Algoritmo de Grover

Reyes Granados Naomi Itzel.

Definición del Problema

Dado un conjunto, llamamos tarea de búsqueda al encontrar un elemento específico.

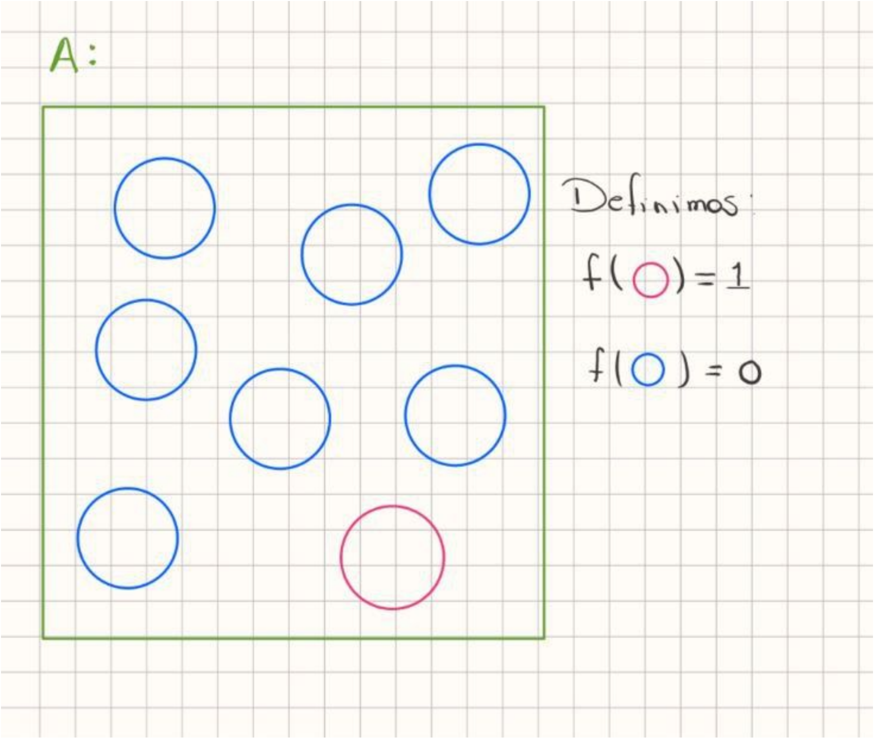
Cualquier tarea de búsqueda se puede expresar con una función $f(x)$ tal que si x es el elemento buscado entonces $f(x)=1$, en otro caso $f(x)=0$.

Definición del Problema

Así el problema general se reduce a dado un conjunto *A* y una función de búsqueda:

$$f : A \rightarrow \{0,1\}$$

Encontrar el valor *x* en *A* tal que *f(x)=1* .



Solución clásica.

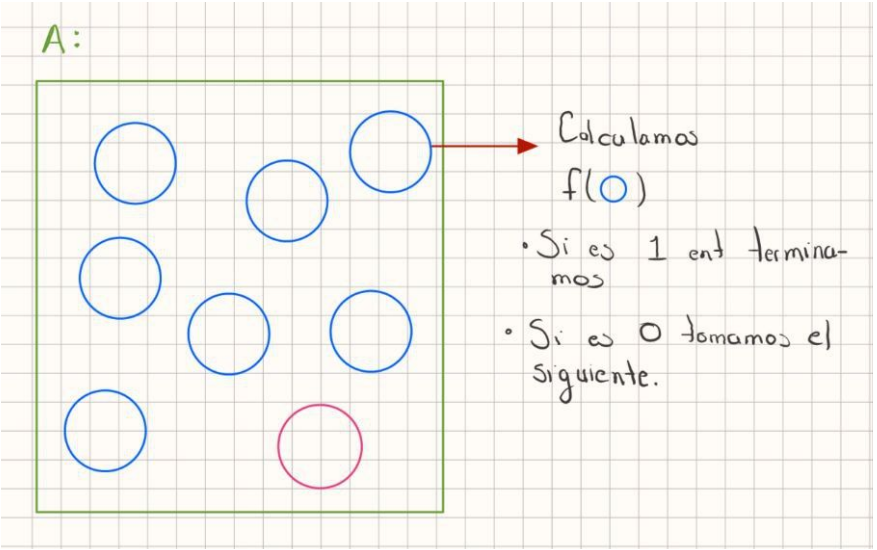
Dado un conjunto A y una función f, cómo se resolvería de manera clásica?

Solución clásica.

Para cada uno de los elementos de nuestro conjunto evaluamos *f* si nos da *1* ya terminamos; si nos da *0* probamos con otro.

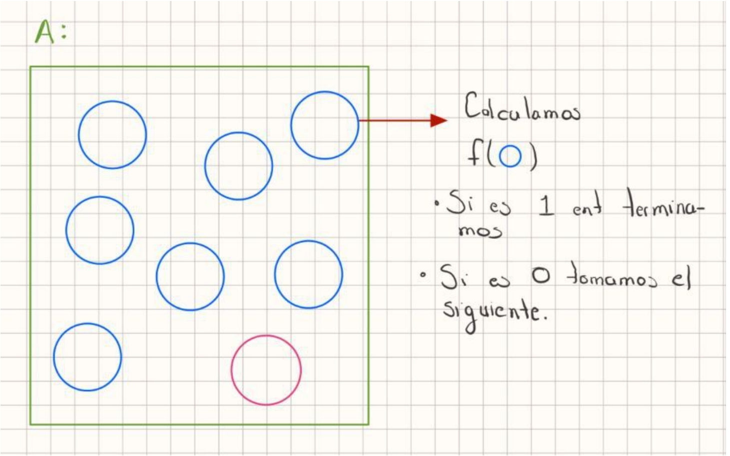
Solución clásica.

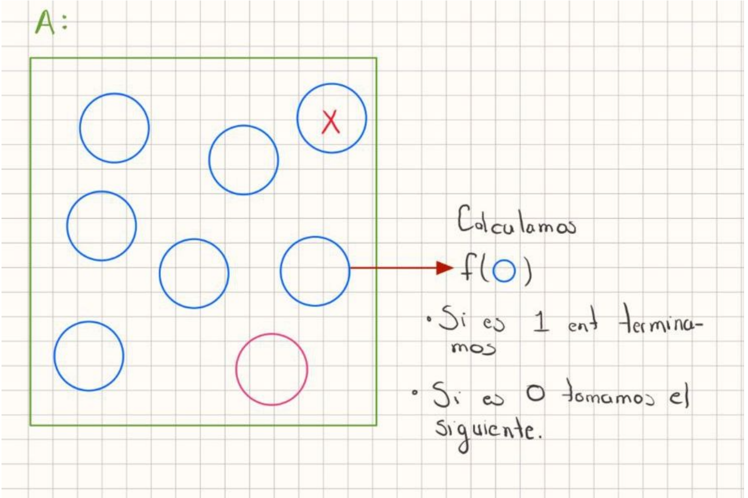
Para cada uno de los elementos de nuestro conjunto evaluamos *f* si nos da *1* ya terminamos; si nos da *0* probamos con otro.



Solución clásica.

Para cada uno de los elementos de nuestro conjunto evaluamos *f* si nos da *1* ya terminamos; si nos da *0* probamos con otro.





Solución clásica.

Qué complejidad tiene el algoritmo?

