Algoritmo de Shor

- Feita a partir da redução do problema da fatoração para "busca em ordem" (pág 260/233).
- Dividido em dois passos básicos (Seção A4.3 do Apêndice 4 - Quantum Computation and Quantum Information).

    1. Mostrar que é possível computar um fator para N se encontrar uma solução $x \neq \pm 1 \pmod N$ para a equação $x^2 = 1 \pmod N$.
    2. Mostrar que um co-primo y escolhido aleatoriamente para N é muito provável ter uma ordem r par e que $y^{r/2} \neq \pm 1 \pmod N$, assim $x \equiv y^{r/2} \pmod N$ é uma solução não trivial para $x^2 = 1 \pmod N$.

Transformada de Fourier Quântica

Transformada em um base ortonormal

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

Exemplos

$$
\begin{aligned}
|0\rangle \to & \quad \frac{1}{\sqrt{2}}\left(e^{\pi i \cdot 0 \cdot 0}|0\rangle + e^{\pi i \cdot 0 \cdot 1}|1\rangle\right) \\
= & \quad \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\
|1\rangle \to & \quad \frac{1}{\sqrt{2}}\left(e^{\pi i \cdot 1 \cdot 0}|0\rangle + e^{\pi i \cdot 1 \cdot 1}|1\rangle\right) \\
= & \quad \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \\
|0 \ldots 0\rangle \to & \quad \frac{1}{\sqrt{N}}\left(|0 \ldots 0\rangle + |0 \ldots 1\rangle + \cdots + |1 \ldots 1\rangle\right) \\
= & \quad \frac{1}{\sqrt{N}}\left(|0 \ldots 0\rangle + |0 \ldots 1\rangle + \cdots + |1 \ldots 1\rangle\right) \\
|1 \ldots 1\rangle \to & \quad \frac{1}{\sqrt{N}}\left(|0 \ldots 0\rangle + e^{2\pi i (N-1)/N}|0 \ldots 1\rangle + \cdots + e^{2\pi i (N-1)(N-1)/N}|1 \ldots 1\rangle\right) \\
= & \quad \frac{1}{\sqrt{N}}\left(|0 \ldots 0\rangle + e^{2\pi i (N-1)/N}|0 \ldots 1\rangle + \cdots + e^{2\pi i (N^2-2N+1)/N}|1 \ldots 1\rangle\right)
\end{aligned}
$$

Conclusão

A transformada atribui mais "peso" quando k se aproxima de $N-1$.

Ação sobre estado arbitrário

$$\sum_{j=0}^{N-1} x_j |j\rangle \to \sum_{k=0}^{N-1} y_k |k\rangle$$

Representação de Produto

$$|j_1 \ldots j_n\rangle \to \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right) \ldots \left(|0\rangle + e^{2\pi i 0.j_1 \cdots j_n}|1\rangle\right)$$

Exemplos

$$
\begin{aligned}
|0\rangle \rightarrow & \quad \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.0_{\mathrm{bin}}}|1\rangle\right) \\
= & \quad \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \\
|1\rangle \rightarrow & \quad \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.1_{\mathrm{bin}}}|1\rangle\right) \\
|1\rangle \rightarrow & \quad \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i/2}|1\rangle\right) \\
= & \quad \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) \\
|00\rangle \rightarrow & \quad \frac{1}{\sqrt{4}}\left(|0\rangle + e^{2\pi i 0.0_{\mathrm{bin}}}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.00_{\mathrm{bin}}}|1\rangle\right) \\
= & \quad \frac{1}{\sqrt{4}}\left(|0\rangle + |1\rangle\right)\left(|0\rangle + |1\rangle\right) \\
= & \quad \frac{1}{\sqrt{4}}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right) \\
|11\rangle \rightarrow & \quad \frac{1}{\sqrt{4}}\left(|0\rangle + e^{2\pi i 0.1_{\mathrm{bin}}}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.11_{\mathrm{bin}}}|1\rangle\right) \\
= & \quad \frac{1}{\sqrt{4}}\left(|0\rangle + e^{2\pi i/2}|1\rangle\right)\left(|0\rangle + e^{2\pi i \cdot 0.75}|1\rangle\right) \\
= & \quad \frac{1}{\sqrt{4}}\left(|0\rangle - |1\rangle\right)\left(|0\rangle - i|1\rangle\right) \\
= & \quad \frac{1}{\sqrt{4}}\left(|00\rangle - i|01\rangle - |10\rangle + i|11\rangle\right)
\end{aligned}
$$

Equivalência

$$
\begin{aligned}
|j\rangle &\rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{2\pi ij\left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1 \dots k_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi ijk_l 2^{-l}} |k_l\rangle \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi ijk_l 2^{-l}} |k_l\rangle \right] \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi ij2^{-l}} |1\rangle \right] \\
&= \frac{\left(|0\rangle + e^{2\pi i0.j_n} |1\rangle\right)\left(|0\rangle + e^{2\pi i0.j_{n-1}j_n} |1\rangle\right) \dots \left(|0\rangle + e^{2\pi i0.j_1j_2\cdots j_n} |1\rangle\right)}{2^{n/2}}
\end{aligned}
$$

Provando notação

$$
\begin{aligned}
\frac{k}{2^n} &= \sum_{l=1}^{n} \frac{k_l}{2^l} \\
&= \frac{k_1}{2^1} + \frac{k_2}{2^2} + \cdots + \frac{k_n}{2^n} \\
&= \frac{k_1 \cdot 2^{n-1}}{2^n} + \frac{k_2 \cdot 2^{n-2}}{2^n} + \cdots + \frac{k_n}{2^n} \\
&= \frac{1}{2^n} \left(k_1 \cdot 2^{n-1} + k_2 \cdot 2^{n-2} + \cdots + k_n\right)
\end{aligned}
$$