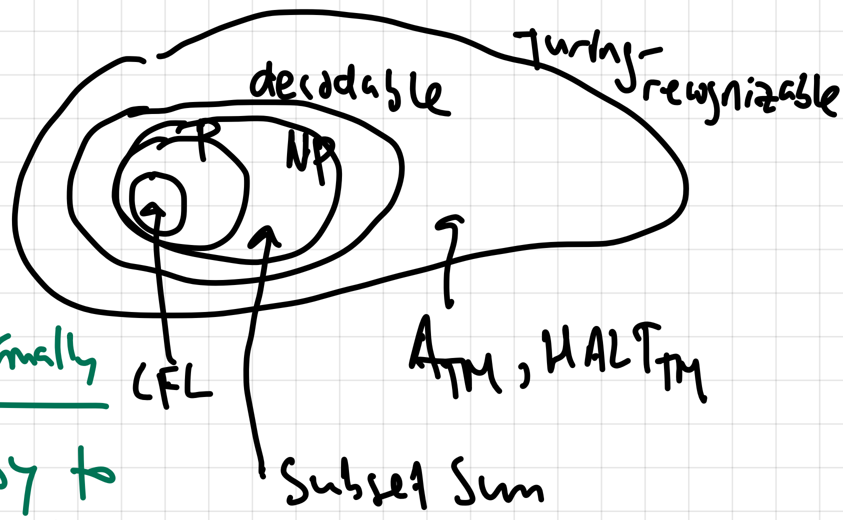
Thu 11/13 | Chapter 7



Last time: P, NP

formally | informally

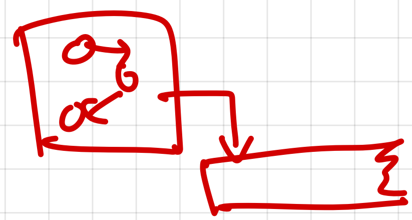
- P: $\bigcup_{k\geq 1} \underbrace{TIME(n^k)}_{\shortparallel}$ — easy to solve

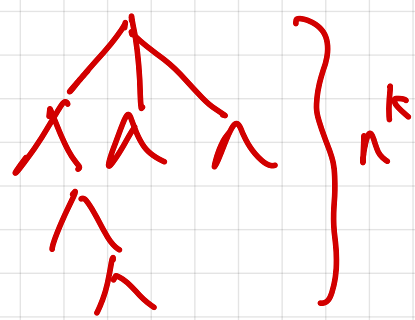
  $\{A \mid \exists\ O(n^k)\text{-time TM that decides } A\}$

- NP: $\bigcup_{k\geq 1} NTIME(n^k)$ — easy to verify

  $= \{A \mid \exists \text{ poly-time verifier for } A\}$

$TIME(n) \subseteq TIME(n^2) \subseteq TIME(n^3) \subseteq \ldots$





To show $A \in P$: give a poly-time ALG

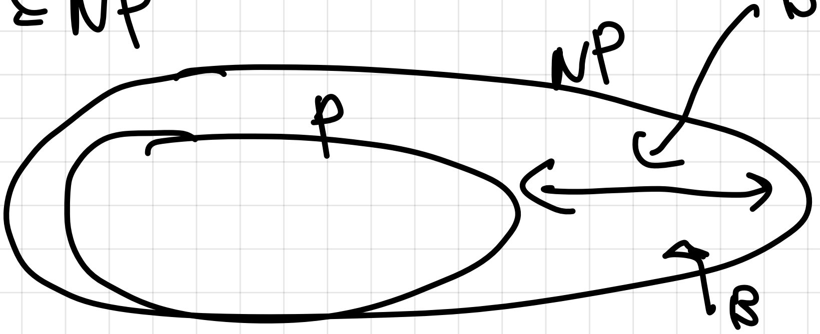
(RELPRIME, PATH, COMP SSO)

To show $A \in NP$: give a poly-time verifier

(Clique, Subset Sum)

Known: $P \subseteq NP$

Big question: Does P=NP?



Millennium Prize Problem: $1 million

Super goal: Show that some problem B satisfies

$$\underbrace{B \in NP}_{\text{easy}} \quad \text{and} \quad \underbrace{B \notin P}_{\text{hard!}}$$

Our goal: Show $B \in NP$ and $A \leq_p B$ for some problem A.

