Analysis

Now we'll analyze Grover's algorithm to understand how it works. We'll start with what could be described as a *symbolic* analysis, where we calculate how the Grover operation G acts on certain states, and then we'll tie this symbolic analysis to a *geometric* picture that's helpful for visualizing how the algorithm works.

Solutions and non-solutions

Let's start by defining two sets of strings.

$$A_0 = \bigl\{x \in \Sigma^n : f(x) = 0\bigr\}$$
$$A_1 = \bigl\{x \in \Sigma^n : f(x) = 1\bigr\}$$

The set A_1 contains all of the solutions to our search problem while A_0 contains the strings that aren't solutions (which we can refer to as *non-solutions* when it's convenient). These two sets satisfy $A_0 \cap A_1 = \varnothing$ and $A_0 \cup A_1 = \Sigma^n$, which is to say that this is a *bipartition* of Σ^n.

Next we'll define two unit vectors representing uniform superpositions over the sets of solutions and non-solutions.

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

Formally speaking, each of these vectors is only defined when its corresponding set is nonempty, but hereafter we're going to focus on the case that neither A_0 nor A_1 is empty. The cases that $A_0 = \varnothing$ and $A_1 = \varnothing$ are easily handled separately, and we'll do that later.

As an aside, the notation being used here is common: any time we have a finite and nonempty set S, we can write $|S\rangle$ to denote the quantum state

vector that's uniform over the elements of S.

Let's also define $|u\rangle$ to be a *uniform* quantum state over all n-bit strings:

$$|u\rangle = \frac{1}{\sqrt{N}} \sum_{x \in \Sigma^n} |x\rangle.$$

Notice that

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

We also have that $|u\rangle = H^{\otimes n}|0^n\rangle$, so $|u\rangle$ represents the state of the register Q after the initialization in step 1 of Grover's algorithm.

This implies that just before the iterations of G happen in step 2, the state of Q is contained in the two-dimensional vector space spanned by $|A_0\rangle$ and $|A_1\rangle$, and moreover the coefficients of these vectors are real numbers. As we will see, the state of Q will always have these properties — meaning that the state is a real linear combination of $|A_0\rangle$ and $|A_1\rangle$ — after any number of iterations of the operation G in step 2.

An observation about the Grover operation

We'll now turn our attention to the Grover operation

$$G = H^{\otimes n} Z_{\mathrm{OR}} H^{\otimes n} Z_f,$$

beginning with an interesting observation about it.

Imagine for a moment that we replaced the function f by the composition of f with the NOT function — or, in other words, the function we get by flipping the output bit of f. We'll call this new function g, and we can express it using symbols in a few alternative ways.

$$g(x) = \neg f(x) = 1 \oplus f(x) = 1 - f(x) = \begin{cases} 1 & f(x) = 0 \\ 0 & f(x) = 1 \end{cases}$$

Notice that

$$(-1)^{g(x)} = (-1)^{1 \oplus f(x)} = -(-1)^{f(x)}$$

for every string $x \in \Sigma^n$, and therefore

$$Z_g = -Z_f.$$

This means that if we were to substitute the function f with the function g, Grover's algorithm wouldn't function any differently — because the states we obtain from the algorithm in the two cases are necessarily equivalent up to a global phase.

This isn't a problem! Intuitively speaking, the algorithm doesn't care which strings are solutions and which are non-solutions — it only needs to be able to *distinguish* solutions and non-solutions to operate correctly.

Action of the Grover operation

Now let's consider the action of G on the quantum state vectors $|A_0\rangle$ and $|A_1\rangle$.

First, let's observe that the operation Z_f has a very simple action on $|A_0\rangle$ and $|A_1\rangle$.

$$Z_f|A_0\rangle = |A_0\rangle$$
$$Z_f|A_1\rangle = -|A_1\rangle$$

Second, we have the operation $H^{\otimes n} Z_{\mathrm{OR}} H^{\otimes n}$. The operation Z_{OR} is defined as

$$Z_{\mathrm{OR}}|x\rangle = \begin{cases} |x\rangle & x = 0^n \\ -|x\rangle & x \neq 0^n, \end{cases}$$

again for every string $x \in \Sigma^n$, and a convenient alternative way to express this operation is like this:

$$Z_{\mathrm{OR}} = 2|0^n\rangle\langle 0^n| - \mathbb{I}.$$

A simple way to verify that this expression agrees with the definition of Z_{OR} is to evaluate its action on standard basis states.

