

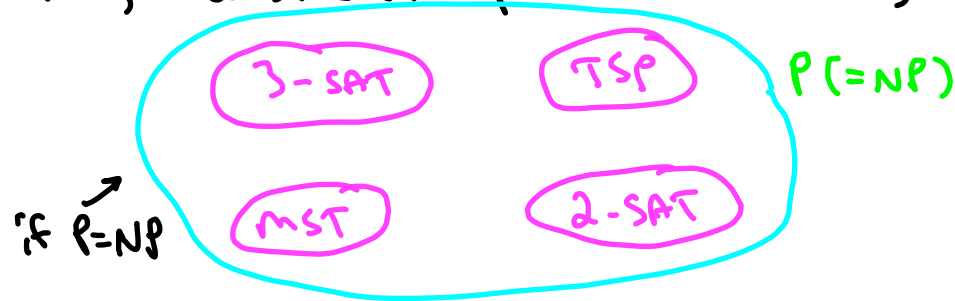
Section 23.4:

The $P \neq NP$ Conjecture

Formal Definition of the $P \neq NP$ Conjecture

Definition: Complexity class P = problems of NP that are polynomial-time solvable. (ex: 2-SAT, search version of MST)

$P \neq NP$ Conjecture: $P \subsetneq NP$. (i.e., at least one NP problem not in P)



Note: a polynomial-time algorithm for an NP-hard problem would refute the $P \neq NP$ Conjecture.

Status of the $P \neq NP$ Conjecture

- one of seven "Millennium Problems" (\$1 million prize)
- majority belief: $P \neq NP$. (dissenter: Kurt Gödel)
- reasoning: humans good at algorithms, bad at impossibility proofs
- also, $P=NP$ would seem to contradict our real-world experience
- a resolution seems far, far away (decades)

Next: ETH and SETH.