Theorem (Used by many sources as the definition of NP)

A language A belongs to NP if and only if there are a polynomial-time decidable relation $R(x,y)$ and a polynomial $q(n)$ such that for all $x \in \Sigma^*$:

$$x \in A \iff (\exists y \in \Sigma^* : |y| \leq q(|x|))\, R(x,y).$$

Proof ($\Leftarrow$): Given R decidable in some polynomial time $p(N)$ and the polynomial $q(n)$, design an NTM like so:

↓ input x

N: $\boxed{\text{Guess } y : |y| \leq q(|x|)}$ nondeterministic, but takes only $q(n)$ time ($n = |x|$)

↓

$\boxed{\text{Use a DTM } M_R \text{ that runs in time } p(N) \text{ to decide } R(x,y)}$ → if yes, accept x → if not, well, some other y might work. Or not...!

Then $L(N) = A$, and the time needed is $\lesssim q(n) + p(N) \leq q(n) + p(\underbrace{n + q(n)}_{|\langle x, y\rangle|})$

The composition of two polynomials is a polynomial, so the time needed by N is bounded by a polynomial. $\therefore A \in NP$.

($\Rightarrow$): By $A \in NP$, we can take an NTM N_A running in some polynomial time $p(n)$ s.t. $L(N_A) = A$. Now use the predicate $T(N_A, x, \vec{c})$ from last lecture. Then for all $x \in \Sigma^*$:

$$x \in A \iff (\exists \vec{c}) : |\vec{c}| \leq p(n)^2\,) \, T(N_A, \vec{x}, \vec{c}).$$

How long is $|\vec{c}|$? At most $p(|x|)$ steps. Each step has an ID $I = \langle q, w, i\rangle$
$|I| \approx |q| + |w| + |i| \leq \log|Q| + n + p(n) + \log(n + p(n)) = O(p(n))$. $|\vec{c}| = O(p(n)^2)$ ⊠

(*) If we remove the condition $|y| \le q(|x|)$ for some polynomial q, what class (bigger than NP) is thereby characterized?

<u>Theorem'</u>: A language A is <u>in RE</u> if and only if there is a $\underbrace{\text{polynomial-time}}_{\text{wlog even linear-time}}$ decidable predicate $R(x,y)$ s.t. for all $x \in \Sigma^*$,

$$\boxed{x \in A \iff (\exists y \in \Sigma^*)\, R(x,y)}$$

this is what matters most → no bound on $|y|$.

The quotes mean that these will <u>not</u> be used as formal notations

Intuitively stated:

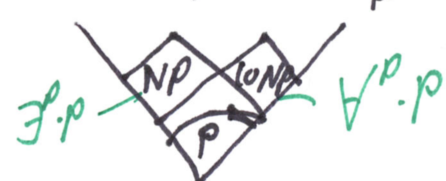
"$\boxed{RE = \exists \cdot REC} = \exists \cdot \text{Lintime}$, $\boxed{NP = \exists^{poly} \cdot P} = \exists^{poly} \cdot \text{Lintime}$"

Since ALL_{TM} is not c.e., nor co-c.e., it cannot be defined with one $\exists$ quantifier on a decidable predicate. "Best" is:

$$\langle M \rangle \in ALL_{TM} \iff \underline{(\forall x \in \Sigma^*)(\exists \vec{c})}\, T(\langle M \rangle, x, \vec{c}).$$

two quantifiers, $\forall\exists$.

A <u>DTM</u> M_R that decides $R(x,y)$ is called a (poly-time) <u>verifier</u> of potential <u>witnesses</u> y <u>for</u> $x \in A$. R itself is then a <u>witness</u> <u>predicate</u>.



[There is an associated topic of Oracles and Turing Reductions skipped for now.]

How about $E_{TM} = \{\langle M \rangle : L(M) = \emptyset\}$?

$$\langle M \rangle \in E_{TM} \iff (\forall x \in \Sigma^*)(\forall \vec{c})\, \neg T(\langle M \rangle, x, \vec{c})$$

"There are no accepting comp's on any x".

Two $\forall\forall$ quantifiers, but they can combine into one → form $\forall z\, R(M,z) \equiv \neg(\exists z)\, \tilde{R}(M,z) \equiv \neg(RE)$.

$$\boxed{\therefore \text{co-}RE = \forall \cdot REC}$$

$\therefore E_{TM} \in$ <u>co-RE</u>.