FINDING A SOLUTION

- 3-SAT
- INDEPENDENT SET
- VERTEX COVER
- SET COVER

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

(1) DOES $(x_1, x_2, x_3) = (1,0,1)$ SATISFY

$(x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_2 \vee \bar{x}_3)$

FINDING A SOLUTION

3-SAT

INDEPENDENT SET

VERTEX COVER

SET COVER

CERTIFY

(1) DOES $(x_1, x_2, x_3) = (1,0,1)$ SATISFY

$$(x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_2 \vee \bar{x}_3) \wedge (\bar{x}_1 \vee x_2 \vee \bar{x}_3)$$

FINDING A SOLUTION

3-SAT

INDEPENDENT SET

VERTEX COVER

SET COVER

CERTIFY

CERTIFICATE ← EVIDENCE OF YES INSTANCE

(I) DOES $\underbrace{(x_1, x_2, x_3)}_{}$ = (1,0,1) SATISFY

$$(x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_2 \vee \bar{x}_3)$$

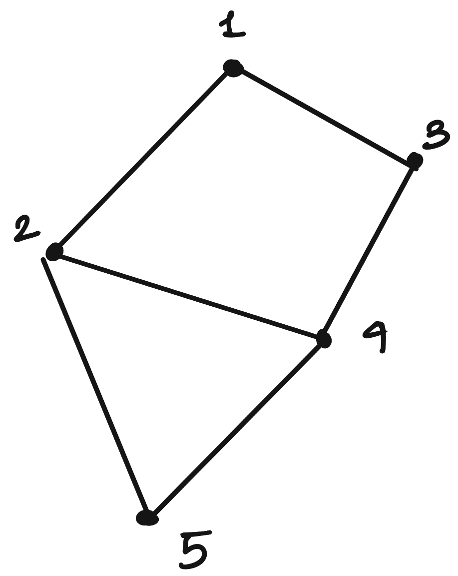
GIVEN AN ASSIGNMENT, WE CAN CHECK IF IT IS A SATSFYING ASSIGNMENT IN POLYNOMIAL TIME.

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

(1) IS THERE AN
INDEPENDENT SET
OF SIZE ATLEAST 2?

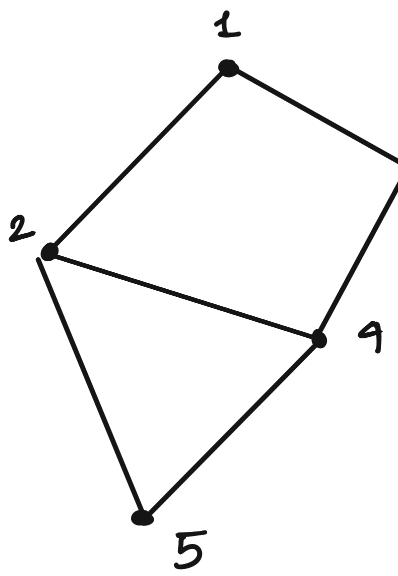


FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

(1) IS THERE AN INDEPENDENT SET OF SIZE ATLEAST 2?



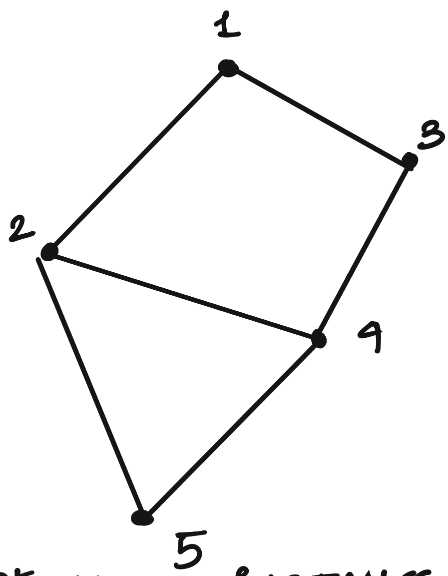
$X = \{2,3\}$

GIVEN X, WE CAN CHECK IF X IS AN INDEPENDENT SET IN POLYNOMIAL TIME.

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY



(1) IS THERE AN INDEPENDENT SET OF SIZE ATLEAST 2?

$\underbrace{X = \{2,3\}}_{\text{CERTIFICATE}}$ ← EVIDENCE OF YES INSTANCE

GIVEN X, WE CAN CHECK IF X IS AN INDPENDENT SET IN POLYNOMIAL TIME.

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

CERTIFYING ALGORITHM SEEMS TO TAKE POLYNOMIAL TIME.

