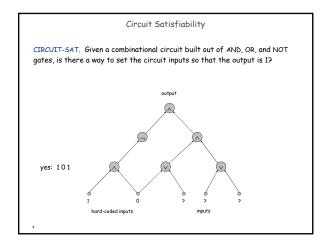
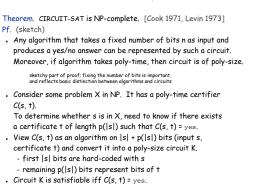
CS 580: Algorithm Design and Analysis

Jeremiah Blocki Purdue University Spring 2018

Homework 5 due on March 29th at 11:59 PM (on Blackboard)



Recap Polynomial Time Reductions $(X \le_p Y)$.P .Decision problems which have a polynomial time algorithm. .NP . Decision problems which have a polynomial time proof certification algorithm. .NP . Decision problems which have a polynomial time proof certification algorithm. . All YES instances have a short proof .NP-Hard . For all X ENP we have a reduction $X \le_p Y$. A decision problem YENP that is at least as hard any other problem $X \in NP$.NP-Complete . A decision problem YENP that is also NP-Hard. .We know that $P \subset NP$ and $NP \subset EXP$, but not if P = NP



The "First" NP-Complete Problem

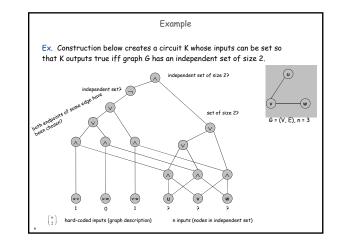
NP-Complete

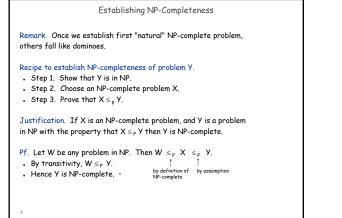
NP-complete. A problem Y in NP with the property that for every problem X in NP, $X \le p Y$.

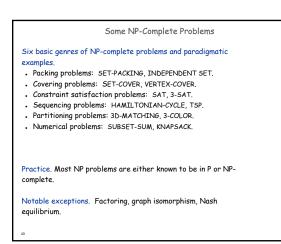
Theorem. Suppose \underline{Y} is an NP-complete problem. Then \underline{Y} is solvable in poly-time iff P = NP.

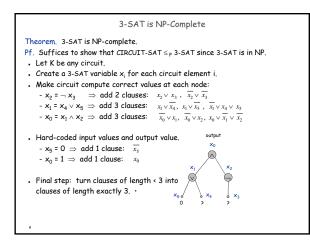
- Pf. \leftarrow If $\underline{P} = \underline{NP}$ then \underline{Y} can be solved in poly-time since \underline{Y} is in \underline{NP} .
- $Pf. \Rightarrow$ Suppose Y can be solved in poly-time.
- Let <u>X be</u> any problem in NP. Since $X \leq_p Y$, we can solve <u>X</u> in poly-time. This implies NP \subseteq P.
- We already know $P \subseteq \overline{NP. Thus P} = NP.$

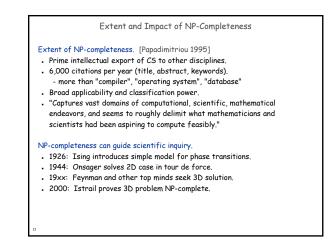
Fundamental question. Do there exist "natural" $\ensuremath{\mathsf{NP}}\xspace$ complete problems?

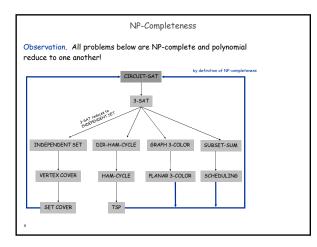


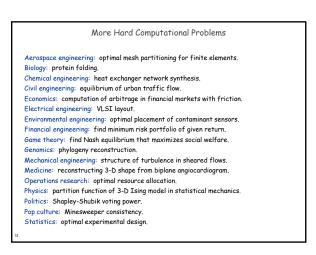












8.9 co-NP and the Asymmetry of NP

Fundamental question. Does NP = co-NP?

NP = co - NP?

