L23: NP Completeness

P: Polynomial time problems.

Decision problems.

Circuit satisfiability

Inputs: A circuit (boolean) C with n inputs.

Q: Is there a satisfying assignment?

Certificate is a "short" string that proves for a specific instance of a problem the answer is YES!

Verification is "easy"

$\Rightarrow \exists$ a polynomial time alg verify

verify(instance, certificate)

verifies in polynomial time that the answer is yes

$p(x) = \sum_{i=0}^{n} a_i x^i$ $\quad O(x^n)$

$q(x) = \sum_{i=0}^{k} \beta_i x^i$ $\quad p(p(x))$

dup(x): print x*x

```
doit(x):
  y = x
  for i = 1..n do
    y = dup(y)
  print y.
```

$2^{|x|}$

NP: Nondeterministic polynomial

Class of all decisions problems where there is a poly time verifier.

co-NP All decision problems s.t. if the answer is no then there is a poly size "proof", and a poly time verifier.

P: Polynomial time

All decisions problems solvable in poly time.

$P \subseteq NP$, $P \subseteq coNP$

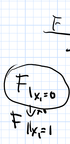
SAT

Input: A boolean formula in CNF form

Q: Is there sat assignment?

$(x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_2 \vee x_n) \wedge \cdots$

clause — and — or



Self-reduction

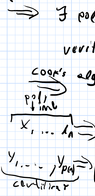
Cook-Levin Theorem 1973

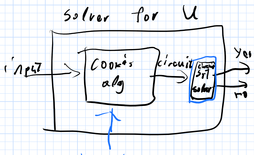
If one can solve circuit SAT in poly time then all the problems in NP can be solved in polynomial time.

U some NP problem

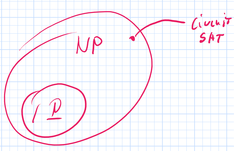
$\Rightarrow \exists$ poly time verifier

verifier(input, certificate)





Reduction from U to circuit SAT.



CSAT is poly solvable then P=NP.

NP-Complete

All problems in NP s.t. if any of them are solvable in poly time then $\forall L \in NP$ are poly solvable.

NP-Hard

All the problems s.t. if any of them are poly solvable $\Rightarrow$ P=NP.

$2^{\log^{O(1)} n} = n^{O(\log n)}$ Quasi-Polynomial

Factoring

n: number

$n = \prod p_i$

p_i's are primes

$2^{O((\#\text{bits of } n)^{1/3})}$

Question: computers poly time alg show algorithm?

Problem X is polynomially equivalent to Circuit SAT.

A decision problem X is in NPC $\Leftrightarrow$ X is poly time equivalent to Circuit SAT.