10. Polynomial Hierarchy

Thursday, April 28, 2022
10:03 AM

<u>Goal</u>

- Describe classes Σ_2, Π_2

  Σ_2: "Sigma-2" ; Π_2: "Pi-2"

Let
$L' = \{\langle \varphi, k\rangle : \varphi$ is a Boolean formula of n variables where the satisfying assigment with the most Trues has k Trues. $\}$

$\exists u : \underbrace{\varphi(u)}_{\text{output of } \varphi \text{ with assignment } u} = \text{True}$ and $\underbrace{|u|}_{\text{number of Trues in } u} = k$ ⇐ NP-like

$\forall u,\ \varphi(u) = \text{True} \rightarrow |u| \le k$ ⇐ coNP-like

$$\boxed{\begin{array}{l} \underline{\text{def}}: L \in \Sigma_2 \text{ if } \exists \text{ a polytime TM } M \text{ and polynomial } q \text{ s.t.} \\ \qquad x \in L \text{ iff } \exists u_1 \in \{0,1\}^{q(|x|)} : \forall u_2 \in \{0,1\}^{q(|x|)}\ M(x, u_1, u_2) = 1. \end{array}}$$

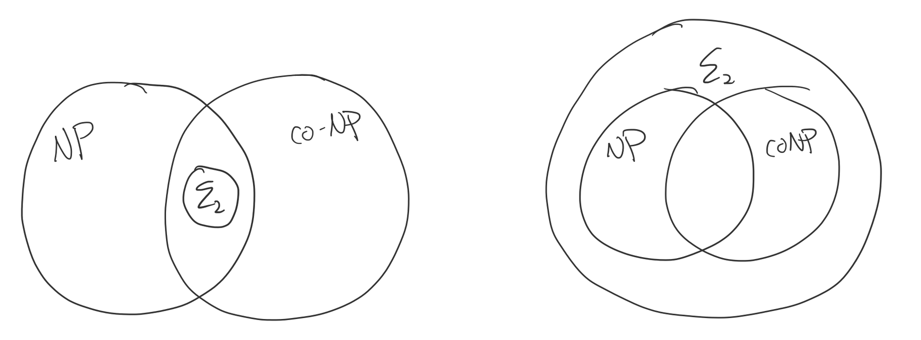
ex: $L' \in \Sigma_2$

Proof: Let $M(\langle \varphi, k\rangle, u_1, u_2)$ evaluate $\varphi(u_1), \varphi(u_2)$ and accept if

- $\varphi(u_1) = \text{True}$
- $|u_1| = k$
- $(\varphi(u_2) = \text{False})$ or $(\varphi(u_2) = \text{True}$ and $|u_2| \le k)$

Then M satisfies the definition.

