

An NP complete problem  $\pi$  is  
 (i) in the class NP

**NP hard** { (ii) All problems in NP are polynomial time reducible to  $\pi$   
 $\forall \pi' \in \text{NP}, \pi' \leq_{\text{poly}} \pi$

Cook-Levin thm: The satisfiability problem of boolean formulae is NP complete.

Given a new problem  $\pi_1$ , try to establish (i). Suppose we can

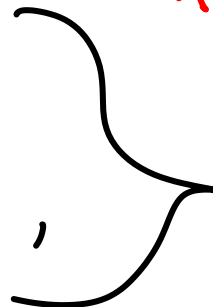
show that some NPC problem  $\pi_2$  is <sup>polynomial</sup> reducible to  $\pi_1$ ,

$$\text{(SAT)} \quad \pi_2 \leq_{\text{poly}} \pi_1$$

$$\pi_1 \leq_{\text{poly}} \pi_2$$

$$\forall \pi \in \text{NP} \quad \pi \leq_{\text{poly}} \pi_2$$

$$\pi \leq_{\text{poly}} \pi_1$$



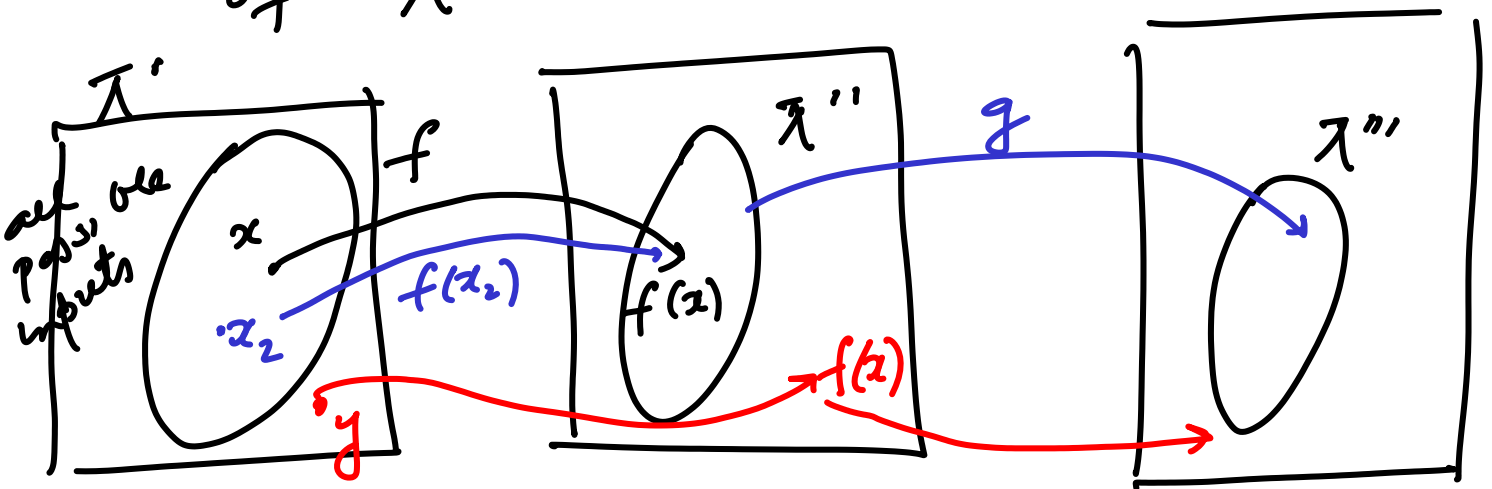
Claim polynomial reduction is transitive

If  $\pi' \leq_{\text{poly}} \pi''$  and  $\pi'' \leq_{\text{poly}} \pi'''$

then  $\pi' \leq_{\text{poly}} \pi'''$

Consider any instance of  $\pi'$ , say  $x$

There exists a polynomial reduction function  $f$  s.t.  $f(x)$  is an instance of  $\pi''$



(i)  $x$  is a YES instance of  $\pi'$  iff  $f(x)$  is a YES instance of  $\pi''$

$$f: \Sigma^* \rightarrow \Sigma^*$$

$\Sigma$ : alphabet

$\Sigma^*$  is the set of all strings

(ii)  $f$  is computable in polynomial time

Claim  $g \circ f$  is a polynomial reduction function from  $\pi'$  to  $\pi'''$

