CSE 417
Introduction to Algorithms
Winter 2007

## NP-Completeness

(Chapter 8)

## Some Algebra Problems (Algorithmic)

Given positive integers $a, b, c$
Question I: does there exist a positive integer x such that $\mathrm{ax}=\mathrm{c}$ ?

Question 2: does there exist a positive integer x such that $a x^{2}+b x=c$ ?

Question 3: do there exist positive integers $x$ and $y$ such that $\mathrm{ax}^{2}+\mathrm{by}=\mathrm{c}$ ?

## A Brief History of Ideas

From Classical Greece, if not earlier, "logical thought" held to be a somewhat mystical ability Mid I800's: Boolean Algebra and foundations of mathematical logic created possible "mechanical" underpinnings
1900: David Hilbert's famous speech outlines program: mechanize all of mathematics?

1930's: Gödel, Church, Turing, et al. prove it's impossible

## More History

## 1930/40's

What is (is not) computable

## 1960/70's

What is (is not) feasibly computable
Goal - a (largely) technology-independent theory of time required by algorithms
Key modeling assumptions/approximations
Asymptotic (Big-O), worst case is revealing
Polynomial, exponential time - qualitatively different


## Another view of Poly vs Exp

Next year's computer will be $2 x$ faster. If I can solve problem of size $n_{0}$ today, how large a problem can I solve in the same time next year?

| Complexity | Increase | E.g. $\mathrm{T}=10^{12}$ |  |
| :--- | :--- | ---: | ---: |
| $\mathrm{O}(\mathrm{n})$ | $\mathrm{n}_{0} \rightarrow 2 \mathrm{n}_{0}$ | $10^{12}$ | $2 \times 10^{12}$ |
| $\mathrm{O}\left(\mathrm{n}^{2}\right)$ | $\mathrm{n}_{0} \rightarrow \sqrt{ } 2 \mathrm{n}_{0}$ | $10^{6}$ | $1.4 \times 10^{6}$ |
| $\mathrm{O}\left(\mathrm{n}^{3}\right)$ | $\mathrm{n}_{0} \rightarrow \sqrt{3} 2 \mathrm{n}_{0}$ | $10^{4}$ | $1.25 \times 10^{4}$ |
| $2^{\mathrm{n} / 10}$ | $\mathrm{n}_{0} \rightarrow \mathrm{n}_{0}+10$ | 400 | 410 |
| $2^{\mathrm{n}}$ | $\mathrm{n}_{0} \rightarrow \mathrm{n}_{0}+1$ | 40 | 41 |

## Polynomial versus exponential

We'll say any algorithm whose run-time is
polynomial is good
bigger than polynomial is bad

Note - of course there are exceptions:
$n^{100}$ is bigger than (1.00I) ${ }^{n}$ for most practical values of $n$ but usually such run-times don't show up
There are algorithms that have run-times like $\mathrm{O}\left(2^{\text {sqr( }}\right.$ (n)/22 $)$ and these may be useful for small input sizes, but they're not too common either

## Some Convenient Technicalities

"Problem" - the general case
Ex: The Clique Problem: Given a graph G and an integer
k , does G contain a k-clique?
"Problem Instance" - the specific cases Ex: Does $\square$ contain a 4-clique? (no) Ex: Does $\qquad$ contain a 3 -clique? (yes)
Decision Problems - Just Yes/No answer
Problems as Sets of "Yes" Instances Ex: CLIQUE $=\{(G, k) \mid G$ contains a $k$-clique $\}$
E.g., ( $\vee<$, 4) $\notin$ CLIQUE
E.g., $(\boxtimes, 3) \in$ CLIQUE

## The class P

Definition: $\mathrm{P}=$ set of (decision) problems solvable by computers in polynomial time. i.e.,

$$
T(n)=O\left(n^{k}\right) \text { for some fixed } k .
$$

These problems are sometimes called tractable problems.