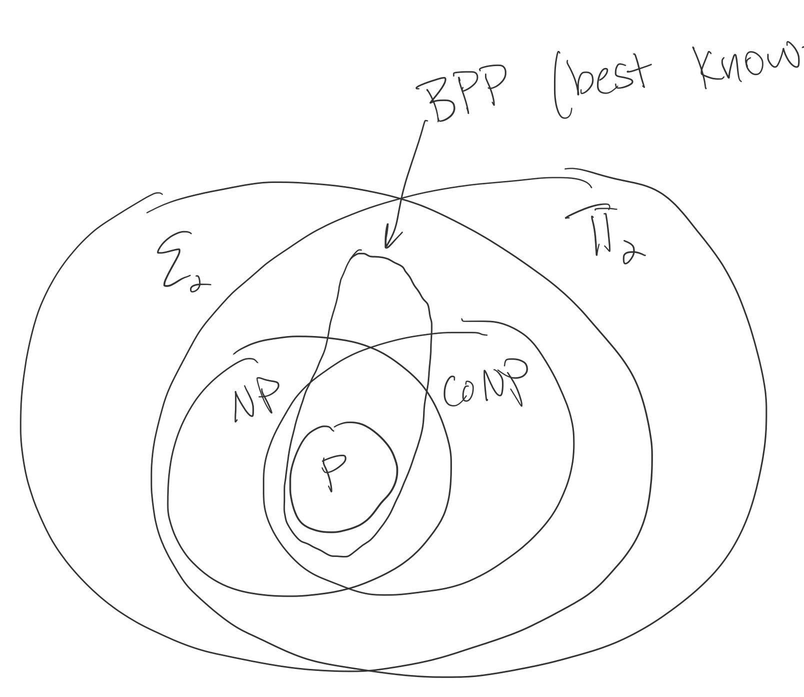
Which is the correct picture? Why



If $L \in NP$, $L \in \Sigma_2$ (use same machine, ignore u_2)
If $L \in coNP$, $L \in \Sigma_2$ (use same machine, ignore u_1)

$$\boxed{\text{def}: L \in \Pi_2 \text{ if } \overline{L} \in \Sigma_2 \qquad (\Pi_2 = co\Sigma_2)}$$

$$\boxed{\begin{array}{l} \underline{\text{def}}: L \in \cancel{\Sigma_2}\ \Pi \text{ if } \exists \text{ a polytime TM } M \text{ and polynomial } q \text{ s.t.} \\ \qquad x \in L \text{ iff } \cancel{\exists}\ \forall\ u_1 \in \{0,1\}^{q(|x|)} : \cancel{\forall}\ \exists\ u_2 \in \{0,1\}^{q(|x|)}\ M(x, u_1, u_2) = 1. \end{array}}$$

