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 $N$ so:

1. input $x$
2. Guess $y$: $|y| \leq q(|x|)$
3. Use a TM $M_R$ that runs in time $p(n)$ to decide $R(x, y)$

If yes, accept $x$

If not, well, some other $y$ might work or not...

Then $N = A$, and the time needed is $t \leq q(n) + p(n) \leq q(n) + p(n + q(n))$.

The composition of two polynomials is a polynomial, so the time needed by $N$ is bounded by a polynomial ($\Rightarrow$).

($\Rightarrow$): By $A \in$ NP, we can take an NTM $N_A$ running in polynomial time $p(n)$ s.t. $L(N_A) = A$. Now use the predicate $T(N_A, x, z)$ from last lecture.

Then:

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

How long is $|z|$? At most $p(|x|)$ steps. Each step has an ID $<q, W, i>$: $|z| \leq (q + |W| + i) \leq \log(q) + n + p(n) + \log(npw) = O(p(n)).$ $|z| = O(p(n)^2)$.
If we remove the condition $|y| \leq \varphi(|x|)$ for some polynomial, what class (bigger than $NP$) is thereby characterized?

**Theorem:** A language $A$ is in $RE$ if and only if there is a polynomial-time decidable predicate $R(x, y)$ such that for all $x \in \Sigma^*$,

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

This is what matters most to no bound on $|y|$. Wlog even linear-time

Intuitively stated:

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

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

$$\langle M \rangle \in \text{ALL}_{TM} \iff (\forall x \in \Sigma^*) (\exists \vec{z}) T(\langle M \rangle, x, \vec{z}).$$

Two quantifiers, $\forall \exists$.

How about $\text{ETM} = \exists \langle M \rangle: L(M) = \emptyset$?

$$\langle M \rangle \in \text{ETM} \iff (\forall x \in \Sigma^*) (\forall \vec{z}) \neg T(\langle M \rangle, x, \vec{z})$$

"There are no accepting computations."

Two $\forall$ quantifiers, but they can combine into one $\forall x R(M, z) \equiv \neg (\exists z) \neg R(M, z) \equiv \neg (\text{RE}).$ \quad$\therefore \text{ETM} \subseteq \neg \text{RE}.$

A $\text{DIM} M$ that decides $R(x, y)$ is called a (poly-time) verifier of potential witnesses $y$ for $x \in A$.

$R$ itself is then a witness predicate.

There is an associated topic of oracles and Turing reductions, skipped for now.