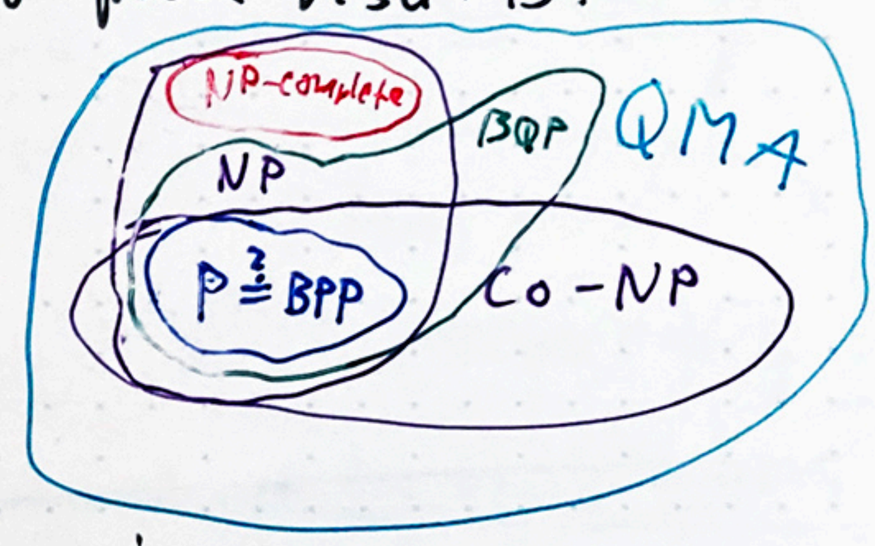
Quantum Complexity Theory

- 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 $\not\subseteq$ BQP

- Physicists assume $P \neq NP$, and use it to prove results.
- $P = BPP$ is probably true.
- $P \neq BQP$ is true if factoring 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 $\neq$ 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 Speed ups

- 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, speedups will never be more than $T^{\sqrt{4}}$

- Restrictions don't necessarily cause speedups, but all exponential speedups occur when restrictions are present.
- QFT is often involved.