28 May 2023

QBF, Polynomial Hierarchy, PSPACE.

1. Quantified Boolean Formulas. (QBF).

(1). Propositional logic with universal & existential quantifications over boolean (or propositional) variables.

Ex. $\forall p \exists q ((p \wedge \neg q) \vee (\neg p \wedge q))$.

(2) Can be written in the following prenex form.

$$Q_1 p_1 Q_2 p_2 \;\cdots\; Q_n p_n \; F$$

↑ quantifier-free.

(3) Computation problems on QBF formulas

① TQBF ---- truth of a given closed QBF formula in the prenex form

② Σ_iSAT --- truth of a given closed QBF formula of the following form:

quantifier alternation (but i times).

$$\exists \vec{p}_1 \forall \vec{p}_2 \;\cdots\; Q_i \vec{p}_i \; F$$

a sequence of existentially quantified propositional variables.

③ Π_iSAT --- similar to Σ_iSAT but for a formula of the following form.

$$\forall \vec{p}_1 \exists \vec{p}_2 \;\cdots\; Q_i \vec{p}_i \; F$$

* Note: $\Sigma_1 SAT = SAT$ ... usual satisfiability problem.

$\Pi_1 SAT = Valid$ ... usual validity problem.

(4) Q: How difficult to solve these algorithmically? Any theoretical tools from computational complexity theory?

2. PSPACE

(1) A decision problem is in PSPACE if it can be solved using only polynomial space w.r.t. the size of the input.

① $P \subseteq PSPACE$ ... why?

② $TQBF \in PSPACE$ ... why?

Think about a recursive (exp-time) algorithm, which uses a pointer to denote the current formula and a stack to store all the inf needed to compute the truth of the input formula.

(2) TQBF is PSPACE-complete.

① encoding of configurations $C \in \{0,1\}^m$ and transition relation $\varphi_M(C, C')$ of a TM.

② Reuse trick via quantifier alternation.

- $\exists C'' \forall D^1 \forall D^2 \left((D^1 = C \wedge D^2 = C'') \vee (D^1 = C'' \wedge D^2 = C') \right) \Rightarrow \psi_{i-1}(D^1, D^2)$

$\parallel$

$\psi_i(C, C')$

- $\psi_m(C, C')$

(3) Exercise : PSPACE-hardness of fol model-checking pb over finite structures.

① $A \models G$ --- input

A: finite structure. G: FOL sentence

true / false --- output.

② TQBF : $Q_1 p_1 Q_2 p_2 \quad Q_n p_n F$

$A = (\{0, 1\}, 0, 1, =)$

$G = Q_1 v_1 Q_2 v_2 \quad Q_n v_n$

$F[{}^{v_1=1}/p_1, {}^{v_2=1}/p_2, \ldots {}^{v_n=1}/p_n]$

③ In fact, the model-checking pb is also PSPACE-complete.