Solución clásica.

Qué complejidad tiene el algoritmo?
Lineal, $O(n)$

Recordatorios.

Para entrar ya en la solución cuántica primero vamos a recordar algunas definiciones.

Recordatorios.

Para dos estados cuales quiera, $|\phi\rangle, |\theta\rangle$, decimos que son perpendiculares si

Recordatorios.

Para dos estados cuales quiera, $|\phi\rangle, |\theta\rangle$, decimos que son perpendiculares si

$$\langle\phi||\theta\rangle = 0$$

Recordatorios.

Para dos estados cuales quiera, $|\phi\rangle, |\theta\rangle$, decimos que son perpendiculares si

$$\langle\phi||\theta\rangle = 0$$

Si más aún, si $|\phi\rangle, |\theta\rangle$ son estados base entonces solo tenemos dos opciones:

1. Si$\langle\phi||\theta\rangle = 0$ entonces
2. Si $\langle\phi||\theta\rangle = 1$ entonces

Recordatorios.

Para dos estados cuales quiera, $|\phi\rangle, |\theta\rangle$, decimos que son perpendiculares si

$$\langle\phi||\theta\rangle = 0$$

Si más aún, si $|\phi\rangle, |\theta\rangle$ son estados base entonces solo tenemos dos opciones:

1. Si$\langle\phi||\theta\rangle = 0$ entonces $|\phi\rangle \neq |\theta\rangle$
2. Si $\langle\phi||\theta\rangle = 1$ entonces

Recordatorios.

Para dos estados cuales quiera, $|\phi\rangle, |\theta\rangle$, decimos que son perpendiculares si

$$\langle\phi||\theta\rangle = 0$$

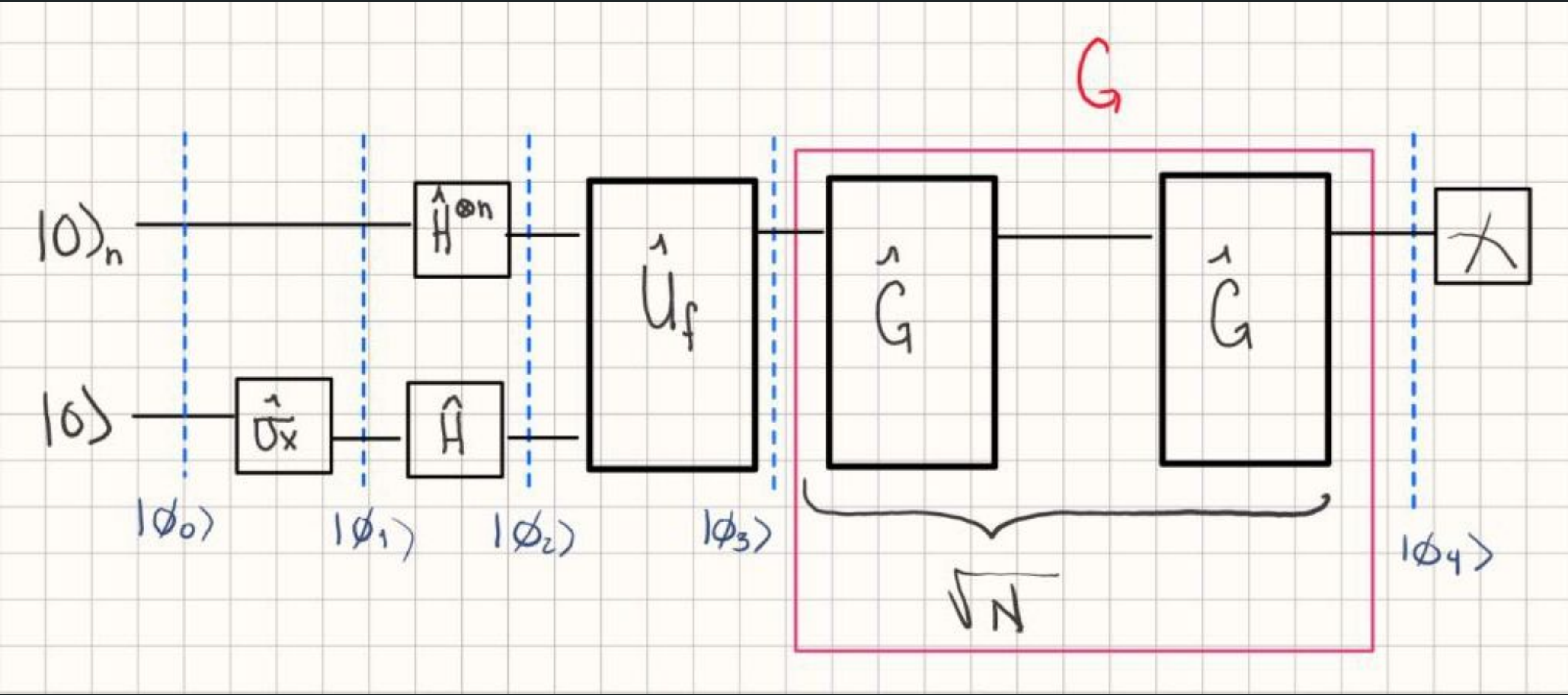
Si más aún, si $|\phi\rangle, |\theta\rangle$ son estados base entonces solo tenemos dos opciones:

1. Si$\langle\phi||\theta\rangle = 0$ entonces $|\phi\rangle \neq |\theta\rangle$
2. Si $\langle\phi||\theta\rangle = 1$ entonces $|\phi\rangle = |\theta\rangle$

Solución cuántica.

Sea $f : \{0,1\}^n \rightarrow \{0,1\}$, tal que para algún valor x en $\{0,1\}^n$ $f(x)=1$. La meta es encontrar a dicho x.

Solución cuántica.



Solución cuántica.

Vamos a ir viendo como evoluciona nuestro estado a través del circuito.

Solución cuántica.

Vamos a ir viendo como evoluciona nuestro estado a través del circuito.

$$|\phi_1\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$$

Solución cuántica.

Vamos a ir viendo como evoluciona nuestro estado a través del circuito.

$$|\phi_1\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$$

$$|\phi_2\rangle = (H^{\otimes(n+1)})|\phi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |\bar{z}\rangle|-\rangle = |s\rangle|-\rangle$$

Solución cuántica.

Vamos a ir viendo como evoluciona nuestro estado a través del circuito.

$$|\phi_1\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$$

$$|\phi_2\rangle = (H^{\otimes(n+1)})|\phi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |\bar{z}\rangle|-\rangle = |s\rangle|-\rangle$$

Sabemos que en $|s\rangle$ está el estado tal que valua a $f(x)$ en 1, digamos sin perdida de generalidad que dicho estado es $|w\rangle$. Definamos al estado $|s'\rangle$ como,

$$|s'\rangle = \frac{1}{\sqrt{2^n-1}} \sum_{j\neq w} |j\rangle$$

Solución cuántica.

Sea $N = 2^n$, entonces podemos reescribir al estado $|s\rangle$ en función de $|s'\rangle$ y $|w\rangle$:

$$|s\rangle = \boxed{}\,|w\rangle + \boxed{}\,|s'\rangle$$

Solución cuántica.