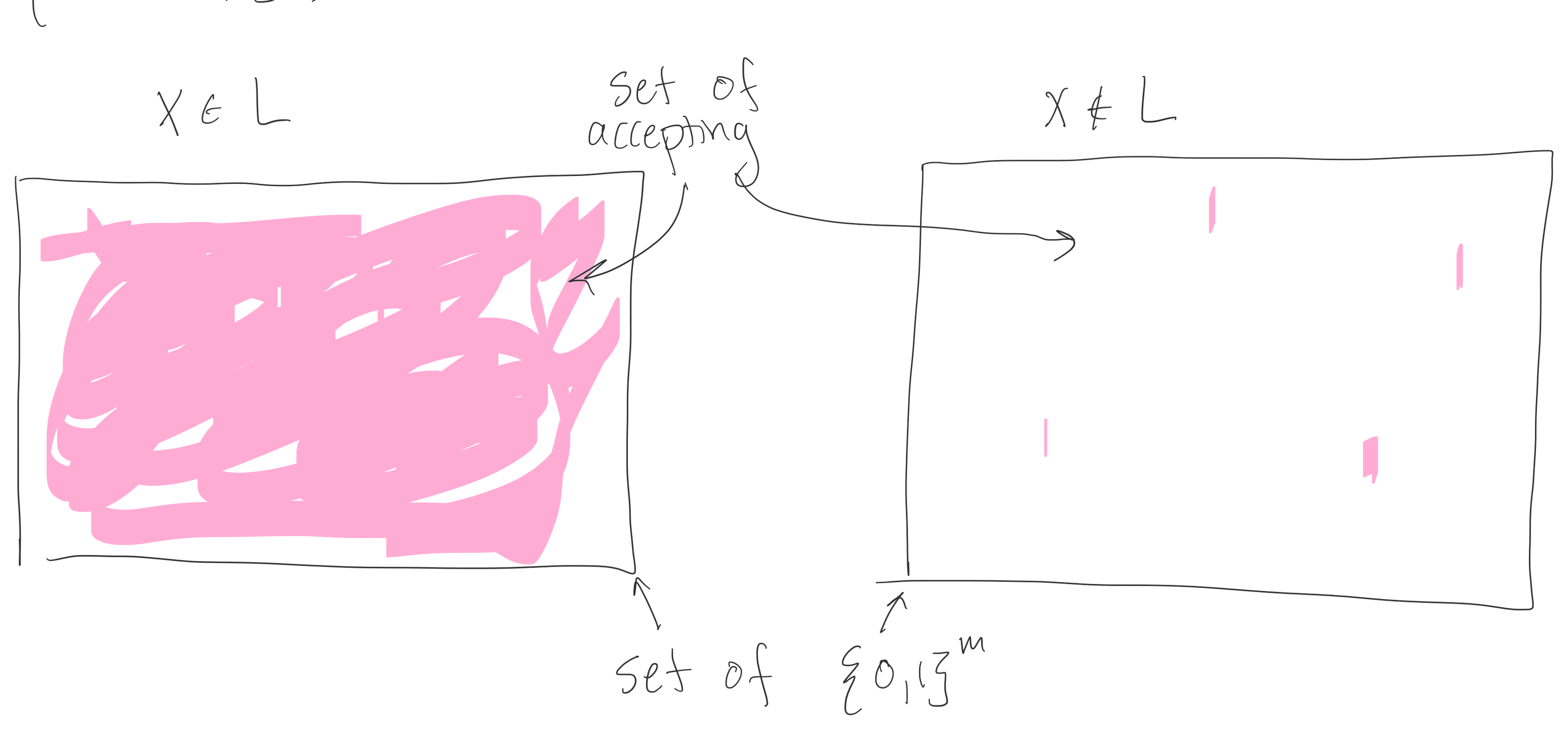


<u>Thm</u>: $BPP \subseteq \Sigma_2$ (on Pset: $BPP \subseteq \Sigma_2 \cap \Pi_2$

<u>Pf</u>: Let $L \in BPP$. Then $\exists$ a PTM M, constant k s.t.
<u>Sketch</u>

- If $x \in L$, $\Pr_u[M(x,u) \text{ accepts}] \ge 1 - 2^{-k}$
- If $x \notin L$, $\Pr_u[M(x,u) \text{ rejects}] \ge 1 - 2^{-k}$

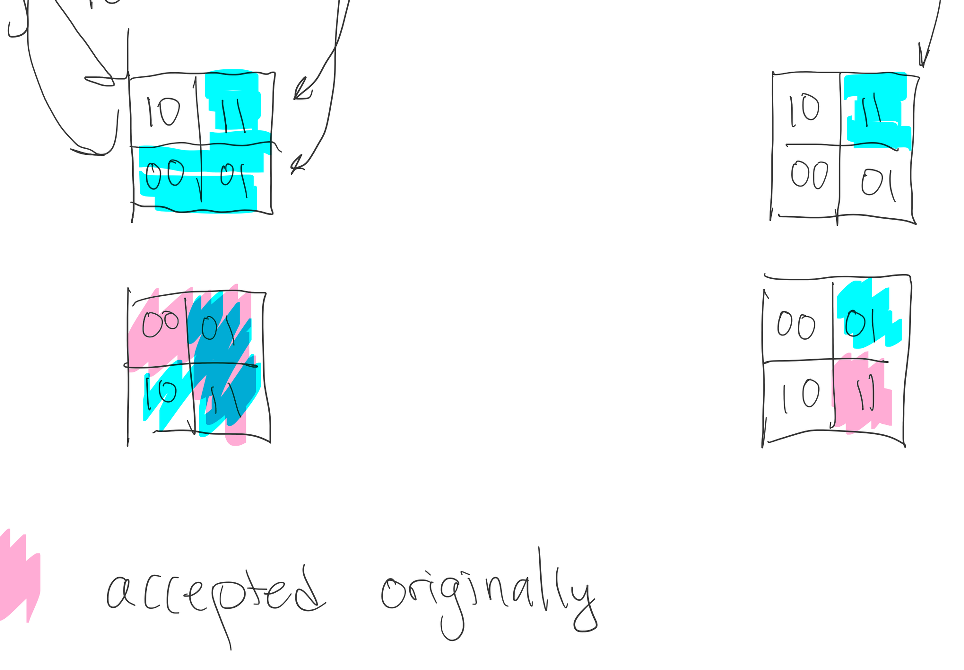
Let m = # of coin flips M uses on input x
$(u \in \{0,1\}^m)$.