Examples: sorting, shortest path, MST, connectivity,
RNA folding \& other dyn. prog. - most of 417
(exceptions: Change-Making/Stamps, TSP)

## Decision problems

Computational complexity usually analyzed using decision problems
answer is just I or 0 (yes or no).
Why?
much simpler to deal with
deciding whether $G$ has a $k$-clique, is certainly no harder than finding a $k$-clique in $G$, so a lower bound on deciding is also a lower bound on finding
Less important, but if you have a good decider, you can often use it to get a good finder. (Ex.: does $G$ still have a k-clique after I remove this vertex?)

## Beyond P?

There are many natural, practical problems for which we don't know any polynomial-time algorithms
e.g. CLIQUE:

Given an undirected graph $G$ and an integer $k$, does $G$ contain a k-clique?
e.g. quadratic Diophantine equations:

Given $a, b, c \in N, \exists x, y \in N$ s.t. $a x^{2}+b y=c$ ?

## Some Problems

## Independent-Set

Given a graph $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ and an integer k , is there a subset $U$ of $V$ with $|U| \geq k$ such that no two vertices in $U$ are joined by an edge.


## Clique:

Given a graph $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ and an integer k , is there a subset $U$ of $V$ with $|\mathrm{U}| \geq \mathrm{k}$ such that every pair of vertices in $U$ is joined by an edge.


Boolean variables $x_{1}, \ldots, x_{n}$ taking values in $\{0, \mathrm{I}\}$. $0=$ false, $\mathrm{I}=$ true
Literals
$\mathrm{x}_{\mathrm{i}}$ or $\neg \mathrm{x}_{\mathrm{i}}$ for $\mathrm{i}=1, \ldots, \mathrm{n}$
Clause
a logical OR of one or more literals
e.g. $\left(x_{1} \vee \neg x_{3} \vee x_{7} \vee x_{12}\right)$

CNF formula
a logical AND of a bunch of clauses


## Some More Problems

## Euler Tour:

Given a graph $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ is there a cycle traversing each edge once.

Hamilton Tour:
Given a graph $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ is there a simple cycle of length V|, i.e., traversing each vertex once.

TSP:
Given a weighted graph $\mathrm{G}=(\mathrm{V}, \mathrm{E}, \mathrm{w})$ and an integer k , is there a Hamilton tour of $G$ with total weight $\leq k$

## Satisfiability

CNF formula example

$$
\left(x_{1} \vee \neg x_{3} \vee x_{7}\right) \wedge\left(\neg x_{1} \vee \neg x_{4} \vee x_{5} \vee \neg x_{7}\right)
$$

If there is some assignment of 0 's and I's to the variables that makes it true then we say the formula is satisfiable
the one above is, the following isn't

$$
x_{1} \wedge\left(\neg x_{1} \vee x_{2}\right) \wedge\left(\neg x_{2} \vee x_{3}\right) \wedge \neg x_{3}
$$

Satisfiability: Given a CNF formula F, is it satisfiable?


## Some Problem Pairs




## More History - As of 1970

Many of the above problems had been studied for decades
All had real, practical applications
None had poly time algorithms; exponential was best known

But, it turns out they all have a very deep similarity under the skin

Common property of these problems

There is a special piece of information, a short hint or proof, that allows you to efficiently (in polynomial-time) verify that the YES answer is correct. BUT, this hint might be very hard to find
e.g.