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

CERTIFYING ALGORITHM SEEMS TO TAKE POLYNOMIAL TIME.

Q: CAN YOU THINK OF A PROBLEM FOR WHICH THE CERTIFYING ALGO TAKES EXPONENTIAL TIME?

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

CERTIFYING ALGORITHM SEEMS TO TAKE POLYNOMIAL TIME.

Q: CAN YOU THINK OF A PROBLEM FOR WHICH THE CERTIFYING ALGO TAKES EXPONENTIAL TIME?

IS THE # PATHS BETWEEN s to $T \geq k$?

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

CERTIFYING ALGORITHM SEEMS TO TAKE POLYNOMIAL TIME.

NP: CLASS OF PROBLEMS FOR WHICH THERE IS AN EFFICIENT CERTYFIER.

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

CERTIFYING ALGORITHM SEEMS TO TAKE POLYNOMIAL TIME.

NP: CLASS OF PROBLEMS FOR WHICH THERE IS AN EFFICIENT CERTYFIER.

P: CLASS OF PROBLEMS THAT BE SOLVED EFFICIENTLY.

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

CERTIFYING ALGORITHM SEEMS TO TAKE POLYNOMIAL TIME.

NP: CLASS OF PROBLEMS FOR WHICH THERE IS AN EFFICIENT CERTYFIER.

P: CLASS OF PROBLEMS THAT BE SOLVED EFFICIENTLY.

SHORTEST PATH
MAXIMUM MATCHING
MAX FLOW

FINDING A SOLUTION

3-SAT
INDEPENDENT SET
VERTEX COVER
SET COVER

CERTIFY

CERTIFYING ALGORITHM SEEMS TO TAKE POLYNOMIAL TIME.

NP: CLASS OF PROBLEMS FOR WHICH THERE IS AN EFFICIENT CERTYFIER.

P: CLASS OF PROBLEMS THAT BE SOLVED EFFICIENTLY.

IS $P \subseteq NP$?

LEMMA : $P \subseteq NP$.

$P \leftarrow$ POLYNOMIALLY SOLVABLE

$\Rightarrow$ POLYNOMIAL CERTIFYER

LEMMA : $P \subseteq NP$.

$P \leftarrow$ POLYNOMIALLY SOLVABLE

$\Rightarrow$ POLYNOMIAL CERTIFYER

IS THERE A PROBLEM IN NP WHICH IS NOT IN P ?

LEMMA : $P \subseteq NP$.

$P \leftarrow$ POLYNOMIALLY SOLVABLE

$\Rightarrow$ POLYNOMIAL CERTIFYER

IS THERE A PROBLEM IN NP WHICH IS NOT IN P ?

OR IS $P = NP$?

LEMMA : $P \subseteq NP$.

$P \leftarrow$ POLYNOMIALLY SOLVABLE

$\Rightarrow$ POLYNOMIAL CERTIFYER

IS THERE A PROBLEM IN NP WHICH IS NOT IN P ?

OR IS $P = NP$?

FAMOUS PROBLEM OF OUR TIMES.

LEMMA : $P \subseteq NP$.

$P \leftarrow$ POLYNOMIALLY SOLVABLE

$\Rightarrow$ POLYNOMIAL CERTIFYER

IS THERE A PROBLEM IN NP WHICH IS NOT IN P ?

OR IS $P = NP$?

FAMOUS PROBLEM OF OUR TIMES.

MANY BELEIVE ANS IS NO,
THOUGH ITS JUST A BELIEF.

3-SAT, INDPENDENT SET,

VERTEX COVER $\in NP$

3-SAT, INDPENDENT SET,

VERTEX COVER $\in P$

???

NOT KNOWN

3-SAT, INDPENDENT SET,

VERTEX COVER $\in$ P

???

NOT KNOWN

SUPPOSE YOU ARE ABLE TO SHOW THAT

3-SAT $\in$ P

WOULD YOU HAVE SOLVED P=NP QUESTION ?

3-SAT, INDPENDENT SET,
VERTEX COVER $\in P$
???

NOT KNOWN

SUPPOSE YOU ARE ABLE TO SHOW THAT
3-SAT $\in P$
WOULD YOU HAVE SOLVED $P = NP$ QUESTION ?