ex: $m=2$

Now consider bitwise adding a string y to each $u \in \{0,1\}^m$

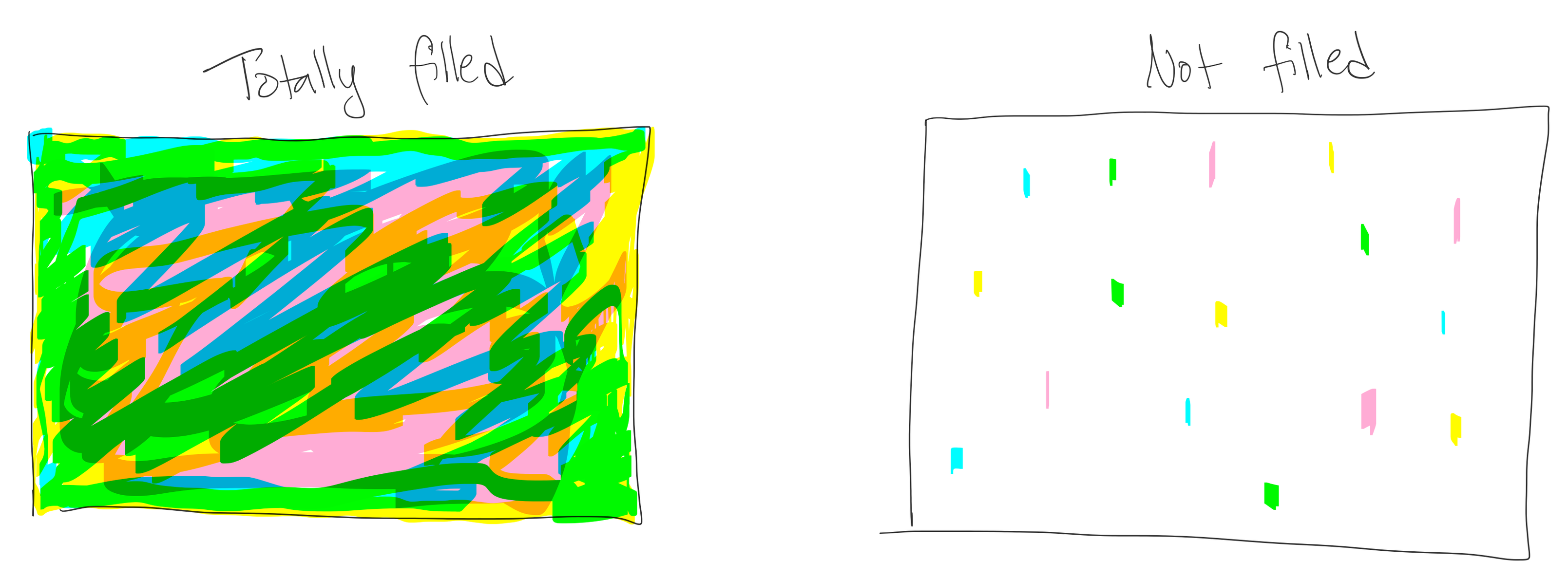
ex: $y = 10$



accepted originally

accepted after adding y

Idea: after adding a few different, randomly chosen y, looks like:



Can prove that for $r = O(\text{poly}(|x|))$, there <u>always</u> exists $y_1, y_2, \cdots y_r$ s.t the entire space $\{0,1\}^m$ is covered

Let $M'(x, u_1, u_2)$ break up u_1 as $(y_1, y_2, \cdots y_r)$. Then consider

```
M'(x, u1, u2):
For i = 1 to r
  | Run M(x, u2 ⊕ yi)
  | If accepts, M' accepts
Reject
```

Checks whether coin sequence
$u_2 \oplus y_1$ accepts
$u_2 \oplus y_2$
⋮

<u>Then</u>:
$x \in L$ iff $\exists \underbrace{u_1}_{\text{list of } y_i\text{'s}} \in \{0,1\}^{rm} : \forall \underbrace{u}_{\text{sequences of coin flips}} \in \{0,1\}^m,\ M'(x, u, u_2)$ accepts

<u>So</u>: $L \in \Sigma_2$

Sorry State of Affairs: