Certificate

Decision Problem

Is there an object that satisfying some condition?

- A certificate is a specif object corresponding to a <u>yes-input</u> such that it can be used to show the validity of that yes-input.

only yes-input needs a certificate.

verifying a certificate

Given a yes-input and its corresponding certificate, by making use of this certificate one verify that the input is actually a yes-input.

The class NP

The class of all problems that can be verified in polynomial time.

$\boxed{\text{NP} :- \text{Nondeterministic Polynomial}}$

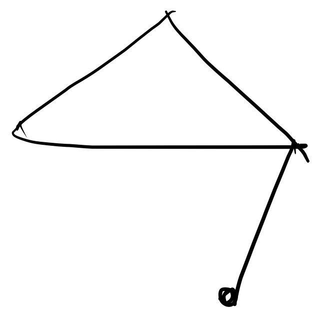
Ex^m **Hamitonian cycle problem (HC)**

Input: An undirected graph G(V, E)

output: Find a cycle that contains each vertex exactly once.

Decision version: (HC-D)

Does G contains a Hamiltonial cycle?



no Hamiltonial cycle exists.

no-input.

Show that HC-D is in NP.

certificate: An ordering of the vertices (corresponding to the ordering along a Hamiltonian cycle)

$$v_{i_1}, v_{i_2}, \ldots\ldots, v_{i_n}$$

verification:

check $v_{i_j} \neq v_{i_l}$ for $j \neq l$

check $(v_{i_j}, v_{i_{j+1}})$ is an edge in the graph

check (v_{i_n}, v_{i_1}) is an edge in " "

verification takes polynomial time

so HC-D is in NP.

Note: certificate is not unique.

Ex^m vertex cover problem is in NP

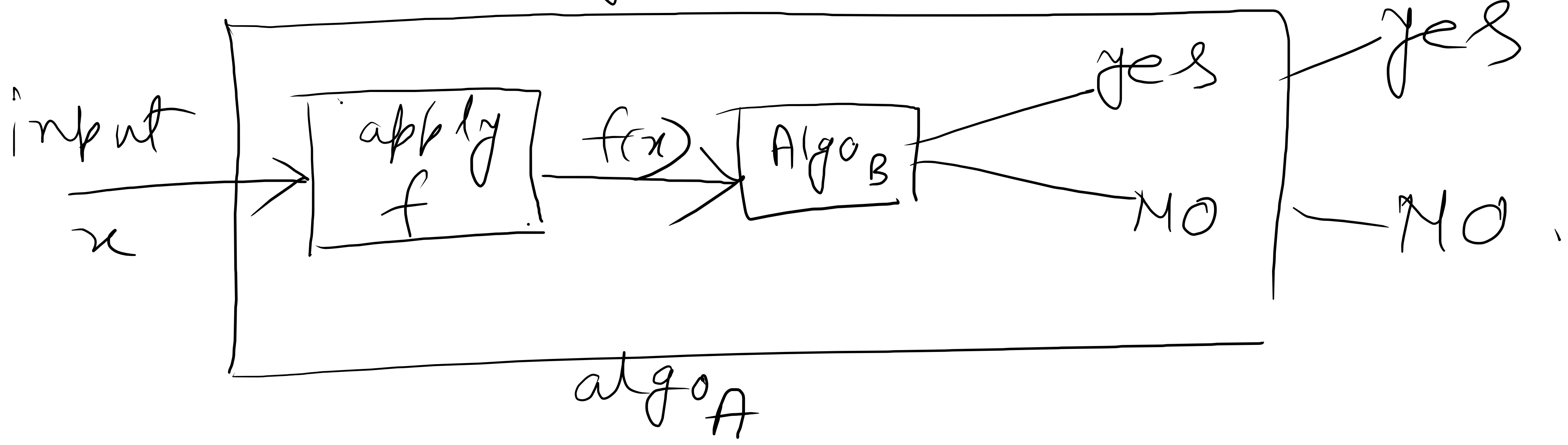
H.W.

Polonaial time reduction

What is a reduction?

Let A and B be two decision problems.

