Polynomial hierarchy

Turing reducibility

Let $A, B \subseteq \{0,1\}^*$.

- Turing reducibility: $A \leq_{\mathrm{T}} B$ if there is a oracle TM $M^{(\cdot)}$, such that M^B recognizes A.
  - I.e. $M^B(x)$ stops for all $x \in \{0,1\}^*$ and $M^B(x) = $ true $\Leftrightarrow x \in A$.
- Polynomial-time Turing reducibility: $A \leq_{\mathrm{T}}^{\mathrm{P}} B$ if there is a oracle TM $M^{(\cdot)}$, such that M^B recognizes A in polynomial time.
- Nondeterministic polynomial-time Turing reducibility: $A \leq_{\mathrm{T}}^{\mathrm{NP}} B$ if there is a oracle TM $M^{(\cdot)}$, such that M^B recognizes A in polynomial time.

Example: SAT$^{\mathrm{c}} \leq_{\mathrm{T}}^{\mathrm{P}}$ SAT

Recursive hierarchy

Let $M_1, M_2, \ldots$ be an enumeration of all oracle Turing machines.

- Languages $A, B \subseteq \{0,1\}^*$ are Turing equivalent if $A \leq_{\mathrm{T}} B$ and $B \leq_{\mathrm{T}} A$. Denote $A \equiv_{\mathrm{T}} B$.
  - Let $[A]$ be the equivalence class of $\equiv_{\mathrm{T}}$ containing A.
- The Turing jump of a language A is

$$A' = \{i \mid M_i^A(i) \text{ stops}\}$$

  (generalize to sets of languages)
- **Theorem.** $A' \not\leq_{\mathrm{T}} A$.
  - Proof: Diagonalization. Similar to halting problem.
- Denote $\Sigma_0 = [\emptyset]$; $\Sigma_i = \Sigma_{i-1} \cup \Sigma'_{i-1}$. Infinite hierarchy

Exact problems

Consider the following problems

- Given a graph G and an integer k. Does the largest clique of G have the size exactly k?
- Given a propositional formula φ. Does there exist any smaller formula φ', such that $\varphi \equiv \varphi'$?
- Given a set $\varphi_1, \ldots, \varphi_m$ of formulas in CNF and a number k. Do there exist $i_1, \ldots, i_k$, such that $\varphi_{i_1} \wedge \cdots \wedge \varphi_{i_k}$ is unsatisfiable?

These do not seem to be in NP. Short certificates seem hard to find.
But these problems are in PSPACE.

Classes Σ_2^p and Π_2^p

- A language $L \subseteq \{0,1\}^*$ is in Σ_2^p, if there is a polynomial-time DTM M and a polynomial q, such that

$$x \in L \Leftrightarrow \exists u \in \{0,1\}^{q(|x|)} \forall v \in \{0,1\}^{q(|x|)} : M(x,u,v) = \text{true}$$

- A language $L \subseteq \{0,1\}^*$ is in Π_2^p, if there is a polynomial-time DTM M and a polynomial q, such that

$$x \in L \Leftrightarrow \forall u \in \{0,1\}^{q(|x|)} \exists v \in \{0,1\}^{q(|x|)} : M(x,u,v) = \text{true}$$

Clearly, $\Sigma_2^p = \text{co}\Pi_2^p$ and vice versa.
$\text{NP}, \text{coNP} \subseteq \Sigma_2^p \cap \Pi_2^p$

Classes Σ_k^p and Π_k^p

- A language $L \subseteq \{0,1\}^*$ is in Σ_k^p, if there is a polynomial-time DTM M and a polynomial q, such that

$$x \in L \Leftrightarrow \underbrace{\exists v_1 \in \{0,1\}^{q(|x|)} \forall v_2 \in \{0,1\}^{q(|x|)} \dots Q v_k \in \{0,1\}^{q(|x|)}}_{k \text{ quantifiers}} : M(x, v_1, \dots, v_k) = \text{true}$$

- A language $L \subseteq \{0,1\}^*$ is in Π_k^p, if there is a polynomial-time DTM M and a polynomial q, such that

$$x \in L \Leftrightarrow \underbrace{\forall v_1 \in \{0,1\}^{q(|x|)} \exists v_2 \in \{0,1\}^{q(|x|)} \dots Q v_k \in \{0,1\}^{q(|x|)}}_{k \text{ quantifiers}} : M(x, v_1, \dots, v_k) = \text{true}$$

- NP $= \Sigma_1^p$, coNP $= \Pi_1^p$. $\Sigma_k^p, \Pi_k^p \subseteq$ PSPACE.

Polynomial hierarchy

- $\mathsf{PH} = \bigcup_{i \in \mathbb{N}} \Sigma_i^p$.
- As $\Sigma_i^p \subseteq \Pi_{i+1}^p$, we also have $\mathsf{PH} = \bigcup_{i \in \mathbb{N}} \Pi_i^p$.
- Generalization of P $\neq$ NP and NP $\neq$ coNP conjectures: Polynomial hierarchy does not collapse.
  - I.e. there is belief that $\Sigma_i^p \neq \Sigma_{i+1}^p$ for all i.
  - Actually, it is a separate conjecture for each i.

