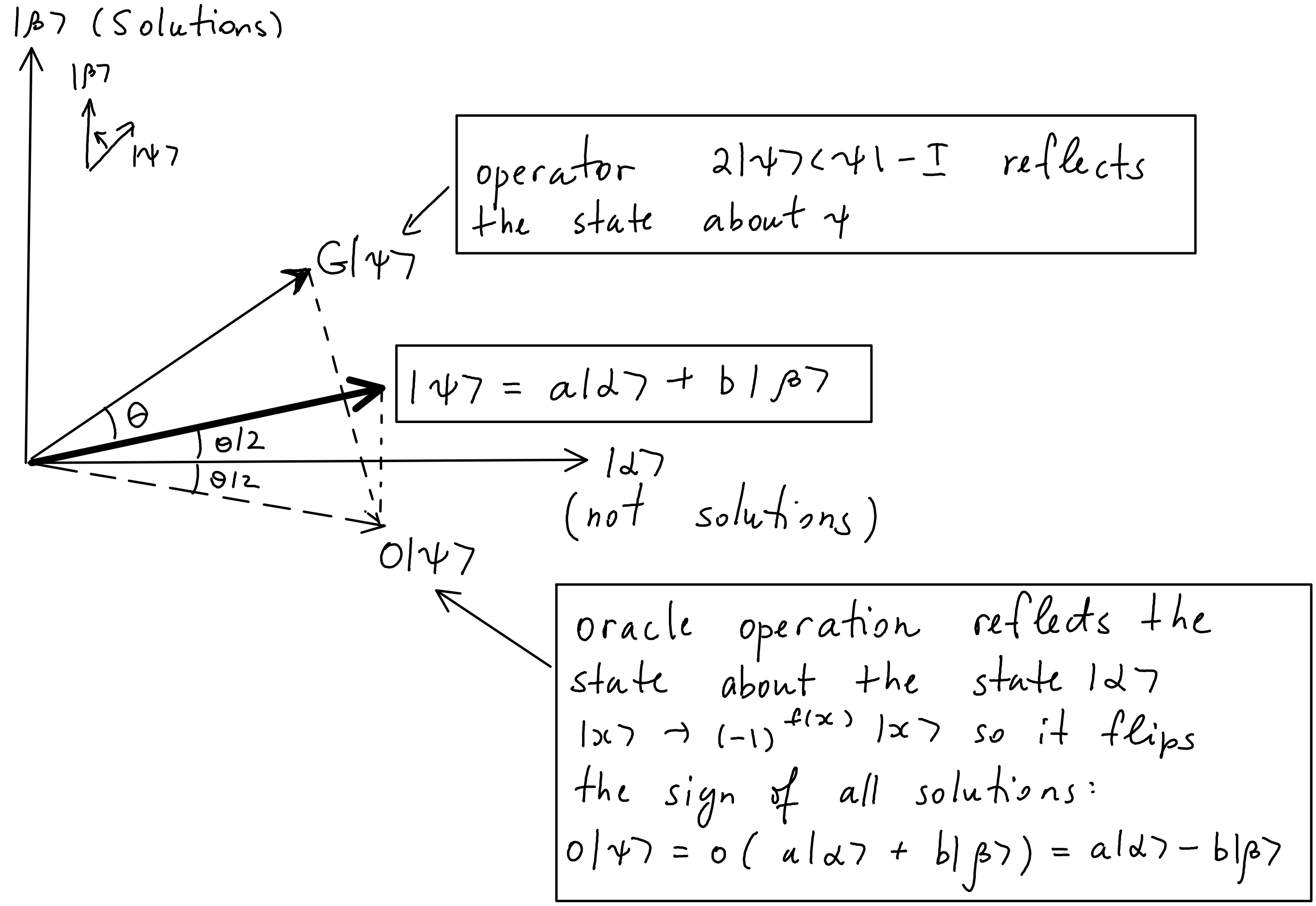
$$|\psi\rangle = \sqrt{\frac{N-M}{N}}\, |\alpha\rangle + \frac{\sqrt{M}}{\sqrt{N}}\, |\beta\rangle = \underbrace{\sum_x{}''}_{\text{(not solutions)}} \sqrt{\frac{N-M}{N}} \frac{1}{\sqrt{N-M}} |x\rangle$$

$$+ \underbrace{\sum_x{}'}_{\text{(solutions)}} \frac{1}{\sqrt{M}} \frac{\sqrt{M}}{\sqrt{N}} |x\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$$

sum over all states from 0 to N-1.