The operation $H^{\otimes n} Z_{\mathrm{OR}} H^{\otimes n}$ can therefore be written like this:

$$H^{\otimes n} Z_{\mathrm{OR}} H^{\otimes n} = 2H^{\otimes n}|0^n\rangle\langle 0^n|H^{\otimes n} - \mathbb{I} = 2|u\rangle\langle u| - \mathbb{I},$$

using the same notation, $|u\rangle$, that we used above for the uniform superposition over all n-bit strings.

And now we have what we need to compute the action of G on $|A_0\rangle$ and $|A_1\rangle$. First let's compute the action of G on $|A_0\rangle$.

$$\begin{aligned}
G|A_0\rangle &= \big(2|u\rangle\langle u| - \mathbb{I}\big) Z_f |A_0\rangle \\
&= \big(2|u\rangle\langle u| - \mathbb{I}\big) |A_0\rangle \\
&= 2\sqrt{\frac{|A_0|}{N}}|u\rangle - |A_0\rangle \\
&= 2\sqrt{\frac{|A_0|}{N}}\left(\sqrt{\frac{|A_0|}{N}}|A_0\rangle + \sqrt{\frac{|A_1|}{N}}|A_1\rangle\right) - |A_0\rangle \\
&= \left(\frac{2|A_0|}{N} - 1\right)|A_0\rangle + \frac{2\sqrt{|A_0|\cdot|A_1|}}{N}|A_1\rangle \\
&= \frac{|A_0| - |A_1|}{N}|A_0\rangle + \frac{2\sqrt{|A_0|\cdot|A_1|}}{N}|A_1\rangle
\end{aligned}$$

And second, let's compute the action of G on $|A_1\rangle$.

$$\begin{aligned}
G|A_1\rangle &= \big(2|u\rangle\langle u| - \mathbb{I}\big) Z_f |A_1\rangle \\
&= -\big(2|u\rangle\langle u| - \mathbb{I}\big) |A_1\rangle \\
&= -2\sqrt{\frac{|A_1|}{N}}|u\rangle + |A_1\rangle \\
&= -2\sqrt{\frac{|A_1|}{N}}\left(\sqrt{\frac{|A_0|}{N}}|A_0\rangle + \sqrt{\frac{|A_1|}{N}}|A_1\rangle\right) + |A_1\rangle \\
&= -\frac{2\sqrt{|A_1|\cdot|A_0|}}{N}|A_0\rangle + \left(1 - \frac{2|A_1|}{N}\right)|A_1\rangle \\
&= -\frac{2\sqrt{|A_1|\cdot|A_0|}}{N}|A_0\rangle + \frac{|A_0| - |A_1|}{N}|A_1\rangle
\end{aligned}$$

In both cases we're using the equation

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

along with the expressions

$$\langle u|A_0\rangle = \sqrt{\frac{|A_0|}{N}} \qquad \text{and} \qquad \langle u|A_1\rangle = \sqrt{\frac{|A_1|}{N}}$$

that follow.

In summary, we have

$$G|A_0\rangle = \frac{|A_0| - |A_1|}{N}|A_0\rangle + \frac{2\sqrt{|A_0| \cdot |A_1|}}{N}|A_1\rangle$$
$$G|A_1\rangle = -\frac{2\sqrt{|A_1| \cdot |A_0|}}{N}|A_0\rangle + \frac{|A_0| - |A_1|}{N}|A_1\rangle.$$

As we already noted, the state of Q just prior to step 2 is contained in the two-dimensional space spanned by $|A_0\rangle$ and $|A_1\rangle$, and we have just established that G maps any vector in this space to another vector in the same space. This means that, for the sake of the analysis, we can focus our attention exclusively on this subspace.

To better understand what's happening within this two-dimensional space, let's express the action of G on this space as a matrix,

$$M = \begin{pmatrix} \frac{|A_0|-|A_1|}{N} & -\frac{2\sqrt{|A_1|\cdot|A_0|}}{N} \\ \frac{2\sqrt{|A_0|\cdot|A_1|}}{N} & \frac{|A_0|-|A_1|}{N} \end{pmatrix},$$

whose first and second rows/columns correspond to $|A_0\rangle$ and $|A_1\rangle$, respectively. So far in this series, we've always connected the rows and columns of matrices with the classical states of a system, but matrices can also be used to describe the actions of linear mappings on different bases like we have here.

