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

Transformada de Fourier Quântica

Transformada em um base ortonormal

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

Exemplos

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

Conclusão

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

Ação sobre estado arbitrário

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

Representação de Produto

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

Exemplos

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

Dúvida

$$
\begin{aligned}
& e^{2\pi i \cdot 0.75} \\
e^{1.5\pi i} = & \quad \left(e^{2\pi i}\right)^{0.75} \\
\left(e^{\pi i}\right)^{3/2} = & \quad \left(e^{2\pi i}\right)^{3/4} \\
\sqrt{-1^3} = & \quad \sqrt[4]{1^3} \\
i \neq & \quad 1
\end{aligned}
$$