3.5 Grover's Search Algorithm

An arbitrary function $f : \{0, \ldots, N-1\} \to \{0,1\}$ is given such that

$$f(x) = \begin{cases} 1, & x = \omega \\ 0, & x \neq \omega \end{cases}$$

where ω is unknown. The goal is to find the "target" ω with as few evaluations of f as possible.

Example. Find whose Bilkent extension is 1347. Then, $f(x) = 1$ iff $x =$EA.

Classical worst case complexity of this problem is N function calls. Classical bounded error complexity is also $O(N)$ since on average we must must perform Np checks

$$f(x) \stackrel{?}{=} 1$$

for a success probability of p.

Suppose we have a quantum oracle that computes

$$U_f : |x\rangle|y\rangle \to |x\rangle|f(x) \oplus y\rangle$$

Bennett et al. (1994) proved that the quantum bounded error complexity is lowerbounded by $O(\sqrt{N})$. Grover (1996) found a $O(\sqrt{N})$ BQP algorithm. This is a square-root speed-up over classical algorithms. This section discusses Grover's algorithm.

We will assume that $N = 2^n$ and use an n-qubit system with basis $\{|x\rangle : x = 0, \ldots, 2^n - 1\}$. Applying the oracle operator in this basis with $|y\rangle$ equal to the particular value shown below,

$$\begin{aligned} U_f\,|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) &= (-1)^{f(x)}|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \\ &= U_\omega|x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \end{aligned}$$

where

$$U_\omega = I - 2|\omega\rangle\langle\omega|$$

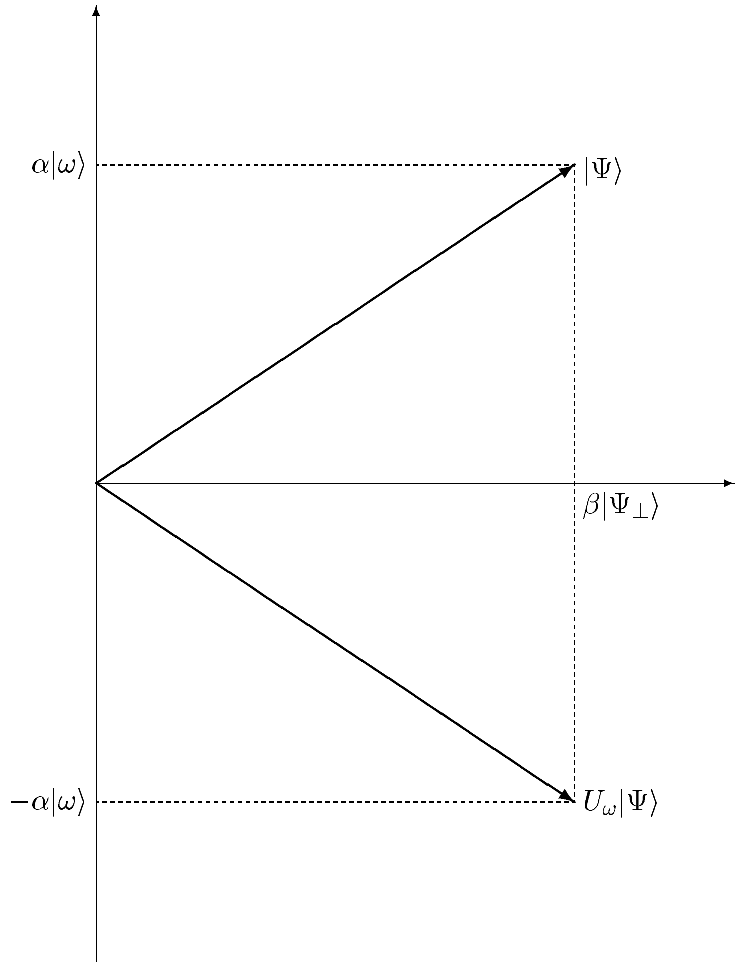
is the "sign-flip" operator

$$U_\omega|x\rangle = \begin{cases} -|x\rangle & x = \omega \\ |x\rangle & x \neq \omega. \end{cases}$$

$U_\omega|\Psi\rangle$ can be visualized as a reflection of $|\Psi\rangle$ about the hyperplane orthogonal to $|\omega\rangle$. This is shown in the following figure by writing

$$|\Psi\rangle = \alpha|\omega\rangle + \beta|\Psi_\perp\rangle$$

where $|\Psi_\perp\rangle$ is orthogonal to $|\omega\rangle$.