. Do $_{\rm Yes}$ instances have succinct certificates iff $_{\rm no}$ instances do?

· Consensus opinion: no

Theorem. If NP \neq co-NP, then P \neq NP.

- Pf idea
- P is closed under complementation.
- If P = NP, then NP is closed under complementation. . In other words, NP = co-NP.
- . This is the contrapositive of the theorem.

Asymmetry of NP

Asymmetry of NP. We only need to have short proofs of $_{\ensuremath{\texttt{yes}}}$ instances.

Ex 1. SAT vs. TAUTOLOGY.

- . Can prove a CNF formula is satisfiable by giving such an assignment.
- . How could we prove that a formula is not satisfiable?

Ex 2. HAM-CYCLE vs. NO-HAM-CYCLE.

- . Can prove a graph is Hamiltonian by giving such a Hamiltonian cycle.
- . How could we prove that a graph is not Hamiltonian?

Remark. SAT is NP-complete and SAT $\equiv P$ TAUTOLOGY, but how do we classify TAUTOLOGY?

not even known to be in NP

Good Characterizations

Good characterization. [Edmonds 1965] NP \cap co-NP.

- . If problem X is in both NP and co-NP, then:
- for yes instance, there is a succinct certificate
- for no instance, there is a succinct disqualifier
- · Provides conceptual leverage for reasoning about a problem.
- Ex. Given a bipartite graph, is there a perfect matching. . If yes, can exhibit a perfect matching.
- If no, can exhibit a set of nodes S such that |N(S)| < |S|.

NP and co-NP

 $\ensuremath{\mathsf{NP}}$. Decision problems for which there is a poly-time certifier. Ex. SAT, HAM-CYCLE, COMPOSITES.

Def. Given a decision problem X, its complement \overline{X} is the same problem with the yes and no answers reverse

Ex. X = { 0, 1, 4, 6, 8, 9, 10, 12, 14, 15, ... } X = { 2, 3, 5, 7, 11, 13, 17, 23, 29, ... }

co-NP. Complements of decision problems in NP. Ex. TAUTOLOGY, NO-HAM-CYCLE, PRIMES.

Good Characterizations

Observation. P \subseteq NP \cap co-NP.

- . Proof of max-flow min-cut theorem led to stronger result that max-flow and min-cut are in P.
- . Sometimes finding a good characterization seems easier than finding an efficient algorithm.

Fundamental open question. Does $P = NP \cap co-NP$?

- . Mixed opinions.
- Many examples where problem found to have a non-trivial good characterization, but only years later discovered to be in P.
- linear programming [Khachiyan, 1979]
- primality testing [Agrawal-Kayal-Saxena, 2002]

Fact. Factoring is in NP \cap co-NP, but not known to be in P.

if poly-time algorithm for factoring, can break RSA cryptosystem

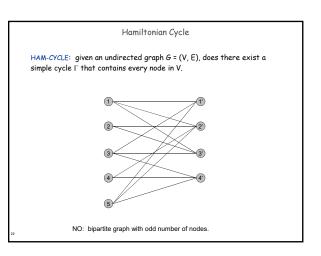


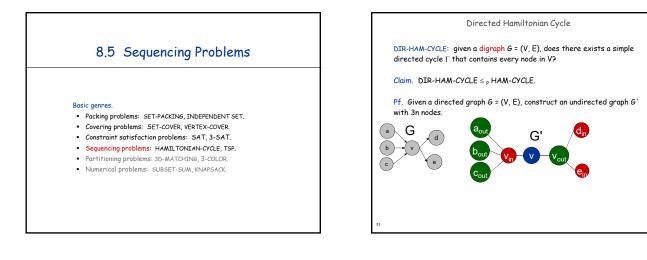
FACTORIZE. Given an integer x, find its prime factorization. FACTOR. Given two integers x and y, does x have a nontrivial factor less than y?

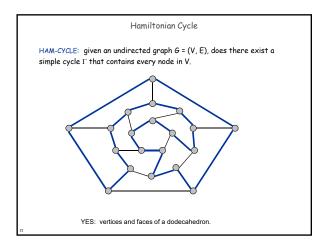
Theorem. FACTOR = $_{P}$ FACTORIZE.

