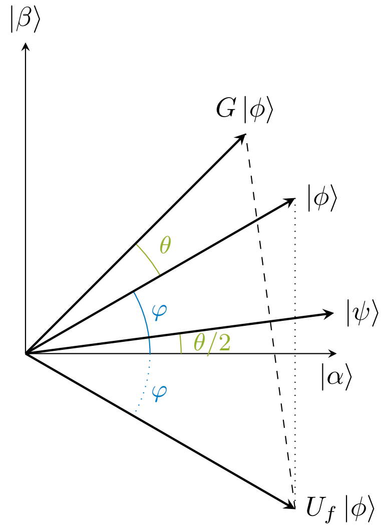
Algebraic derivation of the rotation in Grover's algorithm

Recall that the Grover operator consists of an oracle call followed by a reflection about the equal superposition state $|\psi\rangle$:



$$G = (2|\psi\rangle\langle\psi| - I)\,U_f.$$

One introduces the orthonormal states

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_{f(x)=0} |x\rangle\,, \quad |\beta\rangle = \frac{1}{\sqrt{M}} \sum_{f(x)=1} |x\rangle\,.$$

The equal superposition state,

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

can be expressed in terms of $|\alpha\rangle$ and $|\beta\rangle$ as

$$|\psi\rangle = \underbrace{\cos\left(\tfrac{\theta}{2}\right)|\alpha\rangle + \sin\left(\tfrac{\theta}{2}\right)|\beta\rangle}\,,$$

where (by definition) $\sin(\frac{\theta}{2}) = \sqrt{M/N}$.

Our goal here is an *algebraic* derivation that G performs a rotation by θ in the plane spanned by $|\alpha\rangle$ and $|\beta\rangle$.

We start from an input state $|\phi\rangle$ in the $|\alpha\rangle$-$|\beta\rangle$ plane, which we can parametrize by some angle $\varphi \in [0, 2\pi)$:

$$|\phi\rangle = \cos(\varphi)|\alpha\rangle + \sin(\varphi)|\beta\rangle\,.$$

We now evaluate the following inner product:

application of oracle

$$\begin{aligned}
\langle\psi|U_f|\phi\rangle &= \left(\cos\left(\tfrac{\theta}{2}\right)\langle\alpha| + \sin\left(\tfrac{\theta}{2}\right)\langle\beta|\right)\left(\cos(\varphi)|\alpha\rangle - \sin(\varphi)|\beta\rangle\right)\\
&= \cos\left(\tfrac{\theta}{2}\right)\cos(\varphi) - \sin\left(\tfrac{\theta}{2}\right)\sin(\varphi)\\
&= \cos\left(\tfrac{\theta}{2} + \varphi\right),
\end{aligned} \tag{1}$$

where the last equal sign follows from the formula $\cos(x)\cos(y) - \sin(x)\sin(y) = \cos(x+y)$. Then,

$$\begin{aligned}
G|\phi\rangle &= (2|\psi\rangle\langle\psi| - I)\,U_f|\phi\rangle\\
&= 2|\psi\rangle\langle\psi|U_f|\phi\rangle - U_f|\phi\rangle\\
&= 2\left(\cos\left(\tfrac{\theta}{2}\right)|\alpha\rangle + \sin\left(\tfrac{\theta}{2}\right)|\beta\rangle\right)\cos\left(\tfrac{\theta}{2}+\varphi\right) - \overbrace{\left(\cos(\varphi)|\alpha\rangle - \sin(\varphi)|\beta\rangle\right)}^{U_f|\phi\rangle}\\
&= \left(2\cos\left(\tfrac{\theta}{2}\right)\cos\left(\tfrac{\theta}{2}+\varphi\right) - \cos(\varphi)\right)|\alpha\rangle\\
&\quad + \left(2\sin\left(\tfrac{\theta}{2}\right)\cos\left(\tfrac{\theta}{2}+\varphi\right) + \sin(\varphi)\right)|\beta\rangle\\
&= \cos(\varphi+\theta)|\alpha\rangle + \sin(\varphi+\theta)|\beta\rangle\,.
\end{aligned}$$

rotation by θ

Here we have used Eq. (1) for the third equal sign. Regarding the last equal sign, we can express cosine and sine in terms of the exponential function and obtain

$$\begin{aligned}
2\cos\left(\tfrac{\theta}{2}\right)\cos\left(\tfrac{\theta}{2}+\varphi\right) - \cos(\varphi) &= \frac{1}{2}\left(e^{i\frac{\theta}{2}} + e^{-i\frac{\theta}{2}}\right)\left(e^{i\frac{\theta}{2}+i\varphi} + e^{-i\frac{\theta}{2}-i\varphi}\right) - \frac{1}{2}\left(e^{i\varphi} + e^{-i\varphi}\right)\\
&= \frac{1}{2}\left(e^{i\theta+i\varphi} + e^{-i\varphi} + e^{i\varphi} + e^{-i\theta-i\varphi} - e^{i\varphi} - e^{-i\varphi}\right)\\
&= \frac{1}{2}\left(e^{i\theta+i\varphi} + e^{-i\theta-i\varphi}\right)\\
&= \cos(\varphi+\theta),
\end{aligned}$$

$\cos(x) = \dfrac{e^{ix} + e^{-ix}}{2}$

and similarly for the coefficient of $|\beta\rangle$. In summary, we have derived that

$$G|\phi\rangle = \cos(\varphi+\theta)|\alpha\rangle + \sin(\varphi+\theta)|\beta\rangle\,,$$

which is a rotation by angle θ of the input state $|\phi\rangle$.