Assignment 3 - SoC

To the Quantum Future

July 29, 2023

Here is the assignment for the fourth section of this SoC; as always, you are expected to submit your solutions on your forked/personal git repo.

Some real stuff this week - unleashing some of the power of quantum computation. This may take some time, so please start early!

1. Factorize $15 = 3 \times 5$ on a quantum computer using Shor's algorithm. Computing the unitary taking $|y\rangle$ to $|xy \pmod{15}\rangle$ is the nontrivial part. Can you implement it using swap and X gates?

2. Implement a SAT (you may assume 3-SAT, if you wish) solver running in time $\mathcal{O}(\sqrt{2^n})$ using Grover Search. In particular, here are the rules:

   - You are given a function $f : \{0,1\}^n \to \{0,1\}$ on n boolean variables $x_1, ..., x_n$ in CNF as a string. For example, $f = (x_1 \vee \neg x_2) \wedge (x_3)$. You may make any suitable assumption on bracketing etc for parsing. A solution to f is a boolean vector $\mathbf{x}$ satisfying $f(\mathbf{x}) = 1$. We wish to find such a solution $\mathbf{x}$ using Grover Search.
   - Construct a function called `OR` taking as argument a `QuantumCircuit` ckt, list of qubit indices whose states (either $|0\rangle$ or $|1\rangle$ are the ones to take the logical OR of and a qubit index denoting the qubit to store the result in. Similarly, construct a function `AND`.
   - Now we construct the oracle used in the algorithm using the functions defined in the previous step and a parsed version (as convenient) of f. You may use len(f) (the number of clauses in f is len(f)) ancilla qubits to store the truth values of each clause - just make sure to uncompute them back to the all $|0\rangle$ state after an application of the oracle for correctness.
   - All done? Not quite. When running it, you need to pre-compute the number of solutions M to f to apply the standard Grover Search. You may do that by hand or a classical program, and simply hardcode the value found in your code for each example you test. Note that this limitation to Grover's algorithm can be overcome using Quantum Counting.
   - Well, now you're done. Standard Grover Search to solve this useful problem faster!

3. (Optional) Read a fun paper of your choice on a Quantum Algorithm, say one of for the Shor Fans or for the Grover Guys. Your task is to study the paper and submit a high-level summary of the same.