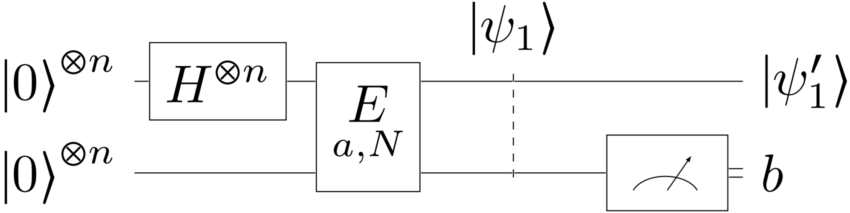
El algoritmo de Shor — Parte 4

Computación Cuántica: Algorítmica y Software

Joaquín Keller

2026 UCV



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

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

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

$$k = \alpha r + \beta \qquad 0 \leq \beta < r$$

$$a^k = a^{\alpha r + \beta} = a^{r\alpha} a^\beta = 1^\alpha a^\beta = a^\beta$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{\alpha,\beta}^{0 \leq \alpha r + \beta < 2^n} |\alpha r + \beta\rangle |a^\beta\rangle$$

sea m_β el entero mas grande tal que $(m_\beta - 1)r + \beta < 2^n$

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

[de notar: $m_\beta = \frac{2^n}{r} + \epsilon \quad 0 \leq \epsilon < 1$]

La medición fija un $\beta_0 \quad b = \underline{a^{\beta_0}}$

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

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

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

$$\boxed{\sum_{k=0}^{N-1} z^k = \begin{cases} N & \text{si } z = 1 \\ \dfrac{1 - z^N}{1 - z} & \text{sino} \end{cases}} \qquad z = e^{-2i\pi \frac{r}{2^n} j} \qquad N = m_{\beta_0}$$

$$S_j = \sum_{\alpha=0}^{m_{\beta_0}-1} e^{-2i\pi \frac{\alpha r}{2^n} j} = \begin{cases} m_{\beta_0} & \text{si } \frac{rj}{2^n} \in \mathbb{Z} \qquad \text{[eso no pasa a menudo]} \\ \dfrac{1 - z^{m_{\beta_0}}}{1 - z} = \dfrac{1 - e^{-2i\pi \frac{rj}{2^n} m_{\beta_0}}}{1 - e^{-2i\pi \frac{rj}{2^n}}} & \text{sino} \end{cases}$$

$$|\psi_2'\rangle = \frac{1}{\sqrt{m2^n}} \sum_{j=0}^{2^n-1} e^{i\delta} S_j |j\rangle \qquad S_j = \sum_{\alpha=0}^{m-1} e^{-2i\pi\frac{\alpha r}{2^n}j} = \begin{cases} m & \textbf{si } \frac{rj}{2^n} \in \mathbb{Z} \\ \dfrac{1-e^{-2i\pi\frac{rj}{2^n}m}}{1-e^{-2i\pi\frac{rj}{2^n}}} & \textbf{sino} \end{cases}$$

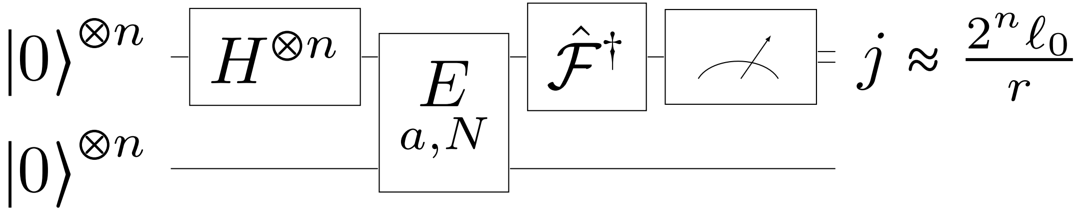
$$|S_j| = \frac{\left|1-e^{-2i\pi\frac{rj}{2^n}m}\right|}{\left|1-e^{-2i\pi\frac{rj}{2^n}}\right|} = \frac{|\sin(\pi rjm/2^n)|}{|\sin(\pi rj/2^n)|} \leq \frac{1}{|\sin(\pi rj/2^n)|}$$

S_j **tiene valores altos cuando** $\boxed{j \approx \frac{2^n \ell}{r}}$ $\qquad N^2 < 2^n$

Núcleo de Dirichlet: $\dfrac{\sin mx}{\sin x}$ $\qquad x = \pi rj/2^n$

Altura del pico: $S_j \approx m \approx \frac{2^n}{r}$ **Ancho:** $\Delta x \approx \frac{1}{m}$ $\qquad \Delta j \approx 1/\pi$

Circuito para el algoritmo de Shor



Fracciones continuas (1)

$$[a_0, a_1, a_2, \ldots, a_M] \equiv a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ldots + \frac{1}{a_M}}}} \qquad a_i \in \mathbb{N}^*$$

