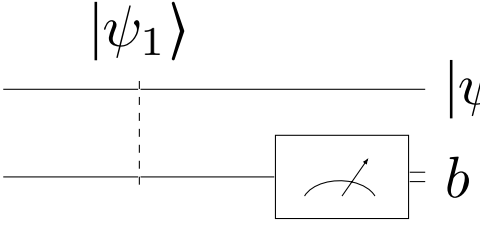
El algoritmo de Shor — Parte 3

Computación Cuántica: Algorítmica y Software

Joaquín Keller

2026 UCV

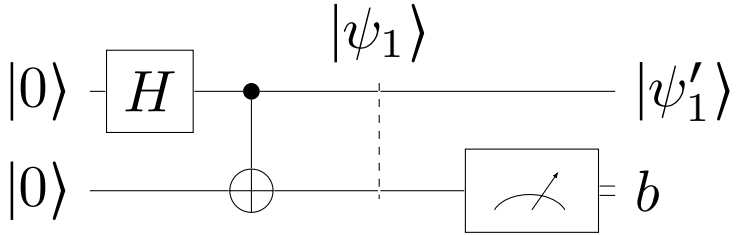
Medición parcial



$$|\psi_1\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$$

$$\begin{cases} \text{si } b = 0 & |\psi_1'\rangle = \dfrac{\alpha\,|0\rangle + \gamma\,|1\rangle}{\sqrt{|\alpha|^2+|\gamma|^2}} \\ \text{si } b = 1 & |\psi_1'\rangle = \dfrac{\beta\,|0\rangle + \delta\,|1\rangle}{\sqrt{|\beta|^2+|\delta|^2}} \end{cases}$$

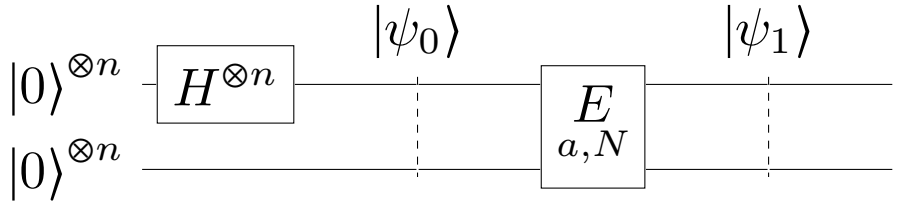
Ejemplo con el estado de Bell



$$|\psi_1\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\begin{cases} \text{si } b = 0 & |\psi_1'\rangle = |0\rangle \\ \text{si } b = 1 & |\psi_1'\rangle = |1\rangle \end{cases} \implies |\psi_1'\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = H|0\rangle$$

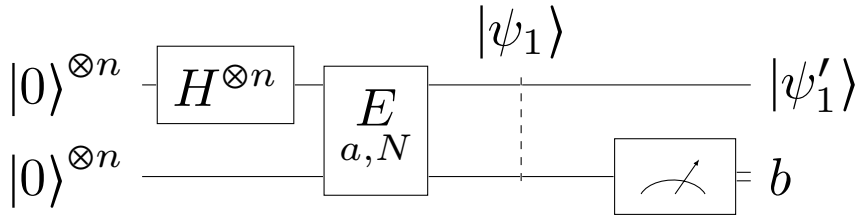
Circuito para el algoritmo de Shor



$$|\psi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |\underline{0}\rangle \qquad |\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |a^k\rangle$$

El circuito calcula todos los a^k mod N para $k \leq N$

Cómo conseguir r, el k que da $a^k \equiv 1 \pmod{N}$?