"is polynomial-time reducible to"

formally

$A \leq_p B$ $\exists$ poly-time function f:

$\forall w$: $w \in A \rightarrow f(w) \in B$

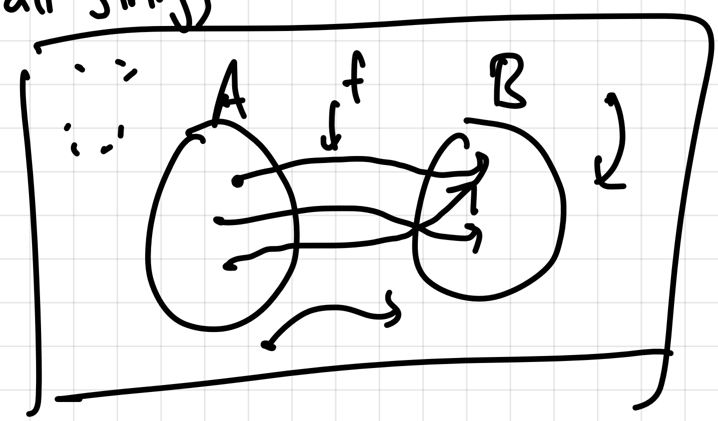
$w \notin A \rightarrow f(w) \notin B$

informally

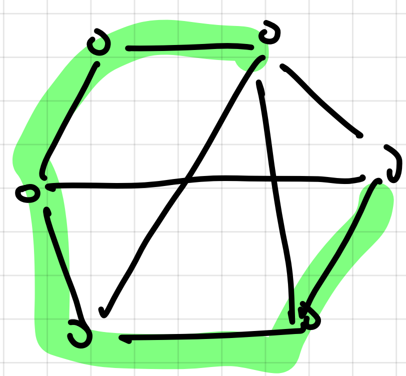
"B is at least as hard as A"

"$A \notin P \Rightarrow B \notin P$"

all strings



Ex 1: $A \leq_p B$

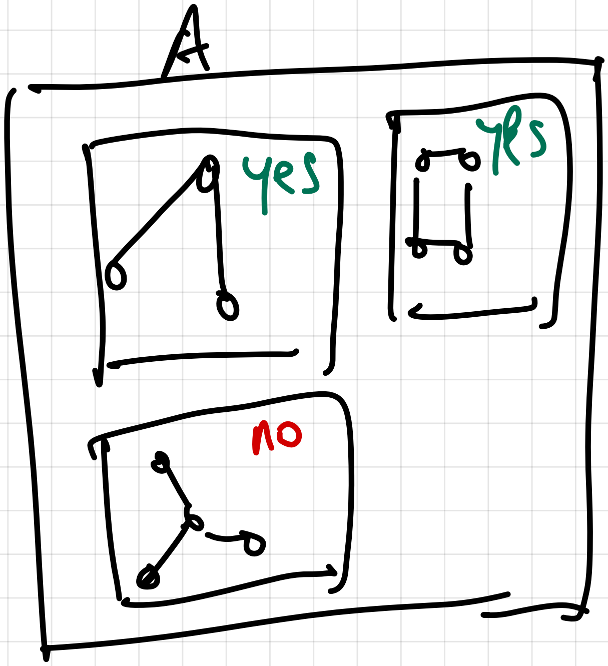


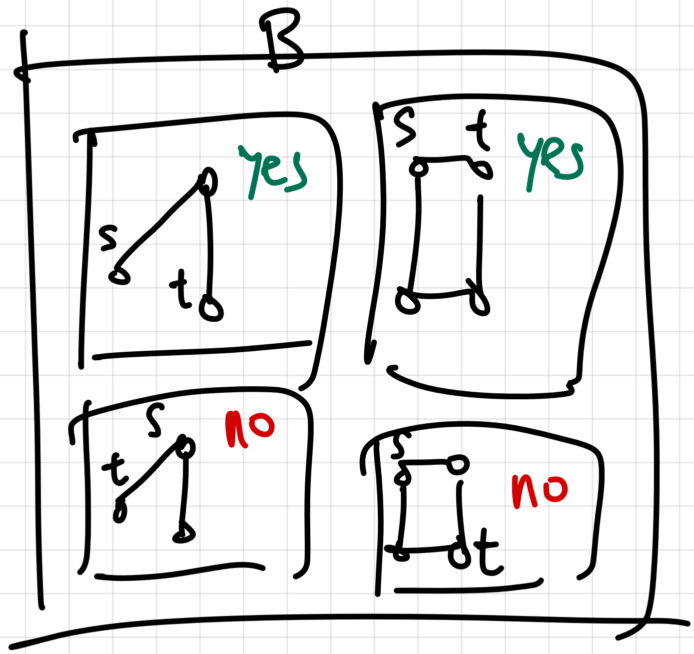
(HP)

