Introducción a los algoritmos cuánticos

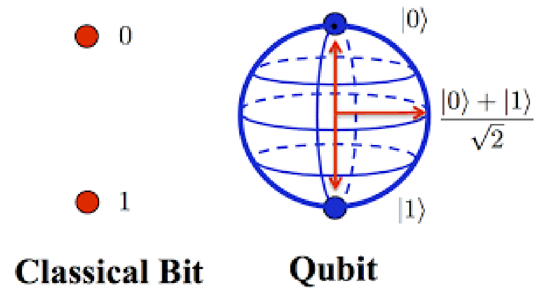
Dominique Spehner

Departamento de Ingeniería Matemática
Universidad de Concepción, Chile

Escuela en computación cuántica, Concepción, 9-13/01/2023

Bits cuánticos (qubits)

El **estado de un sistema cuántico** se representa por un **vector de norma** 1 **de** $\mathcal{H} = \mathbb{C}^N$ (ó de un espacio de Hilbert $\mathcal{H}$ de dim. infinita)



★ **1 qubit :** $\mathcal{H} = \mathbb{C}^2$, base computacional $\{|0\rangle, |1\rangle\}$

$$\boxed{|\psi\rangle = c_0|0\rangle + c_1|1\rangle \quad \in \mathbb{C}^2}$$

$c_{0,1} \in \mathbb{C}$ componentes complejos tales que $|c_0|^2 + |c_1|^2 = 1$.

★ n **qubits :** $\mathcal{H} = \mathbb{C}^{2^n}$, base computacional

$$\{|x\rangle = |x_{n-1}\ldots x_0\rangle = |x_{n-1}\rangle\ldots|x_0\rangle\,;\, x_i = 0,1\}$$

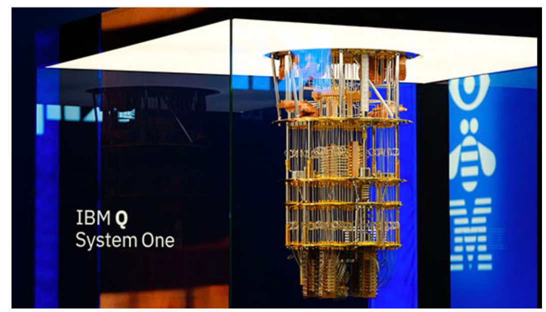
$$\boxed{|\psi\rangle = \sum_{x\in\{0,1\}^n} c_x|x\rangle \quad \in \mathbb{C}^{2^n}}$$

$c_x \in \mathbb{C}$ componentes complejos tales que $\sum_x |c_x|^2 = 1$.

Computadores clásico y cuántico

- **Computador clásico :**

$$\begin{cases} \text{input:} & x = x_n \ldots x_1 \in \{0,1\}^n \\ \text{output:} & y = y_m \ldots y_1 \in \{0,1\}^m \end{cases}$$



- **Computador cuántico :**

$$\begin{cases} \text{input:} & |\psi_0\rangle \in \mathbb{C}^N \ , \ N = 2^n \\ \text{output:} & |\psi\rangle = U|\psi_0\rangle \in \mathbb{C}^N \end{cases}$$

U operador unitario (matriz $N \times N$).

Medición en la base computacional $\{|x\rangle ; x \in \{0,1\}^n\}$:

$\rightsquigarrow$ resultado **aleatorio** $y \in \{0,1\}^n$ con proba $p_y = |\langle y|\psi\rangle|^2$

$\hookrightarrow$ Se extrae **información clásica** del estado cuántico $|\psi\rangle$

Computación con 2 qubits (input + ancilla)

- Sea $f : \{0, 1\} \to \{0, 1\}$ una función booleana. Definimos

$$U_f|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle \;\; \forall\, x, q \in \{0, 1\}$$

donde $\oplus$ es la adición modulo 2 ($0 \oplus 0 = 1 \oplus 1 = 0,\ 0 \oplus 1 = 1 \oplus 0 = 1$)

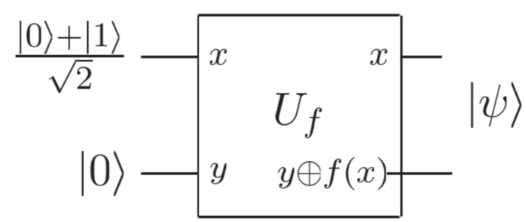
Se extiende U_f a todo $\mathbb{C}^4$ por linealidad.