TSP: the tour itself
Independent-Set, Clique: the vertex set U
Satisfiability: an assignment that makes formula true
Quadratic Diophantine eqns: the numbers $x \& y$

## The complexity class NP

NP consists of all decision problems where
You can verify the YES answers efficiently (in polynomial time) given a short (polynomial-size) hint

And
No hint can fool your polynomial time verifier into saying YES for a NO instance
(implausible for all exponential time problems)
procedure $v(x, h)$
if
x is a well-formed representation of a graph $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ and an integer k ,
and
h is a well-formed representation of a k -vertex subset U of V ,
and
U is a clique in G ,
then output "YES"
else output "I'm unconvinced"

## Example: CLIQUE is in NP

## More Precise Definition of NP

A decision problem is in NP iff there is a polynomial time procedure $v(-,-)$, and an integer $k$ such that
for every YES problem instance $x$ there is a hint h with $|\mathrm{h}| \leq|\mathrm{x}|^{\mathrm{k}}$ such that $\mathrm{v}(\mathrm{x}, \mathrm{h})=\mathrm{YES}$
and
for every NO problem instance $x$ there is no hint $h$ with $|\mathrm{h}| \leq|\mathrm{x}|^{\mathrm{k}}$ such that $\mathrm{v}(\mathrm{x}, \mathrm{h})=$ YES
"Hints" sometimes called "Certificates"

## Is it correct?

For every $x=(G, k)$ such that $G$ contains a $k$-clique, there is a hint $h$ that will cause $v(x, h)$ to say YES, namely $h=a$ list of the vertices in such a k-clique and
No hint can fool $v$ into saying yes if either $x$ isn't well-formed (the uninteresting case) or if $x=(G, k)$ but $G$ does not have any cliques of size $k$ (the interesting case)

## Another example: SAT $\in N P$

Hint: the satisfying assignment $A$
Verifier: $\mathrm{v}(\mathrm{F}, \mathrm{A})=\operatorname{syntax}(\mathrm{F}, \mathrm{A}) \& \&$ satisfies $(\mathrm{F}, \mathrm{A})$
Syntax: True iff $F$ is a well-formed formula \& $A$ is a
truth-assignment to its variables
Satisfies: plug A into F and evaluate
Correctness:
If F is satisfiable, it has some satisfying assignment A , and we'll recognize it
If F is unsatisfiable, it doesn't, and we won't be fooled

## Keys to showing that a problem is in NP

What's the output? (must be YES/NO)
What's the input? Which are YES?
For every given YES input, is there a hint that would help? Is it polynomial length?

OK if some inputs need no hint
For any given NO input, is there a hint that would trick you?

## Solving NP problems without hints

The most obvious algorithm for most of these problems is brute force:
try all possible hints; check each one to see if it works.
Exponential time:
$2^{n}$ truth assignments for $n$ variables
$n$ ! possible TSP tours of $n$ vertices
$\binom{n}{k}$ possible k element subsets of n vertices
etc.
...and to date, every alg, even much less-obvious ones, are slow, too

## Problems in P can also be verified in polynomial-time

Short Path: Given a graph G with edge lengths, is there a path from $s$ to $t$ of length $\leq \mathrm{k}$ ?

Verify: Given a purported path from $s$ to $t$, is it a path, is its length $\leq \mathrm{k}$ ?

Small Spanning Tree: Given a weighted undirected graph G , is there a spanning tree of weight $\leq \mathrm{k}$ ?

Verify: Given a purported spanning tree, is it a spanning tree, is its weight $\leq \mathrm{k}$ ?
(But the hints aren't really needed in these cases...)

## P vs NP vs Exponential Time

Theorem: Every problem in
NP can be solved deterministically in exponential time

Proof: "hints" are only $\mathrm{n}^{\mathrm{k}}$ long; try all $2^{n^{k}}$ possibilities, Needle say by backtracking. If any succeed, say YES; if all fail, say NO .


Every problem in P is in NP one doesn't even need a hint or problems in P so just ignore any hint you are given

Every problem in NP is in exponential time
l.e., $P \subseteq N P \subseteq E x p$

We know $P \neq \operatorname{Exp}$, so either $P \neq N P$, or $N P \neq \operatorname{Exp}$ (most likely both)


35

## P vs NP

## Theory

$P=N P$ ?
Open Problem!
I bet against it

Practice
Many interesting, useful, natural, well-studied problems known to be NP-complete
With rare exceptions, no one routinely succeeds in finding exact solutions to large, arbitrary instances


## NP-complete Problems

We are pretty sure that no problem in NP - P can be solved in polynomial time.
Non-Definition: NP-complete $=$ the hardest problems in the class NP. (Formal definition later.) Interesting fact: If any one NP-complete problem could be solved in polynomial time, then all NP problems could be solved in polynomial time.