A Hamiltonian Path contains every vertex exactly once.

$$A = \{ \langle G \rangle \mid G \text{ has a HP} \}$$

$$B = \{ \langle G, \overset{\text{vertices in } G}{s, t} \rangle \mid G \text{ has an } \underbrace{s \to t \text{ HP}}_{\text{HP from } s \text{ to } t} \}$$





Our goal: translate/transform any instance X of A into an instance f(X) of B (in poly time)

"reduction from A to B"

s.t. (1) X is a "yes" instance of A

→ f(X) ↓ of B

(2) X is a "no" ______ A

→ f(X) ↓ of B

Attempt #1 (incorrect):

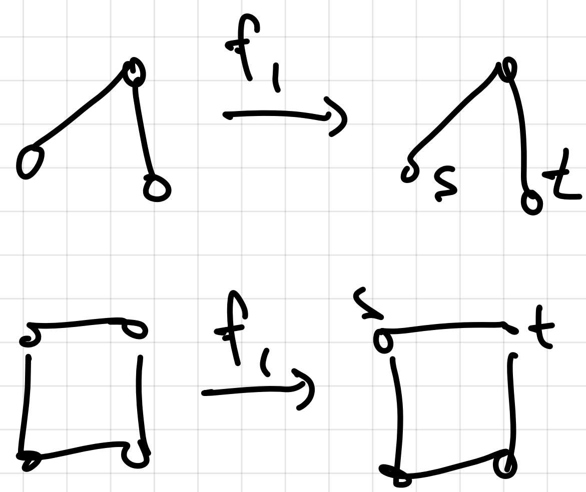
instance of A

$f_1(G)$

$G' = G$

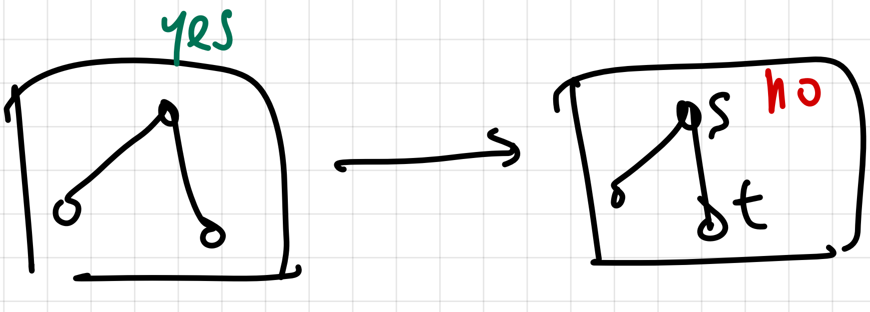
s,t = arbitrary vertices in G

return $\underbrace{\langle G', s, t \rangle}_{\text{instance of } B}$



1. want: G has HP $\Rightarrow$ G' has $s \to t$ HP

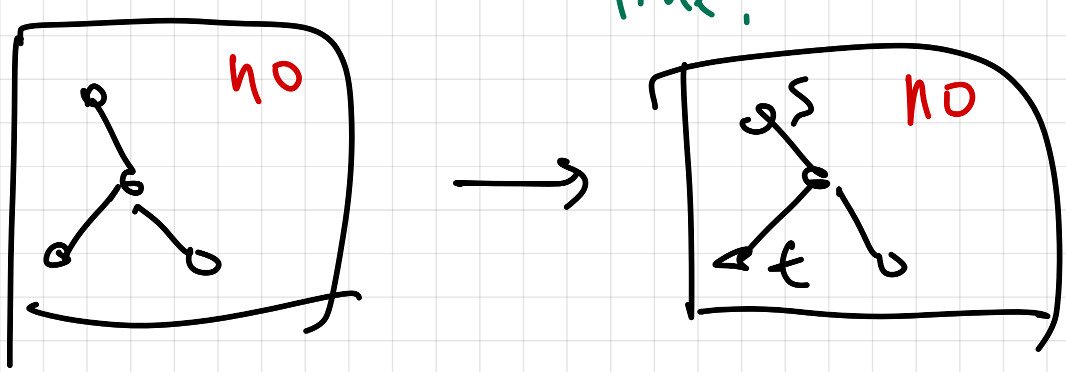
Problem/Counterexample:



2. want: G does not have HP $\Rightarrow$ G' does not have an $s \to t$ HP

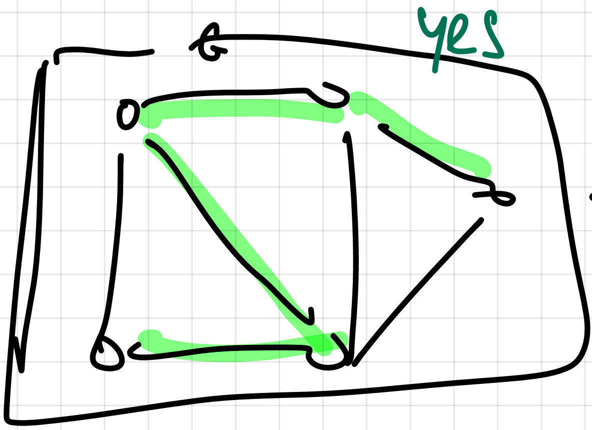
$\Leftarrow$

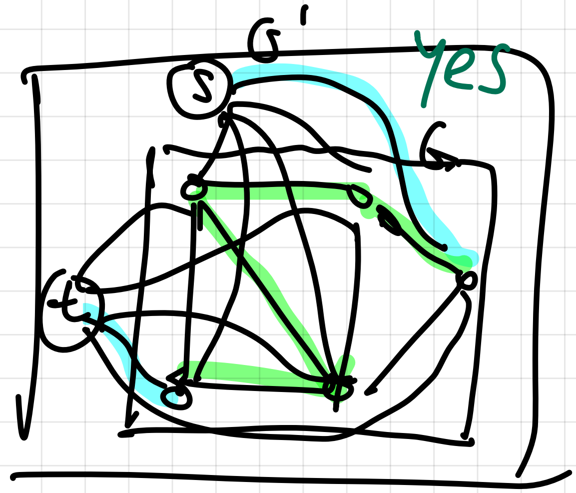
True!



Attempt #2 (correct):

ideally: if G has HP P, let s,t = endpoints of P





f(G):

G' = G

add two vertices s, t to G'

for each vertex u in G:

  add edges {s, u}, {t, u} to G'

return $\langle G', s, t \rangle$

(1) G has HP P

⇒ we can construct an s→t HP in G' by taking P and adding two of the new edges ({s, one endpoint of P} / {t, other endpoint of P})

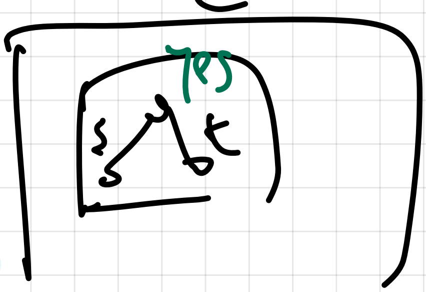
(2) G does not have HP

⇒ G' does not have s→t HP

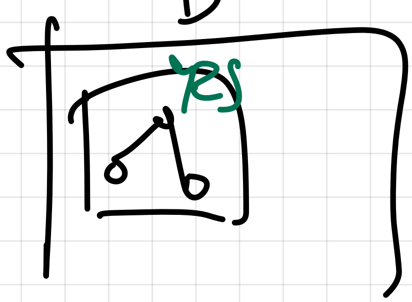
Example 2:

$$\overbrace{\left\{\langle G, s, t\rangle \;\middle|\; \begin{matrix}\text{G has an}\\ \text{s→t HP}\end{matrix}\right\}}^{C} \le_p \underbrace{\left\{\langle G\rangle \;\middle|\; \begin{matrix}\text{G has}\\ \text{a HP}\end{matrix}\right\}}_{D}$$

