CSE 417 Introduction to Algorithms Winter 2005

NP-Completeness (Chapter 6)

1

Some Algebra Problems (Algorithmic)

Given positive integers a, b, c

Question 1: does there exist a positive integer x such that ax = c ?

Question 2: does there exist a positive integer x such that $ax^2 + bx = c$?

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

2

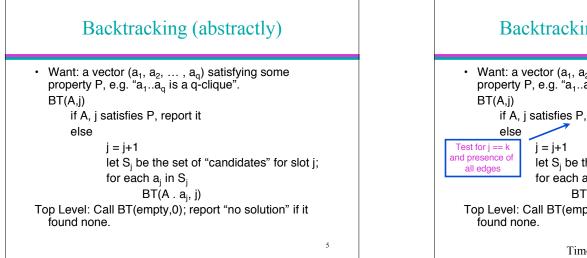
4

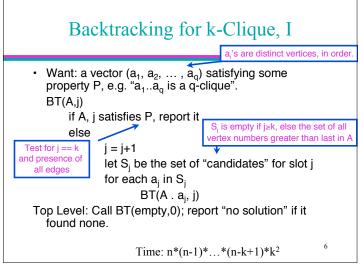
1

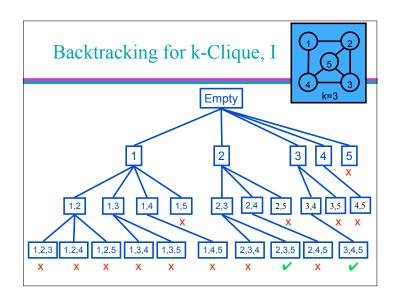
The Clique Problem
Given: a graph G=(V,E) and an integer k
Question: is there a subset U of V with IUI ≥ k such that every pair of vertices in U is joined by an edge.

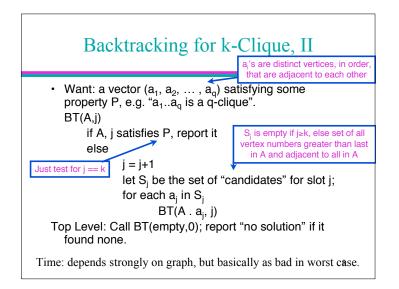
Solving The Clique Problem

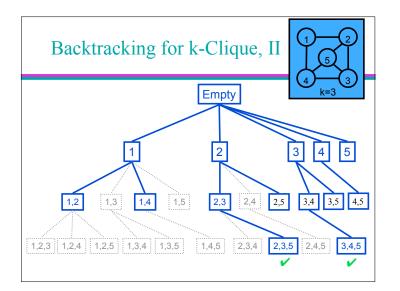
- A simple way:
 - Systematically list all possible sets of exactly k nodes
 - For each such set, check whether all pairs are neighbors
- A general approach for problems like this: Backtracking





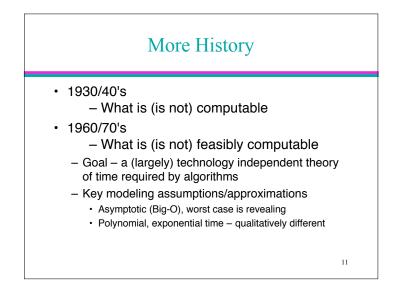


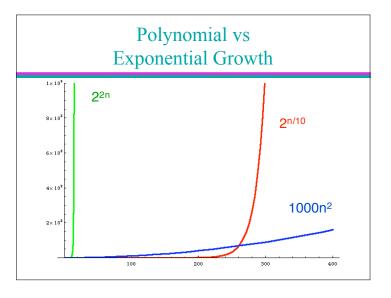




A Brief History of Ideas

- From Classical Greece, if not earlier, "logical thought" held to be a somewhat mystical ability
- Mid 1800'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





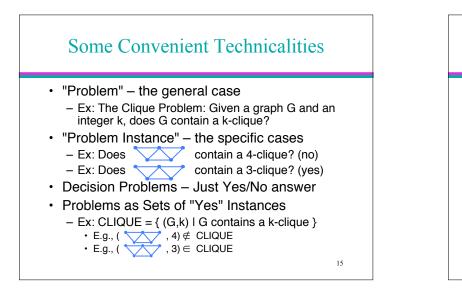
Another view of Poly vs Exp

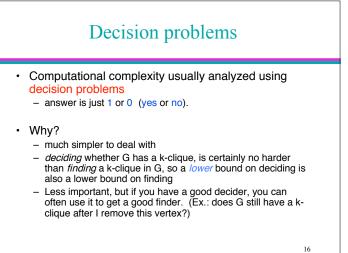
Next year's computer will be 2x faster. If I can solve problem of size n_0 today, how large a problem can I solve in the same time next year?