Remember: our states $|x\rangle$ represent indexes of elements 0 ... N-1 to be searched.

The action of a Grover iteration

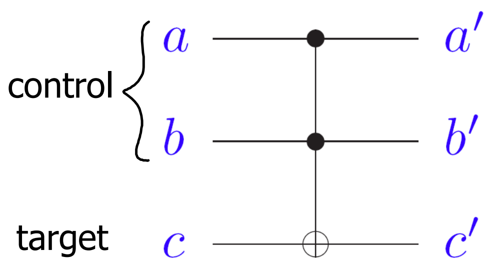


Product of two reflections is a rotation. Therefore, repeated applications of Grover iteration move vector $|\psi\rangle$ closer to $|\beta\rangle$. The measurement will give a solution with high probability since $|\beta\rangle$ includes all solutions.

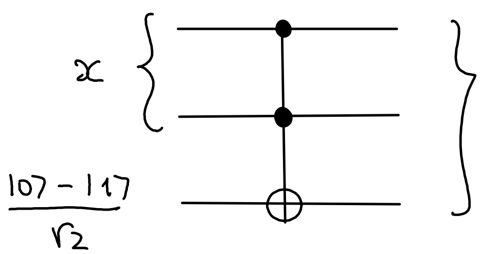
Quantum search: a two-bit example

N= 4

We use a version of Toffoli gate as a oracle.



If both a and b are $|1\rangle$ flip $|c\rangle$.



This will work as oracle to mark solution $x_0 = 3$ since it will change sign for $|11\rangle$

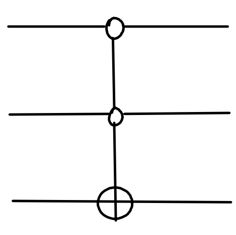
$$|11\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \to |11\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -|11\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

marks the solution $x_0 = 3$

Oracle: $|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle$

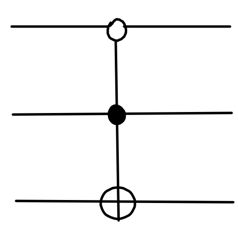
$f(x) = 0$ for $x_0 = 0, 1, 2$; $f(x) = 1$ for $x_0 = 3$

The following versions of Toffoli gate can be used for x_0=0, 1, 2:



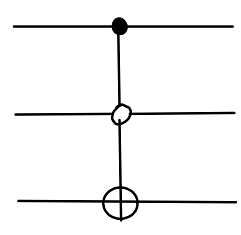
$x_0 = 0$

$|00\rangle$



$x_0 = 1$

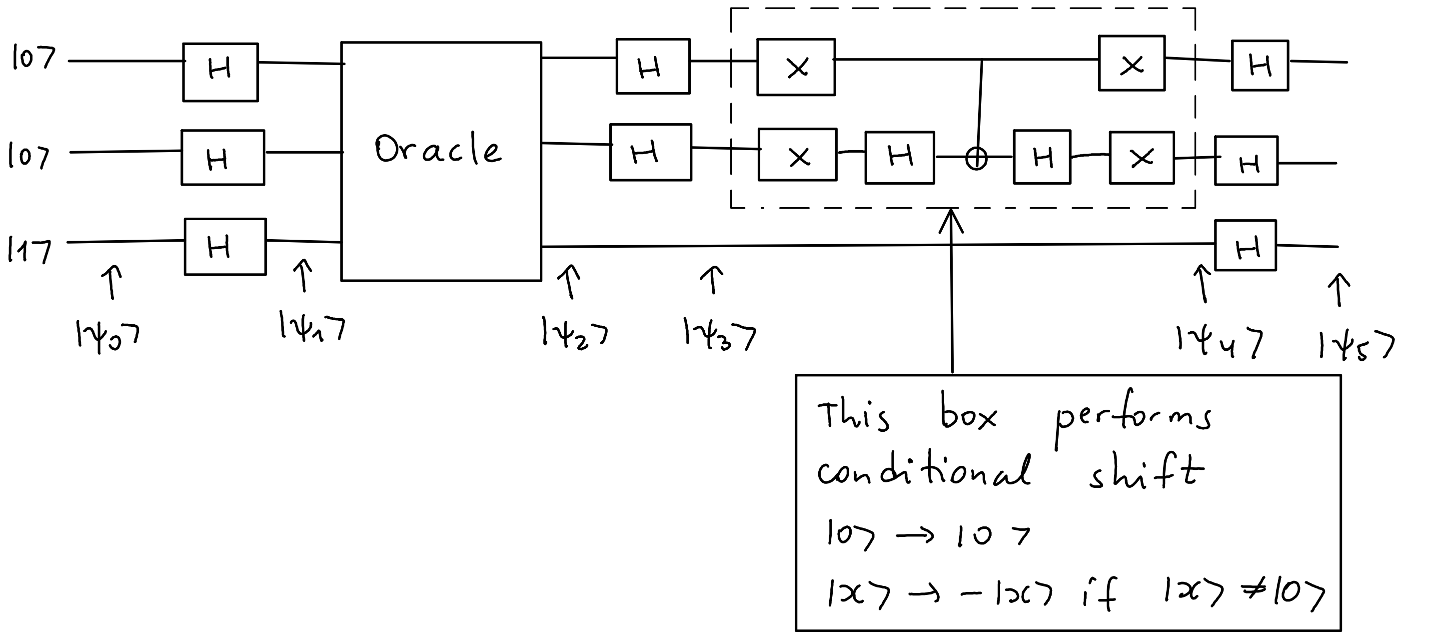
$|01\rangle$



$x_0 = 2$

$|10\rangle$

Circuit for a two-bit quantum search



Exercise for the class: demonstrate that the measurement on first two qubits after this circuit will give |01> when the corresponding oracle (x_0=1) is used.

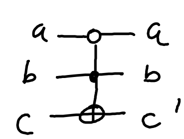
Our initial state is $|\psi_0\rangle = |00\underset{\uparrow}{1}\rangle$ oracle qubit

$$|\psi_1\rangle = H|0\rangle H|0\rangle H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$= \frac{1}{\sqrt{4}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{\text{oracle qubit}}$$

$$|\psi_2\rangle = \underset{\text{oracle}}{O}|\psi_1\rangle = \frac{1}{\sqrt{4}}(|00\rangle + |10\rangle + |11\rangle)\frac{|0\rangle - |1\rangle}{\sqrt{2}} + |01\rangle\frac{|1\rangle - |0\rangle}{\sqrt{2}}$$

This version of Toffoli gate



flips c if $|ab\rangle = |01\rangle$.
Otherwise, nothing changes.

$$|\psi_2\rangle = \frac{1}{2}\left[\,|00\rangle - |01\rangle + |10\rangle + |11\rangle\,\right]\underbrace{\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]}$$

Oracle qubit does not change and is not used in the remaining circuit. Therefore, we can omit it from now on.

Next, we consider how $H^{\otimes 2}$ gates affect $|\psi_2\rangle = \frac{1}{2}\left[|00\rangle - |01\rangle + |10\rangle + |11\rangle\right]$

(omitted oracle qubit)

$$H^{\otimes 2}|00\rangle = \frac{1}{2}\{|00\rangle + |01\rangle + |10\rangle + |11\rangle\}$$

$$H^{\otimes 2}|01\rangle = \frac{1}{2}\{|00\rangle - |01\rangle + |10\rangle - |11\rangle\}$$

$$H^{\otimes 2}|10\rangle = \frac{1}{2}\{|00\rangle + |01\rangle - |10\rangle - |11\rangle\}$$

$$H^{\otimes 2}|11\rangle = \frac{1}{2}\{|00\rangle - |01\rangle - |10\rangle + |11\rangle\}$$

$$\begin{aligned}|\psi_3\rangle = H^{\otimes 2}|\psi_2\rangle = \frac{1}{4}\{\, & |00\rangle + |01\rangle + \cancel{|10\rangle} + |11\rangle \\ & - \cancel{|00\rangle} + |01\rangle - \cancel{|10\rangle} + \cancel{|11\rangle} \\ & + \cancel{|00\rangle} + \cancel{|01\rangle} - |10\rangle - \cancel{|11\rangle} \\ & + |00\rangle - \cancel{|01\rangle} - |10\rangle + |11\rangle \,\}\end{aligned}$$