Luego U_f es un operador unitario, ya que

$$\langle x, q \oplus f(x)|x', q' \oplus f(x')\rangle = \langle x|x'\rangle\langle q \oplus f(x)|q' \oplus f(x')\rangle = \delta_{x,x'}\delta_{q,q'}$$

$\Rightarrow \{U_f|x\rangle|q\rangle;\, x, q = 0, 1\}$ es una base ortonormal.

- Si el estado inicial del qubit 1 es la superposición $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, el estado final



$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|q \oplus f(0)\rangle + |1\rangle|q \oplus f(1)\rangle)$$

"contiene" ambas valores $f(0)$ y $f(1)$.

¿ Como extraer esta información contenida en $|\psi\rangle$?

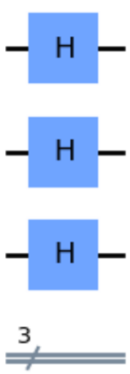
Computación con $n+1$ qubits

- Sea $f:\{0,1\}^n \to \{0,1\}$ una función booleana. Definimos
$$U_f|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle \;\; \forall\, x \in \{0,1\}^n, q \in \{0,1\}$$
Se extiende U_f por linealidad en un op. unitario en $\mathbb{C}^{2^{n+1}}$.

- Puerta de Hadamard:

$$\begin{cases} H|0\rangle &= \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ H|1\rangle &= \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{cases}, \quad \mathrm{Mat}(H) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- Transformación de Hadamard sobre los n primeros qubits:



$$\begin{aligned} |\psi_0\rangle &= H^{\otimes^n} \otimes \mathbb{1}|0\ldots0\rangle|0\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\ldots\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle \\ &= 2^{-\frac{n}{2}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle \end{aligned}$$

- $U_f|\psi_0\rangle = \dfrac{1}{\sqrt{N}} \displaystyle\sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle \;,\;\; N = 2^n$

Paralelismo cuántico

$|\psi\rangle = U_f|\psi_0\rangle = N^{-1/2} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$ contiene todos los valores $f(x)$ en **una sola evaluación** de f.

¿ Como extraer esta información contenida en $|\psi\rangle$?

Paralelismo cuántico

$|\psi\rangle = U_f|\psi_0\rangle = N^{-1/2} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$ contiene todos los valores $f(x)$ en **una sola evaluación** de f.

¿ Como extraer esta información contenida en $|\psi\rangle$?

Medición en la base computacional $\rightarrow$ *resultado aleatorio* *si se obtiene* $y \in \{0,1\}^n$ *para los qubits* $1, \dots, n$ *(proba* $p_y = 2^{-n}$*) luego el valor de* $f(y)$ *es el resultado sobre el qubit* $n+1$.

$\hookrightarrow$ Eso lo puede hacer un computador clásico, eligiendo y al azar y calculando $f(y)$ (necesita una sola evaluación de f).

Paralelismo cuántico

$|\psi\rangle = U_f|\psi_0\rangle = N^{-1/2} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$ contiene todos los valores $f(x)$ en **una sola evaluación** de f.

¿ Como extraer esta información contenida en $|\psi\rangle$?

Medición en la base computacional $\rightsquigarrow$ *resultado aleatorio, si se obtiene $y \in \{0,1\}^n$ para los qubits $1,\ldots,n$ (proba $p_y = 2^{-n}$) luego el valor de $f(y)$ es el resultado sobre el qubit $n+1$.*

$\hookrightarrow$ Eso lo puede hacer un computador clásico, eligiendo y al azar y calculando $f(y)$ (necesita una sola evaluación de f).

Encodar la información sobre f en las **fases** de los componentes de $U_f|\psi_0\rangle$ y usar la propiedad de **interferencia cuántica**

