10: Polynomial Hierarchy

2022-10-17

Goal: Describe classes

Let $L = \{\varphi(x_1, \dots, x_n) \mid \varphi$ = Boolean formula of n variables where the satisfying assignment with the most 1's has at least $\frac{n}{2}$ 1's$\}$

Suppose $\exists M$ $\forall x \in L$ $\exists u \in \{0,1\}^{poly(|x|)}$ $M(x,u) = 1$

$\forall x \notin L$ $\forall u \in \{0,1\}^{poly(|x|)}$ $M(x,u) = 0$

Then $\exists u_1, u_2 \in \{0,1\}^{poly(|x|)}$ $M(x,u_1) = 1$ ← NP statement

$\forall u$: $\varphi(u)$ = True $\rightarrow |u| \in k$ ← coNP statement

Goal: $\forall x \in \{0,1\}^{poly(|x|)}$ $\exists u \in \{0,1\}^{poly(|x|)}$ $\forall u_2 \in \{0,1\}^{poly(|x|)}$ $M(x,u_1,u_2) = 1$

def: Let $L \in \Sigma_2$ if $\exists$ a polytime TM M and a polynomial g s.t.
$x \in L$ iff $\exists u_1 \in \{0,1\}^{g(n)}$ $\forall u_2 \in \{0,1\}^{g(n)}$ $M(x,u_1,u_2) = 1$

ex $L \in \Sigma_2$

Proof: Let $M(\langle x, y_1, y_2 \rangle, u_1, u_2)$ evaluate $\varphi(u_1)$, $\varphi(u_2)$ and accept if:
- $\varphi(u_1)$ = True
- $|u_1| = k$
- $(\varphi(u_2)$ = False$)$ or $(\varphi(u_2)$ = True and $|u_2| \in k)$

By def $L \in \Sigma_2$

u_1: 0 0 0 0 1 1 1 1

Which is the correct picture? Why?

$L \in NP \rightarrow$ Can use u_1 to describe that yes-inst. y_1
$L \in coNP \rightarrow$

def: $L \in \Pi_2$ if $\bar{L} \in \Sigma_2$

def: $L \in \Pi_2$ iff $\exists$ a polytime TM M and polynomial g s.t.
$x \in L$ iff $\forall u_1 \in \{0,1\}^{g(n)}$ $\exists u_2 \in \{0,1\}^{g(n)}$ $M(x,u_1,u_2) = 1$

$\Pi_2 \supseteq \Sigma_2$

Thm: $BPP \subseteq \Sigma_2$ (or Post: $BPP \subseteq \Sigma_2 \cap \Pi_2$)

Pf: Sketch: Let $L \in BPP$. $\exists$ a PTM M that runs in polynomial time, s.t.
- If $x \in L$, $\Pr[M(x,y) \text{ accepts}] \geq 1 - \frac{1}{3^n}$
- If $x \notin L$, $\Pr[M(x,y) \text{ accepts}] \leq \frac{1}{3^n}$

Let $m = \Phi(x)$ be the # bits used on input x
$\Rightarrow u \in \{0,1\}^m$

= accepting run for M sequence

ex: $m = 3$

= accepted seq. originally

= accept after transformation

Idea

Can prove that for $r = O(poly(|x|))$, there strings exists $y_1, y_2, \dots, y_r$ st the entire space $\{0,1\}^m$ is covered.

Let $M(x,u,u_1)$ break up u into $(y_1, y_2, \dots, y_r)$. Then consider

```
M(x,u,u1):
For i = 1 to r
    Run M(x,yi)
    If accepts, M accepts
Reject
```

Checks whether coin sequence y_i accepts y_i.

Proof:
$x \in L$ iff $\exists u_1 \in \{0,1\}^m$: $\forall y \in \{0,1\}^m$, $M(x,u,u_1)$ accepts

bit of y_is

sequences of coin flips

So: $L \in \Sigma_2$

Sorry State of Affairs

Goals:
- Describe the Polynomial Hierarchy
- Understand why it is unlikely to collapse

Announcements
- Gradescope/Piazza2022
- Gq/Jace (anti-procrastination station)

New Strategy: Shift goal post

ex:

Quantifiers Polynomial time

$BQP + BPP$ — Polynomial time Bounded Error — Two Hard

If $BQP = BPP$ Take $\frac{P}{2}$-NP — Two Hard — Take polynomial hierarchy collapses to 2nd level

Σ_1, Σ_2? Σ_k?

def: For $i \geq 0$, $L \in \Sigma_i$ if $\exists$ a polytime TM M and a polynomial g s.t.

$$x \in L \leftrightarrow \exists u_1 \in \{0,1\}^{g(|x|)} \forall u_2 \in \{0,1\}^{g(|x|)} \dots Q_i u_i \in \{0,1\}^{g(|x|)} M(x, u_1, u_2, \dots u_i) = 1$$

Q_i is $\forall$ if i is even, $\exists$ if i is odd

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

Polynomial Hierarchy

$\Sigma_1 = NP$

$\Pi_1 = coNP$

Π_2

def: For $i \geq 0$, $L \in \Pi_i$ if $\exists$ a polytime TM M and a polynomial g s.t.

$$x \in L \text{ iff } \forall u_1 \in \{0,1\}^{g(|x|)} \exists u_2 \in \{0,1\}^{g(|x|)} \dots Q_i u_i \in \{0,1\}^{g(|x|)} M(x, u_1, u_2, \dots u_i) = 1$$

($\exists$ → $\forall$, $\forall$ → $\exists$)

Q_i: $\exists$ if i is even, $\forall$ if i is odd

What is Σ_0?

A) P B) NP C) coNP

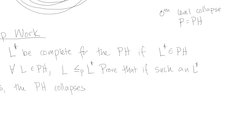
What is Σ_1?

A) P B) NP C) coNP

People Strongly Believe:

$\forall i \geq 1$: (analogous to)
- $\Sigma_{i+1} \neq \Sigma_i$ — $P \neq NP$
- $\Sigma_i \neq \Pi_i$ — $NP \neq coNP$
- $\Pi_{i+1} \neq \Pi_i$ — $P \neq coNP$

Collapse: If for all $j \geq c$, $\Sigma_j = \Sigma_c$, we say "The PH collapses to the cth level"



Group Work

Let L^* be complete for the PH if $L^* \in PH$ and $\forall L \in PH$, $L \leq_p L^*$. Prove that if such an L^* exists, the PH collapses.

Pf:

Consequence

General Strategy:
1.
2.

Theorem If $P = NP$ then the PH collapses (to 0th level)

Pf: We will prove by induction on i that if $P = NP$ then $P = \Sigma_i$ and $P = \Pi_i$

Base Case for $i = 1$: $\Sigma_1 = NP$. By our assumption $P = NP$, so $P = \Sigma_1$. If $P = NP$, then $P = coNP$ (Prev HW), so $P = \Pi_1$

Inductive Step: Let $k \geq 1$. Assume for induction that $P = \Sigma_k$. Let $L \in \Sigma_{k+1}$