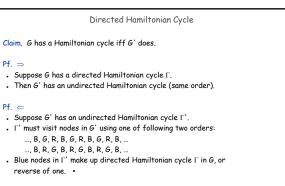
Theorem. FACTOR is in NP \cap co-NP.

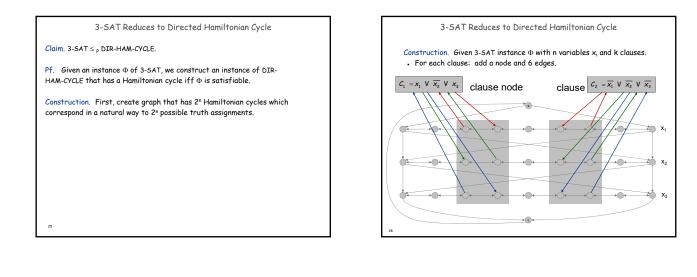
- Pf.Certificate: a factor p of x that is less than y.
- Disqualifier: the prime factorization of x (where each prime factor is less than y), along with a certificate that each factor is prime.

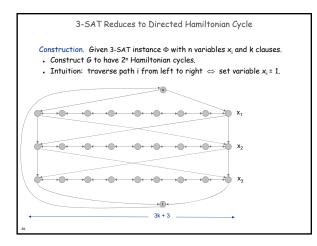


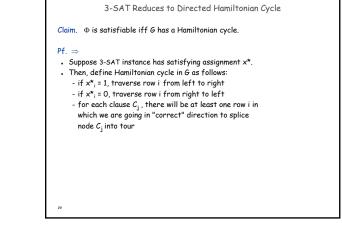


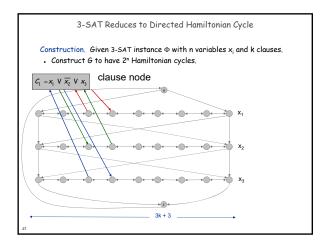


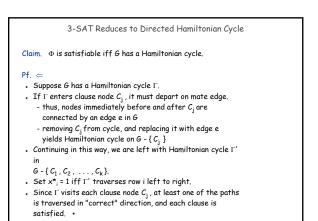


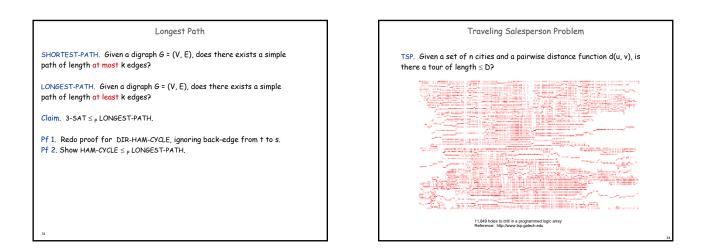


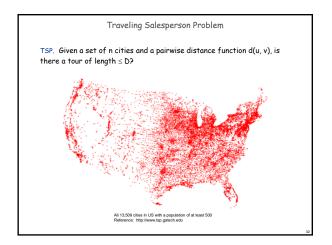


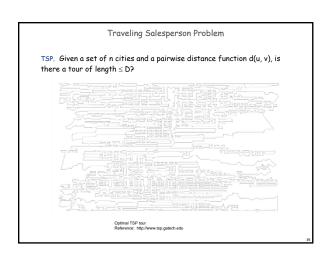


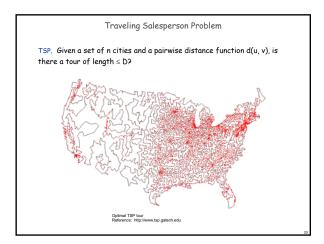


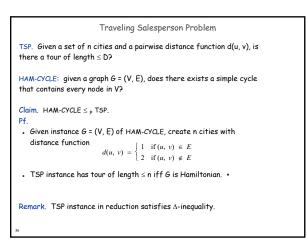


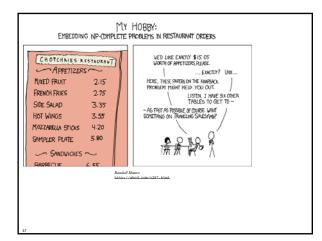


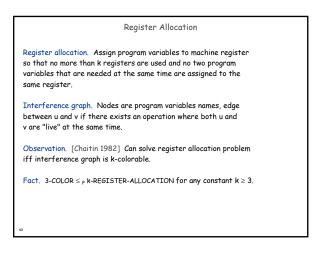


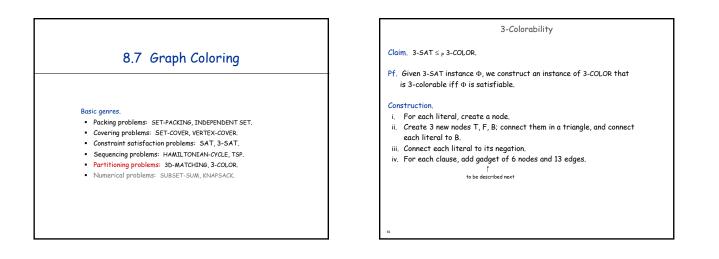


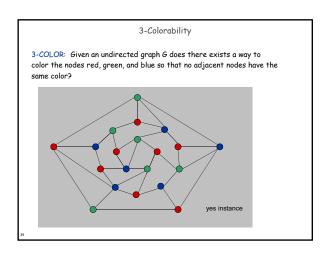


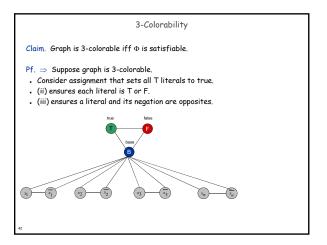


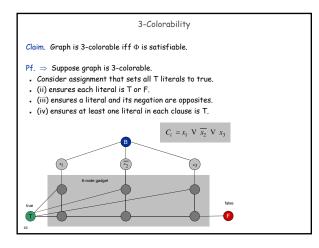


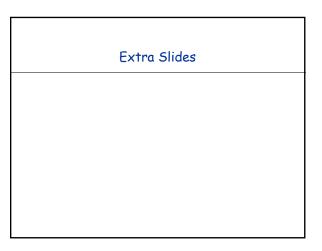