$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |a^k\rangle \qquad k = \alpha r + \beta \quad 0 \le \beta < r \quad 0 \le \alpha < 2^n/r$$

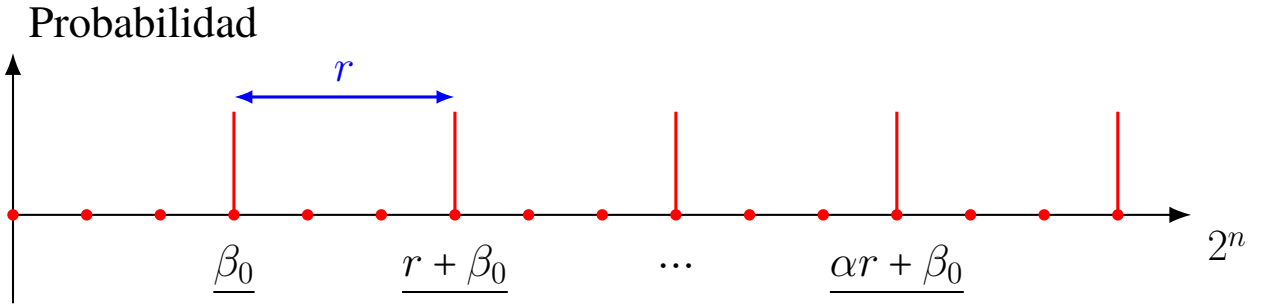
Hipótesis simplificadora: $r|2^n$ $\qquad |\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\beta=0}^{r-1} \sum_{\alpha=0}^{\frac{2^n}{r}-1} |\alpha r + \beta\rangle\, |a^\beta\rangle$

La medición fija un β_0 $\quad b = \underline{a^{\beta_0}}$ $\qquad |\psi_1'\rangle = \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{\frac{2^n}{r}-1} |\alpha r + \beta_0\rangle$

Medición de $|\psi_1'\rangle$

$$|\psi_1'\rangle = \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{\frac{2^n}{r}-1} |\alpha r + \beta_0\rangle$$

Una distribución de probabilidad periódica



Transformada discreta de Fourier

$$\mathcal{F} : \mathbb{C}^N \to \mathbb{C}^N$$
$$x \mapsto \mathcal{F}(x) = \tilde{x}$$

$$\tilde{x}_k = \frac{1}{N} \sum_{j=0}^{N-1} x_j e^{-2i\pi \frac{kj}{N}}$$

Transformada cuántica de Fourier

$$\hat{\mathcal{F}} |\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{kj}{2^n}} |\underline{j}\rangle \quad = \quad \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} \omega^{kj} |\underline{j}\rangle \qquad \text{con } \omega = e^{\frac{2i\pi}{2^n}}$$

Estado cuántico $|\psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k |\underline{k}\rangle$ por linearidad $\hat{\mathcal{F}} |\psi\rangle = \sum_{k=0}^{2^n-1} \alpha_k \hat{\mathcal{F}} |\underline{k}\rangle$

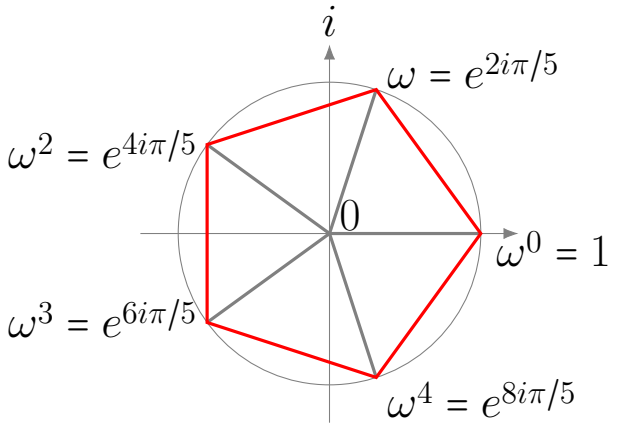
$$\sum_{k=0}^{N-1} z^k = 1 + z + z^2 + \ldots + z^{N-1} = \begin{cases} N & \text{si } z = 1 \\ \dfrac{1 - z^N}{1 - z} & \text{sino} \end{cases}$$