NO BECAUSE YOU HAVE SHOWN THAT

3-SAT, INDEPENDENT SET,
VERTEX COVER $\in P$


NP
P
SP
MAX MATCH
MAX FLOW
3-SAT
IS
VC


NP
P
SP
MAX MATCH
MAX FLOW
3-SAT
IS
VC

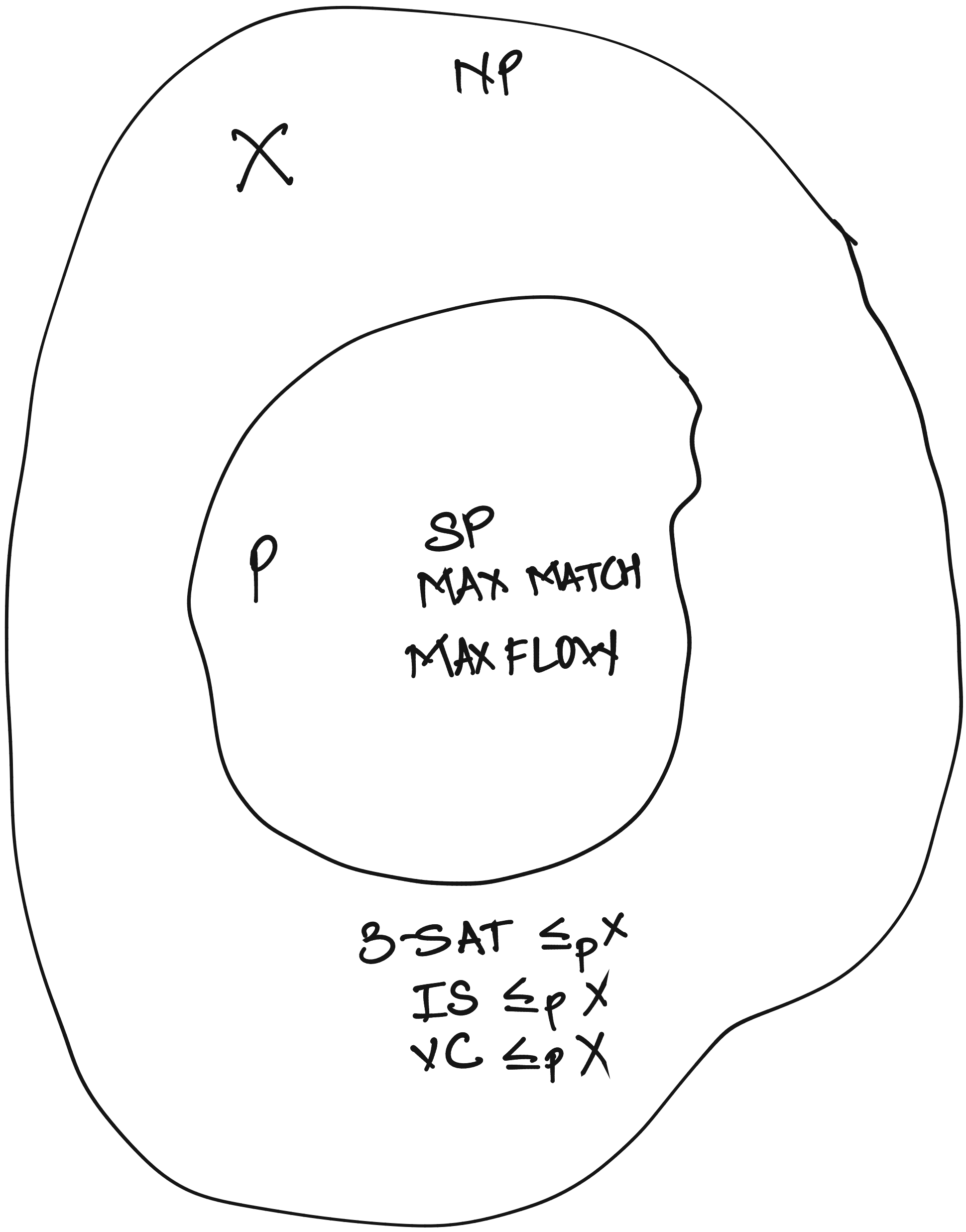
NP-COMPLETE PROBLEM:

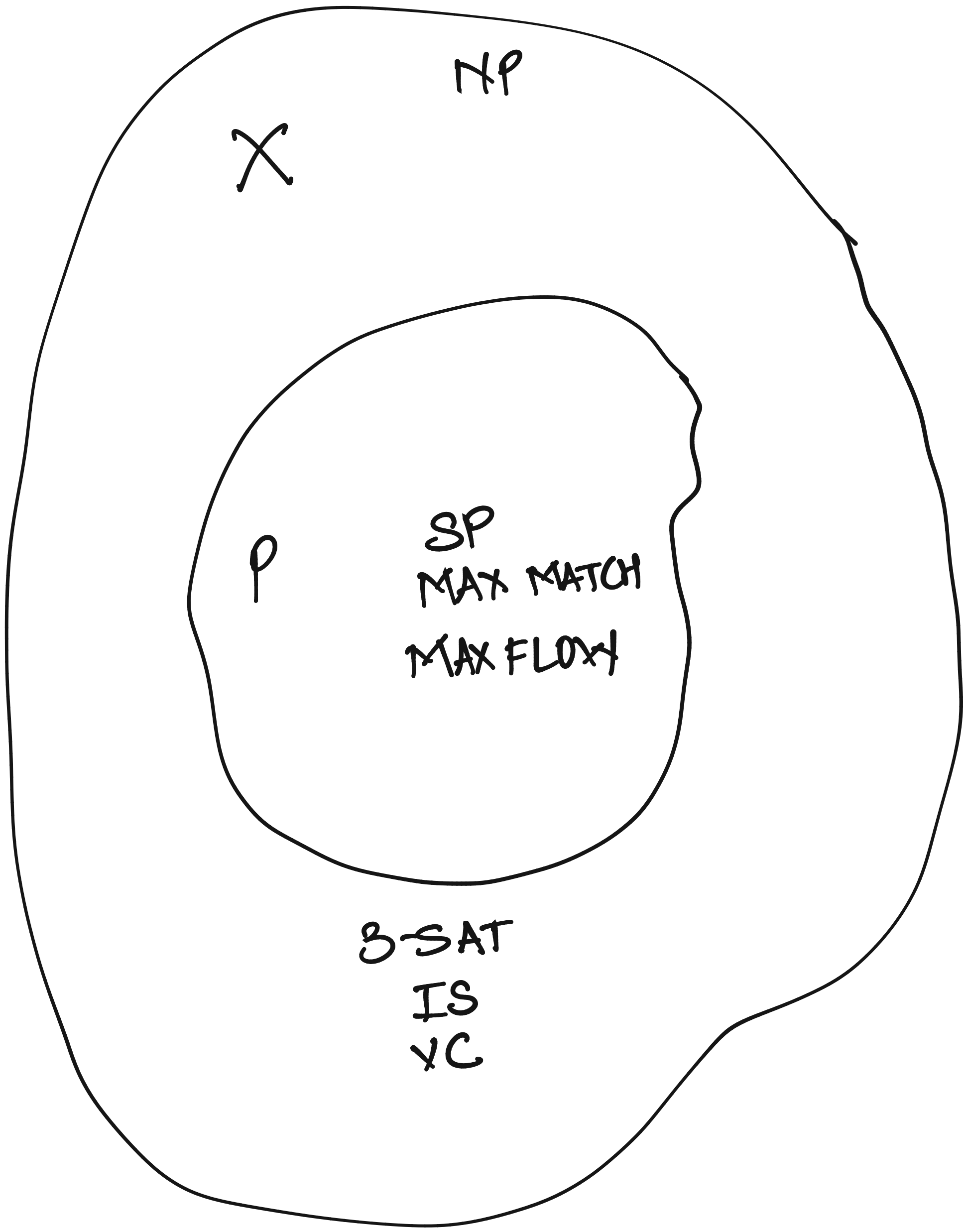
A PROBLEM X IS NP-COMPLETE IF

(a) $X \in NP$ and

(b) FOR ANY $Y \in NP$,

$Y \leq_p X$.