In addition to oracle calls, the Grover algorithm uses the following operator, known as the "inversion about the mean" operator,

$$U_s = 2|s\rangle\langle s| - I$$

where

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

is the uniform superposition of all n-qubit states. For an arbitrary state

$$|\psi\rangle = \sum_x a_x |x\rangle$$

$$\langle s|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x a_x = \sqrt{N}\langle a\rangle$$

where $\langle a\rangle$ is the mean amplitude. So,

$$U_s|\psi\rangle = \sum_x (2\langle a\rangle - a_x)|x\rangle$$

Thus, U_s transforms the amplitudes as

$$U_s : a_x \to 2\langle a \rangle - a_x$$

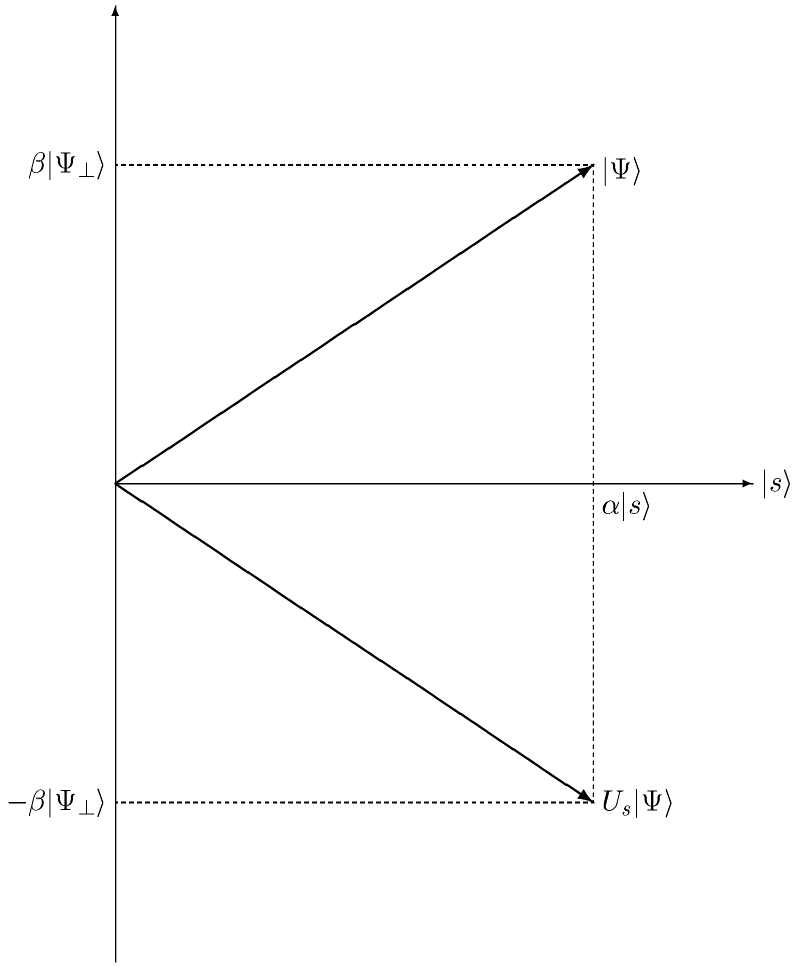
This can be interpreted as the "inversion of amplitudes about the mean." Any amplitude which was greater than the mean amplitude becomes smaller after the operation, and vice versa.

Geometrically, U_s too can be visualized as a reflection operator as shown in the following figure where we have written an arbitrary given state $|\Psi\rangle$ as

$$|\Psi\rangle = \alpha|s\rangle + \beta|\Psi_\perp\rangle$$

where $|\Psi_\perp\rangle$ is now orthogonal to $|s\rangle$. Then,

$$U_s|\Psi\rangle = \alpha|s\rangle - \beta|\Psi_\perp\rangle$$



The Grover operator is defined as

$$R_g = U_s U_\omega = (2|s\rangle\langle s| - I)(I - 2|\omega\rangle\langle\omega|).$$

Given a state $|\Psi\rangle$, write

$$|\Psi\rangle = |\Psi_1\rangle + |\Psi_2\rangle$$

where $|\Psi_1\rangle$ is in the $|\omega\rangle - |s\rangle$ plane, $|\Psi_2\rangle$ in its orthogonal complement. It is readily seen that

$$R_g|\Psi_2\rangle = -|\Psi_2\rangle.$$

On the other hand, by sketching a figure, one sees that $R_g|\Psi_1\rangle$ is a rotation of $|\Psi_1\rangle$ in the $|\omega\rangle - |s\rangle$ plane by 2θ radians where

$$\theta = |\sin^{-1}(\langle s|\omega\rangle)| = \sin^{-1}(1/\sqrt{N}) \sim 1/\sqrt{N}.$$

We now state the Grover algorithm. The $|y\rangle$-register is not shown explicitly in the statement.

1. Initial registers

$$\rightarrow |s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

2. Apply the Grover iteration R_g successively $r = \sqrt{N}\pi/4$ times

$$\rightarrow R_g^{\otimes r}|s\rangle$$

3. Measure all n qubits

$$\rightarrow x_0$$

The algorithm works because the initial state $|s\rangle$ is rotated by

$$2r\theta = 2(\sqrt{N}\pi/4)\theta \approx \pi/2$$

radians and becomes almost aligned with $|\omega\rangle$. We have

$$P(x_0 = \omega) = \sin^2[(2r+1)\theta] \approx 1 - O(\frac{1}{N}).$$