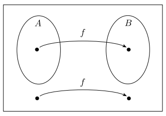
TM (3), Decidability (4)

- (**TM**) $M = (Q, \underbrace{\Sigma}_{\text{input}} \subseteq \Gamma, \underbrace{\Gamma}_{\text{tape}}, \delta, q_0, q_{\text{accept}}, q_{\text{reject}})$, where $\sqcup \in \Gamma$ (**blank**), $\sqcup \notin \Sigma$, $q_{\text{reject}} \neq q_{\text{accept}}$, and $\delta : Q \times \Gamma \longrightarrow Q \times \Gamma \times \{\text{L}, \text{R}\}$
- (**unrec.**) $\overline{A_{TM}}$, $\overline{EQ_{\mathsf{TM}}}$, EQ_{CFG}, $\overline{HALT_{\mathsf{TM}}}$, $\text{REGULAR}_{\mathsf{TM}} = \{M \text{ is a TM and } L(M) \text{ is regular}\}$, E_{TM}, $EQ_{\mathsf{TM}} = \{M_1 \text{ and } M_2 \text{ are TMs and } L(M_1) = L(M_2)\}$
- (**rec.**) accepts if $w \in L$, rejects/loops if $w \notin L$.
  - There exists some languages that are not rec.
  - (**co-TR**) if its complement is rec.
  - Every inf. rec. lang. has an inf. dec. subset.
  - (**rec. but not undec**)A_{TM}, $HALT_{TM} = \{\langle M, w\rangle \mid M \text{ is a TM that halts on } w\}$, $D = \{p \mid p \text{ is an int. poly. with an int. root}\}$, $\overline{EQ_{\mathsf{CFG}}}$, $\overline{E_{\mathsf{TM}}}$
- (**dec.**) accepts if $w \in L$, rejects if $w \notin L$.
  - A_{DFA}, A_{NFA}, A_{REX}, E_{DFA}, EQ_{DFA}, A_{CFG}, E_{CFG}, every CFL, every finite lang., A_{LBA}, ALL_{DFA}, $A\varepsilon_{\mathsf{CFG}}$,
- $L \text{ is dec.} \iff L \text{ is rec.} \land L \text{ is co-TR} \iff \exists \text{TM decides } L.$
- (**decider**) TM that halts on all inputs.
- (**Rice**) Let P be a lang. of TM desc., such that (*i*) P is nontrivial (not empty and not all TM desc.) and (*ii*) for each two TM M_1 and M_2, we have $L(M_1) = L(M_2) \implies (\langle M_1\rangle \in P \iff \langle M_2\rangle \in P)$. Then P is undecidable.

Reducibility (5)

- $f : \Sigma^* \to \Sigma^*$ is **computable** if there exists a TM M s.t. for every $w \in \Sigma^*$, M halts on w and outputs $f(w)$ on its tape.



- A is **m. reducible** B (denoted by $A \leq_{\text{m}} B$), if there is a comp. func. $f : \Sigma^* \to \Sigma^*$ s.t. for every w, we have $w \in A \iff f(w) \in B$. (Such f is called the **m. reduction** from A to B.)
- (5.22) If $A \leq_{\text{m}} B$ and B is dec., then A is dec.
- (5.23) If $A \leq_{\text{m}} B$ and A is undec., then B is undec.
- (5.28) If $A \leq_{\text{m}} B$ and B is rec., then A is rec.
- (5.29) If $A \leq_{\text{m}} B$ and A is not rec., then B is not rec.
- (e5.6) If $A \leq_{\text{m}} B$ and $B \leq_{\text{m}} C$, then $A \leq_{\text{m}} C$.

Complexity (7)

- ((**Run. time**) decider M is a $f(n)$**-time TM**.) $f : \mathbb{N} \to \mathbb{N}$, where $f(n)$ is the max. num. of steps that DTM (or NTM) M takes on any n-length input (and any branch of any n-length input. resp.).
- TIME$(t(n)) = \{L \mid L \text{ is dec. by an } O(t(n))\text{-time DTM}\}$.
- NTIME$(t(n)) = \{L \mid L \text{ is dec. by an } O(t(n))\text{-time NTM}\}$.
- $\text{P} = \bigcup_{k \in \mathbb{N}} \text{TIME}(n^k)$
- (**verifier** for L) TM V s.t. $L = \{w \mid \exists c : V(\langle w, c\rangle) = \text{accept}\}$.
  - (**certificate** for $w \in L$) str. c s.t. $V(\langle w, c\rangle) = \text{accept}$.
- $\text{NP} = \bigcup_{k \in \mathbb{N}} \text{NTIME}(n^k)$ (i.e. lang. decidable by a PT NTM).
- $\text{NP} = \{L \mid L \text{ is decidable by a PT verifier}\}$.
- $\text{P} \subseteq \text{NP}$.
- $\text{CLIQUE} = \{\langle G, k\rangle \mid G \text{ is an undir. g. with a } k\text{-clique}\}$.
- $\text{SUBSET-SUM} = \{\langle S, k\rangle \mid S \text{ is a m. set of int.} \land \exists\, T \subseteq S : \sum_{x \in T} x = k\}$.
- $f : \Sigma^* \to \Sigma^*$ is **PT computable** if there exists a PT TM M s.t. for every $w \in \Sigma^*$, M halts with $f(w)$ on its tape.
- A is **PT (mapping) reducible** to B, denoted $A \leq_P B$, if there exists a PT computable func. $f : \Sigma^* \to \Sigma^*$ s.t. for every $w \in \Sigma^*$, $w \in A \iff f(w) \in B$. (in such case f is called the **PT reduction** of A to B).
  - If $A \leq_P B$ and $B \in \text{P}$, then $A \in \text{P}$.
  - If $A \leq_P B$ and $B \leq_P A$, then A and B are **PT equivalent**, denoted $A \equiv_P B$.
    - $\equiv_P$ is an equivalence relation on NP.
    - $\text{P} \setminus \{\emptyset, \Sigma^*\}$ is an equivalence class of $\equiv_P$.
- B is **NP-complete** if $B \in \text{NP}$, and, $\forall A \in \text{NP}$, $A \leq_P B$.
  - (examples) CLIQUE, SUBSET-SUM, SAT, 3SAT, VERTEX-COVER, HAMPATH, UHAMATH.
- If $B \in \text{NP-complete}$ and $B \in \text{P}$, then $\text{P} = \text{NP}$.
- If $B \in \text{NP-complete}$ and $C \in \text{NP}$ s.t. $B \leq_P C$, then $C \in$ NP-complete.
- If $\text{P} = \text{NP}$, then $\text{NP-complete} = \text{P} = \text{NP}$.