NP
X
P
SP
MAX MATCH
MAX FLOW
3-SAT $\le_p$ X
IS $\le_p$ X
VC $\le_p$ X



IF YOU SHOW $X \in P$, THEN

IF YOU SHOW $X \in P$, THEN
ALL PROBLEMS OF NP ARE IN P

OR NP = P

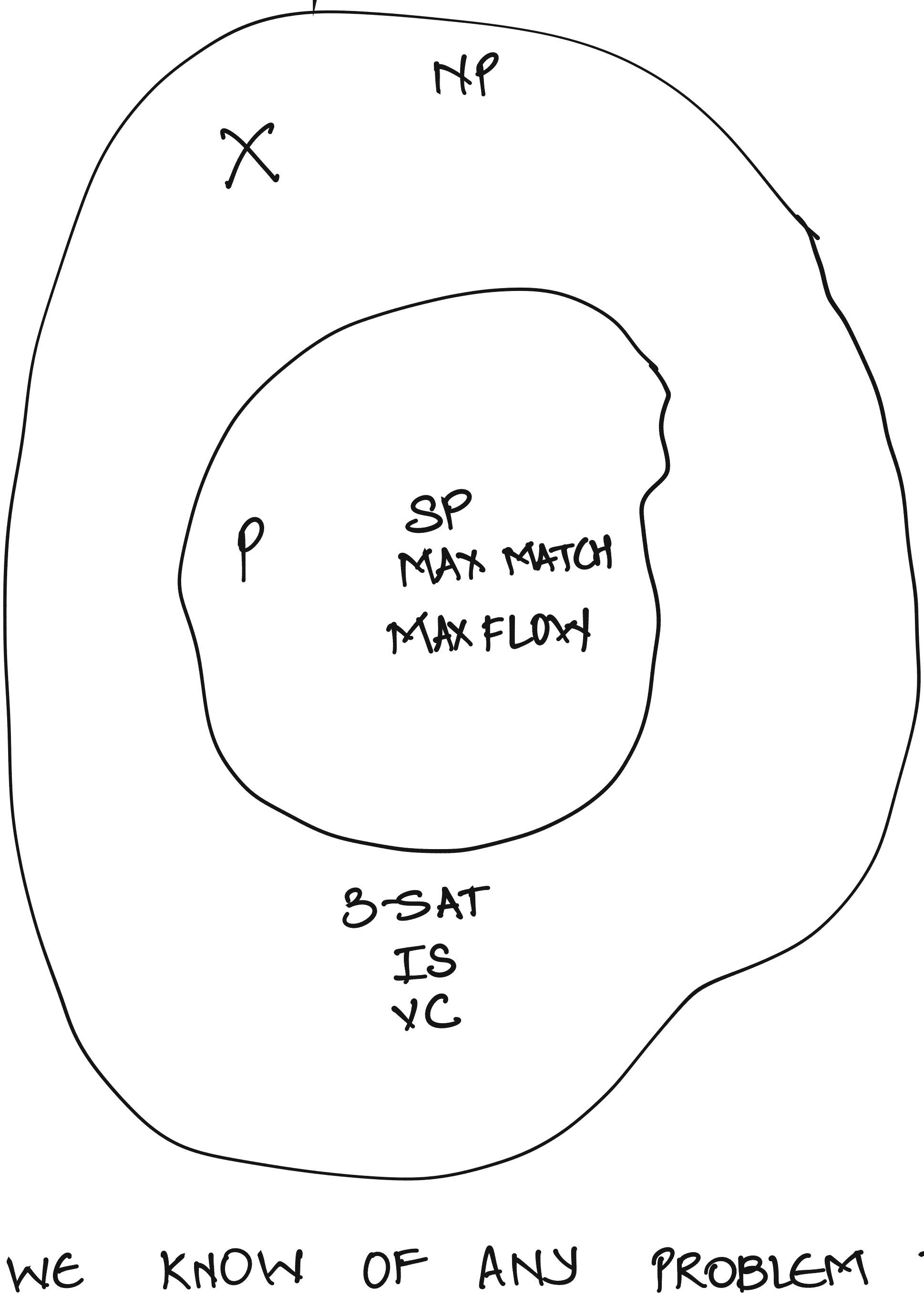
NP-COMPLETE PROBLEM:

A PROBLEM X IS NP-COMPLETE IF

(a) $X \in NP$ and

(b) FOR ANY $Y \in NP$,

$Y \leq_p X$.



DO WE KNOW OF ANY PROBLEM THAT IS NP-COMPLETE?

