P and NP

So far ...

Polynomial multiplication $O(n \log n)$

Minimum Spanning Trees $O((n+m)\log(n))$

All pairs shortest paths $O(n^3)$

...

Def: A problem is efficiently solvable if it can be solved in polynomial time $= O(n^k)$

(in theory; in practice, efficient can even mean $O(n)$ only)

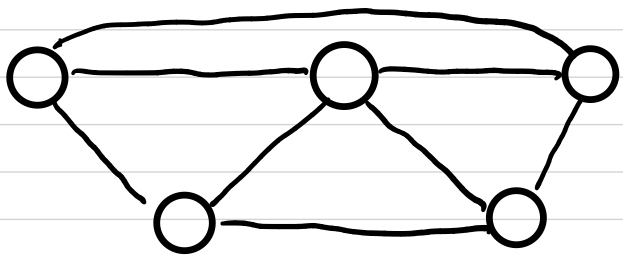
Def: P = "complexity class" of all problems which are efficiently solvable

Def: NP = class of problems whose solutions can be verified efficiently

3-coloring

Input: Graph $G=(V,E)$

Solution: A coloring $c: V \to \{Red, Green, Blue\}$ s.t. each edge receives 2 different colors



Trivial alg: Try all colorings. 3^n total colorings.

Best alg: 1.3289^n time

3-coloring $\in$ NP: Verify(Input $G=(V,E)$, Solution $c: V \to \{R,G,B\}$)

$\forall$ edges $(u,v) \in E$, check $c(u) \neq c(v)$.

Factorization

Input: n-bit number N

Solution: two numbers $p, q > 1$ s.t. $p \cdot q = N$

Trivial alg: try dividing N by every $1 < p \leq \sqrt{N}$. Time $\sqrt{N} = \sqrt{2^n} = 2^{n/2}$.

Best known alg: General number field sieve. Time $\underline{C^{n^{1/3} \log(n)^{2/3}}}$.

Not known to be in P!

Claim: Factorization $\in NP$

Pf: Verify(Input N, Solution p and q)

1.) Check $p, q > 1$.

2.) Check $p \cdot q = N$. $\leftarrow$ $O(n^2)$ time (or less)

Rudrata Cycle aka Hamiltonian Cycle

Input: Graph $G=(V,E)$

Solution: tour = cycle visiting every node exactly once

Trivial alg: Try all $n!$ ways of ordering vertices

Best known alg: Time $O(1.657^n)$

Not known to be in P!

Fact: Hamiltonian Cycle $\in NP$.

Eulerian cycle: find cycle visiting each edge exactly once

in P!

Traveling Salesperson Problem (TSP)

Input: Graph $G=(V,E)$ w/ edge weights
Solution: tour w/ low total weight

Optimization version: Min-TSP
Find the tour w/ min total weight.

Best known alg: time $O(n^2 2^n)$

Min-TSP $\in$ NP??? $\longleftarrow$ Probably not!

Search version: Search-TSP
Find a tour w/ total weight $\leq B$ $\longleftarrow$ "Budget" (part of input)

Fact: Search TSP $\in$ NP

Decision version: Decision-TSP
Does there exist a tour w/ weight $\leq B$? (Yes/No answer)

Fact: Dec-TSP $\in$ NP

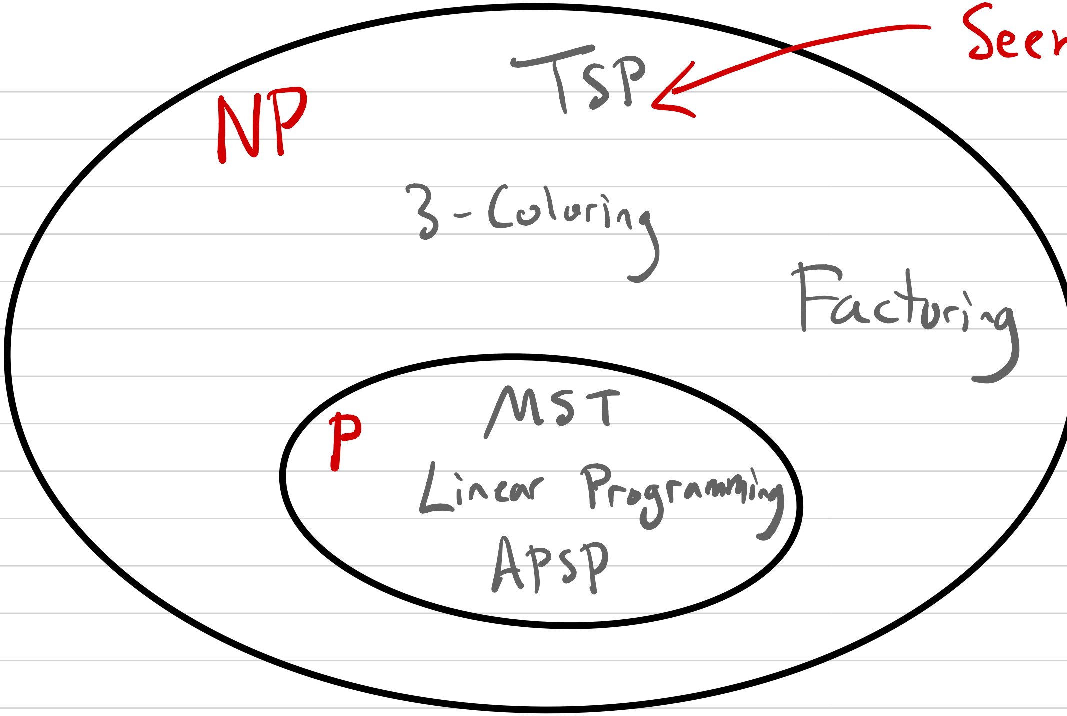
Things not in NP: 1. Optimization versions of problems
believed to be
2. Counting versions of problems
"How many 3-colorings of G are there?"
3. Really, really hard problems (Halting)

Super, duper formally: • NP typically defined for decision problems
(in complexity theory course, CS 172)
• we'll allow for search problems too

Thm: $P \subseteq NP$

E.g. Minimum Spanning tree (in P)
Input: $G=(V,E)$ w/ edge weights
Output: Minimum spanning Tree T

Claim: $MST \in NP$
Pf:
$\text{Verify}\left(\begin{matrix}\text{Input} & \text{Solution} \\ G, & T\end{matrix}\right)$:
1. Run Kruskal(G). Let $T^* =$ its output.
2. Check $\text{cost}(T) = \text{cost}(T^*)$.



Seemingly really hard!

(in theory... can be easy in practice!)

Biggest open problem in TCS: Is $P = NP$?