3 Polynomial Hierarchy.

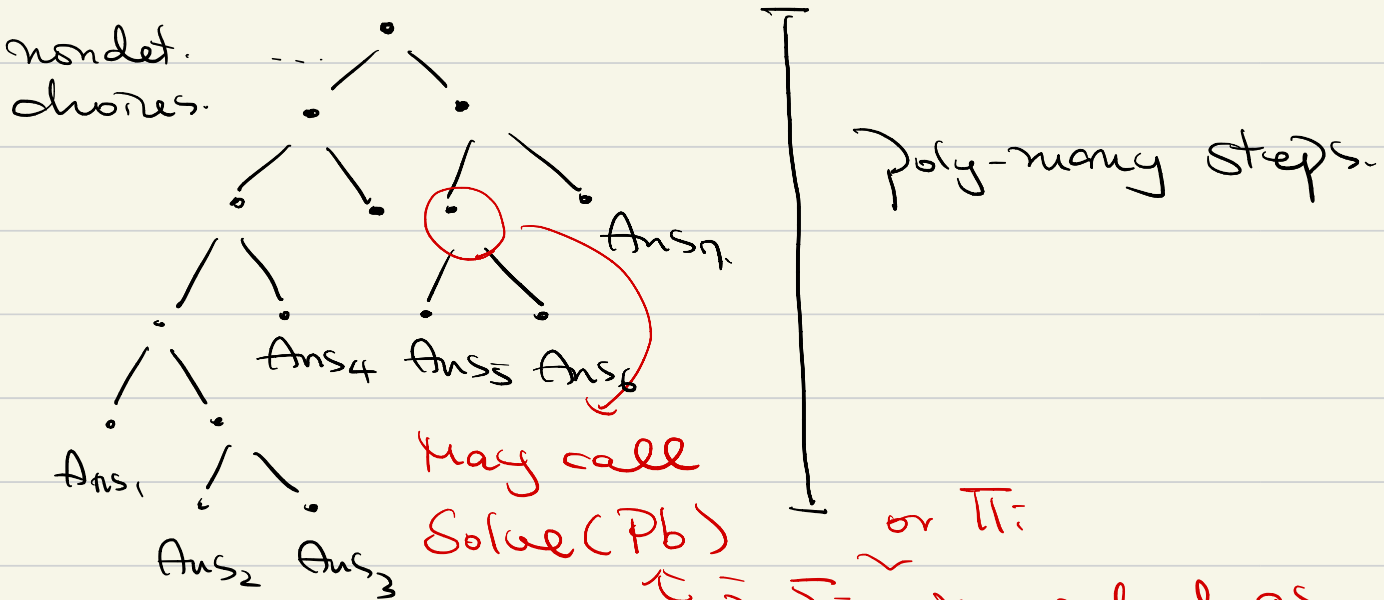
c1) $\Sigma_0 := \Pi_0 := P$

$\Sigma_{i+1} := NP^{\Pi_i}$ ... polytime by a nondet. TM with an oracle to Σ_i.

$\Pi_{i+1} := coNP^{\Sigma_i}$

complement of NP^{Σ_i}

① Intuition of Σ_{i+1} & Π_{i+1}



← in Σ_i or Π_i regarded as a single step.

NP ... Some Ans_i = true. --- return true.

otherwise -- return false.

coNP ... all Ans_i = true ... return true

otherwise return false

② We may assume the oracle for Σ_i only. Similar to the use of a solver for SAT to solve Validity.

③ $\Sigma_1 = NP$, $\Pi_1 = coNP$.

(2) $\Sigma_i SAT$ ···· Σ_i - complete.

$\Pi_i SAT$ ··· Π_i - complete.

Intuitively, the use of Π_i in the def'n of Σ_{i+1}, and " Σ_i in the " of Π_{i+1} correspond to the alternation of quantifiers.

$$PH = \bigcup_{i=0}^{\infty} \Sigma_i = \bigcup_{i=0}^{\infty} \Pi_i.$$

$PH \subseteq PSPACE$ (Think about $\Sigma_i SAT$, $\Pi_i SAT$, TQBF)

(3) People believe that $PH \neq PSPACE$.

① If PH has a complete pb, then $\exists i$ s.t. $PH = \Sigma_i$.

($\because$ the pb should belong to Σ_i).

Thus, collapse of the hierarchy.

② But PSPACE has a complete pb, such as TQBF.

People think that this is unlikely.

(4) VC-Dim $= \{ \langle \mathcal{S}, k \rangle : \text{VC-dim}(\mathcal{S}) \geq k \}$.

① VC-Dim is Σ_3

② Prove this by reduction from Σ_3SAT.

$$\exists \underbrace{\vec{p}}_{k} \forall \underbrace{\vec{q}}_{k} \exists \underbrace{\vec{r}}_{k}. F \longmapsto \langle C, k+1 \rangle.$$

(shattered. $\mathcal{S} = \{ S_1, \ldots, S_m \}$.

VC-dim. .. max shattered set.
size of)

$(\vec{u}, \vec{v}, v', \vec{w}) \in \{0,1\}^k \times \{0,1\}^k \times \{0,1\} \times \{0,1\}^k$.

$S(\vec{u}, \vec{v}, v', \vec{w}) \subseteq \{0,1\}^k \times \{1, \ldots, k+1\}$.

$= \{ (\vec{y}, z) \mid \vec{y} = \vec{u}$ and $(v'\vec{v})_z = 1 \}$.

$\mathcal{S} = \{ S(\vec{u}, \vec{v}, v', \vec{w}) \mid F(\vec{u}, \vec{v}, \vec{w})$ is true$\}$.

Then, $\exists \vec{p} \forall \vec{q} \exists \vec{r}\ F$ true iff.

VC-dim$(\mathcal{S}) \geq k+1$.

* $\forall \vec{q} \exists \vec{r}\ F[\vec{a}/\vec{p}]$ true.

$\Rightarrow \{ (\vec{a}, 1), \ldots, (\vec{a}, k+1) \}$ is shattered.

by $\mathcal{S}_0 = \{ S(\vec{a}, \vec{v}, v', \vec{w}) \mid F(\vec{a}, \vec{v}, \vec{w})$ true$\}$.

$\therefore$ VC-dim $\geq k+1$

* VC-dim $\geq k+1$

$\{(\vec{y}_1, z_1), \ldots, (\vec{y}_{k+1}, z_{k+1})\}$ is shattered.

But $\exists \vec{a} \in \{0,1\}^k$ s.t.

$\{(\vec{a}, 1), \ldots, (\vec{a}, k+1)\}$.

Thus, $\forall \vec{q} \, \exists \vec{r} \, F(\vec{a}, \vec{q}, \vec{r})$ true.

each shattering set implies
the existence of $\vec{r}$ for each $\vec{q}$.