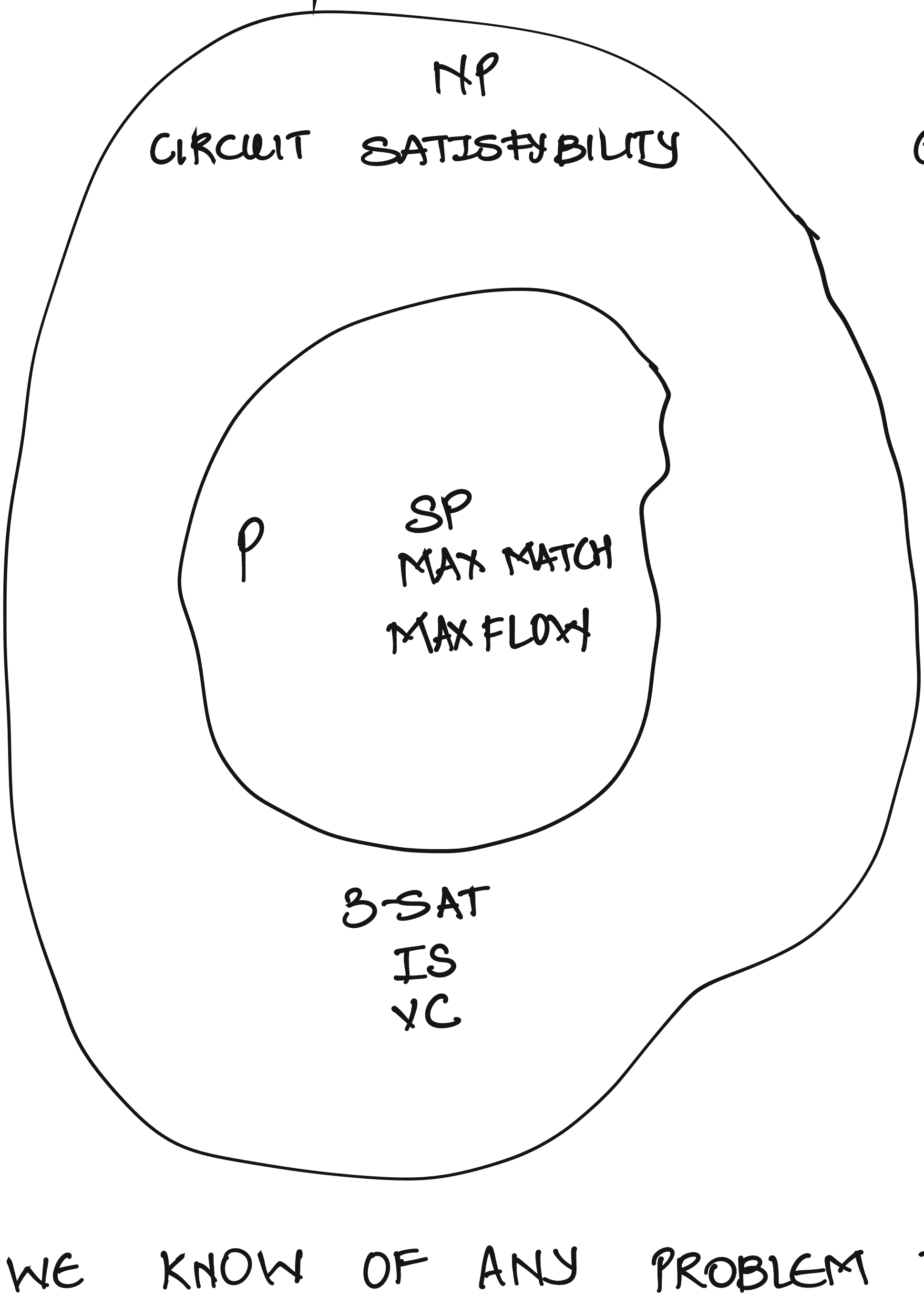
NP-COMPLETE PROBLEM:

A PROBLEM X IS NP-COMPLETE IF

(a) $X \in NP$ and

(b) FOR ANY $Y \in NP$,

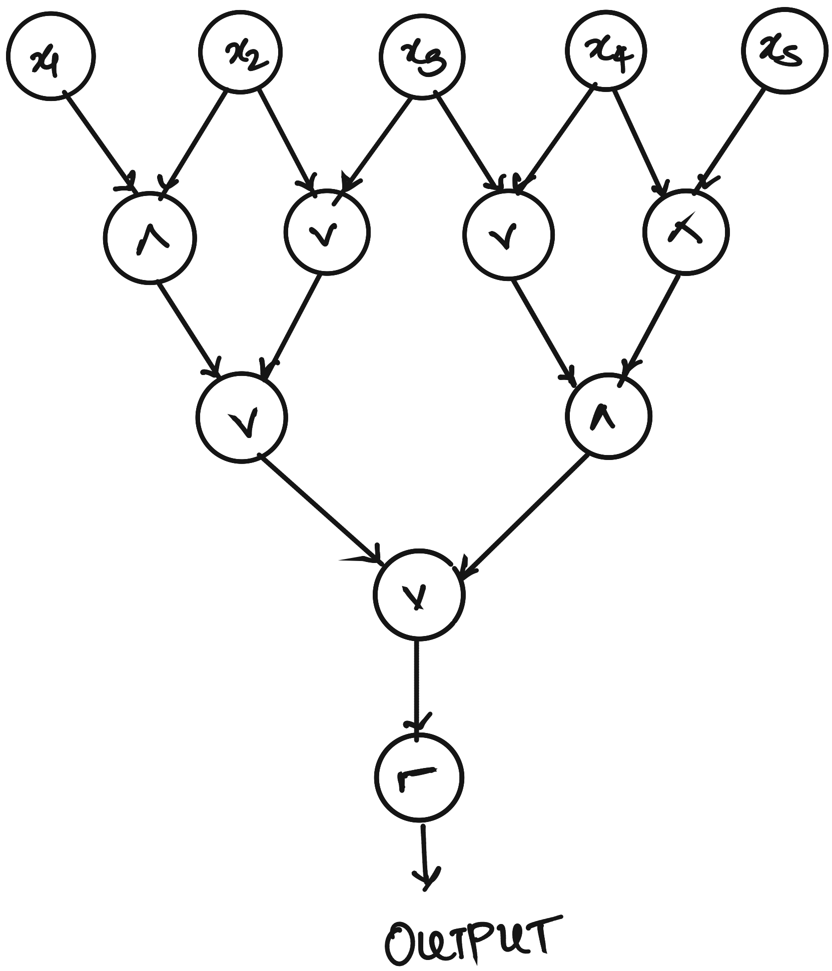
$Y \le_p X$.