Demonstración:

$$(1 - z)(1 + z + z^2 + \ldots + z^{N-1}) = \begin{array}{l} 1 + z + z^2 + \ldots + z^{N-1} \\ \quad - z - z^2 - \ldots - z^{N-1} - z^N \end{array} = 1 - z^N$$

Con $z = e^{2i\pi \frac{j}{N}}$ $\qquad 1 - z^N = 1 - e^{2i\pi j} = 0$

$$\frac{1}{N} \sum_{k=0}^{N-1} e^{2i\pi \frac{kj}{N}} = \frac{1}{N} \sum_{k=0}^{N-1} (e^{2i\pi \frac{j}{N}})^k = \begin{cases} 1 & \text{si } \frac{j}{N} \text{ es entero} \\ 0 & \text{sino} \end{cases}$$



$\omega = e^{\frac{2i\pi}{N}}$

ejemplo con $N = 5$

La transformada cuántica de Fourier es unitaria

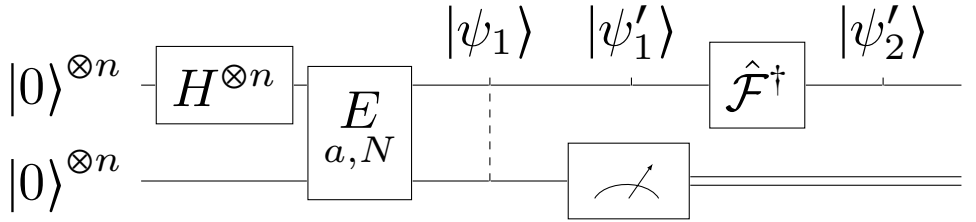
Transforma la base $|\underline{0}\rangle, |\underline{1}\rangle, \ldots, |\underline{2^n - 1}\rangle$ en otra base ortonormal

Definición de ortonormal: $p \neq q \Rightarrow \langle p|q\rangle = 0 \quad$ y $\quad \langle p|p\rangle = 1$

$$\langle \hat{\mathcal{F}}\underline{k}|\hat{\mathcal{F}}\underline{\ell}\rangle = \left(\hat{\mathcal{F}}^\dagger \langle \underline{k}| \right)\hat{\mathcal{F}}\,|\underline{\ell}\rangle = \left(\tfrac{1}{\sqrt{2^n}} \sum_{p=0}^{2^n-1} e^{-2i\pi\frac{kp}{2^n}} \langle \underline{p}| \right)\left(\tfrac{1}{\sqrt{2^n}} \sum_{q=0}^{2^n-1} e^{2i\pi\frac{\ell q}{2^n}} |\underline{q}\rangle \right)$$

$$= \tfrac{1}{2^n} \sum_{p=0}^{2^n-1} \sum_{q=0}^{2^n-1} e^{\frac{2i\pi}{2^n}(\ell q - kp)} \langle p|q\rangle = \tfrac{1}{2^n} \sum_{p=0}^{2^n-1} e^{\frac{2i\pi}{2^n}(\ell p - kp)} \langle p|p\rangle = \tfrac{1}{2^n} \sum_{p=0}^{2^n-1} \left(e^{2i\pi\frac{\ell-k}{2^n}}\right)^p$$

$$= \begin{cases} 1 & \text{si } k = \ell \text{ ya que } \frac{\ell-k}{2^n} \text{ es entero} \\ 0 & \text{si } k \neq \ell \text{ ya que } \frac{\ell-k}{2^n} \text{ no es entero porque } 0 < |\ell - k| < 2^n \end{cases}$$