Complete problems for Σ_i^p and Π_i^p

Completeness according to the reduction $\leq_{\mathrm{m}}^{\mathrm{P}}$.

$$\Sigma_i\mathsf{SAT} = \{\exists u_1 \forall u_2 \cdots Q_i u_i : \varphi(u_1, u_2, \ldots, u_i) = \mathsf{true}\}$$
$$\Pi_i\mathsf{SAT} = \{\forall u_1 \exists u_2 \cdots Q_i u_i : \varphi(u_1, u_2, \ldots, u_i) = \mathsf{true}\}$$

where

- φ is a Boolean formula
- $u_1, \ldots, u_i$ are vectors of Boolean variables
- Quantifications are alternating

Theorem. Σ_iSAT is Σ_i^p-complete. Π_iSAT is Π_i^p-complete.

Defining Σ_i^p and Π_i^p through oracle TMs

Theorem. $\Sigma_i^p = \mathsf{NP}^{\Sigma_{i-1}\mathsf{SAT}}$. $\Pi_i^p = \mathsf{co}\Sigma_i^p$.

Collapsing

Theorem. If $\Sigma_i^p = \Pi_i^p$, then $\Sigma_{i+1}^p = \Sigma_i^p$.
Corollary. If $\Sigma_i^p = \Pi_i^p$, then $\Sigma_j^p = \Sigma_i^p$ for all $j \geq i$.

PH-**completeness**

Theorem. If PH has complete problems then polynomial hierarchy collapses.
Corollary. If PH $=$ PSPACE then polynomial hierarchy collapses.

Σ_k^p and game-playing

- Imagine a two-player game with perfect information
  - A set of possible states, a starting state, possible ending states with indication who won and lost.
  - For each state: possible legal moves for both players.
  - Both players always know the state the game is in.
- Can the first player win in k half-moves?

$$\underbrace{\exists \text{my move } \forall \text{opp.'s move } \exists \text{my move } \ldots}_{k \text{ quantifications}} \text{I win!}$$

Exercise. What is the meaning of Π_k^p?

Alternating Turing Machines

- Transition relation similar to NTM-s.
  - For simplicity assume that each configuration of M has exactly two possible successors.
- Each state labeled with $\exists$ or $\forall$.
- Acceptance condition:
  - A configuration with state q_{acc} leads to accepting configuration;
  - A configuration with a state labeled with $\exists$ leads to accepting configuration if at least one of its successors leads to accepting configuration.
  - A configuration with a state labeled with $\forall$ leads to accepting configuration if both of its successors lead to accepting configuration.
  - $x \in \{0,1\}^*$ is accepted if starting configuration with x leads to accepting configuration.

Class ATIME(T), Σ_iATIME(T), Π_iATIME(T)

- $L \in$ ATIME(T) if exists an ATM M and constant c, such that for all $x \in \{0,1\}^*$:
  - All paths in the configuration graph of M, starting from the initial configuration of x, have length at most $c \cdot T(|x|)$;
  - $x \in L$ iff M accepts x.
- $L \in \Sigma_i$TIME(T), if exist M, c satisfying the conditions above, and
  - The initial state of M is labeled with $\exists$;
  - on all paths in the configuration graph of M, there are at most $i - 1$ switches between $\exists$ and $\forall$.
- $L \in \Pi_i$TIME(T), if
  - ...same as above, but initial state is labeled with $\forall$.

Equivalences

Theorems.

- $\Sigma_i^p = \bigcup_c \Sigma_i\mathsf{TIME}(\lambda n.n^c)$
- $\Pi_i^p = \bigcup_c \Pi_i\mathsf{TIME}(\lambda n.n^c)$
- $\bigcup_c \mathsf{ATIME}(\lambda n.n^c) = \mathsf{PSPACE}$

Time-space tradeoffs for SAT

- $L \in \mathsf{TISP}(T, S)$ if exists DTM M that accepts L in time $O(T)$ and in space $O(S)$
- **Theorem.** SAT $\notin \mathsf{TISP}(\lambda n.n^{1.1}, \lambda n.n^{0.1})$.

Lemma on efficiency of reduction

Lemma. If SAT $\in$ TISP$(\lambda n.n^{1.1}, \lambda n.n^{0.1})$ then NTIME$(\lambda n.n) \subseteq$ TISP$(\lambda n.n^{1.1} \cdot polylog(n), \lambda n.n^{0.1} \cdot polylog(n))$.

Claim. If $L \in$ NTIME(T), then L can be recognized by some oblivious NTM in time $\lambda n.T(n) \log T(n)$.

- The head movement only depends on n, not on L;
- Position of head at each step; and previous step when the head was at a certain position, can be computed in time $polylog(n)$.

Claim. If L is recognized in time T by some oblivious NTM, then there exists a reduction f from L, to SAT, such that

- $|f(x)| \in O(T)$;
- Each bit of $f(x)$ can be computed in time $polylog(|x|)$.

