Eficiencia Cuántica del Algoritmo de Shor

Descripción del Problema:

- Factorizar un número N en sus factores primos.

Complejidad Clásica:

- Algoritmo más eficiente: GNFS
- Complejidad: $O(\exp((\log N)^{1/3}(\log\log N)^{2/3}))$

Principios Cuánticos Utilizados:

- **Superposición:** Representa múltiples estados simultáneamente.
- **Entrelazamiento:** Correla qubits para operaciones paralelas.
- **Interferencia Cuántica:** Amplifica soluciones correctas.

Algoritmo de Shor:

1. **Reducción Clásica a Problema de Período:**
   - Elige a tal que $1 < a < N$.
   - Encuentra el período r de $a^x \mod N$.
   - Si r es par y $a^{r/2} \not\equiv -1 \mod N$, entonces $\gcd(a^{r/2} \pm 1, N)$ da factores de N.
2. **Búsqueda Cuántica del Período:**
   - Usa la Transformada de Fourier Cuántica (QFT) para encontrar r en tiempo polinomial.

Complejidad Cuántica:

- **QFT:** Complejidad $O((\log N)^2)$.
- **Total:** $O((\log N)^2(\log\log N)(\log\log\log N))$.

Demostración de Complejidad:

- Operador unitario U (multiplicación modular) en tiempo polinomial.
- QFT sobre n qubits ($n = \log N$) en $O(n^2)$.
- Algoritmo de Shor en $O((\log N)^2(\log\log N)(\log\log\log N))$.

Conclusión:

- El algoritmo de Shor resuelve la factorización en tiempo polinomial usando cómputo cuántico, mostrando una ventaja significativa sobre los algoritmos clásicos.