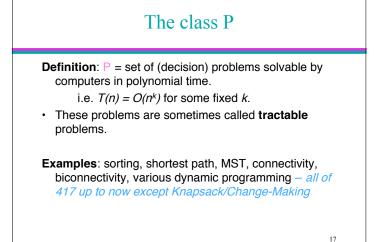
Complexity	Increase	E.g. T=10 ¹²	
O(n)	$n_0 \rightarrow 2n_0$	10 ¹²	2 x 10 ¹²
O(n ²)	$n_0 \rightarrow \sqrt{2} n_0$	10 ⁶	1.4 x 10 ⁶
O(n ³)	$n_0 \rightarrow 3\sqrt{2} n_0$	10 ⁴	1.25 x 10 ⁴
2 ^{n /10}	$n_0 \rightarrow n_0 + 10$	400	410
2 ⁿ	$n_0 \rightarrow n_0 + 1$	40	41

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:
 - n¹⁰⁰ is bigger than (1.001)ⁿ for most practical values of n but usually such run-times don't show up
 - There are algorithms that have run-times like $O(2^{n/22})$ and these may be useful for small input sizes, but they're not too common either

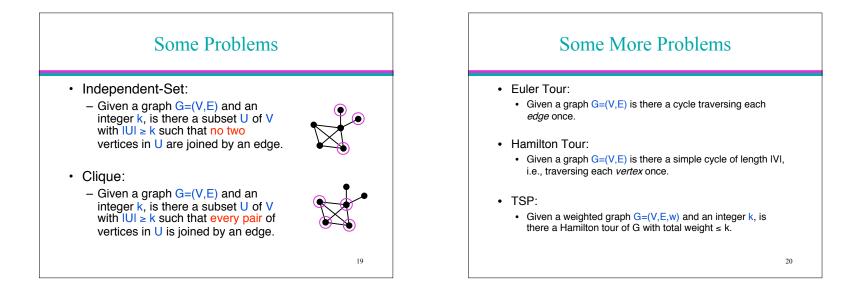


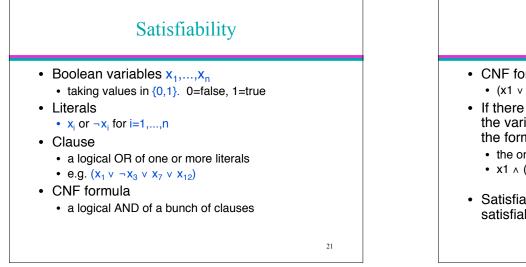




Beyond **P**?

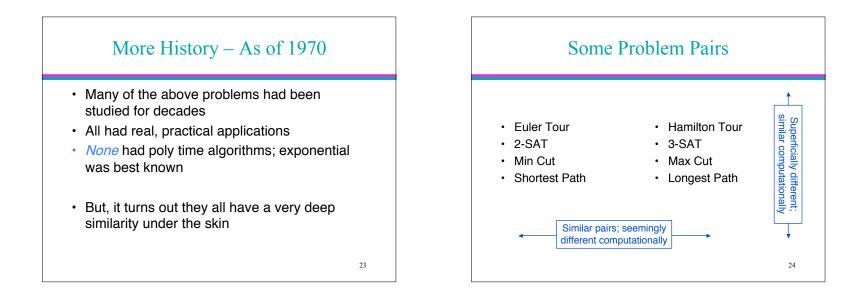
- There are many natural, practical problems for which we don't know any polynomial-time algorithms
- e.g. CLIQUE:
 - Given a weighted graph G and an integer k, does there exist a k-clique in G?
- e.g. quadratic Diophantine equations:
 - Given a, b, $c \in N$, $\exists x, y \in N$ s.t. $ax^2 + by = c$?





Satisfiability

- CNF formula example
 - (x1 v ¬x3 v x7 v x12) ∧ (x2 v ¬x4 v x7 v x5)
- If there is some assignment of 0's and 1's to the variables that makes it true then we say the formula is *satisfiable*
 - the one above is, the following isn't
 - x1 ^ (¬x1 v x2) ^ (¬x2 v x3) ^ ¬x3
- Satisfiability: Given a CNF formula F, is it satisfiable?



Common property of these problems

 There is a special piece of information, a short hint or proof, that allows you to efficiently (in polynomialtime) verify that the YES answer is correct. This hint might be very hard to find

• e.g.

