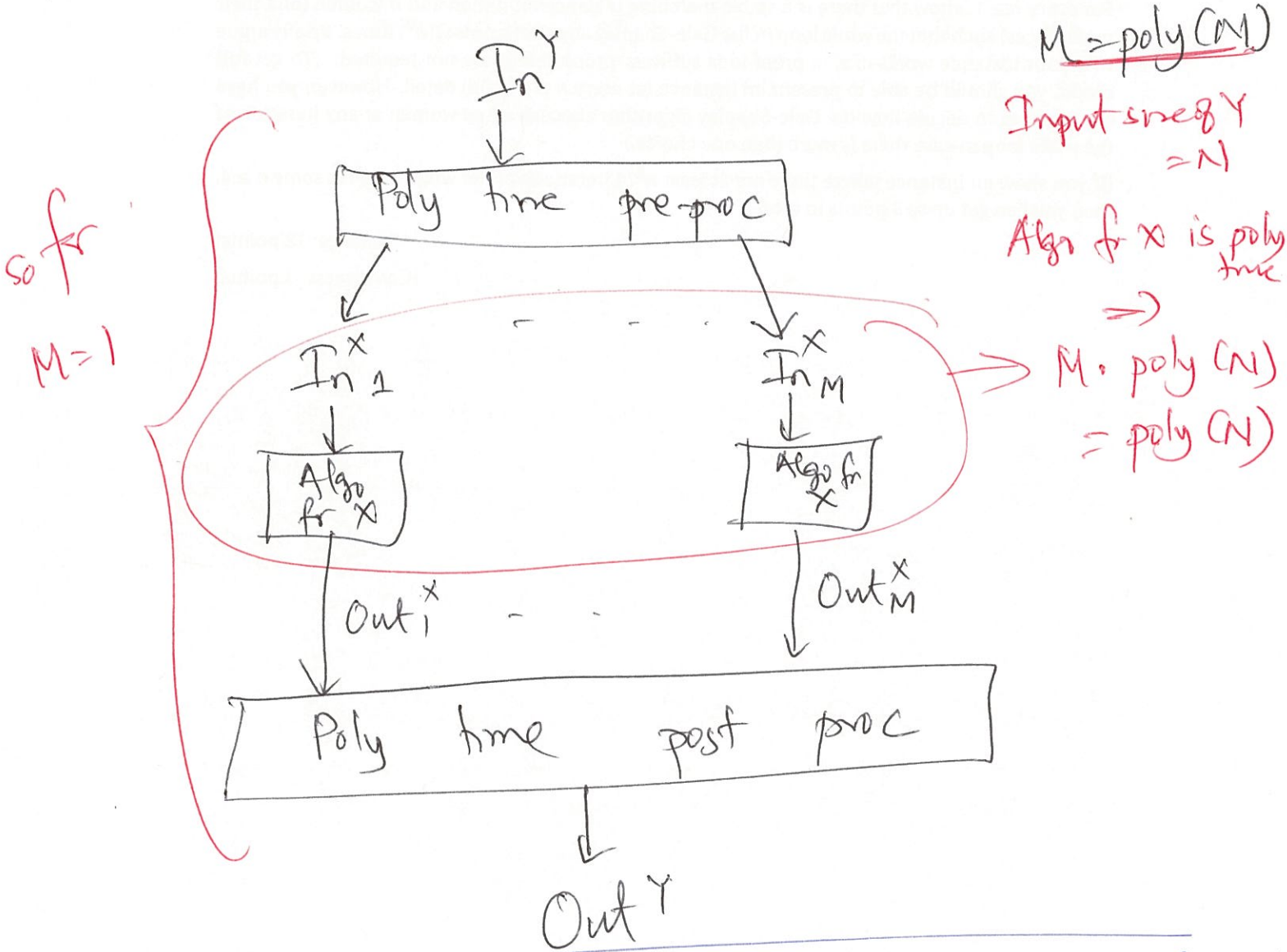
Nov 30

$Y \leq_p X$

→ Y is poly time reducible to X

≡ ∃ a poly time reduc from Y to X

Solve: In^Y - - - - → Out^Y



Example: HW 2 Q2 $\leq_p$ Stable matching (M=1)

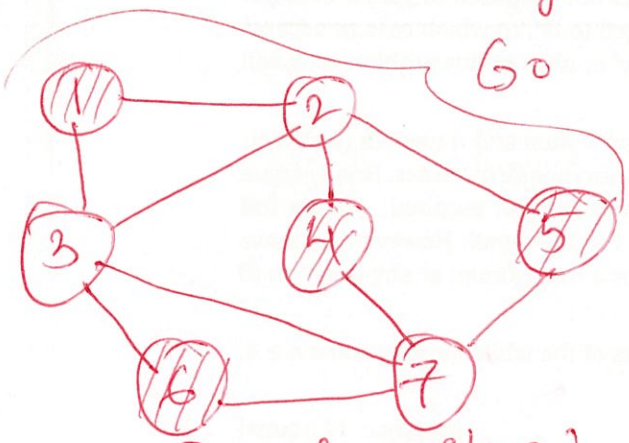
Going forward: ONLY consider problems with Boolean Output.