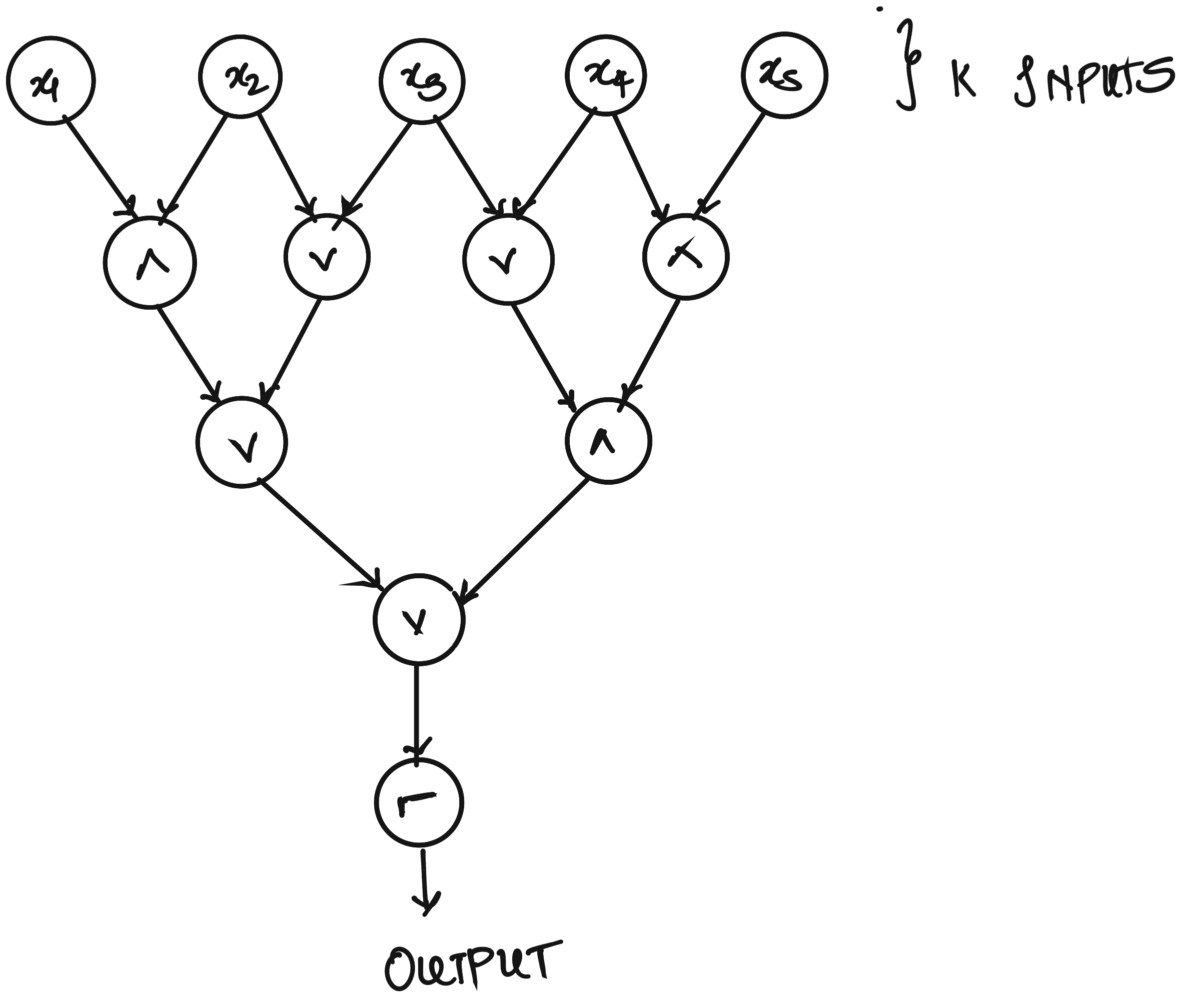
COOK & LEVIN 1971

DO WE KNOW OF ANY PROBLEM THAT IS NP-COMPLETE?

CIRCUIT SATISFYBILITY



CIRCUIT SATISFYBILITY



<u>Q</u>: DOES THERE EXISTS AN INPUT FOR WHICH OUTPUT = 1. ?

AN INPUT THAT SATISFIES THE CIRCUIT

CIRCUIT SATISFYBILITY IS NP-COMPLETE.

ASSUME THAT I AM ABLE TO SHOW
CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

CIRCUIT SATISFYBILITY IS NP-COMPLETE.

ASSUME THAT I AM ABLE TO SHOW

CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

3SAT IS NP-COMPLETE

REMEMBER

NP-COMPLETE PROBLEM:

A PROBLEM X IS NP-COMPLETE IF

(a) $X \in NP$ and

(b) FOR ANY $Y \in NP$,

$Y \leq_p X$.

<u>LEMMA</u> : IF X IS NP-COMPLETE & $\exists\, Y \in NP$ S.T $X \leq_p Y$, THEN Y IS NP-COMPLETE

CIRCUIT SATISFYABILITY $\leq_p$ 3-SAT

3-SAT IS NP-COMPLETE

CIRCUIT SATISFYABILITY $\leq_p$ 3-SAT

3-SAT IS NP-COMPLETE

3-SAT $\leq_p$ INDEPENDENT SET

INDEPENDENT SET IS NP-COMPLETE