## More Connections

Some Examples in NP
Satisfiability
Independent-Set
Clique
Vertex Cover
All hard to solve; hints seem to help on all
Very surprising fact:

```
Fast solution to any gives
    fast solution to all!
```



## The class NP-complete (cont.)

Thousands of important problems have been shown to be NP-complete.

Fact (Dogma): The general belief is that there is no efficient algorithm for any NP-complete problem, but no proof of that belief is known.

Examples: SAT, clique, vertex cover, Hamiltonian cycle, TSP, bin packing.

## Does $\mathrm{P}=\mathrm{NP}$ ?

This is an open question.
To show that $P=N P$, we have to show that every problem that belongs to NP can be solved by a polynomial time deterministic algorithm.
No one has shown this yet. (It seems unlikely to be true.)

## Complexity Classes of Problems



## Is all of this useful for anything?

Earlier in this class we learned techniques for solving problems in P .

Question: Do we just throw up our hands if we come across a problem we suspect not to be in P?

## Dealing with NP-complete Problems

What if I think my problem is not in P?

Here is what you might do:
I) Prove your problem is NP-hard or -complete
(a common, but not guaranteed outcome)
2) Come up with an algorithm to solve the problem usually or approximately.

## Reductions: a useful tool

Definition: To reduce $A$ to $B$ means to solve $A$, given a subroutine solving $B$.

Example: reduce MEDIAN to SORT Solution: sort, then select ( $\mathrm{n} / 2$ )nd
Example: reduce SORT to FIND_MAX Solution: FIND_MAX, remove it, repeat
Example: reduce MEDIAN to FIND_MAX
Solution: transitivity: compose solutions above.

## Reductions: Why useful

Definition: To reduce $A$ to $B$ means to solve $A$, given a subroutine solving $B$.

Fast algorithm for $B$ implies fast algorithm for $A$ (nearly as fast; takes some time to set up call, etc.)

If every algorithm for A is slow, then no algorithm for $B$ can be fast.

$$
\text { "complexity of A" } \leq \text { "complexity of B" + "complexity of reduction" }
$$

## SAT is NP-complete

## Cook's theorem: SAT is NP-complete

## Satisfiability (SAT)

A Boolean formula in conjunctive normal form (CNF) is satisfiable if there exists a truth assignment of 0's and I's to its variables such that the value of the expression is $I$. Example:
$S=(x+y+\neg z) \cdot(\neg x+y+z) \cdot(\neg x+\neg y+\neg z)$
Example above is satisfiable. (We can see this by setting $\mathrm{x}=\mathrm{I}, \mathrm{y}=\mathrm{I}$ and $\mathrm{z}=0$.)

## NP-complete problem:

Vertex Cover
Input: Undirected graph $G=(V, E)$, integer $k$.
Output: True iff there is a subset C of V of size $\leq k$ such that every edge in $E$ is incident to at least one vertex in $C$.

Example: Vertex cover of size $\leq 2$.