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

25

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)

26

28

<section-header><list-item><list-item><list-item><list-item><list-item><list-item><list-item>

Example: CLIQUE is in NP

procedure v(x,h)

if

x is a well-formed representation of a graph G = (V, E) and an integer k,

and

h is a well-formed representation of a k-vertex subset U of V, $% \left({V_{\rm{s}}} \right) = 0$

and

U is a clique in G, then output "YES" else output "I'm unconvinced"

Is it correct?

 For every x = (G,k) such that G contains a kclique, 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)

29

31

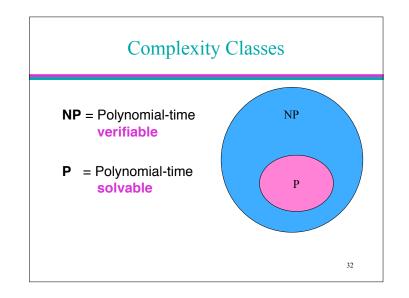
Another example: $SAT \in NP$

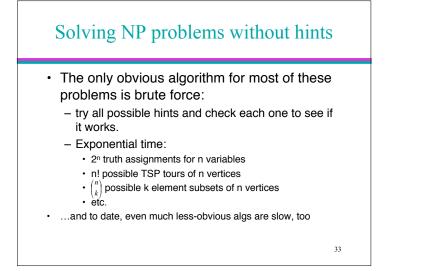
- · Hint: the satisfying assignment A
- Verifier: v(F,A) = syntax(F,A) && satisfies(F,A)
 - Syntax: True iff F is a well-formed formula & A is a truth-assignment to its variables
 - Satisfies: plug A into F and evaluate
- · Correctness:
 - If F is satisfiable, it has some satisfying assignment A, and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

30

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?





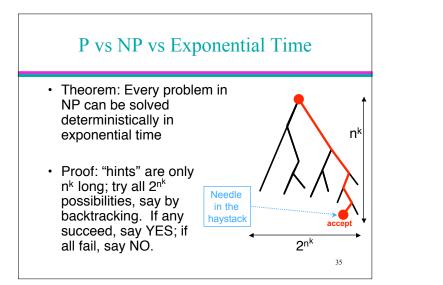
Problems in P can also be verified in polynomial-time

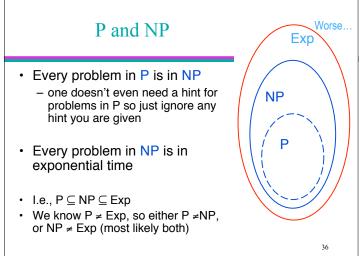
<u>Shortest Path</u>: Given a graph *G* with edge lengths, is there a path from *s* to *t* of length $\leq k$?

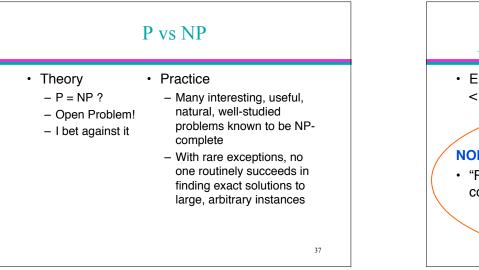
Verify: Given a purported path from *s* to *t*, is it a path, is its length $\leq k$?

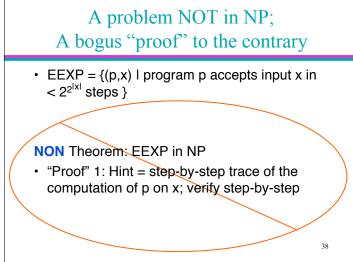
<u>Small Spanning Tree</u>: Given a weighted undirected graph G, is there a spanning tree of weight $\leq k$?

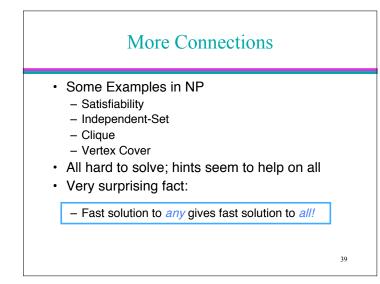
Verify: Given a purported spanning tree, is it a spanning tree, is its weight ≤ *k*?







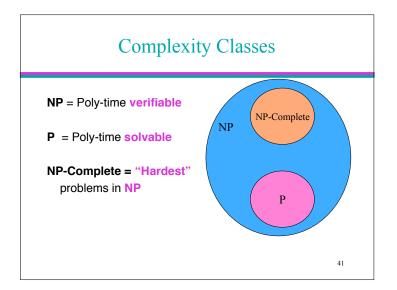




The class NP-complete

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.



