Quantum Algorithm: Grover's Search Algorithm

Category: Search and Optimization | **Speedup:** Grover's algorithm provides a quadratic speedup over classical algorithms for unstructured search problems. It can find a unique target item in an unsorted database of N items in O(sqrt(N)) queries, compared to O(N) queries for classical brute-force search.

Key Concepts

- Quantum Superposition
- Quantum Entanglement
- Quantum Oracle
- Amplitude Amplification
- Diffusion Operator (Grover Operator)
- Inversion about the Average

Quantum Gates

Gate	Qubits	Purpose
Hadamard	[0, 1, 2]	To create an equal superposition of all possible states, initializing the search space.
Oracle (U_f)	[0, 1, 2, 3]	To mark the target state(s) by applying a phase shift (e.g., -1) to their amplitude. The specific implementation depends on the problem.
Controlled-Z (or similar multi-controlled gate)	[0, 1, 2, 3]	Part of the diffusion operator, specifically the phase inversion for the |0...0> state, often constructed with X gates and a multi-controlled-Z or Toffoli variant.

X (NOT)	[0, 1, 2]	Used in conjunction with the multi-controlled phase gate within the diffusion operator to implement inversion about the average.

Applications

- Unstructured database search
- Solving NP-complete problems (by transforming them into search problems)
- Optimization problems (finding optimal solutions in a search space)
- Cryptanalysis (e.g., breaking symmetric key cryptography, though less impactful than Shor's for asymmetric)
- Satisfiability problems (SAT)

NISQ: 4/10