In NP? Exercise

$3 S A T \leq_{p}$ VertexCover


51

3 SAT $\leq_{p}$ VertexCover



52


## Correctness of " 3 SAT $\leq_{p}$ VertexCover"

Summary of reduction function f: Given formula, make graph G with one group per clause, one node per literal. Connect each to all nodes in same group, plus complementary literals $(x,-x)$. Output graph G plus integer $k=2 *$ number of clauses. Note: $f$ does not know whether formula is satisfiable or
$G$ has $k$-cover; does not try to find satisfying assignment or cover.
Correctness:
Show f poly time computable: A key point is that graph size is polynomial in formula size; mapping basically straightforward
Show c in 3 -SAT iff f$)=(\mathrm{G}, \mathrm{k})$ in VertexCover
$(\Rightarrow)$ Given an assignment satisfying $c$, pick one true literal per clause. Add other 2 nodes of each triangle to cover. Show it is a cover: 2 per triangle cover triangle edges; only true literals (but perhaps not all true literals) uncovered, so at least one end of every ( $x, \sim x$ ) edge is covered
$(\leftarrow)$ Given a $k$-vertex cover in G , uncovered labels define a valid (perhaps partial) uncovered node in each clause triangle (else some other clause triangle has > I uncovered node, hence an uncovered edge.)

## Utility of " 3 SAT $\leq_{p}$ VertexCover"

Suppose we had a fast algorithm for VertexCover, then we could get a fast algorithm for 3SAT:

Given 3-CNF formula w, build Vertex
Cover instance $y=f(w)$ as above, run the fast
VC alg on $y$; say "YES, w is satisfiable" iff VC alg says
"YES, $y$ has a vertex cover of the given size"
On the other hand, suppose no fast alg is possible for 3SAT, then we know none is possible for VertexCover either.

## Polynomial-Time Reductions

Definition: Let $A$ and $B$ be two problems.
We say that $A$ is polynomially reducible to $B$ if there exists a polynomial-time algorithm $f$ that converts each instance $x$ of problem $A$ to an instance $f(x)$ of $B$ such that
$x$ is a YES instance of $A$ iff
$f(x)$ is a YES instance of $B$.

$$
x \in A \quad \Leftrightarrow \quad f(x) \in B
$$

## Polynomial-Time Reductions (cont.)

Define: $A \leq_{p} B$ " $A$ is polynomial-time reducible to
$B$ ", iff there is a polynomial-time computable function $f$ such that: $x \in A \Leftrightarrow f(x) \in B$
$\stackrel{\circ}{9}$
"complexity of $A " \leq$ "complexity of $B "+$ "complexity of $f$ "
(1) $A \leq P B$ and $B \in P \Rightarrow A \in P$
(2) $A \leq p B$ and $A \notin P \Rightarrow B \notin P$
(3) $A \leq p B$ and $B \leq p C \Rightarrow A \leq p C$ (transitivity)

## Definition of NP-Completeness

Definition: Problem B is NP-hard if every problem in NP is polynomially reducible to $B$.

Definition: Problem B is NP-complete if:
(I) $B$ belongs to NP, and
(2) B is NP-hard.

## Using an Algorithm for $\boldsymbol{B}$ to

 Solve AAlgorithm to solve A

"If $A \leq p$, and we can solve $B$ in polynomial time, then we can solve $A$ in polynomial time also."
Ex: suppose $f$ takes $O\left(n^{3}\right)$ and algorithm for $B$ takes $O\left(n^{2}\right)$. How long does the above algorithm for $A$ take?

## Proving a problem is NPcomplete

Technically, for condition (2) we have to show that every problem in NP is reducible to B. (yikes!) This sounds like a lot of work.

For the very first NP-complete problem (SAT) this had to be proved directly.
However, once we have one NP-complete problem, then we don't have to do this every time.
Why? Transitivity.

## Re-stated Definition

Lemma: Problem B is NP-complete if:
(I) B belongs to NP, and
(2') A is polynomial-time reducible to B , for some problem A that is NP-complete.

That is, to show ( $2^{\prime}$ ) given a new problem B, it is sufficient to show that SAT or any other NPcomplete problem is polynomial-time reducible to B.

