Quantum Complexity Theory

- Complexity & algorithms are closely related
- It's easier to classify complexity problems if we restrict ourselves to Decision problems
- Classes include P, BPP, BQP

- Other classes:
  - NP: if answer is yes, can be verified in polynomial time (P)
  - NP-complete: within NP, the hardest problems.
  - QMA: Quantum Merlin-Arthur. Includes NP.
  - Quantum equivalent of NP-solutions can be verified in BQP
  - co-NP: NP but when the answer is no instead of yes.

  and NP ≠ BQP

- Physicists assume P ≠ NP, and use it to prove results.
- P = BPP is probably true.
- P ≠ BQP is true if factoring is not in P

- Some problems are in BQP AND NP.
- Others are in one but not the other, going both ways.
- Strongly believed that NP-complete and BQP are mutually exclusive.
- These imply that BQP ≠ QMA
- Factoring is in BQP, NP, and co-NP. This is true for many BQP problems.
- NP-complete is NOT in co-NP.
- There are other classes as well, including "statistical zero-knowledge."
Quantum Speedups

- When should we expect speedups, and how much should we expect them to speed up by?

Query Complexity

- Instead of measuring complexity in runtime, measure it in number of queries.
- It's hard to correlate query complexity results with standard complexity results, but they are useful results.
- Still restricted to decision problems.
- Most problems can be converted to decision problems.
  - Example: Grover's search can be converted by asking whether $x$ exists s.t. $f(x) = 1$.

If an algorithm restricts the allowed inputs, it is likely to result in a speedup of a higher order.

In general:
- Quantum speedups are at most polynomial if they allow any function $f$.
- If flipping input bits is allowed, classical algorithm will be at most $O(T^2)$ when quantum is $O(T)$.
- 2020 research proved that if all inputs are allowed, speedup will never be more than $T^{3/4}$.
- Restrictions don't necessarily cause speedups, but all exponential speedups occur when restrictions are present.
- A FIt is often involved.