Computational Intractability

P : class of problems that have poly-time algorithms

- model independent

We will work with decision problems

↳ Equivalent to search versions

Search

Given $G(V,E)$ & u,v → find The shortest path from u to v

Decision

Given $G(V,E)$, u,v,i

– Answer "yes" if the i^{th} bit in the shortest path from u to v is a $\underline{1}$

Languages $L \subseteq \{0,1\}^*$ are abstractions of computational problems

$L \in P$ if there is a polytime algorithm A

↳ Turing machine

RAM, ...

s.t $\forall x \in \{0,1\}^*$

if $x \in L$, then $A(x) = 1$

if $x \notin L$, then $A(x) = 0$

Solving vs Verifying

CIRCUIT SAT $= \{ \varphi \mid \exists$ an assignment to the variables of φ s.t $\varphi(x) = 1 \}$

Boolean circuit

* Trivial algorithm: Try all the 2^n assignments

* Verification: if φ is satisfiable, then $\exists$ a witness that can be checked

satisfying assignment ← a witness

NP (Non-deterministic Poly-time)

$L \in NP$ if $\exists$ poly-time algorithm A that takes two inputs s.t $\forall x \in \{0,1\}^*$

* if $x \in L$, then $\exists y \in \{0,1\}^*$ s.t $|y| = |x|^c$ & $A(x,y) = 1$

* if $x \notin L$, then $\forall y \in \{0,1\}^*$ s.t $|y| = |x|^c$ $A(x,y) = 0$

$\exists$ a poly-time verifier A that can be convinced of membership iff $x \in L$

Some examples

- $SAT = \{\phi \mid \phi \text{ is satisfiable}\}$

  witness: satisfying assignment

- $VC = \{(G,k) \mid G \text{ has a VC of size} \leq k\}$

  witness: vertex cover

Not all problems are in NP!

- $PRIMES = \{n \mid n \text{ is a prime number}\}$

  ↳ what is a short certificate to convince primality?

  - PRIMES $\in$ NP (not trivial to show)
  - PRIMES $\in$ P (AKS 2002)
  - $\exists$ easily verifiable certificate to show that n is not prime

- Linear Programming → has a P-time algorithm

$$f = \min \sum_{i=1}^{n} c_i x_i$$

- Check if $f \leq K$

$$\text{s.t.} \sum_{i=1}^{n} a_{ij} x_j \geq b_j$$

$$\forall j \in \{1, 2, .., m\}$$

$$a_{ij}, b_j, c_i \in \mathbb{R}$$

- Not clear why the witness should have a repres. poly in input