# NP-pairs & Co.

A **disjoint NP-pair** is a pair (A, B) of nonempty sets A and B such that A, B ∈ NP and A∩B = ∅.
A **separator** is a set S such that $A \subseteq S$ and $B \subseteq \bar{S}$.

(A, B) is **many-one reducible** in polynomial-time to (C, D) ($(A, B) \leq_m^{pp} (C, D)$), if there exists a polynomial-time computable function f such that f(A) ⊆ C and f(B) ⊆ D.

(A, B) is **Turing reducible** in polynomial-time to (C, D) ($(A, B) \leq_T^{pp} (C, D)$), if there exists a polynomial-time oracle Turing machine M such that for every separator S of (C, D), L(M,S) is a separator of (A, B).

The **canonical pair** of f is the disjoint NP-pair $(SAT^*, REF_f)$:

$$\begin{aligned} \mathrm{SAT}^* &= \{(x, 0^n) \mid x \in \mathrm{SAT}\} \\ \mathrm{REF}_f &= \{(x, 0^n) \mid \neg x \in \mathrm{TAUT} \text{ and } \exists y[|y| \leq n \text{ and } f(y) = \neg x]\}. \end{aligned}$$

**Theorem 1.** For every disjoint NP-pair (A, B) there exists a proof system f such that $(SAT^*, REF_f) \equiv_m^{pp} (A, B)$.

Let f and f' be two propositional proof systems. We say that f simulates f' if there is a polynomial p and function $h : \Sigma^* \to \Sigma^*$ such that for every $w \in \Sigma^*$, $f(h(w)) = f'(w)$ and $|h(w)| \leq p(|w|)$.
A proof system is optimal if it simulates every other proof system.

One proof system $\Pi_w$ is **simulated** by another one $\Pi_s$ if the shortest proof for every tautology in $\Pi_s$ is at most polynomially longer than its shortest proof in $\Pi_w$.
The notion of **p-simulation** is similar, but requires also a polynomial-time computable function for translating the proofs from $\Pi_w$ to $\Pi_s$.
A **(p-)optimal propositional proof system** is one that (p-)simulates all other propositional proof systems.

An **acceptor** for a language L is an algorithm that answers 1 for $x \in L$ and does not stop otherwise.
An **acceptor O is optimal** if for any other (correct) acceptor A, for every x ∈ L, the acceptor O stops on x in time bounded by a polynomial in |x| and the time taken by A(x).

**Theorem 1.** Optimal acceptors for TAUT exist <=> p-optimal proof systems for TAUT exist.
(TAUT - language of all propositional tautologies)