Problem: Independent Set (IS)

$G = (V, E)$

(Q1 HW7 special case of G being a path)

Def: An IS of G is a subset $S \subseteq V$ s.t NO edges exist between ANY $u \neq v \in V$



G_0

$\{1,4\}$ ✓ $\{3,7\}$ ✗

$\{1,4,7\}$ ✗ $\{3,4,5\}$ ✓

$\{1,4,5,6\}$ ✓ $(= |V|)$

Formal problem: **Input:** $G = (V, E)$; $0 \leq k \leq n$

Output: TRUE iff $\exists$ an IS of size $\geq k$.

Examples: $G_0; 2$ ✓ $G_0; 3$ ✓ $G_0; 4$ ✓ $G_0; 5$ ✗

Note: Every subset of an IS is also an IS

Problem 2: Vertex Cover

$G = (V, E)$; $C \subseteq V$ is a vertex cover ($C \in VC$) if ALL edges $e \in E$ has at least one endpoint in C.

Examples: G_0 : $\{1,2,3,4,5,6,7\}$ ✓

$\{1,2,3,4,5,6\}$ ✓ $\{1,2,6,7\}$ ✓

$\{3,7\}$ ✓ $\{1,7\}$ ✗ $\{1,2,7\}$ ✗

Lemma: Let $G = (V, E)$. $S \subseteq V$ is an IS $\iff$ $V \setminus S$ is a VC

Formal problem: **Input:** $G = (V, E)$; $0 \leq k \leq n$

Output: TRUE iff G has a VC of size $\leq k$.

Examples: $G_0; 6$ ✓ $G_0; 3$ ✓ $G_0; 2$ ✗

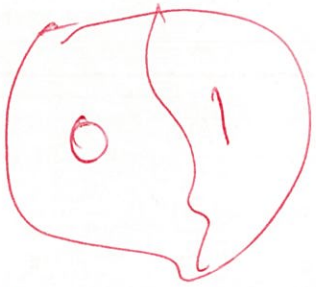
THM: (1) $IS \leq_p VC$ (2) $VC \leq_p IS$

↑ Pf on Friday

Recall: Problem Y with output $\{0,1\}$

$\equiv Y$ is a subset of all possible inputs with output = 1.

{note: if $w \notin Y \Rightarrow$ output for $Y = 0$}



Algorithmic problem: Given an input w

{Eg: $w = G; k$
Y = set of all G with an IS of size $\geq k$.

is $w \stackrel{?}{\in} Y$

Def: Given an algo A & input w
$A(w)$ as its output.
$\in \{0,1\}$

Def: An algo A solves the problem Y if
$\forall$ inputs w $\quad A(w) = 1 \iff w \in Y$

Recall: A is poly time if $\forall$ inputs w, $A(w)$ can be computed in poly $(|w|)$ time

$|w| = N$
poly $(N) = N^c$ for some constant c

DEF: $\mathcal{P}$: set of all problems that can be solved by a poly time algo.

Q: Is the shortest path problem $\in \mathcal{P}$
(i/p: G, s,t o/p: cost of shortest s-t path?)

NO: since output is not in $\{0,1\}$

↳ i/p: G, s, t, k o/p: TRUE if $\exists$ an s-t path of cost $\leq k$.

Efficient verification (book: certification)

Q: Is $w \in Y$?

Eg: Y is IS

$w = G; k$

↳ A certificate/witness is a string that supports the claim that $w \in Y$

Def: B is an efficient verifier for Y if

(1) B takes as input w, t & output $B(w,t) \in \{0,1\}$
(w: input, t: witness)

(2) B runs in time poly $(|w|)$

(3) $w \in Y \iff \exists$ a string/witness t s.t (i) $|t| \leq$ poly $(|w|)$ AND (ii) $B(w,t) = 1$

Eg. Y = IS i/p: $G; k$

Witness: $S \subseteq V$ of size $|S| = k$

Q: $\exists$ an efficient verifier