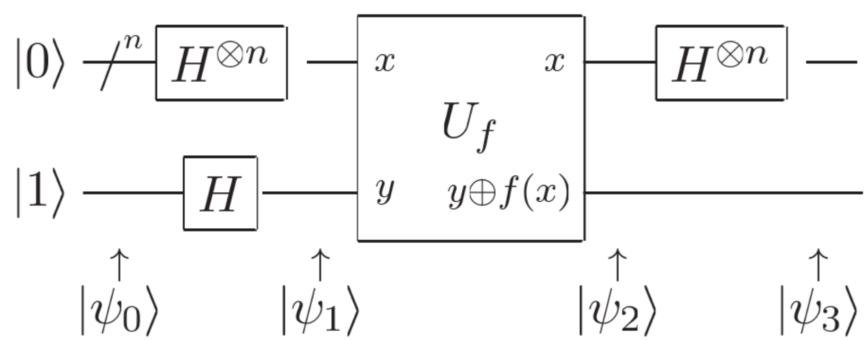
Algoritmo de Deutsch-Josza

- **Tarea computacional:**
  Suponga que $f : \{0,1\}^n \to \{0,1\}$ *satisface*
  (1) f *es constante ó (2)* f *es balanceada, esto es,* $f(x) = 1$
  $(f(x) = 0)$ *para exactamente la mitad de los* $x \in \{0,1\}^n$.
  Queremos saber cual de las propiedades (1) ó (2) satisface f.
- Para resolver esta tarea, un computador clásico necesita evaluar $f(x)$ para $2^{n-1} + 1$ valores de x, en el peor de los casos.
-

Algoritmo de Deutsch-Josza

- **Tarea computacional:**
  Suponga que $f : \{0,1\}^n \to \{0,1\}$ *satisface*
  (1) f *es constante ó (2)* f *es balanceada, esto es,* $f(x) = 1$
  $(f(x) = 0)$ *para exactamente la mitad de los* $x \in \{0,1\}^n$.
  Queremos saber cual de las propiedades (1) ó (2) satisface f.

- Para resolver esta tarea, un computador clásico necesita evaluar $f(x)$ para $2^{n-1} + 1$ valores de x, en el peor de los casos.



- **Algoritmo cuántico:**
$$\begin{cases} \text{input:} & |\psi_0\rangle = |0\ldots0\rangle|1\rangle \\ \text{output:} & |\psi_3\rangle = \underbrace{H^{\otimes^n} \otimes \mathbb{1}}_{\text{interferometría}}\; U_f\, H^{\otimes^{n+1}}|\psi_0\rangle \end{cases}$$

Estado final (detalle del cálculo)

$$|\psi_1\rangle = H^{\otimes^{n+1}}|\psi_0\rangle = 2^{-\frac{n+1}{2}} \sum_{x\in\{0,1\}^n} |x\rangle(|0\rangle - |1\rangle)$$

$$|\psi_2\rangle = U_f|\psi_1\rangle = 2^{-\frac{n+1}{2}} \sum_{x\in\{0,1\}^n} \underbrace{(-1)^{f(x)}}_{\text{factor de fase}} |x\rangle(|0\rangle - |1\rangle)$$

donde usamos $|f(x)\rangle - |f(x)\oplus 1\rangle = (-1)^{f(x)}(|0\rangle - |1\rangle)$.

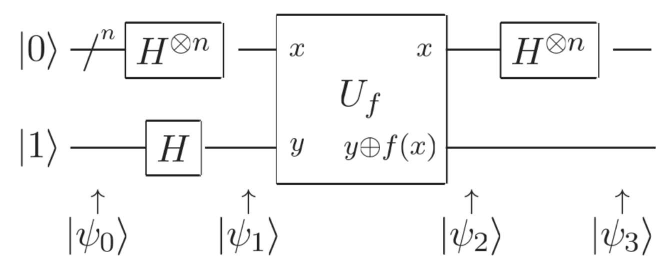
Es fácil mostrar que

$$H^{\otimes^n}|x\rangle = 2^{-\frac{n}{2}} \sum_{z\in\{0,1\}} (-1)^{x\cdot z}|z\rangle \;\; \text{con} \;\; x\cdot z = \sum_{i=1}^{n} x_i z_i$$

$$\Rightarrow |\psi_3\rangle = H^{\otimes^n} \otimes \mathbb{1}|\psi_2\rangle = \underbrace{2^{-n} \sum_{x,z\in\{0,1\}^n} (-1)^{f(x)+x\cdot z}|z\rangle}_{|\Phi_3\rangle} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Resultados de la medición

- **Estado final** $|\psi_3\rangle = |\phi_3\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$



$$|\phi_3\rangle = 2^{-n} \sum_{x,z \in \{0,1\}^n} (-1)^{f(x) + x \cdot z} |z\rangle$$

- **Caso 1:** $f(x) = $ const.

$$\langle 0 \ldots 0 | \phi_3 \rangle = 2^{-n} \sum_x (-1)^{f(x)} = \pm 1 \;\Leftrightarrow\; |\phi_3\rangle = \pm |0 \ldots 0\rangle$$