Time to alternation

Lemma. $\mathsf{TISP}(n^{12}, n^2) \subseteq \Sigma_2\mathsf{TIME}(n^8)$.

Proof. M accepts x in space $c \cdot |x|^2$ and time $c \cdot |x|^{12}$ iff

- Exist configurations $C_0, C_1, \ldots, C_{c \cdot |x|^6}$ of M, such that
- for each $i \in \{0, \ldots, c \cdot |x|^6\}$
- C_i is reachable from C_{i-1} in $|x|^6$ steps. Also, C_0 and $C_{c \cdot |x|^6}$ are initial and final configurations.

Last check can be made in time $|x|^6$. The configurations take space $|x|^8$.

The Padding Argument

If $\mathbf{CL}_1(f(n))$ and $\mathbf{CL}_2(g(n))$ are complexity classes that are characterized by the resources (time of space) they allow to spend to the machines that accept languages belonging to these classes. The resources are measured by functions $f(n)$ and $g(n)$ respectively (with O-precision), where n is the input size.

Theorem: If $\mathbf{CL}_1(f(n)) \subseteq \mathbf{CL}_2(g(n))$ then $\mathbf{CL}_1(f(n^c)) \subseteq \mathbf{CL}_2(g(n^c))$ for every constant $c \in \mathbb{N}$.
Proof: Let $L \in \mathbf{CL}_1(f(n^c))$ and M be a machine that decides L in $f(n^c)$-time(or space). If $c = 1$, the statement is trivial. Otherwise, if $c \geq 2$, define a new language

$$L' = \{x01^{|x|^c - |x| - 1} \colon \; x \in L\} \; .$$

Padding argument

Define a new machine $M'(y)$ that accepts iff y is in the form $x01^{|x|^c-|x|-1}$ and $M(x) = 1$. Machine M' works with resources $f(|x|^c) = f(|y|)$ and hence,

$$L' \in \mathbf{CL}_1(f(n)) \subseteq \mathbf{CL}_2(g(n)) \ .$$

Hence, there is a $\mathbf{CL}_2$-machine N' that decides L' in $g(n)$-time (or space). Finally, define a machine $N(x) \equiv N'(x01^{|x|^c} - |x| - 1)$, which decides L with resources

$$g(\left|x01^{|x|^c-|x|-1}\right|) = g(|x|^c) \ .$$

Hence, $L \in \mathbf{CL}_2(g(|x|^c))$.

Corollary: If $\mathbf{NTIME}(n) \subseteq \mathbf{DTIME}(n^{1.2})$ then

$$\mathbf{NTIME}(n^{10}) \subseteq \mathbf{DTIME}(n^{12}) \ .$$

Relationship on DTIME, NTIME, Σ_2TIME

Lemma. If NTIME$(n) \subseteq$ DTIME$(n^{1.2})$ then Σ_2TIME$(n^8) \subseteq$ NTIME$(n^{9.6})$.

Proof. Padding argument gives NTIME$(n^8) \subseteq$ DTIME$(n^{9.6})$.
$L \in \Sigma_2$TIME$(n^8) \Leftrightarrow$ exists DTM M working in time $O(n^8)$, s.t.

$$x \notin L \Leftrightarrow \forall u \in \{0,1\}^{c|x|^8} \exists v \in \{0,1\}^{c|x|^8} : M(x,u,v) = 0$$

hence exists NTM M' working in time $O(n^8)$, s.t.

$$x \notin L \Leftrightarrow \forall u \in \{0,1\}^{c|x|^8} : M'(x,u) = 1$$

hence exists DTM M'' working in time $O(n^{9.6})$, s.t.

$$x \notin L \Leftrightarrow \forall u \in \{0,1\}^{c|x|^8} : M''(x,u) = 0$$
$$x \in \mathsf{L} \Leftrightarrow \exists u \in \{0,1\}^{c|x|^8} : M''(x,u) = 1$$

hence exists NTM M''' working in time $O(n^{9,6})$, that recognizes L.

Putting it together

$\mathsf{SAT} \in \mathsf{TISP}(n^{1.1}, n^{0,1})$

$\mathsf{TISP}(n^{1.2}, \ldots) \subseteq \mathsf{DTIME}(n^{1.2})$

$\mathsf{NTIME}(n) \subseteq \mathsf{TISP}(n^{1.2}, n^{0.2})$

padding

$\mathsf{NTIME}(n^{10}) \subseteq \mathsf{TISP}(n^{12}, n^{2})$

$\mathsf{TISP}(n^{12}, n^{2}) \subseteq \Sigma_2\mathsf{TIME}(n^{8})$

$\Sigma_2\mathsf{TIME}(n^{8}) \subseteq \mathsf{NTIME}(n^{9.6})$

Thus $\mathsf{NTIME}(n^{10}) \subseteq \mathsf{NTIME}(n^{9.6})$, contradiction

Separating PH and PSPACE

Theorem. There exists $A \subseteq \{0,1\}^*$, such that $\mathsf{PH}^A \neq \mathsf{PSPACE}^A$. More generally, for each k there exist oracles, relative to which the polynomial hierarchy has exactly k levels.