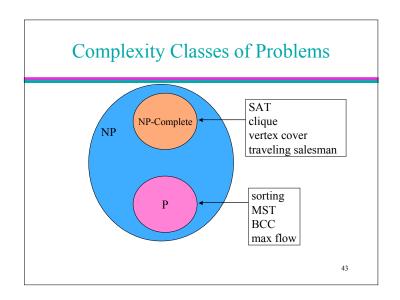
The class NP-complete (cont.)

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.

42

44



Does P = NP?

- · This is an open question.
- To show that P = NP, 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.)

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:

- 1) 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 (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.

47

45

Reductions: Why useful

46

48

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.

"complexity of A" < "complexity of B" + "complexity of reduction"

The growth of the number of NPcomplete problems

- Steve Cook (1971) showed that SAT was NP-complete.
- Richard Karp (1972) found 24 more NP-complete problems.
- Today there are thousands of known NP-complete problems.
 - Garey and Johnson (1979) is an excellent source of NP-complete problems.

49

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 1's to its variables such that the value of the expression is 1. Example:

 $S=(x+y+\neg z) \cdot (\neg x+\gamma+z) \cdot (\neg x+\neg y+\neg z)$ Example above is satisfiable. (We can see this by setting x=1, y=1 and z=0.)

50

How do you prove problem *A* is NP-complete?

1) **Prove** *A* **is in NP:** show that given a solution, it can be verified in polynomial time.

2) Prove that A is NP-hard:

a) Select a known NP-complete problem B.

b) Describe a polynomial time computable algorithm that computes a function *f*, mapping *every* instance of *B* to an instance of *A*. (that is: $B \leq_p A$)

c) Prove that if b is a *yes*-instance of *B* then f(b) is a *yes*-instance of *A*. Conversely, if f(b) is a *yes*-instance of *A*, then b must be *yes*-instance of *B*.

d) Prove that the algorithm computing *f* runs in polynomial time.

51

NP-complete problem: Vertex Cover

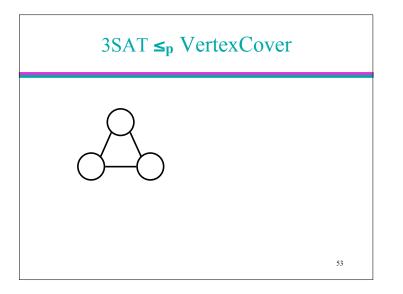
Input: Undirected graph G = (V, E), integer k. **Output**: True iff there is a subset C of V of size $\leq k$ such that every edge in E is incident to at least one vertex in C.

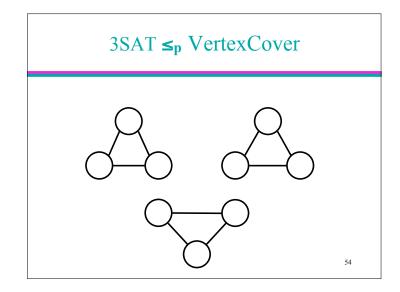
Example: Vertex cover of size ≤ 2 .