Caso 2: f balanceada

$$\langle 0 \ldots 0 | \phi_3 \rangle = 2^{-n} \sum_x (-1)^{f(x)} = 0 \;\Leftrightarrow\; |\phi_3\rangle \perp |0 \ldots 0\rangle$$

- Medición en la base computacional sobre los qubits $1, \ldots, n$:

Caso 1: resultado $y = 0$ con proba $p_0 = |\langle 0 \ldots 0 | \phi_3 \rangle|^2 = 1$

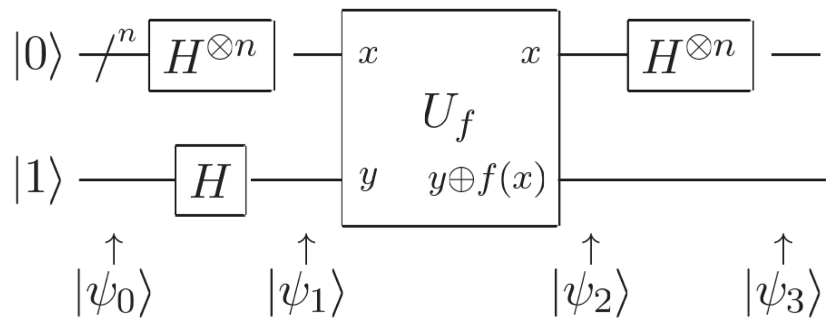
Caso 2: resultado $y \neq 0$ con proba $p_\perp = \sum_{y \neq 0} |\langle y | \phi_3 \rangle|^2 = 1$

Resumen: algoritmo de Deutsch-Josza

- **Tarea:** *Suponga que* $f : \{0,1\}^n \to \{0,1\}$ *satisface*
  (1) f *es constante ó (2)* f *es balanceada.*
  Hallar cual alternativa (1) ó (2) es la correcta.

- **"Oráculo"**:

$$U_f|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$$
$$x \in \{0,1\}^n, q \in \{0,1\}$$



- **Algoritmo:**

Input:	$\lvert\psi_0\rangle = \lvert 0 \ldots 0\rangle\lvert 1\rangle$
Output:	$\lvert\psi_3\rangle = H^{\otimes^n} \otimes \mathbb{1}\, U_f\, H^{\otimes^{n+1}}\lvert\psi_0\rangle$
Medición:	base computacional, sobre los qubits $1, \ldots, n$
Resultado:	$y = 0$ si y solo si $f =$ const. (sin error)
Runtime:	una sola evaluación de U_f.

Transformación de Fourier cuántica

- **Transformación de Fourier (TF) discreta:**

$$\mathrm{TF}(c)_{\hat{y}} = N^{-1/2} \sum_{\hat{x}=0}^{N-1} c_{\hat{x}}\, e^{2\mathrm{i}\pi \frac{\hat{x}\hat{y}}{N}} \ , \ \hat{y} \in \{0, \ldots, N-1\}$$

- **Transformación de Fourier cuántica:**

$$U_{\mathrm{TF}} |\hat{x}\rangle = N^{-1/2} \sum_{\hat{y}=0}^{N-1} e^{2\mathrm{i}\pi \frac{\hat{x}\hat{y}}{N}} |\hat{y}\rangle \ \text{ con } \ |\hat{y}\rangle = |y_{n-1} \ldots y_0\rangle$$

$N = 2^n$

$y_{n-1} \ldots y_0 =$ representación binaria de $\hat{y} \in \{0, \ldots, N-1\}$.