While it isn't at all obvious at first glance, the matrix M is what we obtain by *squaring* a simpler-looking matrix.

$$\begin{pmatrix} \sqrt{\frac{|A_0|}{N}} & -\sqrt{\frac{|A_1|}{N}} \\ \sqrt{\frac{|A_1|}{N}} & \sqrt{\frac{|A_0|}{N}} \end{pmatrix}^2 = \begin{pmatrix} \frac{|A_0|-|A_1|}{N} & -\frac{2\sqrt{|A_1|\cdot|A_0|}}{N} \\ \frac{2\sqrt{|A_0|\cdot|A_1|}}{N} & \frac{|A_0|-|A_1|}{N} \end{pmatrix} = M$$

The matrix

$$\begin{pmatrix} \sqrt{\frac{|A_0|}{N}} & -\sqrt{\frac{|A_1|}{N}} \\ \sqrt{\frac{|A_1|}{N}} & \sqrt{\frac{|A_0|}{N}} \end{pmatrix}$$

is a *rotation matrix*, which we can alternatively express as

$$\begin{pmatrix} \sqrt{\frac{|A_0|}{N}} & -\sqrt{\frac{|A_1|}{N}} \\ \sqrt{\frac{|A_1|}{N}} & \sqrt{\frac{|A_0|}{N}} \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

for

$$\theta = \sin^{-1}\left(\sqrt{\frac{|A_1|}{N}}\right).$$

This angle θ is going to play a very important role in the analysis that follows, so it's worth stressing its importance here as we see it for the first time.

In light of this expression of this matrix, we observe that

$$M = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}^2 = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix}.$$

This is because rotating by the angle θ two times is equivalent to rotating by the angle 2θ. Another way to see this is to make use of the alternative expression

$$\theta = \cos^{-1}\left(\sqrt{\frac{|A_0|}{N}}\right),$$

together with the *double angle* formulas from trigonometry:

$$\cos(2\theta) = \cos^2(\theta) - \sin^2(\theta)$$
$$\sin(2\theta) = 2\sin(\theta)\cos(\theta).$$

In summary, the state of the register Q at the start of step 2 is

$$|u\rangle = \sqrt{\frac{|A_0|}{N}}|A_0\rangle + \sqrt{\frac{|A_1|}{N}}|A_1\rangle = \cos(\theta)|A_0\rangle + \sin(\theta)|A_1\rangle,$$

and the effect of applying G to this state is to rotate it by an angle 2θ within the space spanned by $|A_0\rangle$ and $|A_1\rangle$. So, for example, we have

$$G|u\rangle = \cos(3\theta)|A_0\rangle + \sin(3\theta)|A_1\rangle$$
$$G^2|u\rangle = \cos(5\theta)|A_0\rangle + \sin(5\theta)|A_1\rangle$$
$$G^3|u\rangle = \cos(7\theta)|A_0\rangle + \sin(7\theta)|A_1\rangle$$

and in general

$$G^t|u\rangle = \cos\big((2t+1)\theta\big)|A_0\rangle + \sin\big((2t+1)\theta\big)|A_1\rangle.$$

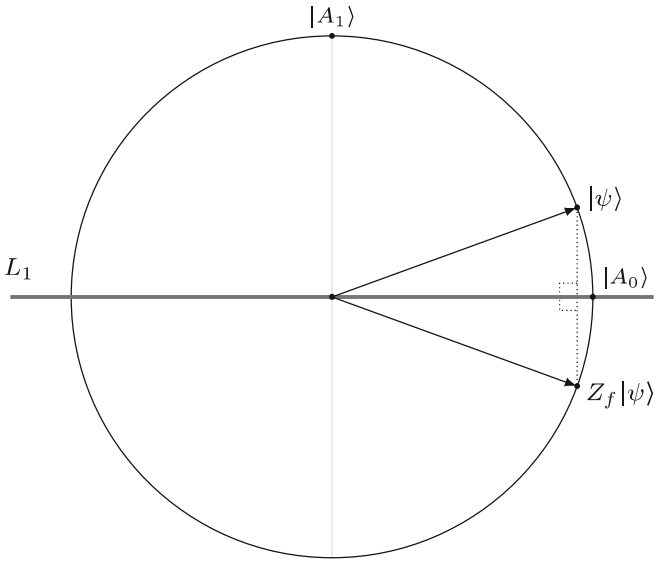
Geometric picture

Now let's connect the analysis we just went through to a geometric picture. The idea is that the operation G is the product of two *reflections*, Z_f and $H^{\otimes n} Z_{\text{OR}} H^{\otimes n}$. And the net effect of performing two reflections is to perform a *rotation*.