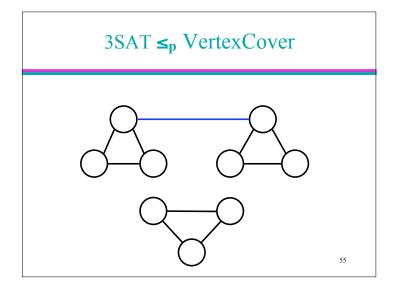


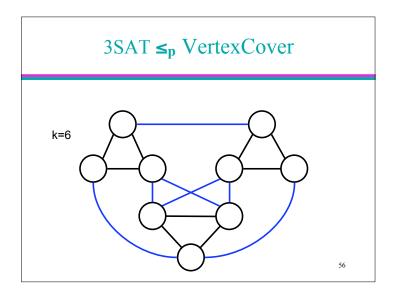
52

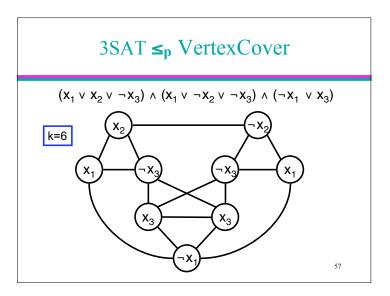
In NP? Exercise

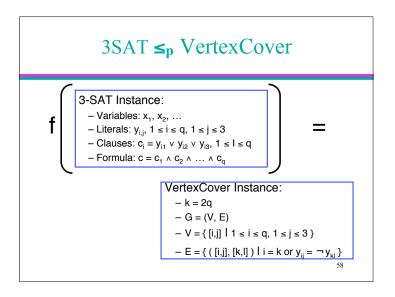


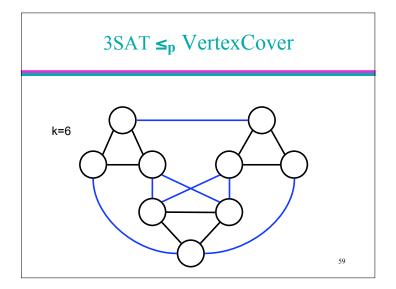


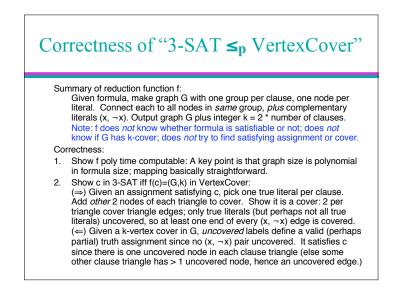












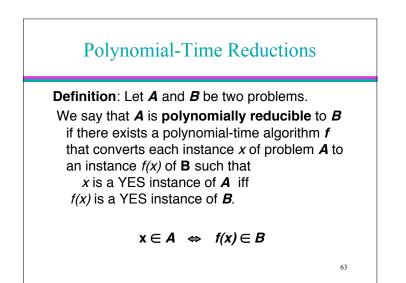
Utility of "3-SAT ≤_p VertexCover"

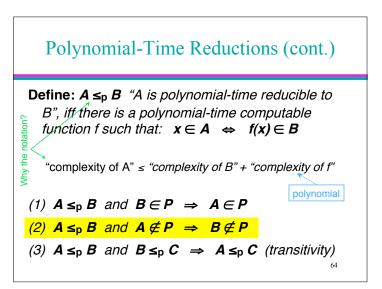
- *Suppose* we had a fast algorithm for VertexCover, then we could get a fast algorithm for 3SAT:
 - Given 3-CNF formula w, build VertexCover instance y = f(w) as above, run the fast VC alg on y, say "YES, w is satisfiable" iff VC alg says "YES, y has a vertex cover of the given size"
- On the other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

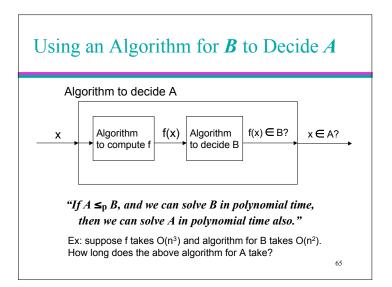
61

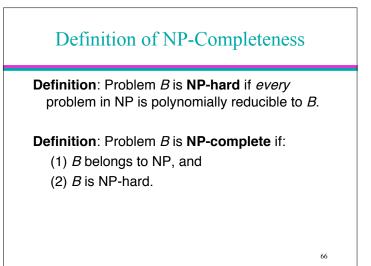
"3-SAT ≤_p VertexCover" Retrospective

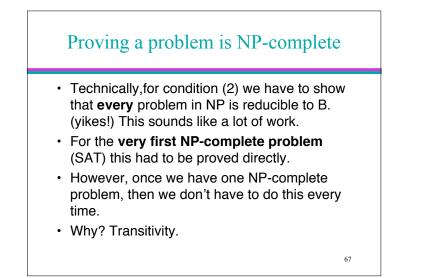
- Previous slide: two suppositions
- Somewhat clumsy to have to state things that way.
- Alternative: abstract out the key elements, give it a name ("polynomial time reduction"), then properties like the above always hold.











Re-stated Definition

Lemma: Problem *B* is NP-complete if:

- (1) 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') given a new problem *B*, it is sufficient to show that SAT or any other NP-complete problem is polynomial-time reducible to *B*.

Usefulness of Transitivity

Now we only have to show $L' \leq_p L$, for <u>some</u> problem $L' \in NP$ -complete, in order to show that L is NP-hard. Why is this equivalent?

 Since L'∈ NP-complete, we know that L' is NP-hard. That is:

 \forall L" \in NP, we have L" \leq_{p} L'

If we show L' ≤_p L, then by transitivity we know that: ∀L''∈ NP, we have L'' ≤_p L.

Thus L is NP-hard.

69

Ex: VertexCover is NP-complete

- 3-SAT is NP-complete (shown by S. Cook)
- 3-SAT ≤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

