Quantum Algorithms: An Overview

Introduction

- Even though large-scale quantum computing doesn't yet exist, quantum algorithms still exist (realized through superconductors and trapped ions, etc…)
    - Iris: it would be nice to be able to map technologies to the implementations
- Quantum speedup measured through asymptotic analysis on algorithms (i.e. Big-O notation)
- Quantum mechanics are highly related to linear algebraic concepts; as a result, matrices and vectors can be used to represent qubits and quantum gates

Hidden Subgroup Problem and Cryptography

- Motivated by the fact that RSA cryptosystems depend on unsolvable problems (from a time perspective with very large numbers)
    - Iris: Are qubits one-to-one in mapping integers of say, 64-classical bits?
    - Qishen: Yes, the prior paper seems to suggest this notion if you want to recycle qubits - otherwise you would only need a very limited number of qubits
    - Karpur: Qubits don't store more information than classical bits, and the communication rate is not necessarily higher (as it relates to teleportation)... the problems in the paper are simple expressions in terms of qubits and then the fact that it is implemented in qubits gives more powerful and capable computation
- HSP: factoring, discrete, logarithm, isomorphism, and shortest vector problem

Search and Optimization

- Unstructured search is an NP-class problem (O(2^n) in classical computing)
- Grover's algorithm solves unstructured search in O(n^{½}) time using *amplitude amplification* technique for quantum speedup over classical algorithms (which can be applied to solving linear equations)
    - When performing a computation, a probability is output
    - Certain bases need to be added to ensure reversibility
    - Hadamard Gate: used to put qubits into superposition
        - Iris: does it make sense to combine a Hadamard gate with another gate and how would it be useful?
        - Mark: this will be demonstrated with the full circuit of Grover's algorithm
        - Qishen: There is a control bit that is simultaneously zero or one and applying a not gate simultaneously produces outputs for both potential situations (of the bit being zero or one)
        - Karpur: One particular application would be back tracing through a series of computations which could be used with a combination of control bits and Hadamard gates
        - Mark: in every step, the Hadamard gate is used to construct the control bit so as to ensure that the quantum state can be transformed in all states
- Can be applied to graph connectivity to solve faster than classical computing as well
- Main Idea: Quantum computer is better because certain operations that will take multiple steps in a classical computer can be done simultaneously with a quantum computer

        - Apply a Hadamard gate to the input, then apply the oracle to the result, afterwards not all possibilities will be equally likely
        - Iris: how do you detect that a probability is more likely if you cannot measure a qubit without collapsing it?
        - Mark: It has to do with the amplitude of the qubit, which will be large enough after a constant number of computations that we can make a reasonable assessment
        - Sam: Do certain problems lend themselves to few executions and is there a way to know in advance?
        - Mark: It is particular to the problem itself, there is a mathematical computation that can be done - there is a range, but an upper bound
    - Sam: How likely is it that the development of quantum algorithms will extend to a point where quantum computing is generally applicable?
    - Iris: Problems that are inherently quantum in nature are better suited for quantum computing

Quantum Walks and Simulations

- Given a Hamiltonian system and an initial state, we can perform quantum simulations for which no efficient classical algorithm is known
- Quantum walks can also be applied to Markov Chains
- Iris: WIll problems present themselves in a quantum way?
- Karpur: It would require training a bunch of quantum physicists how to develop algorithms or a bunch of computer scientists to think outside of a classical lens

Outlook

- There are limitations of quantum algorithms