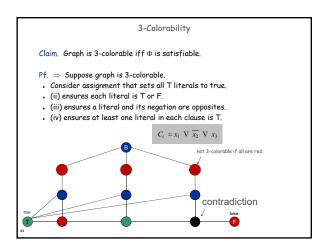


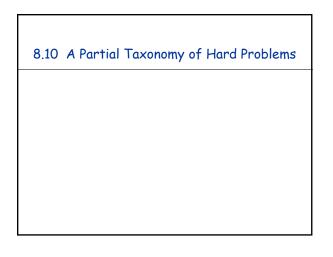


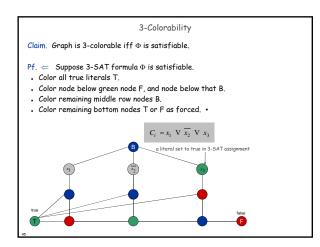


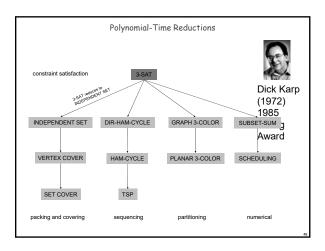


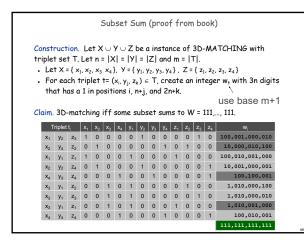


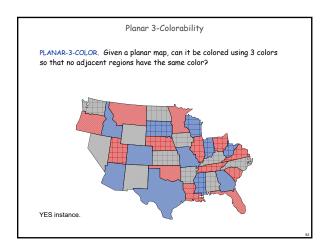


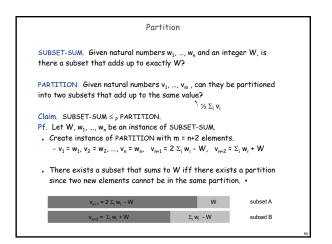


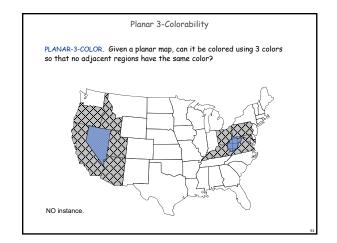


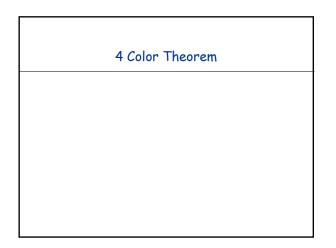


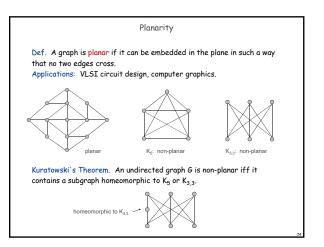


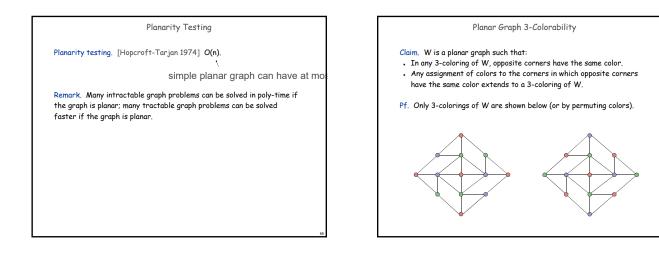


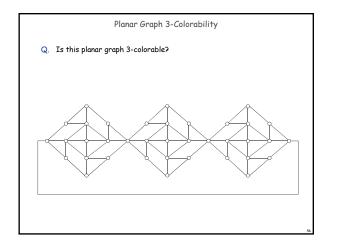


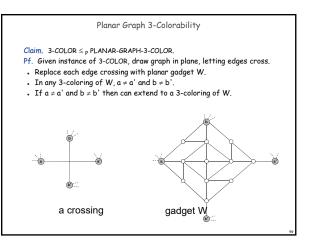


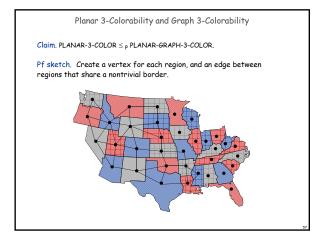


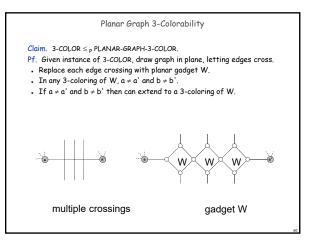












Planar k-Colorability PLANAR-2-COLOR. Solvable in linear time. PLANAR-3-COLOR. NP-complete. PLANAR-4-COLOR. Solvable in O(1) time. Theorem. [Appel-Haken, 1976] Every planar map is 4-colorable. . Resolved century-old open problem. . Used 50 days of computer time to deal with many special cases.

• First major theorem to be proved using computer.

False intuition. If $\ensuremath{\mathsf{PLANAR-3-COLOR}}$ is hard, then so is $\ensuremath{\mathsf{PLANAR-4-COLOR}}$ and $\ensuremath{\mathsf{PLANAR-5-COLOR}}$.

Polynomial-Time Detour

Graph minor theorem. [Robertson-Seymour 1980s]

Corollary. There exist an $O(n^3)$ algorithm to determine if a graph can be embedded in the torus in such a way that no two edges cross.

Pf of theorem. Tour de force.

Polynomial-Time Detour

Graph minor theorem. [Robertson-Seymour 1980s]

Corollary. There exist an $O(n^3)$ algorithm to determine if a graph can be embedded in the torus in such a way that no two edges cross.

Mind boggling fact 1. The proof is highly non-constructive! Mind boggling fact 2. The constant of proportionality is enormous!

Unfortunately, for any instance G = (V, E) that one could fit into the known universe, one would easily prefer n^{70} to even constant time, if that constant had to be one of Robertson and Seymour's. - David Johnson

Theorem. There exists an explicit O(n) algorithm. Practice. LEDA implementation guarantees $O(n^3)$.