Sea $N = 2^n$, entonces podemos reescribir al estado $|s\rangle$ en función de $|s'\rangle$ y $|w\rangle$:

$$|s\rangle = \frac{1}{N}|w\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|s'\rangle$$

Solución cuántica.

obs. Qué pasa con $\langle w||s'\rangle$? y por tanto estos estados son

Solución cuántica.

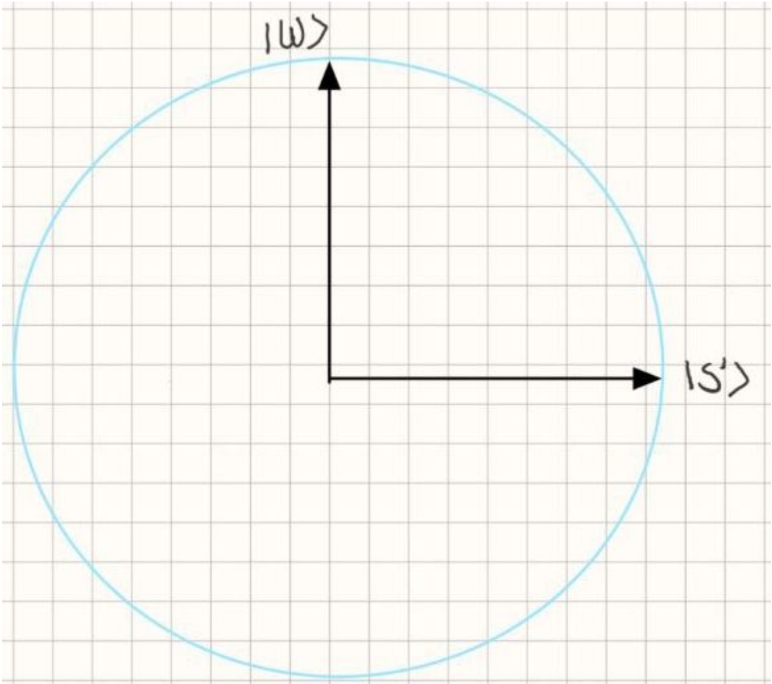
obs. Qué pasa con $\langle w||s'\rangle$? Es cero y por tanto estos estados son

Solución cuántica.

obs. Qué pasa con $\langle w||s'\rangle$? Es cero y por tanto estos estados son perpendiculares.

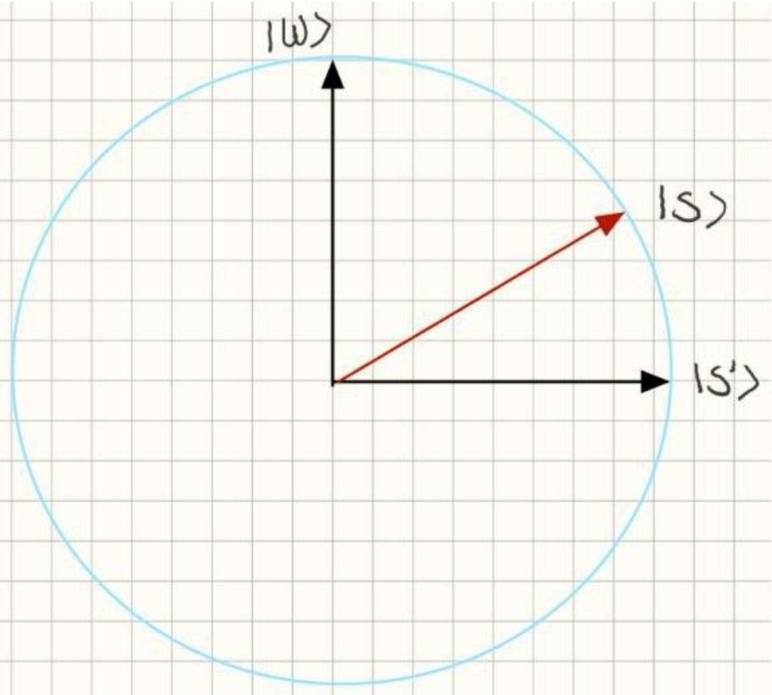
Solución cuántica.

obs. Qué pasa con $\langle w||s'\rangle$? Es cero y por tanto estos estados son perpendiculares.



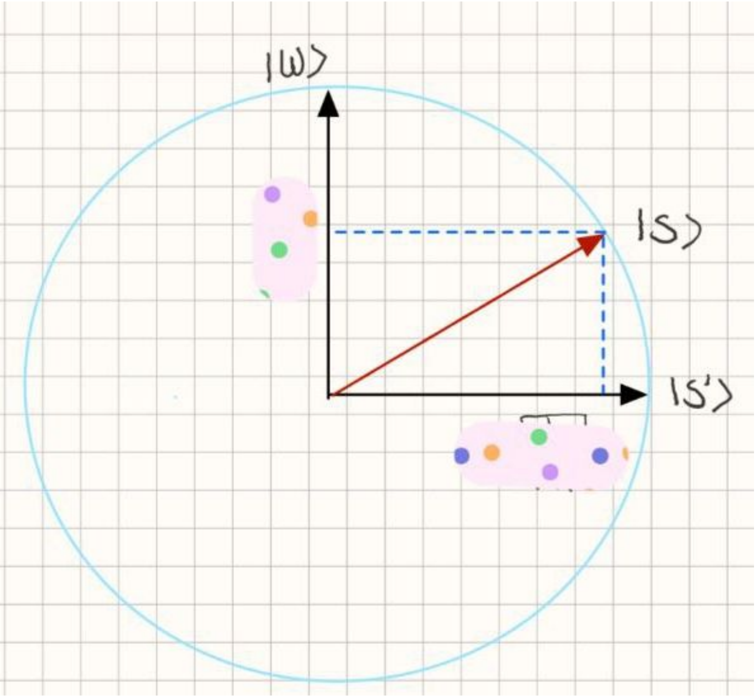
Solución cuántica.

Podemos ver representado así a nuestro estado |s> :



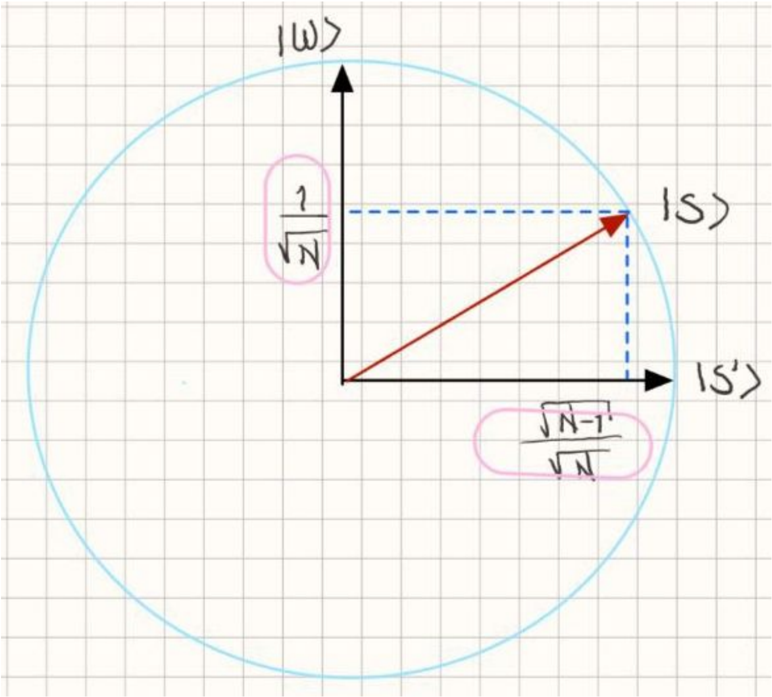
Solución cuántica.