## Ex: VertexCover is NP-complete

3-SAT is NP-complete (shown by S. Cook)
3 -SAT $\leq_{p}$ VertexCover
VertexCover is in NP (we showed this earlier)
Therefore VertexCover is also NP-complete

So, poly-time algorithm for VertexCover would give poly-time algs for everything in NP

## Usefulness of Transitivity

Now we only have to show L' $\leq_{p} L$, for some NP-complete problem L', in order to show that L is NP-hard. Why is this equivalent?
I) Since $L$ ' is NP-complete, we know that $L$ ' is NP-hard. That is:
$\forall L^{\prime \prime} \in N P$, we have $L^{\prime \prime} \leq_{p} L^{\prime}$
2) If we show $L^{\prime} \leq_{P} L$, then by transitivity we know that: $\forall L " \in N P$, we have $L " \leq_{p} L$.
Thus L is NP-hard.

## NP-complete problem: 3-Coloring

Input: An undirected graph $G=(\mathrm{V}, \mathrm{E})$.
Output: True iff there is an assignment of at most 3 colors to the vertices in $G$ such that no two adjacent vertices have the same color.

Example:

In NP? Exercise


## A 3-Coloring Gadget:

In what ways can this be 3-colored?


69


## Correctness of " 3 SAT $\leq_{p} 3$ Coloring"

Summary of reduction function $f$ :
Given formula, make G with T-F-N triangle, I pair of literal nodes per variable, 2 or" gadgets per clause, connected as in example.
Correctness:
Show f poly time computable: A key point is that graph size is polynomial in formula size; graph looks messy, but pattern is basically straightforward. Show c in 3 -SAT iff $\mathrm{f}(\mathrm{c})$ is 3 -colorable
$(\Rightarrow)$ Given an assignment satisfying c , color literals T/F as per assignment; can color "or" gadgets so output nodes are T since each clause is satisfied. $(\Leftarrow)$ Given a 3 -coloring of $f(c)$, name colors T-N-F as in example. All square nodes are $T$ or $F$ (since all adjacent to $N$ ). Each variable pair ( $x i$, $\sim$ xi) must have complementary labels since they're adjacent. Define assignment based on colors N \& F. Clause output nodes must be colored since they're adjacent to hence it is a satisfying assignment

## Planar 3-Coloring is also NP-Complete



## Common Errors in NP-completeness Proofs

Backwards reductions
Bipartiteness $\leq_{S} S A T$ is true, but not so useful. ( $\mathrm{XYZ} \leq_{p}$ SAT shows $X Y Z$ in NP, does not show it's hard.)
Sloooow Reductions
"Find a satisfying assignment, then output..."
Half Reductions
Delete dashed edges in 3Color reduction. It's still true that " $c$ satisfiable $\Rightarrow G$ is 3 colorable", but 3colorings don't necessarily give good assignments.

## Coping with NP-Completeness

Is your real problem a special subcase?
E.g. 3-SAT is NP-complete, but 2-SAT is not;

Ditto 3-vs 2-coloring
E.g. maybe you only need planar graphs, or degree 3 graphs, or ...
Guaranteed approximation good enough?
E.g. Euclidean TSP within 1.5 * Opt in poly time

Clever exhaustive search may be fast enough in practice, e.g. Backtrack, Branch \& Bound, pruning
Heuristics - usually a good approximation and/or usually fast

## NP-complete problem: TSP

Input: An undirected graph $\mathrm{G}=(\mathrm{V}, \mathrm{E})$ with integer edge weights, and an integer $b$.

Output: YES iff there is a simple cycle in G passing through all vertices (once),

with total cost $\leq \mathrm{b}$.

## 2x Approximation to EuclideanTSP

A TSP tour visits all vertices, so contains a spanning tree, so TSP cost is > cost of min spanning tree.
Find MST
Find "DFS" Tour
Shortcut


TSP $\leq$ shortcut $<$ DFST $=2 *$ MST $<2 *$ TSP

## TSP - Nearest Neighbor Heuristic

Recall NN Heuristic


Fact: $N N$ tour can be about $(\log n) \times o p t$, i.e.

$$
\lim _{n \rightarrow \infty} \frac{N N}{O P T} \rightarrow \infty
$$

(above example is not that bad)