Hipótesis simplificadora: $r|2^n$

$$|\psi_1'\rangle = \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{\frac{2^n}{r}-1} |\alpha r + \beta_0\rangle$$

$$|\psi_2'\rangle = \hat{\mathcal{F}}^\dagger |\psi_1'\rangle = \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{\frac{2^n}{r}-1} \hat{\mathcal{F}}^\dagger |\alpha r + \beta_0\rangle = \frac{\sqrt{r}}{\sqrt{2^n}} \sum_{\alpha=0}^{\frac{2^n}{r}-1} \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-2i\pi \frac{\alpha r + \beta_0}{2^n} j} |\underline{j}\rangle$$

$$= \frac{\sqrt{r}}{2^n} \sum_{j=0}^{2^n-1} \sum_{\alpha=0}^{\frac{2^n}{r}-1} e^{-2i\pi \frac{\alpha r}{2^n} j} e^{-2i\pi \frac{\beta_0}{2^n} j} |\underline{j}\rangle = \frac{\sqrt{r}}{2^n} \sum_{j=0}^{2^n-1} \left(\sum_{\alpha=0}^{\frac{2^n}{r}-1} e^{-2i\pi \frac{\alpha j}{2^n/r}} \right) e^{-2i\pi \frac{\beta_0}{2^n} j} |\underline{j}\rangle$$

$$|\psi_2'\rangle = \frac{\sqrt{r}}{2^n} \sum_{j=0}^{2^n-1} \left(\sum_{\alpha=0}^{\frac{2^n}{r}-1} e^{-2i\pi \frac{\alpha j}{2^n/r}} \right) e^{-2i\pi \frac{\beta_0}{2^n} j} \left| \underline{j} \right\rangle$$

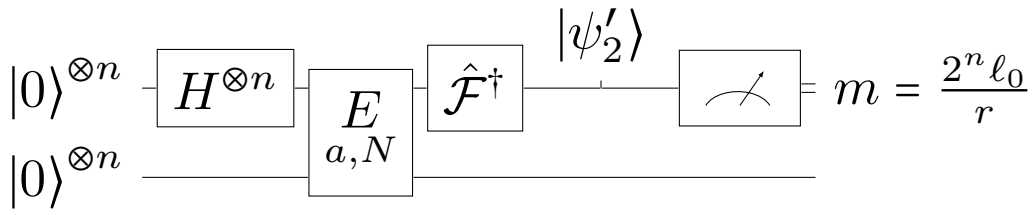
$$\frac{r}{2^n} \sum_{\alpha=0}^{\frac{2^n}{r}-1} e^{-2i\pi \frac{\alpha j}{2^n/r}} = \begin{cases} 1 & \text{si } \frac{j}{2^n/r} \text{ es un entero} \\ 0 & \text{sino} \end{cases}$$

Los j tales que $\frac{j}{2^n/r}$ sea entero son los múltiples de $\frac{2^n}{r}$ es decir que $j = \ell \frac{2^n}{r}$

$$0 \leq j < 2^n \Leftrightarrow 0 \leq \frac{j}{2^n/r} < r \Leftrightarrow \quad 0 \leq \ell < r$$

$$|\psi_2'\rangle = \frac{1}{\sqrt{r}} \sum_{\frac{j}{2^n/r} \in \mathbb{N}}^{0 \leq j < 2^n} e^{-2i\pi \frac{\beta_0}{2^n} j} \left| \underline{j} \right\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{-2i\pi \frac{\beta_0}{r} \ell} \left| \frac{2^n \ell}{r} \right\rangle$$

β_0 desaparece con la medición



Como calcular r utilizando m?

1. Reducir la fracción $\frac{m}{2^n} \to \frac{p}{q}$
2. Si $q = 1$ es decir si ℓ_0 es un múltiple de r, correr de nuevo el circuito
3. Calcular a^q, si $a^q = 1$ entonces $r = q$ ■
4. Si $a^q \neq 1$ es que $\text{mcd}(\ell_0, r) \neq 1$ y q es un divisor de r
   Empezar de nuevo el algoritmo con $a' = a^q$, sabemos que $r' = r/q$
   Como r tiene un número finito de divisores, el proceso tiene fin

Puntos por tratar

Como hacer sin la hipótesis: $r|2^n$

es decir cuando r no es una potencia de 2

Circuito y complejidad algorítmica de $\hat{\mathcal{F}}$

la transformada cuántica de Fourier