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

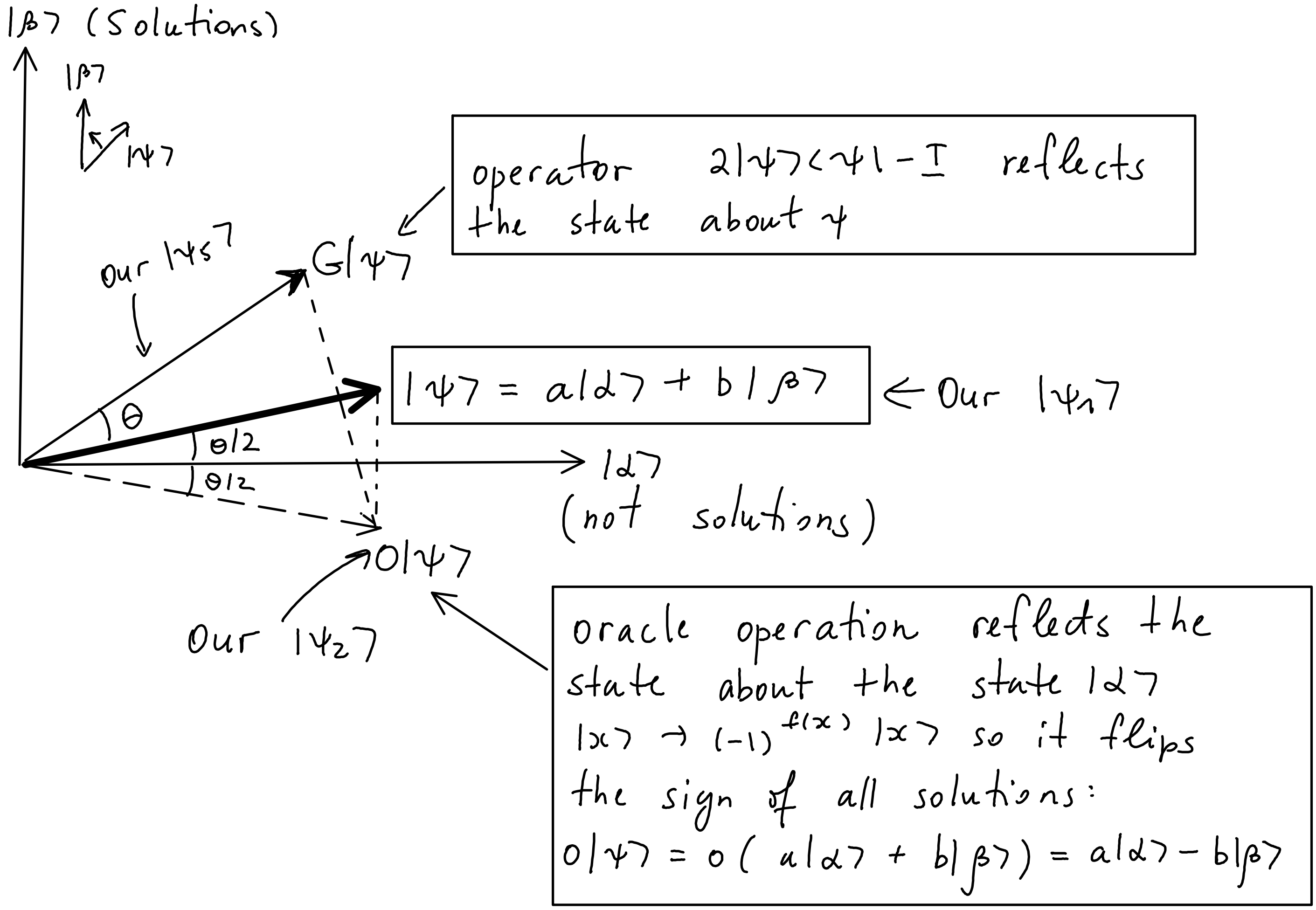
$$|\psi_4\rangle = S_3|\psi_3\rangle = \frac{1}{2}\{|00\rangle - |01\rangle + |10\rangle - |11\rangle\}$$

Conditional phase shift, all signs are flipped except for $|00\rangle$.

$$\begin{aligned}|\psi_5\rangle = H^{\otimes 2}|\psi_4\rangle = \frac{1}{4}\{\, & \cancel{|00\rangle} + |01\rangle + \cancel{|10\rangle} + \cancel{|11\rangle} \\ & - \cancel{|00\rangle} + |01\rangle - \cancel{|10\rangle} + \cancel{|11\rangle} \\ & + \cancel{|00\rangle} + |01\rangle - \cancel{|10\rangle} - \cancel{|11\rangle} \\ & - \cancel{|00\rangle} + |01\rangle + \cancel{|10\rangle} - \cancel{|11\rangle} \,\}\end{aligned}$$

$$= \frac{1}{4}\cdot 4|01\rangle = |01\rangle \equiv |x_0\rangle!$$

Let's illustrate the geometric representation on this example.