- Se puede mostrar que U_{TF} es un op. unitario sobre $\mathbb{C}^N$ y

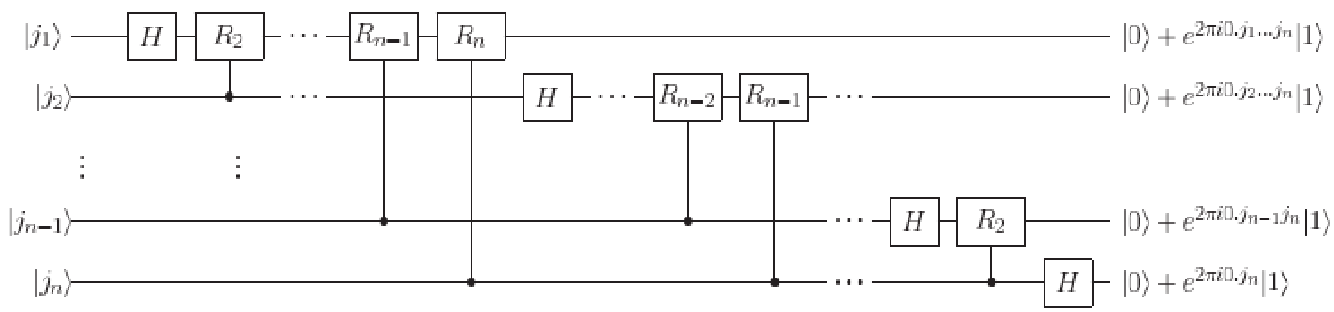
$$|\psi\rangle = \sum_{\hat{x}} c_{\hat{x}} |\hat{x}\rangle \ \Rightarrow \ U_{\mathrm{FT}} |\psi\rangle = \sum_{\hat{y}} \mathrm{TF}(c)_{\hat{y}} |\hat{y}\rangle$$

$\hookrightarrow$ $U_{\mathrm{TF}}|\psi\rangle$ contiene los M coeficientes de la TF discreta de $(c_{\hat{x}})_{\hat{x}=0,\ldots,N-1}$ (*paralelismo cuántico*).

Pero está información está “escondida” en el estado cuántico!

Transformación de Fourier cuántica (2)

- Es posible implementar U_{TF} con un circuito de n qubits usando $O(n^2)$ puertas cuánticas H, C$-U$ y SWAP.



$\leftrightarrow$ los algoritmos clásicos FFT necesitan $O(n2^n)$ puertas.

- Entre otros algoritmos cuánticos, el **algoritmo de Shor** usa la TF cuántica U_{FT}. Este algoritmo factoriza un número entero en números primos en un tiempo $O(n^3)$.

  $\hookrightarrow$ los algoritmos clásicos conicidos se demorran más que $O(n^\alpha)$ para cada $\alpha > 0$!

Clases de complejidad

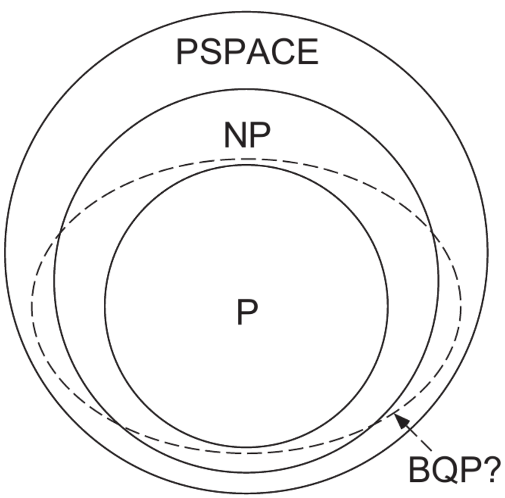
¿ Un computador cuántico es más eficiente que uno clásico?

Las clases de complejidad permiten cuantificar que tan difíciles son las tareas computacionales

- Clase P: *se puede solucionar la tarea en un tiempo polinomial* $O(N^\alpha)$
- Clase NP: *chequear que una solución resuelve la tarea es de clase* P
- Clase $PSPACE$: *se puede solucionar la tarea con* $O(N^\alpha)$ *bits (pero no necesariamente en tiempo polinomial)*

Tenemos $P \subset NP \subset PSPACE$, pero no se sabe si las inclusiones son estrictas!

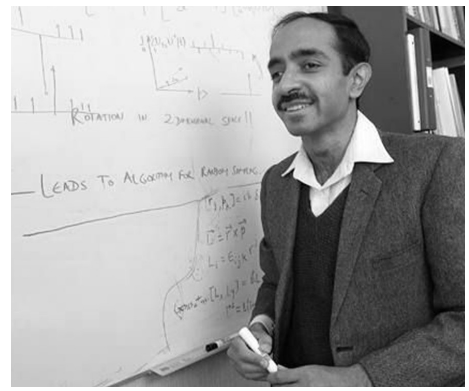
- Clase cuántica BQP: *se puede solucionar la tarea con un computador cuántico en un tiempo polinomial con una pequeña probabilidad de error.*



Algoritmo de busqueda de Grover

- **Tarea computacional:** *suponemos que podemos evaluar* $f : \{0,1\}^n \to \{0,1\}$ *de manera eficiente (oráculo).* *Decimos que* $w \in \{0,1\}^n$ *es una solución si* $f(w) = 1$*.* Queremos **hallar todas las soluciones** w.