Composition of polynomials is a polynomial

$$f(x) = x^3$$

$$g(x) = x^2$$

$$g(f(x)) = x^6$$

length of  
the string

$|x|$ . length of input  $x$

Time to compute  $f$  is  $|x|^3$

$f(x)$  is now of length  $|x|^3$

$g$  is applied to  $f(x)$

Cook's theorem was published in 1971

Karp published proofs of reduction  
for 6 very basic problems

(i) Hamilton  
Circuit

(ii) Coloring  
3-colorable

(iii) Partition (N) 3dim  
matching

### 3-CNF

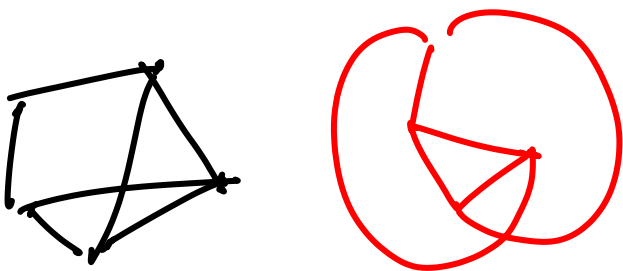
SATISFIABILITY OF BOOLEAN FORMULA IN  
CONJUNCTIVE NORMAL FORM with exactly  
3 literals per clause is NPC

$$(x_{11} \vee x_{12} \vee x_{13}) \wedge (x_{21} \vee x_{22} \vee x_{23}) \dots$$

literals mean  
a variable  $x$  or  $\bar{x}$

Are there problems in NP not known to be in P and neither known to be NPC?

(1) Graph Isomorphism



Ladner's theorem

If  $P \neq NP$  then  
- there are problems in NP which are neither NP complete nor in P

(2) Factorization

(3) ~~Primality testing~~

## Partition problem

Given set  $S$  of  $n$  integers  $x_1, x_2, \dots, x_n$   
can we partition  $S$  into  $S_1, S_2$  s.t.

$$\sum_{i \in S_1} x_i = \sum_{i \in S_2} x_i$$

3, 8, 20, 5, 4, 9

28

Partition problem  
is known to be NPC

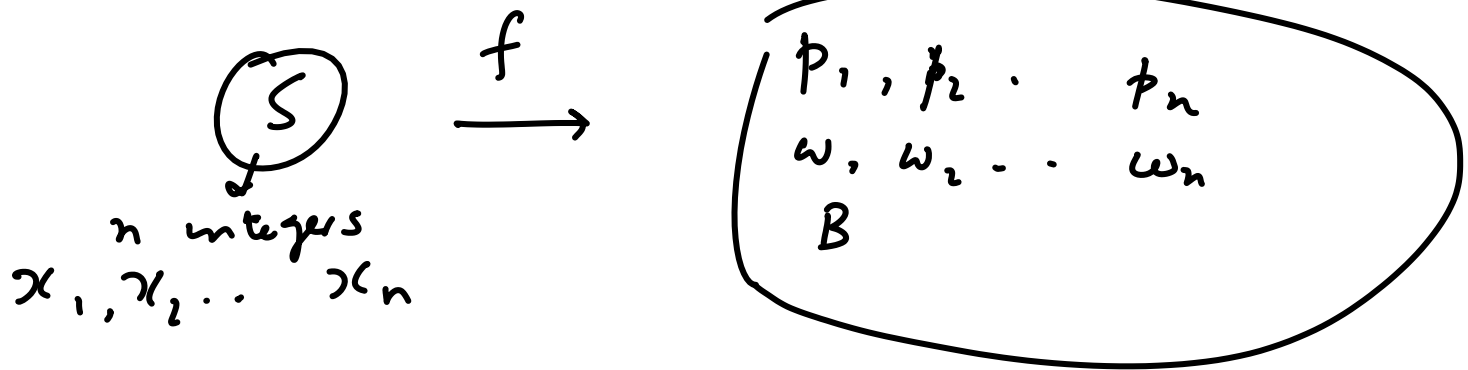
## Knapsack problem

Given profits  $p_1, p_2, \dots, p_n$   
weights  $w_1, w_2, \dots, w_n$   
Knapsack capacity  $B$   
maximize profit

Partition  $\propto$  poly knapsack

(If we succeed  
then Knapsack  
is NP-H but  
not NPC)

Given any instance  $I$  of the partition  
problem we can map it to an instance  
 $I'$  of knapsack s.t.  $I'$  can provide the  
soln to  $I$



$$B = \frac{\sum x_i}{2} \quad \max \sum p_i y_i$$

$$w_i = x_i \quad p_i = \cancel{x_i} \quad y_i \in \{0, 1\}$$

Claim : The knapsack has profit  $B$   
 iff  $S$  has a partition.

The reduction can be done in polynomial  
 -time