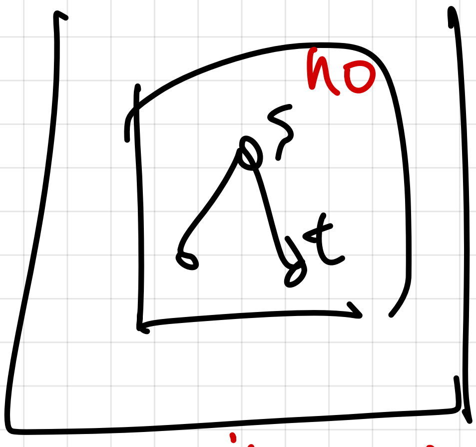
C

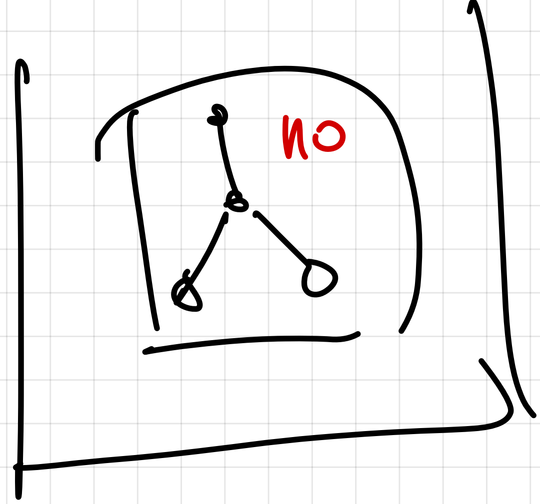


D



D





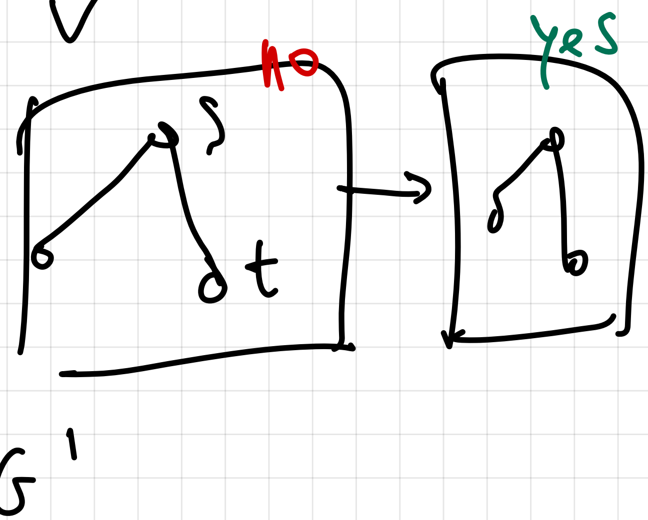
Attempt #1 (incorrect):

f(G, s, t):

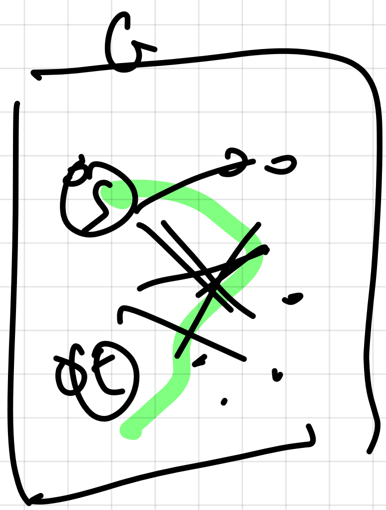
return G' = G

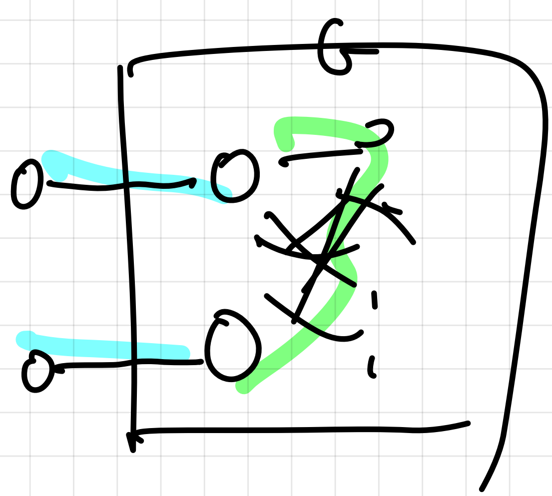
① ✓

②



Attempt #2 (correct):





yes ⇒ yes

no ⇒ no