- El **algoritmo de Grover** permite resolver esta tarea con $O(\sqrt{N/M})$ evaluaciones de f con una probabilidad $\simeq 1$, donde $N = 2^n$ y M es el número de soluciones.



$\leftrightarrow$ un computador clásico necesita N evaluaciones de f (testear para cada $x \in \{0,1\}^N$ si $f(x) = 1$).

Oráculo O_f

$$U_f|x,q\rangle = |x, q\oplus f(x)\rangle\ ,\ \ x\in\{0,1\}^n, q\in\{0,1\}$$

$\Rightarrow\ U_f\otimes H|x\rangle|1\rangle = U_f|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) = O_f|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$ con

$$O_f|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} -|x\rangle & \text{si } x \text{ es solución} \\ |x\rangle & \text{si } x \text{ no es solución} \end{cases}$$

- **Estado inicial:**

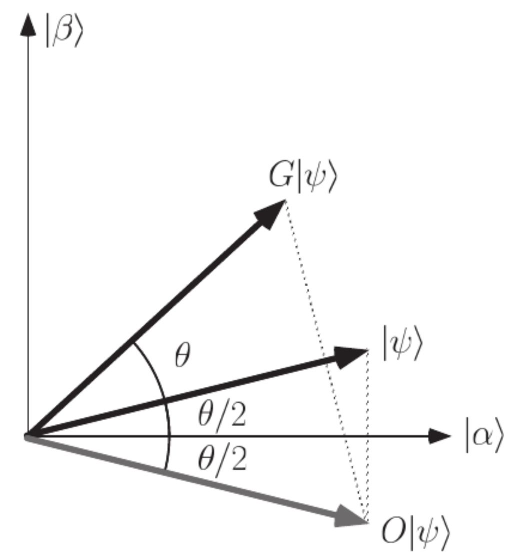
$|\psi_0\rangle = H^{\otimes^n}|0\ldots0\rangle = \frac{1}{\sqrt{N}}\sum_{x\in\{0,1\}^n}|x\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle$, donde

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

$$|\beta\rangle = \frac{1}{\sqrt{M}}\sum_{w,f(w)=1}|w\rangle$$

son **vectores por buscar** y $\cos^2\frac{\theta}{2} = \frac{N-M}{N}$.

$$\boxed{\Rightarrow\ O_f|\psi_0\rangle = \cos\tfrac{\theta}{2}|\alpha\rangle - \sin\tfrac{\theta}{2}|\beta\rangle}$$



Operador de Grover G_f

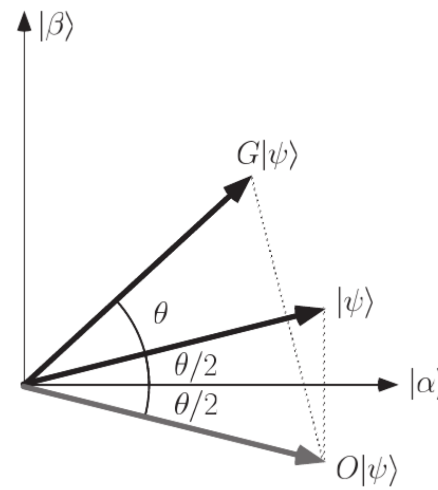
- Combinar O_f con una reflexión con respecto a $|\psi_0\rangle$,

$$R_{\psi_0} = 2|\psi_0\rangle\langle\psi_0| - \mathbb{1} = H^{\otimes^n}(2|0\rangle\langle 0| - \mathbb{1})H^{\otimes^n}$$

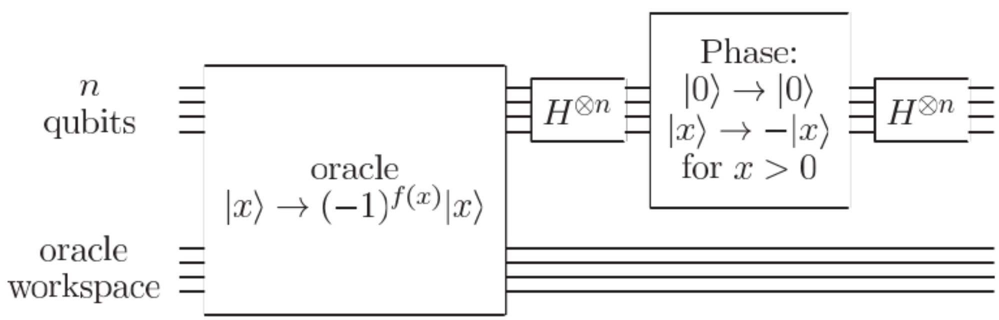
La compuesta de 2 reflexiones es una rotación

$$\boxed{|\psi_0\rangle \to G_f|\psi_0\rangle = R_{\psi_0} O_f |\psi_0\rangle \ , \ \frac{\theta}{2} \to \frac{3\theta}{2}}$$

