The class NP of languages is:

<u>intuitively</u>: any language L where ~~string~~ a string $w \in L$ iff there is a certificate that a <u>checker</u> says "yes" to.
└ scalable.

e.g. "G,k" $\in$ k-Clique iff $\exists C$ "G,k,C" $\in$ clique_eval

e.g. "φ" $\in$ formula_sat iff $\exists p$ "φ,p" $\in$ formula_eval

certificate   checker

i.e. a yes/no question requiring search for a way to satisfy a checker

└ e.g. a truth assignment   i.e. a certificate
a set of k vertices

<u>Formally</u>

$L \in NP$ means $\forall w \in \Sigma^*$ $w \in L$ iff $\exists C$ $T(w,C)$ for some ~~scalable~~ polynomial-time bounded checker $T()$.

To show a language $L \in NP$:

define a polynomial-time solvable checker $\tau(w, c)$

s.t. $w \in L$ iff $\exists c\ \tau(w, c)$

where c must be polynomial in size relative to $|w|$

the "certificate", what you are searching for

i.e. show that checking $w \in L$ is essentially a search for a certificate that checks easily once found.

Example PARTITION: Given a multiset M (a set where duplicates are allowed) of natural numbers, can M be divided into M_1 & M_2 that have the same sum?

PARTITION = { "M" | M can be divided into M_1 & M_2 of same sum }

partition_check = { "M, M_1, M_2" | does $M = M_1 \cup M_2$ and $sum(M_1) = sum(M_2)$? } $\in P$

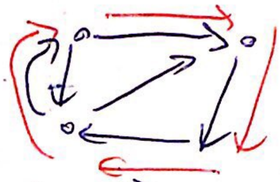
"M" $\in$ PARTITION iff $\exists M_1, M_2$ s.t. "M, M_1, M_2" $\in$ partition_check

$\exists c$ $\tau(w, c)$

$\therefore$ PARTITION $\in NP$

Example A graph $G=(V,E)$ has a Hamiltonian path if there is a cycle (a path of edges from a vertex back to itself) containing each $v \in V$ exactly once.

Given G, is there a Hamiltonian path?



HAM_PATH $= \{$ "G" $\mid \exists P$ a Ham. path in $G\}$

HAM-PATH_CHECK $= \{$ "G, P" $\mid$ where P is a path in G, P is a Hamiltonian path in $G\}$ $\in P$

"G" $\in$ HAM-PATH iff $\exists P$ "G,P" $\in$ Ham-path_check

$\therefore$ HAM-PATH $\in NP$

Example

Given three sets S, T, and U, and a compatibility relation R, a subset of $S \times T \times U$ of triples.

Is there a subset of R whose triples use each member of S, T, and U exactly once?

Formalize and show $\in NP$ as exercise.