

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 $x \not\equiv \pm 1 \pmod{N}$ para a equação $x^2 \equiv 1 \pmod{N}$.
 2. Mostrar que um co-primo y escolhido aleatoriamente para N é muito provável ter uma ordem r par e que $y^{r/2} \not\equiv \pm 1 \pmod{N}$, assim $x \equiv y^{r/2} \pmod{N}$ é uma solução não trivial para $x^2 \equiv 1 \pmod{N}$.

Transformada de Fourier Quântica

Transformada em um base ortonormal

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

Exemplos

$$\begin{aligned}
|0\rangle &\rightarrow \frac{1}{\sqrt{2}} (e^{\pi i \cdot 0 \cdot 0} |0\rangle + e^{\pi i \cdot 0 \cdot 1} |1\rangle) \\
&= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \\
|1\rangle &\rightarrow \frac{1}{\sqrt{2}} (e^{\pi i \cdot 1 \cdot 0} |0\rangle + e^{\pi i \cdot 1 \cdot 1} |1\rangle) \\
&= \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
|0 \dots 0\rangle &\rightarrow \frac{1}{\sqrt{N}} (|0 \dots 0\rangle + |0 \dots 1\rangle + \dots + |1 \dots 1\rangle) \\
&= \frac{1}{\sqrt{N}} (|0 \dots 0\rangle + |0 \dots 1\rangle + \dots + |1 \dots 1\rangle) \\
|1 \dots 1\rangle &\rightarrow \frac{1}{\sqrt{N}} (|0 \dots 0\rangle + e^{2\pi i(N-1)/N} |0 \dots 1\rangle + \dots + e^{2\pi i(N-1)(N-1)/N} |1 \dots 1\rangle) \\
&= \frac{1}{\sqrt{N}} (|0 \dots 0\rangle + e^{2\pi i(N-1)/N} |0 \dots 1\rangle + \dots + e^{2\pi i(N^2-2N+1)/N} |1 \dots 1\rangle)
\end{aligned}$$

Conclusão

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

Ação sobre estado arbitrário

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

Representação de Produto

$$|j_1 \dots j_n\rangle \rightarrow \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i 0 \cdot j_n} |1\rangle) (|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0 \cdot j_1 \dots j_n} |1\rangle)$$

Exemplos

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

Dúvida

$$e^{\pi i} = -1$$

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

$$\begin{aligned}
e^{\pi i 3/2} &= (e^{\pi i})^{3/2} \\
&= (-1)^{3/2} \\
&= \sqrt{(-1)^3} \\
&= \sqrt{(-1)^2 \cdot (-1)} \\
&= -\sqrt{-1} \\
&= -i
\end{aligned}$$