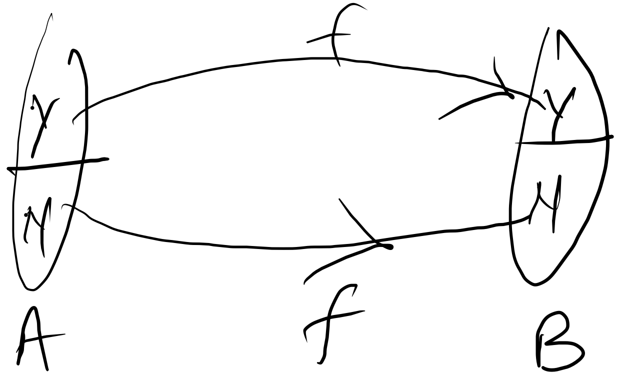
In reduction, we find a transformation f from A to B so that there will be algorithms $algo_A$ for solving A and $Algo_B$ for solving B and the algorithm $Algo_B$ can be a part of $Algo_A$ to solve A.



Polynomial time reduction

A polynomial time reduction from A to B is a transformation f such that:

- f transforms x of A into an instance $f(x)$ of B and x is an yes-instance iff $f(x)$ is an yes-instance.

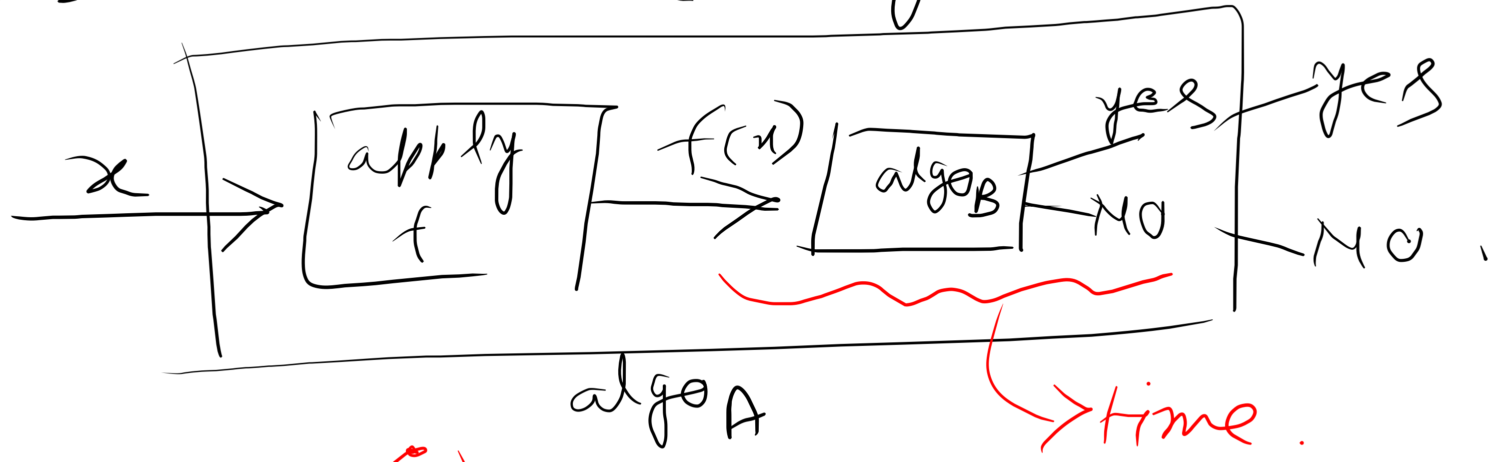


- $f(x)$ is computable in polynomial time (in size of x)

A is polynomial time reducible to B and is denoted by $\boxed{A \le_p B}$

Thm $A \le_p B$ and if B is solvable in polynomial time then A is solvable in polynomial time.

Pictorially



$Algo_B$ takes $O(|f(x)|^c)$ time.

$x \to f(x)$ time: $O(|x|^k)$

total time: $O(|x|^k + |f(x)|^c)$

relation between $|x|$ and $|f(x)|$

$|f(x)|$ outputsize $|x|^k$ running time $\Big\}$ $|f(x)| \le |x|^k$