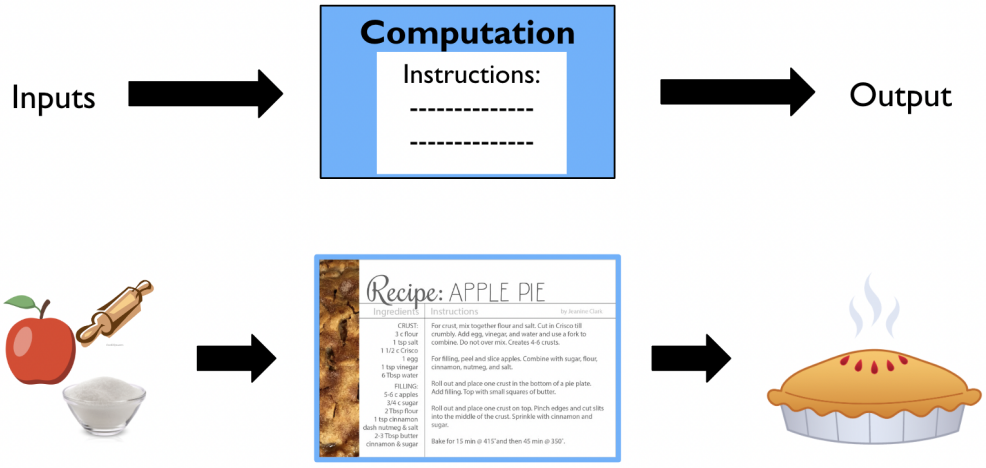
Week 7 Summary of Key Concepts

Lecture

In lecture this week, we took a step back to review the parts of the stack we have seen so far and survey the landscape of the next level: Quantum Algorithms and Protocols. We will be exploring many of these algorithms and protocols throughout the rest of the year now that we have developed many of the skills necessary to do so.

1. **Quantum algorithms** are a specific procedure for solving a computational problem using quantum physics. They are like recipes for the computer to make/do something for us.



2. **Quantum protocols** are a set of standard rules that allow electronic devices to communicate with each other using quantum physics. They are like contracts between multiple devices that help them understand how to work together.

3. We are currently in the era of **NISQ** (**Noisy Intermediate Scale Quantum**) devices, where we are starting to see real quantum computers come into existence. However, they are smaller and noisier (more prone to errors) than the ideal quantum computers we are striving towards. A big question in QISE today is what the best applications of these devices are.

4. We surveyed four quantum algorithms:

a. **The Deutsch-Jozsa Algorithm**
    i. Discovered in 1992 by David Deutsch and Richard Jozsa, this quantum algorithm was the first to show significant theoretical improvements over classical algorithms.
    ii. It does not solve/do anything of interest as far as we know.
    iii. A core technique of this algorithm is **phase kickback** where a CX gate provided with two different superpositions will allow the control qubit to sneak away with information about both states.
b. **Shor's Algorithm**
    i. Discovered in 1996 by Peter Shor, this quantum algorithm was one of the first algorithms to be significantly better than classical algorithms and be useful.
    ii. It can prime factorize arbitrarily large numbers, which is a core part of many cybersecurity (encryption) schemes today–namely RSA.
    iii. A core technique of this algorithm is **quantum fourier transform (QFT)** where superpositions with very special properties are created that can represent periodic/recurring patterns well.
c. **Grover's Algorithm**
    i. Discovered in 1996 by Lov Grover, this quantum algorithm is yet another improvement over classical algorithms (though the improvement is less than with Shor's algorithm) that is useful.
    ii. It can search over an unorganized database or list and find what you're looking for more efficiently than any classical algorithm could.
    iii. A core technique of this algorithm is **amplitude amplification** where a special circuit can "amplify" (increase) the probability of measuring a particular state or set of states.
d. **Near-term Algorithms**
    i. This is the name for the family of algorithms that are particularly relevant in the NISQ era. They are usually **hybrid** algorithms where they use both classical and quantum computation to do something that neither could do alone.
    ii. They have tended to come in a few different forms:
        - Variational: going back and forth between quantum and classical computers

- Simulation: using quantum systems (quantum computers) to simulate other quantum systems (ex: molecules for creating medicine)
- Machine learning: attempting to merge two of the most cutting edge fields in computer science

5. We surveyed three quantum protocols:
    a. **Quantum Teleportation**
        i. Discovered in 1993 by a large team of scientists, this protocol allows us to send a quantum state to someone far away using entangled qubits and classical bits.
        ii. This is considered a fundamental piece of creating a **quantum internet**, which is actively being developed in several places around the world.
    b. **Quantum Key Distribution**
        i. This protocol allows two people to communicate perfectly securely. Even if someone else is looking at the information they're sending, their presence will be detectable and they won't be able to learn anything about the original communication.
        ii. We will see this next week!
    c. **Superdense Coding**
        i. Discovered in 1970 by Charles H. Bennett and Stephen Wiesner is a protocol where we can send the equivalent of multiple classical bits with just one quantum bit.

Lab

In lab this week, we learned about loops and conditionals in general and with Qiskit. These are vital tools for making more advanced circuits that we will see in action next week! The cheat sheets below summarize the key syntax that we have seen:

Qiskit Cheat Sheet
Loops and Conditionals Cheat Sheet