

22.2.2

Certifiers/Verifiers

Certifiers

Definition 22.1.

An algorithm $C(\cdot, \cdot)$ is a certifier for problem X if the following two conditions hold:

- For every $s \in X$ there is some string t such that $C(s, t) = \text{"yes"}$
- If $s \notin X$, $C(s, t) = \text{"no"}$ for every t .

The string t is called a **certificate** or **proof** for s .

Efficient (polynomial time) Certifiers

Definition 22.2 (Efficient Certifier.).

A certifier C is an efficient certifier for problem X if there is a polynomial $p(\cdot)$ such that the following conditions hold:

- For every $s \in X$ there is some string t such that $C(s, t) = \text{"yes"}$ and $|t| \leq p(|s|)$.
- If $s \notin X$, $C(s, t) = \text{"no"}$ for every t .
- $C(\cdot, \cdot)$ runs in polynomial time in the size of s .

Example: Independent Set

- 1 **Problem:** Does $G = (V, E)$ have an independent set of size $\geq k$?
 - 1 **Certificate:** Set $S \subseteq V$.
 - 2 **Certifier:** Check $|S| \geq k$ and no pair of vertices in S is connected by an edge.

THE END

...

(for now)