Initial function $N = 4 \quad M = 1$ (one solution)

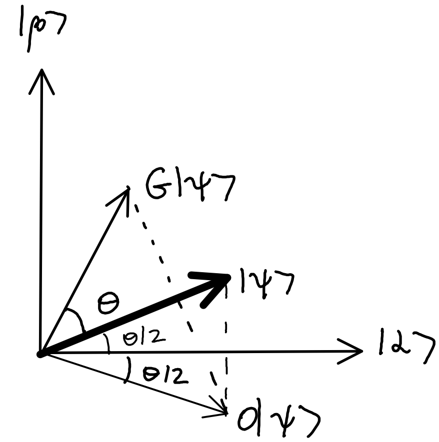
$$|\psi_1\rangle = \frac{1}{2}\{|00\rangle + |01\rangle + |10\rangle + |11\rangle\}$$ (Randomized register)

$$= \frac{\sqrt{3}}{\sqrt{4}}\frac{1}{\sqrt{3}}\underbrace{\{|00\rangle + |10\rangle + |11\rangle\}}_{\text{not solutions}} + \underbrace{\frac{1}{\sqrt{4}}|01\rangle}_{\text{solution}}$$

$$= \underbrace{\sqrt{\frac{N-M}{M}}}_{\sqrt{3}/\sqrt{4}}\underbrace{\left(\underbrace{\frac{1}{\sqrt{N-M}}}_{1/\sqrt{3}}\underbrace{\sum_x{}'' |x\rangle}_{(|00\rangle + |10\rangle + |11\rangle)}\right)}_{= |\alpha\rangle} + \underbrace{\sqrt{\frac{M}{N}}}_{\frac{1}{\sqrt{4}}}\underbrace{\left(\frac{1}{\sqrt{M}}\sum_x{}' |x\rangle\right)}_{|\beta\rangle}$$

$$\boxed{\begin{aligned} |\alpha\rangle &= \frac{1}{\sqrt{3}}(|00\rangle + |10\rangle + |11\rangle) \\ |\beta\rangle &= \frac{1}{\sqrt{4}}|01\rangle \end{aligned}}$$

Angle θ is determined from:



$$|\psi\rangle = \underbrace{\sqrt{\frac{N-M}{N}}}_{\cos\frac{\theta}{2}} |\alpha\rangle + \underbrace{\sqrt{\frac{M}{N}}}_{\sin\frac{\theta}{2}} |\beta\rangle$$

$$|\psi\rangle = \cos\frac{\theta}{2} |\alpha\rangle + \sin\frac{\theta}{2} |\beta\rangle$$

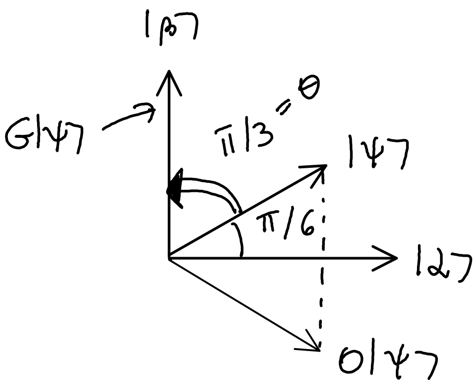
$$O|\psi\rangle = \cos\frac{\theta}{2} |\alpha\rangle - \sin\frac{\theta}{2} |\beta\rangle$$

$$G|\psi\rangle = \cos\frac{3\theta}{2} |\alpha\rangle - \sin\frac{3\theta}{2} |\beta\rangle$$

The θ is the rotation angle for Grover iteration.

In our case,

$$|\psi\rangle = \frac{\sqrt{3}}{\sqrt{4}} |\alpha\rangle + \frac{1}{\sqrt{4}} |\beta\rangle \Rightarrow \cos\frac{\theta}{2} = \frac{\sqrt{3}}{2} \quad \boxed{\theta = \frac{\pi}{3}}$$



$$\theta/2 = \pi/6$$

Therefore, one Grover iteration will rotate $|\psi\rangle$ to $|\beta\rangle$ exactly.

$$G|\psi\rangle = \underbrace{\cos\frac{3\theta}{2}}_{} |\alpha\rangle + \underbrace{\sin\frac{3\theta}{2}}_{} |\beta\rangle \equiv |\beta\rangle$$

$$\sin\frac{\pi}{2} = 1$$

$$\cos\frac{3\theta}{2} = \cos\frac{\pi}{2} = 0$$

$$\theta = \pi/3$$