$\hookrightarrow$ amplifica la componente de $|\psi\rangle$ segun $|\beta\rangle$



G_f



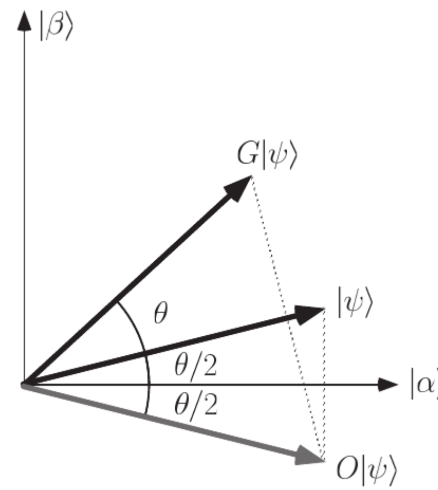
Operador de Grover G_f

- Combinar O_f con una reflexión con respecto a $|\psi_0\rangle$,

$$R_{\psi_0} = 2|\psi_0\rangle\langle\psi_0| - \mathbb{1} = H^{\otimes^n}(2|0\rangle\langle 0| - \mathbb{1})H^{\otimes^n}$$

La compuesta de 2 reflexiones es una rotación

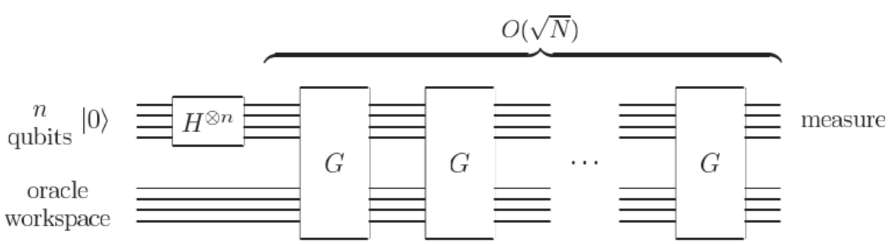
$$\boxed{|\psi_0\rangle \to G_f|\psi_0\rangle = R_{\psi_0}\, O_f|\psi_0\rangle \ , \ \frac{\theta}{2} \to \frac{3\theta}{2}}$$



$\hookrightarrow$ amplifica la componente de $|\psi\rangle$ segun $|\beta\rangle$

- Aplicando $k = E(\frac{\pi-\theta}{2\theta})$ veces la rotación G_f, $|\psi_0\rangle$ se transforma como

$$G_f^k|\psi_0\rangle \simeq |\beta\rangle = M^{-1/2} \sum_{w, f(w)=1} |w\rangle$$

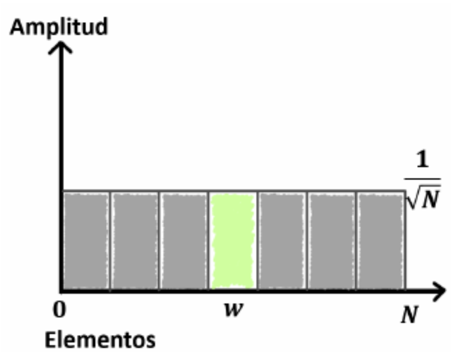


- Al medir en la base computacional, se obtienen las soluciones w

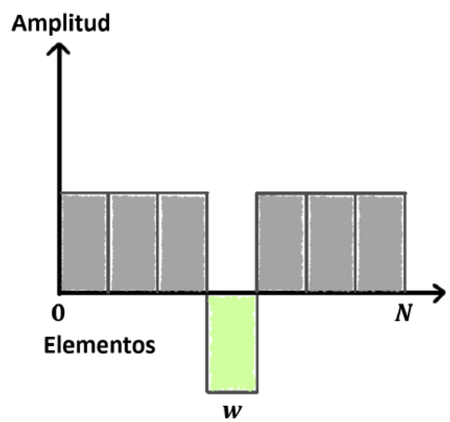
Caso particular $M = 1$ (solución única)

