Assignment 4

Quantumania

July 2024

This week you will be implementing some real stuff that is known as the power of quantum computation!

1 Questions

1. Write an implementation of Shor's Algorithm and factorise $15 = 5 \times 3$ using it. Implementing the unitary taking $|y\rangle$ to $|xy \pmod{15}\rangle$ is the non-trivial part.

2. Implement a SAT solver using Grover's Search as a subroutine to bring the search time down to $\mathcal{O}(\sqrt{2^n})$. Here are the steps to achieve this:

   - You are given a function $f : \{0,1\}^n \to \{0,1\}$ on n boolean variables $x_1, \ldots, x_n$ in CNF form as a string. For example, $f = (x_1 \vee \neg x_2) \wedge (x_3)$. You can assume any reasonable bracketing for parsing.
   - A solution to f is a boolean vector $\mathbf{x}$ that satisfies $f(\mathbf{x}) = 1$. We need to find such a solution $\mathbf{x}$ using Grover's search.
   - Construct a function called OR that takes a QuantumCircuit object, a list of qubit indices whose states (either $|0\rangle$ or $|1\rangle$) are to be logically ORed, and a qubit index to store the result. Similarly, construct a function called AND.
   - Using the functions defined above and a parsed version of f, construct the oracle for Grover's algorithm. You can use len(f) (the number of clauses in f) ancilla qubits to store the truth values of each clause, and make sure to reset them to the $|0\rangle$ state after the oracle application for correctness.
   - Precompute the number of solutions M to f using classical methods and hardcode this value in your code for each example tested. Note that this limitation can be overcome using Quantum Counting.
   - Implement the standard Grover search algorithm to solve the SAT problem efficiently.