Yingtai Feng
CSC 405

Quantum Computing

This Wednesday, Dr. Rafael Nepomechie gave an introduction to quantum computing, including what is it, its importance, and a glance into its future.

To start off, Dr. Nepomechie gave a distinction between classical and quantum mechanics. Quantum mechanics started in early 1900’s, and it describes phenomena on atomic scale, while classical mechanics which started much earlier in late 1600’s describes everything else, including conventional computers. This difference can be observed in the difference between classical bits (Cbit) and quantum bit (qubit). In classical mechanics, data is encoded into bits, each of which is always in one of the two states, 0 or 1. However, in quantum mechanics, data is encoded with complex numbers in addition to the two states. The complex numbers allow data to be in superpositions of states. This superposition brings in uncertainty which means quantum algorithms are usually probabilistic, and it allows for trying out different paths in a calculation, reducing the number of steps needed for traditionally time-consuming problems. In this quantum computation process, we start with qubits in known initial state, which is 0. Then we perform unitary transformations that are by nature reversible. After a sequence of these transformations we perform measurements. Quantum computation consists of these three stages, and it differs from classical computing in storing information as qubits and the unitary transformations it performs.

Dr. Nepomechie then talked about quantum computers today. Since we are still in primitive stage of development in quantum computing, we have primitive quantum computers developed by IBM that are available. He demonstrated that we can use the 5-qubit and 16-qubit devices freely on IBM’s website. 20-qubit and 50-qubit devices also exist, and they may be available for a fee. The quantum computers we have today mark a significant progress in this field. Although they may still be primitive compared to the work still need to be done in this field, quantum computers today can already solve some complex problems that could not be solved previously.

Dr. Nepomechie then talked about the future of quantum computing and some applications of it. With advanced quantum computers, Nepomechie mentioned that we can accomplish two major tasks. The first one is to break RSA encryption, which is a modern encryption method that is based on the fact that large integers (~400 digit) cannot, in practice, be factored. Quantum computers could break through this limitation of integer factorization using Shor’s algorithm. In fact, a quantum computer with 10^3 qubits could factor such numbers. This application shows that there is still significant amount of work to do in quantum computing, and we are still far from building advanced quantum computers with 10^3 qubits. The other application is in search. Typically, searching for one integer in a list of N integers require about N operations. However, using Grover’s algorithm, a quantum computer would only require about square root of N operations, which is a drastic reduction in the number of operations. From these two applications, we can see the potential of quantum computing and its revolutionary ability to solve traditionally unsolvable problems.

Although we still have much more work to do in quantum computing, significant progress has already been achieved. Quantum computing may have revolutionary applications, and we have yet to see those progress come to fruition.