Podemos ver representado así a nuestro estado |s> :



Solución cuántica.

Podemos ver representado así a nuestro estado |s> :



Solución cuántica.

Vamos a ir viendo como evoluciona nuestro estado a través del circuito.

$$|\phi_1\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$$

$$|\phi_2\rangle = (H^{\otimes(n+1)})|\phi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |\bar{z}\rangle|-\rangle = |s\rangle|-\rangle$$

$$\text{Con } |s\rangle = \frac{1}{N}|w\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|s'\rangle$$

$$|\phi_3\rangle = U_f|\phi_2\rangle = U_f|s\rangle|-\rangle = \frac{1}{N}U_f|w\rangle|-\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}U_f|s'\rangle|-\rangle$$

Solución cuántica.

$$|\phi_3\rangle = U_f|\phi_2\rangle = U_f|s\rangle|-\rangle = \frac{1}{N}U_f|w\rangle|-\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}U_f|s'\rangle|-\rangle$$

Aplicando Kickback

$$|\phi_3\rangle = \frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{f(\bar{z})}|\bar{z}\rangle|-\rangle$$

Solución cuántica.

$$|\phi_3\rangle = U_f|\phi_2\rangle = U_f|s\rangle|-\rangle = \frac{1}{N}U_f|w\rangle|-\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}U_f|s'\rangle|-\rangle$$

Aplicando Kickback

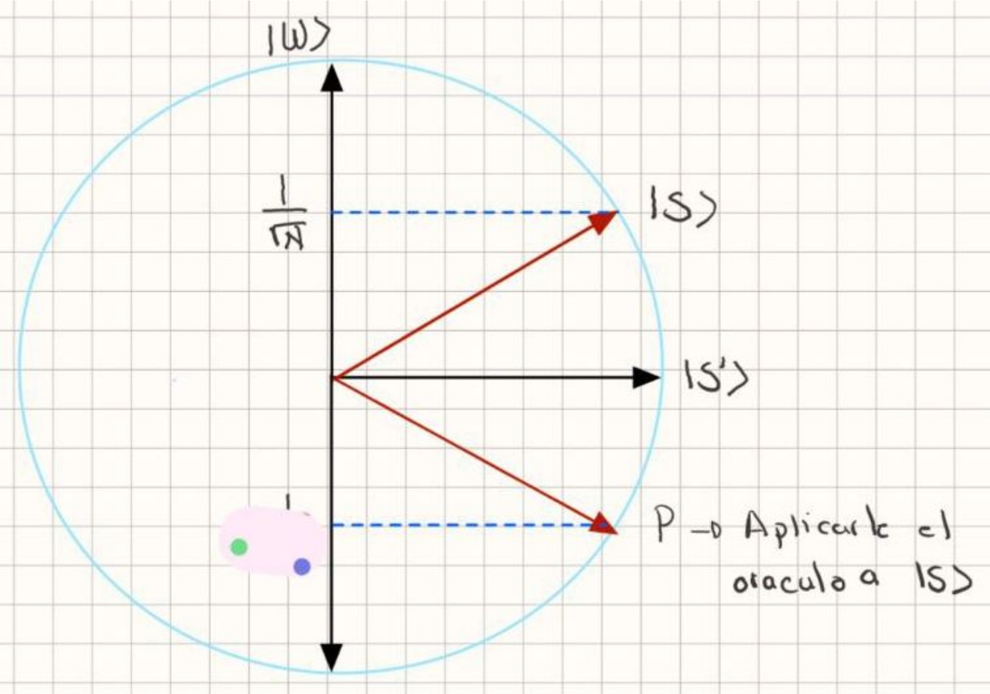
$$|\phi_3\rangle = \frac{1}{\sqrt{2^n}}\sum_{z\in\{0,1\}^n}(-1)^{f(\bar{z})}|\bar{z}\rangle|-\rangle$$

Recordamos que el único estado donde f es 1 es cuando $\bar{z} = w$, así

$$|\phi_3\rangle = -\frac{1}{N}|w\rangle|-\rangle + \frac{\sqrt{N-1}}{\sqrt{N}}|s'\rangle|-\rangle$$

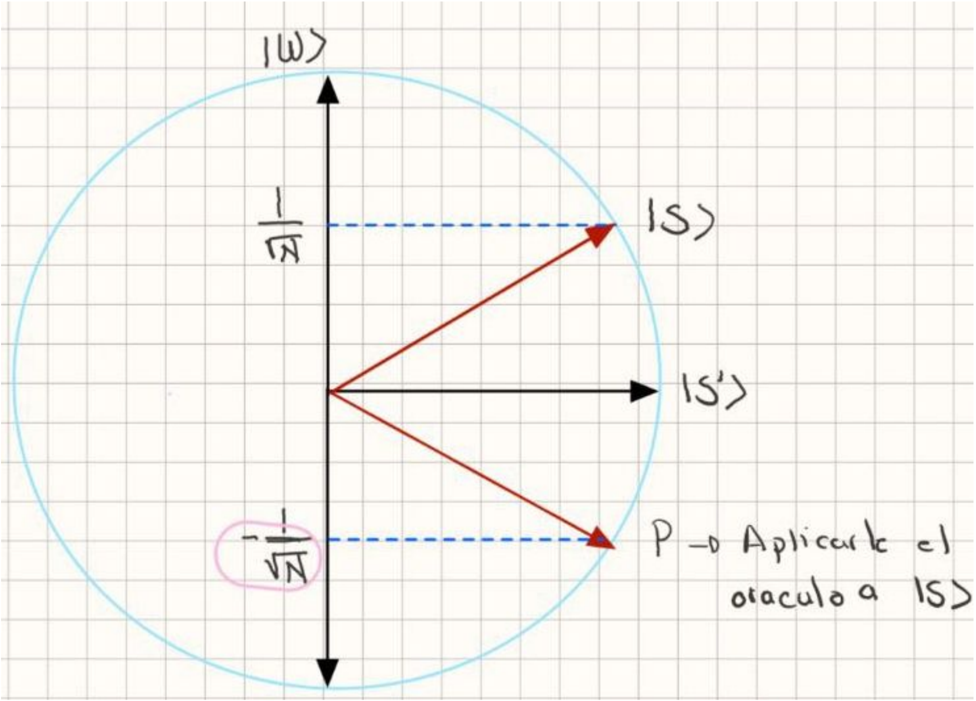
Solución cuántica.

Así a nuestro estado |φ3⟩ se visualiza como:



Solución cuántica.