Ejemplo: $\frac{31}{13} = 2 + \frac{5}{13} = a_0 + \frac{1}{\frac{13}{5}}$ $\qquad \frac{13}{5} = 2 + \frac{3}{5} = a_1 + \frac{1}{\frac{5}{3}}$

$\frac{5}{3} = 1 + \frac{2}{3} = a_2 + \frac{1}{\frac{3}{2}}$ $\qquad \frac{3}{2} = 1 + \frac{1}{2} = a_3 + \frac{1}{a_4}$

$\mathcal{O}(n)$ etapas $\quad n$: número de dígitos

$$\frac{31}{13} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}$$

$$[a_0, a_1, a_2, a_3, a_4] = [2, 2, 1, 1, 2]$$

Fracciones continuas (python)

```
def cf(p: int, q: int):
    """ returns [a0,a1,...,am] of p/q """
    l = []
    while q:
        a = p // q
        l.append(a)
        p, q = q, p - a * q
    return l
```

Fracciones continuas (ejemplos)

$$\frac{355}{113} = 3 + \frac{1}{7+\frac{1}{16}}$$

$$\frac{415}{93} = 4 + \frac{1}{2+\frac{1}{6+\frac{1}{7}}}$$

$$\frac{213}{256} = \frac{213}{2^8} = \frac{1}{1+\frac{1}{4+\frac{1}{1+\frac{1}{20+\frac{1}{2}}}}}$$

Fracciones convergentes (1)

$$x = \frac{p}{q} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

$$x_0 = a_0 \qquad p_0/q_0$$

$$x_1 = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} \qquad p_1/q_1$$

$$x_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{\frac{a_1 a_2 + 1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_2 a_1 a_0 + a_2 + a_0}{a_2 a_1 + 1} \qquad p_2/q_2$$

$$p_{-2} = 0 \quad p_{-1} = 1 \qquad q_{-2} = 1 \quad q_{-1} = 0$$

$$p_k = a_k p_{k-1} + p_{k-2} \qquad q_k = a_k q_{k-1} + q_{k-2}$$

$$p_0 = a_0 \qquad q_0 = 1$$

$$p_1 = a_1 a_0 + 1 \qquad q_1 = a_1$$

$$p_2 = a_2(a_1 a_0 + 1) + a_0 = a_2 a_1 a_0 + a_2 + a_0 \qquad q_2 = a_2 a_1 + 1$$

Fracciones convergentes (python)

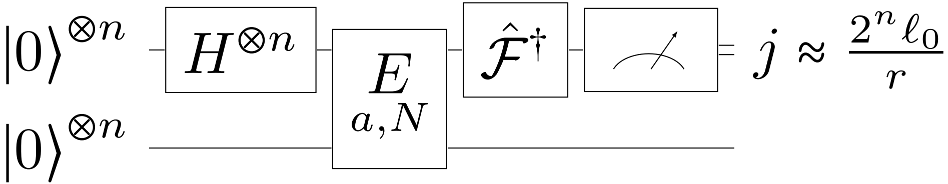
```python
def convergents_from_cf(cf):
    """ returns [(p0,q0),(p1,q1),...,(p,q)] """
    convergents = []
    p_2, p_1,  q_2, q_1 = 0, 1,  1, 0
    for a in cf:
        p = a * p_1 + p_2
        q = a * q_1 + q_2
        convergents.append((p, q))
        p_2, p_1 = p_1, p
        q_2, q_1 = q_1, q
    return convergents
```

Fracciones convergentes (ejemplos)

$$\frac{355}{113} = 3 + \frac{1}{7+\frac{1}{16}} \qquad 3 \qquad \frac{22}{7} \qquad \frac{355}{113}$$

$$\frac{415}{93} = 4 + \frac{1}{2+\frac{1}{6+\frac{1}{7}}} \qquad 4 \qquad \frac{9}{2} \qquad \frac{58}{13} \qquad \frac{415}{93}$$

$$\frac{213}{256} = \frac{213}{2^8} = \frac{1}{1+\frac{1}{4+\frac{1}{1+\frac{1}{20+\frac{1}{2}}}}} \qquad \frac{4}{5} \qquad \frac{5}{6} \qquad \frac{104}{125} \qquad \frac{213}{256}$$



1. Calcular las fracciones convergentes de $j/2^n$: $[\frac{p_0}{q_0}, \frac{p_1}{q_1}, ..., \frac{j}{2^n}]$

2. Los $q_i < N$ son candidatos para r

3. Si $\forall q_i \quad a^{q_i} \bmod N \neq 1$ correr el circuito de nuevo

El número de veces que hay que correr el circuito es polinomial en el número de dígitos