- Si $f(x) = 1 \;\Leftrightarrow\; x = w$, luego $M = 1$ y $|\beta\rangle = |w\rangle$

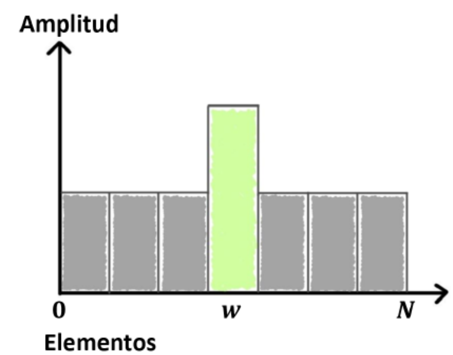
$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$



$O_f|\psi_0\rangle$



$G_f|\psi_0\rangle$



- **¿ Cuantas veces se tiene que aplicar la rotación G_f ?**

$$\sin\frac{\theta}{2} = \langle w|\psi_0\rangle = N^{-\frac{1}{2}} \;\Rightarrow\; k = E\left(\frac{\pi-\theta}{2\theta}\right) \simeq \frac{\pi}{4N^{-\frac{1}{2}}} = \frac{\pi\sqrt{N}}{4}$$

Número de evaluaciones y proba de error

- Más generalmente, si hay $M \ll N$ soluciones, luego $\frac{\theta}{2} \simeq \sqrt{M/N}$ y el número de aplicaciones de G_f es

$$\boxed{k \simeq \frac{\pi}{4}\sqrt{\frac{N}{M}}}$$

NOTA: si M es desconicido, existe un algoritmo basado en la **estimación de fase** (usando la TF cuántica) que permite hallar M con una buena precisión.

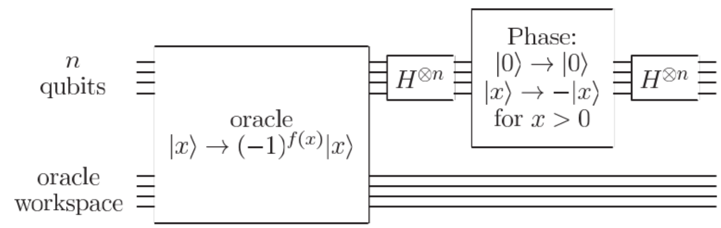
- **Proba de error:** $G_f^k|\psi_0\rangle = \cos\theta_k|\alpha\rangle + \sin\theta_k|\beta\rangle$, $\theta_k = k\theta + \frac{\theta}{2}$

$$\Rightarrow\ p_{\mathsf{Er}} = \sum_{f(x)=0} |\langle x|G_f^k|\psi_0\rangle|^2 = \sum_{f(x)=0} \cos^2\theta_k |\langle x|\alpha\rangle|^2$$

$$= \cos^2\theta_k \ \leqslant\ \sin^2\frac{\theta}{2} \simeq \frac{\theta^2}{4} \simeq \frac{M}{4N}$$

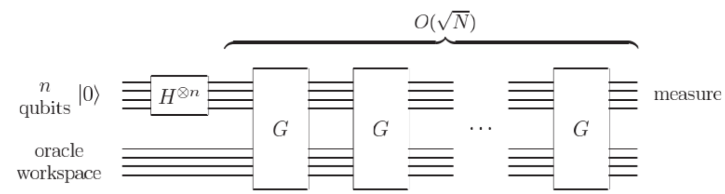
Resumen: algoritmo de Grover

- *Input:* oráculo O_f, número de soluciones M
- *Ouptut:* una solucioń $w \in \{0,1\}^n$,
  $f(w) = 1$.



$$|0\ldots0\rangle|1\rangle \to |\psi_0\rangle = H^{\otimes^{n+1}}|0\ldots0\rangle|1\rangle \to G_f^k|\psi_0\rangle = \cos\theta_k|\alpha\rangle + \sin\theta_k|\beta\rangle$$

- *Medición:* base computacional,
  qubits $1,\ldots,n$



- *Resultado:* $\begin{cases} w \in \{\text{soluciones}\} & \text{con proba } \simeq 1/M \\ x \notin \{\text{soluciones}\} & \text{con proba } p_{\mathrm{Er}} \leqslant \frac{M}{4N} \end{cases}$
- *Runtime:* $O(\sqrt{N/M})$ aplicaciones del oráculo O_f.

Al repetir $O(M)$ veces el algoritmo $\to$ todas las soluciones.

Gracias por su atención!