COL 351 Lecture 35 2023/04/12

Topic : More Polynomial-time Verification, coNP

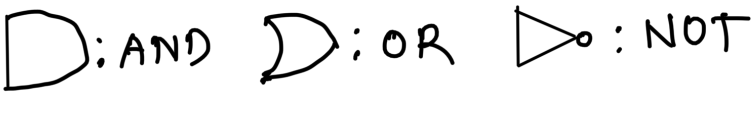
Announcements:

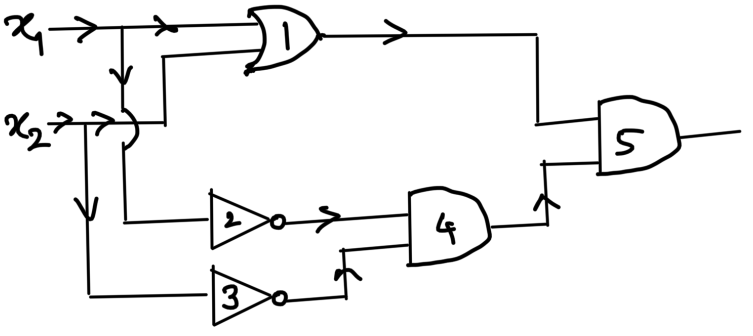
1. Pre-quiz tutorial today 19:30-onward Bharti-501
2. Quiz 4 tomorrow 12:00-13:00, LH114,
3. Next lecture tomorrow 19:30-20:30 Bharti-501.

CIRCUIT-SAT

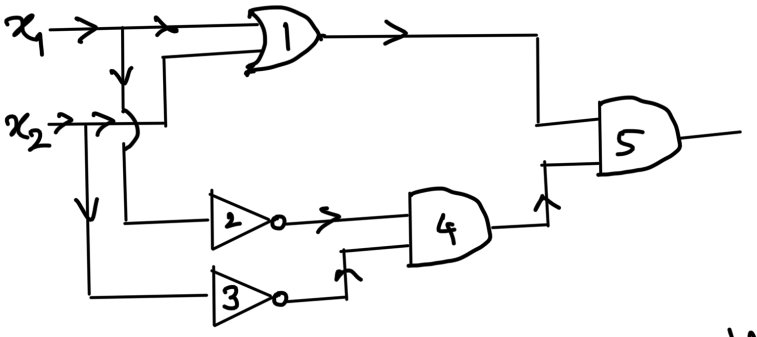
Input: A combinational boolean circuit over n variables, containing m gates.

Output: Does there exist a boolean input (a.k.a. a satisfying assignment) to the circuit that makes its output TRUE?





vars = 2
gates = 5
gate1: x_1 OR x_2
gate2: NOT x_1
gate3: NOT x_2
gate4: gate2 AND gate3
gate5: gate4 AND gate1.
OUTPUT: gate5.



Prover

Verifier

"The circuit has a satisfying assignment"

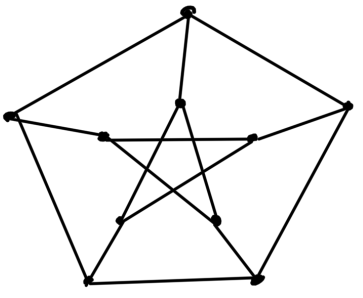
"Prove it"

"Here is an assignment:
$x_1 = \ldots \quad x_2 = \ldots \quad x_n = \ldots$

Runs through the description of the circuit, and checks whether the output is TRUE.

GRAPHISO:

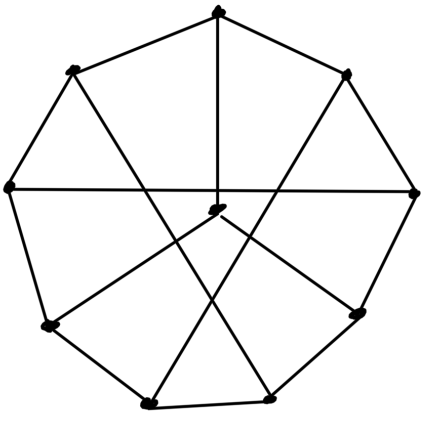
Input: Two graphs, $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$.



Output: Are G_1 and G_2 isomorphic to each other?

ie $\exists$? a bijective function $h: V_1 \to V_2$ such that $\forall\ u_1, v_1 \in V_1$

$$\{u_1, v_1\} \in E_1 \iff \{h(u_1), h(v_1)\} \in E_2$$



Verifier (G_1, G_2, h) $(h: V_1 \to V_2)$

- Check whether h is bijective.
- For each pair $(u_1, v_1) \in V_1 \times V_1$:
  Check whether $\{u_1, v_1\} \in E_1 \Leftrightarrow \{h(u_1), h(v_1)\} \in E_2$.

PRIME:

Input: +ve integer m (in binary)

Output: Is m a prime?

Is PRIME $\in$ NP? — not clear.

$\overline{\text{PRIME}} \in$ NP.

Verifier for $\overline{\text{PRIME}}$: On input m, r:
If r divides m and $1 < r < m$, accept
Else reject.

```
for i = 2 to ⌊√m⌋:
    if i divides m:
        Return NO
Return YES
```

↑ Not a polynomial-time algorithm.

Fact [AKS]: PRIME $\in$ P ($\because \overline{\text{PRIME}} \in$ P) } Well outside the scope of COL351

Claim: If $Q \in$ P then $\overline{Q} \in$ P.

Definition: A decision problem Q is said to be in the complexity class coNP if $\overline{Q} \in$ NP.

Claim: P $\subseteq$ NP $\cap$ coNP.

Claim: If $Q \in$ NP $\cap$ coNP, then $\overline{Q} \in$ NP $\cap$ coNP.

Open question: Which of the following is true?