Así a nuestro estado |φ3⟩ se visualiza como:



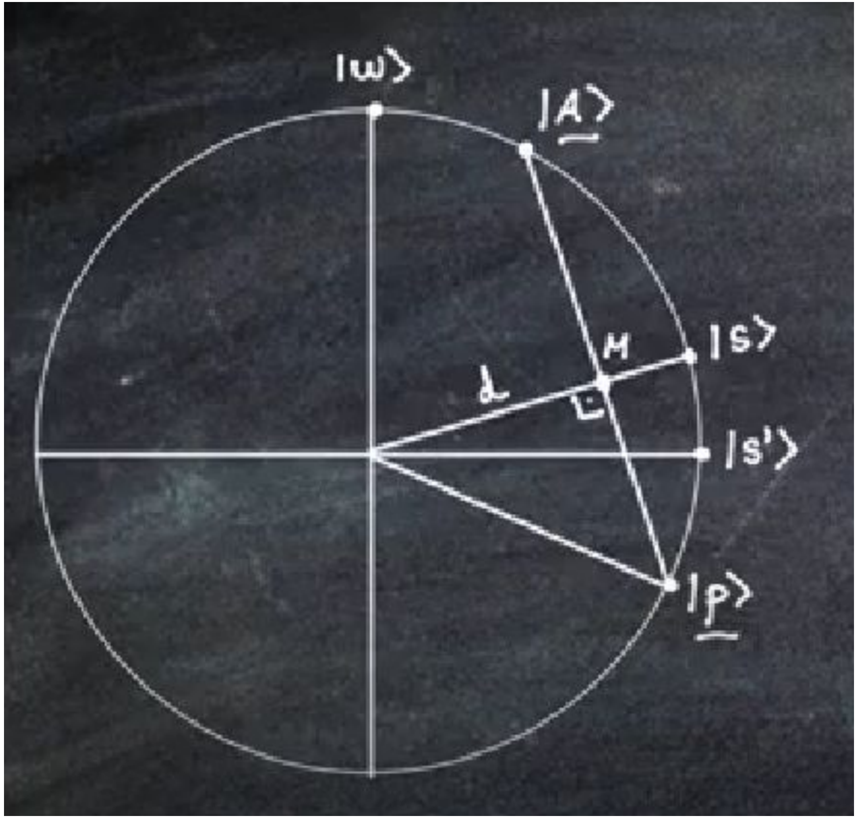
Solución cuántica.

Vamos a definir la compuerta G como:

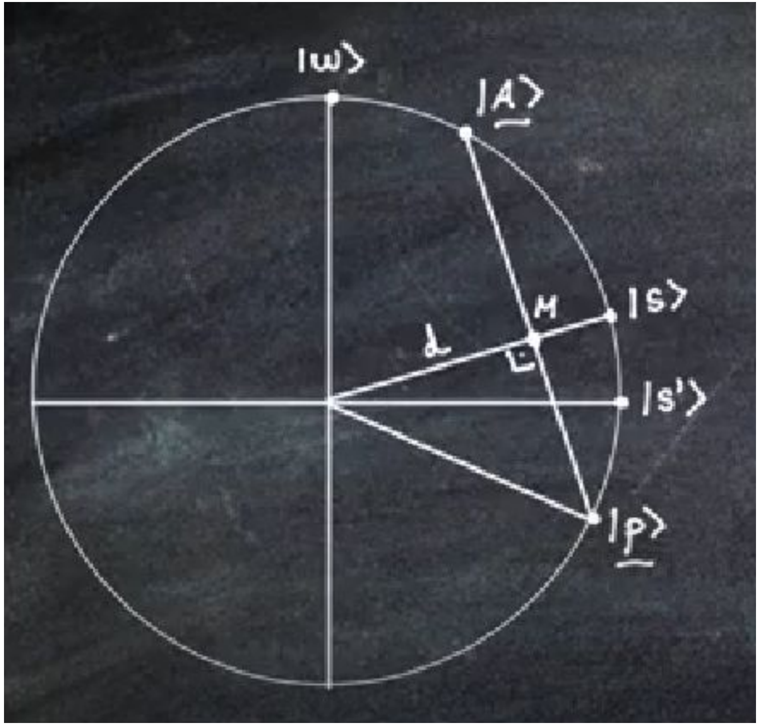
$$2|s\rangle\langle s| - I$$

Lo que hará está compuerta es aplicar simetría para el estado $|P\rangle$ sobre el estado $|s\rangle$, de tal forma que la probabilidad de medir $|w\rangle$ aumente.

Solución cuántica.

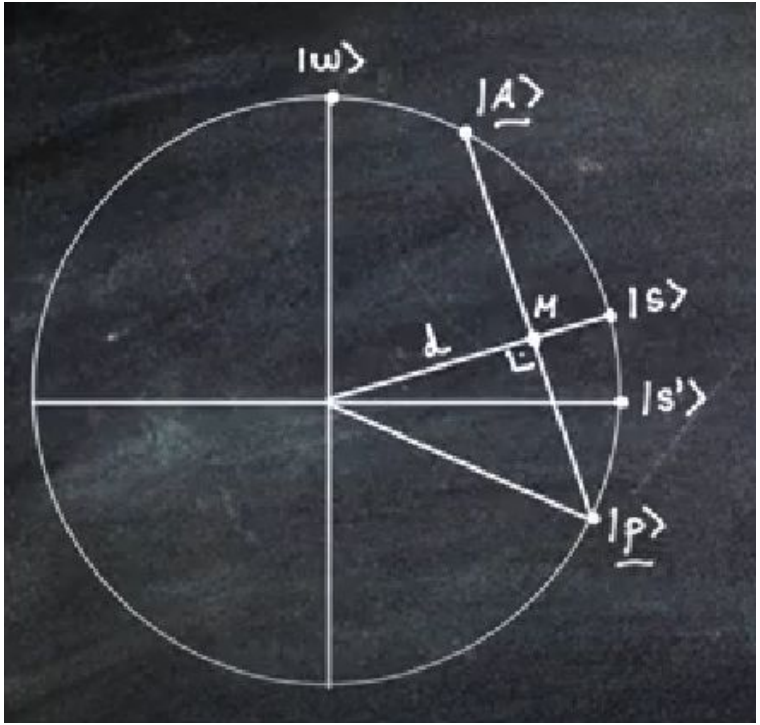


Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

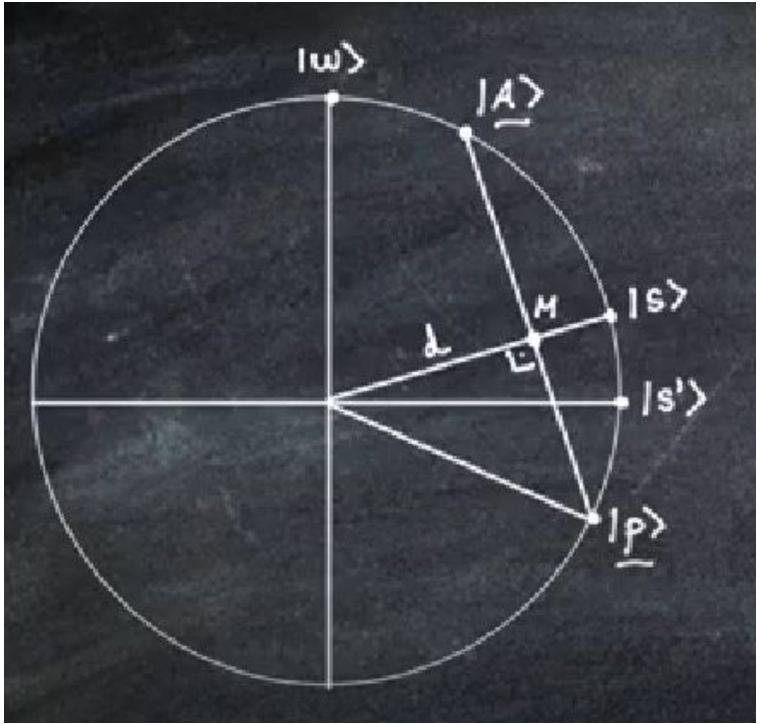
Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

$M =$

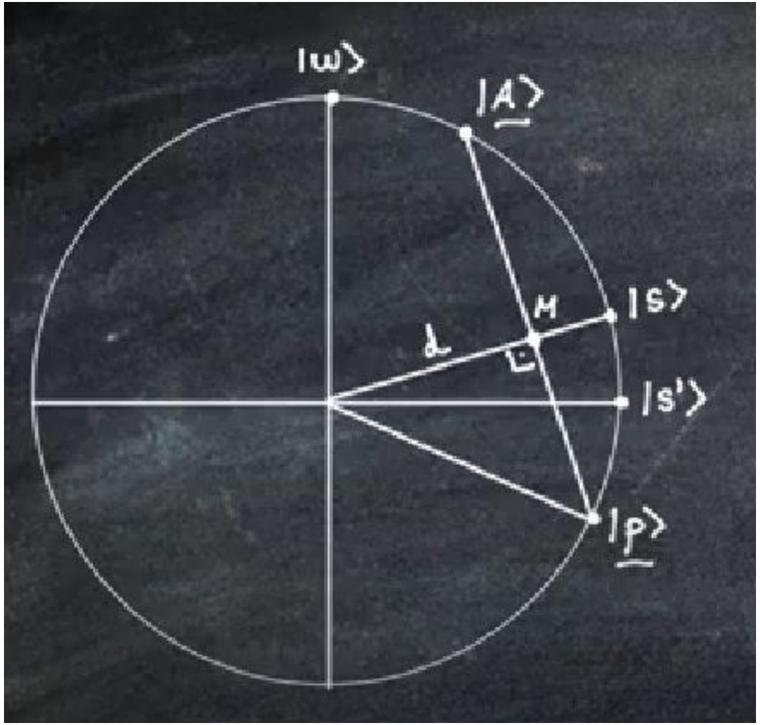
Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$

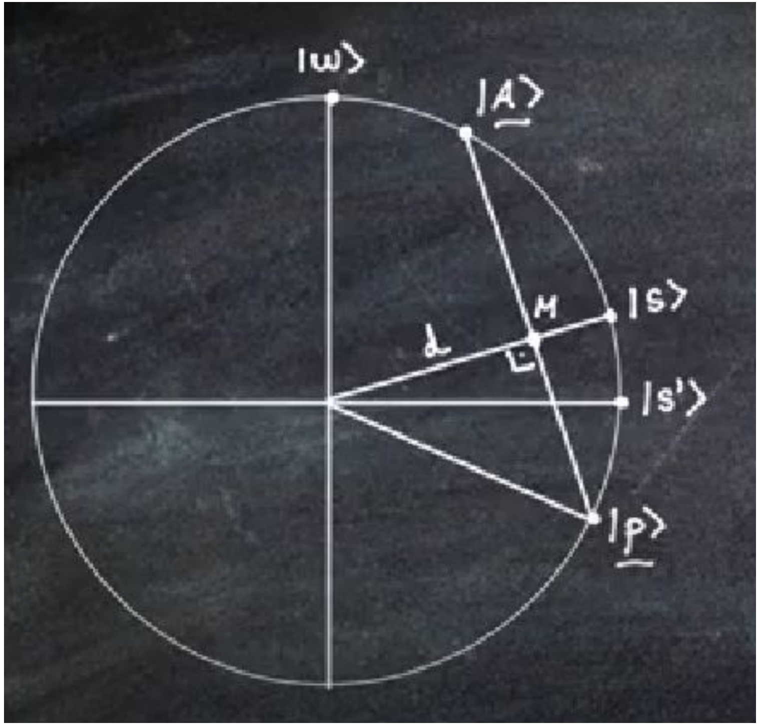
Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$
$$p\bar{M} = \quad\rangle$$

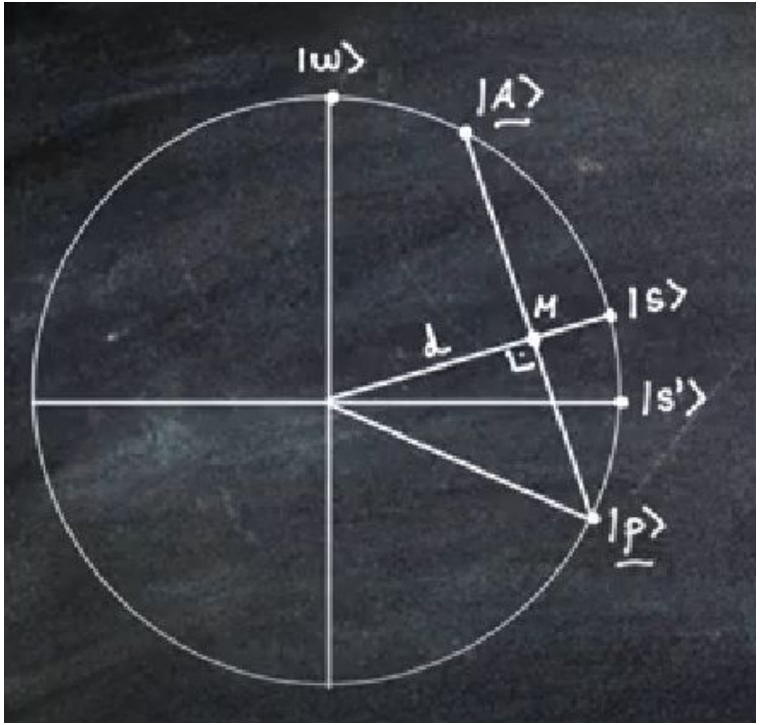
Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

Solución cuántica.



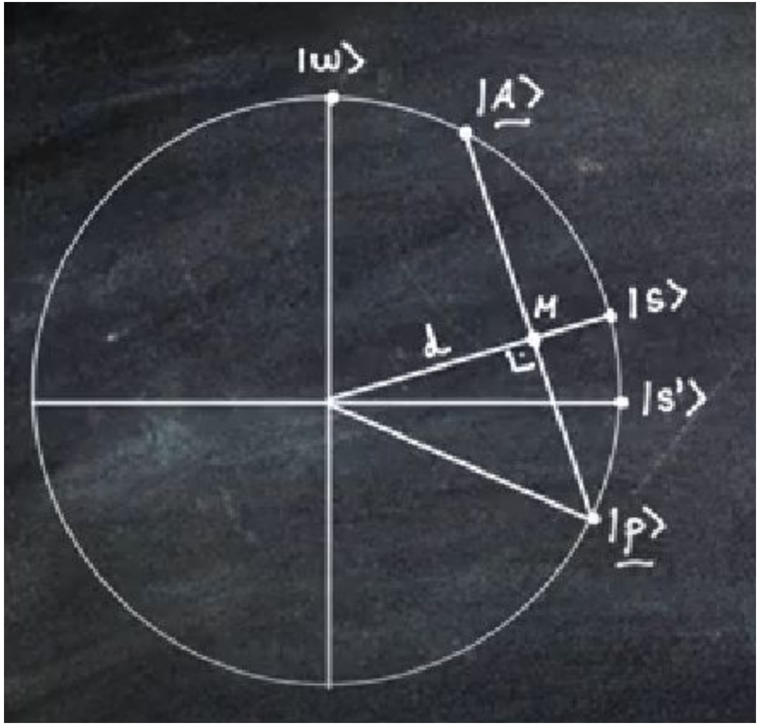
Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

Notamos que $p\bar{M}$ es perpendicular a $|s\rangle$ por tanto.

$$\langle s||(d|s\rangle - |p\rangle)\rangle =$$

Solución cuántica.



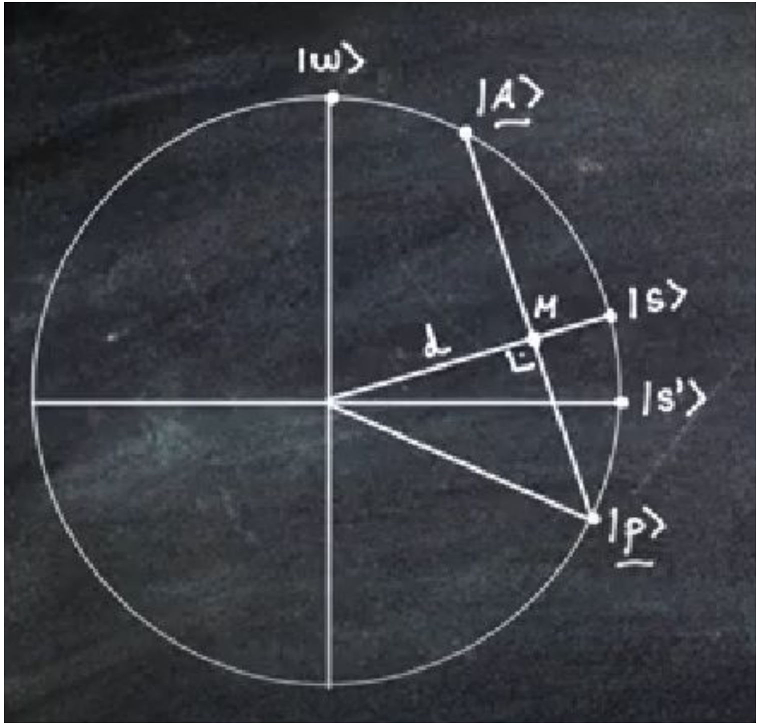
Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

Notamos que $p\bar{M}$ es perpendicular a $|s\rangle$ por tanto.

$$\langle s||(d|s\rangle - |p\rangle)\rangle = 0$$

Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

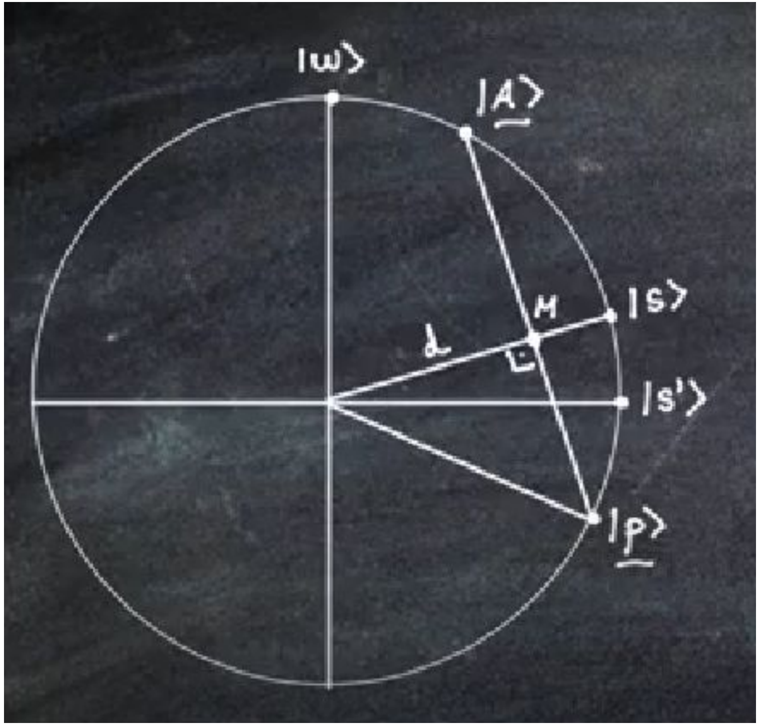
$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

Notamos que $p\bar{M}$ es perpendicular a $|s\rangle$ por tanto.

$$\langle s||(d|s\rangle - |p\rangle)\rangle = 0$$

Despejando tenemos $d =$

Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

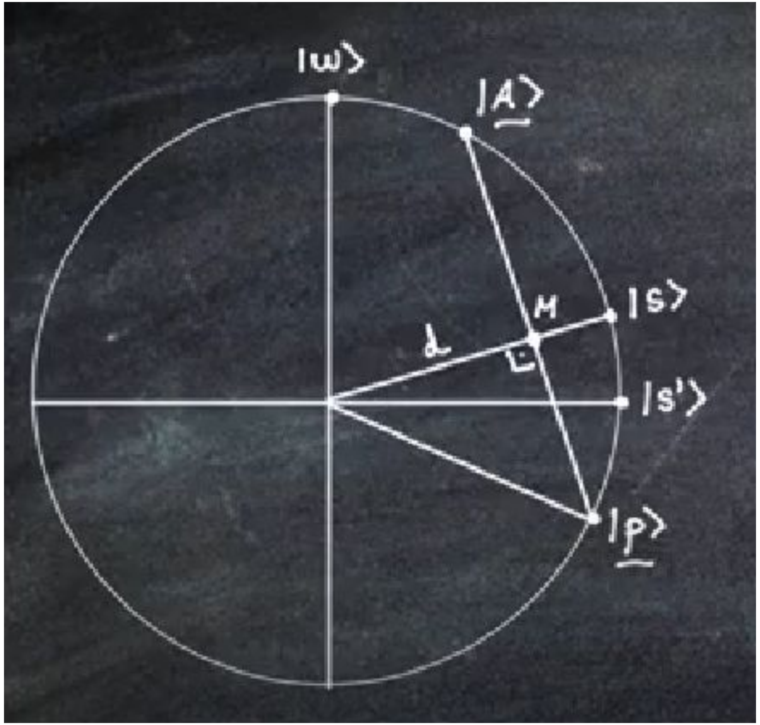
$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

Notamos que $p\bar{M}$ es perpendicular a $|s\rangle$ por tanto.

$$\langle s||(d|s\rangle - |p\rangle)\rangle = 0$$

Despejando tenemos $d = \langle s||p\rangle$

Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

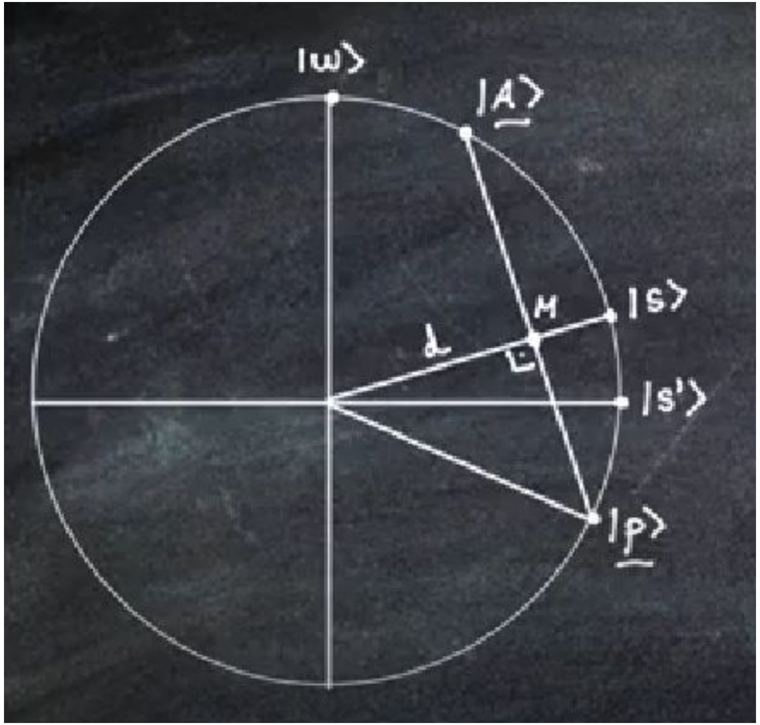
Notamos que $p\bar{M}$ es perpendicular a $|s\rangle$ por tanto.

$$\langle s||(d|s\rangle - |p\rangle)\rangle = 0$$

Despejando tenemos $d = \langle s||p\rangle$
Sustituyendo en M tenemos,

$$M = |s\rangle\langle s||p\rangle$$

Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

Notamos que $p\bar{M}$ es perpendicular a $|s\rangle$ por tanto.

$$\langle s||(d|s\rangle - |p\rangle)\rangle = 0$$

Despejando tenemos $d = \langle s||p\rangle$

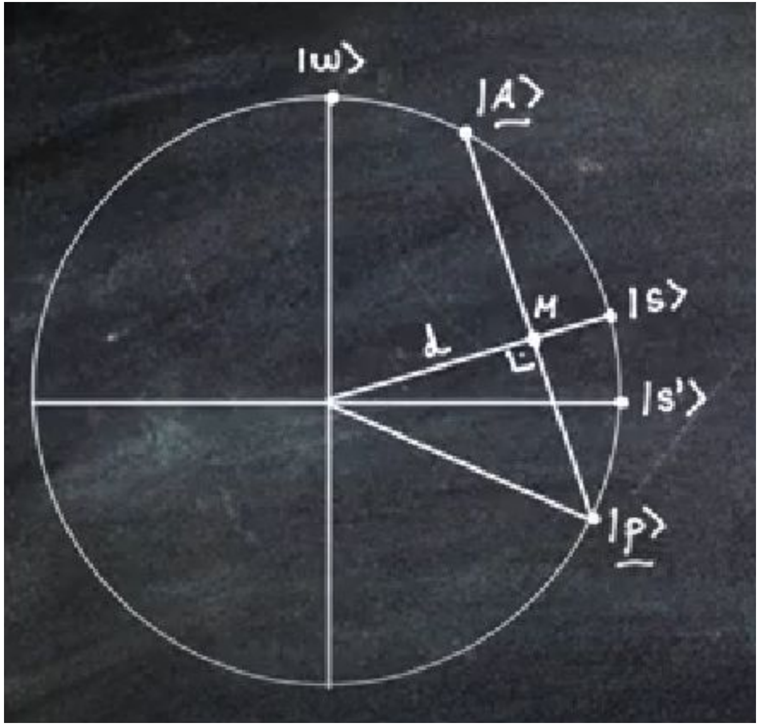
Sustituyendo en M tenemos,

$$M = |s\rangle\langle s||p\rangle$$

Sustituyendo en $p\bar{M}$ tenemos,

$$p\bar{M} = |s\rangle\langle s||p\rangle - |p\rangle$$

Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

Notamos que $p\bar{M}$ es perpendicular a $|s\rangle$ por tanto.

$$\langle s||(d|s\rangle - |p\rangle)\rangle = 0$$

Despejando tenemos $d = \langle s||p\rangle$

Sustituyendo en M tenemos,

$$M = |s\rangle\langle s||p\rangle$$

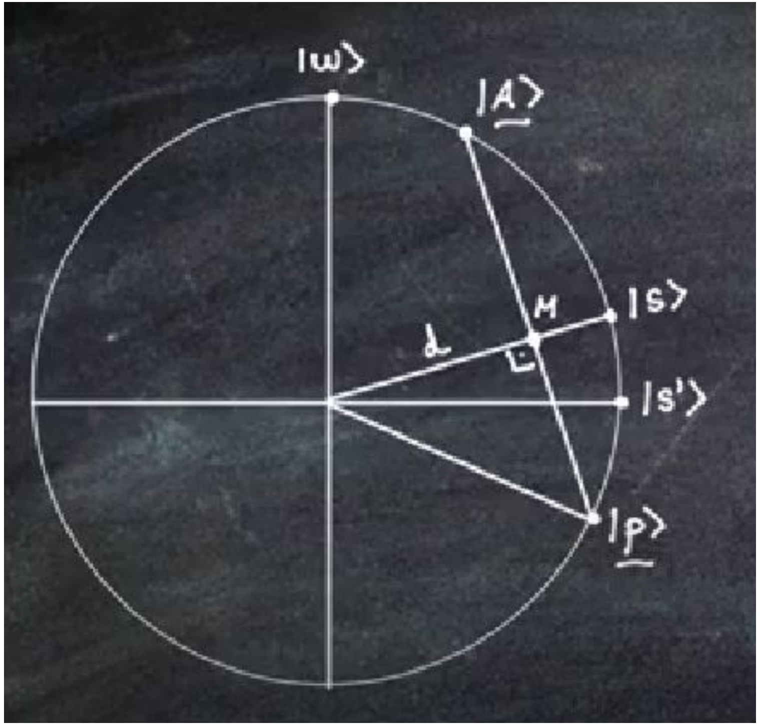
Sustituyendo en $p\bar{M}$ tenemos,

$$p\bar{M} = |s\rangle\langle s||p\rangle - |p\rangle$$

Finalmete obtenemos que,

$$|A\rangle = M + p\bar{M} =$$

Solución cuántica.



Notemos que $|A\rangle = M + p\bar{M}$

$$M = d|s\rangle$$
$$p\bar{M} = d|s\rangle - |p\rangle$$

Notamos que $p\bar{M}$ es perpendicular a $|s\rangle$ por tanto.

$$\langle s||(d|s\rangle - |p\rangle)\rangle = 0$$

Despejando tenemos $d = \langle s||p\rangle$

Sustituyendo en M tenemos,

$$M = |s\rangle\langle s||p\rangle$$

Sustituyendo en $p\bar{M}$ tenemos,

$$p\bar{M} = |s\rangle\langle s||p\rangle - |p\rangle$$

Finalmete obtenemos que,

$$|A\rangle = M + p\bar{M} = 2|s\rangle\langle s||p\rangle - |p\rangle = (2|s\rangle\langle s| - I)|p\rangle$$

Cual es la utilidad de esta compuerta en el algoritmo?

Por qué se necesitan raíz de n iteraciones?

https://www.youtube.com/watch?v=2UzmFiei9h0&list=PLhYoqmlacCv-6t6gCJIuE8Ok8my9y1K_u&index=5