Let's start with Z_f. As we already observed previously, we have

$$Z_f |A_0\rangle = |A_0\rangle$$
$$Z_f |A_1\rangle = -|A_1\rangle.$$

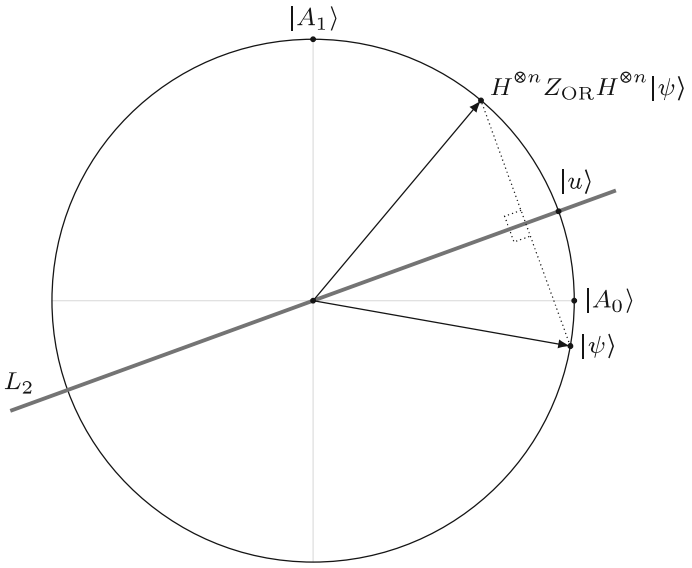
Within the two-dimensional vector space spanned by $|A_0\rangle$ and $|A_1\rangle$, this is a *reflection* about the line parallel to $|A_0\rangle$, which we'll call L_1. Here's a figure illustrating the action of this reflection on a hypothetical unit vector $|\psi\rangle$, which we're assuming is a real linear combination of $|A_0\rangle$ and $|A_1\rangle$.



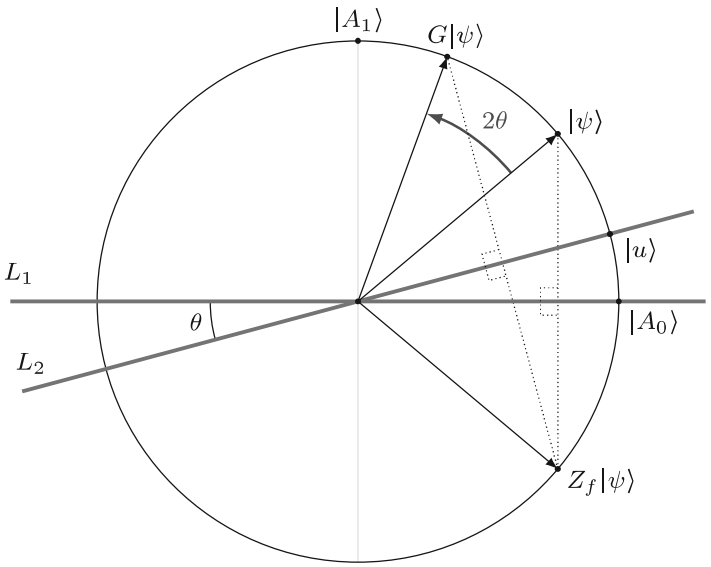
Second we have the operation $H^{\otimes n} Z_{\text{OR}} H^{\otimes n}$, which we've already seen can be written as

$$H^{\otimes n} Z_{\text{OR}} H^{\otimes n} = 2|u\rangle\langle u| - \mathbb{I}.$$

This is also a reflection, this time about the line L_2 parallel to the vector $|u\rangle$. Here's a figure depicting the action of this reflection on a unit vector $|\psi\rangle$.



When we compose these two reflections, we obtain a rotation — by twice the angle between the lines of reflection — as this figure illustrates.



This explains, in geometric terms, why the effect of the Grover operation is to rotate linear combinations of $|A_0\rangle$ and $|A_1\rangle$ by an angle of 2θ.

Was this page helpful?

Yes No

Report a bug, typo, or request content on GitHub ↗.

Previous page

Next page

© IBM Corp., 2017-2025