CIRCUIT SATISFYABILITY $\leq_p$ 3-SAT

3-SAT IS NP-COMPLETE

3-SAT $\leq_p$ INDEPENDENT SET

INDEPENDENT SET IS NP-COMPLETE

INDEPENDENT SET $\leq_p$ VERTEX COVER

VERTEX COVER IS NP-COMPLETE

SET COVER IS NP-COMPLETE

CIRCUIT SATISFYABILITY $\leq_p$ 3-SAT

3-SAT IS NP-COMPLETE

3-SAT $\leq_p$ INDEPENDENT SET

INDEPENDENT SET IS NP-COMPLETE

INDEPENDENT SET $\leq_p$ VERTEX COVER

VERTEX COVER IS NP-COMPLETE
SET COVER IS NP-COMPLETE

WE KNOW THOUSANDS OF PROBLEMS THAT ARE NP-COMPLETE.

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$$(x_1 \vee x_2) \wedge (x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_2 \vee \bar{x}_4)$$

↑

CAN YOU CONVERT THE ABOVE PROBLEM INTO A 3SAT PROBLEM.

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$$(x_1 \vee x_2) \wedge (x_1 \vee \bar{x}_2 \vee x_3) \wedge (x_2 \vee \bar{x}_4)$$

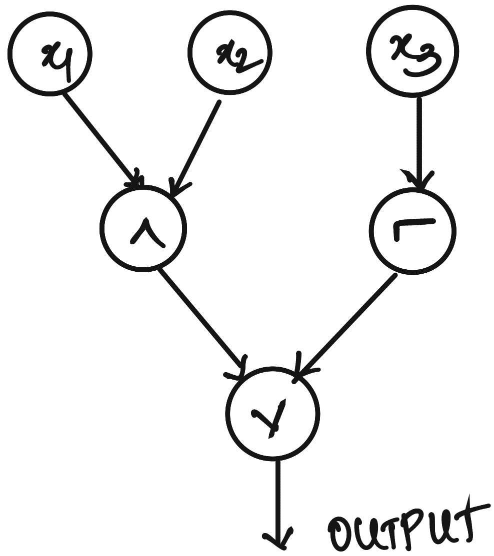
↑

CAN YOU CONVERT THE ABOVE PROBLEM INTO A 3SAT PROBLEM.

ADD A NEW VARIABLE x_5

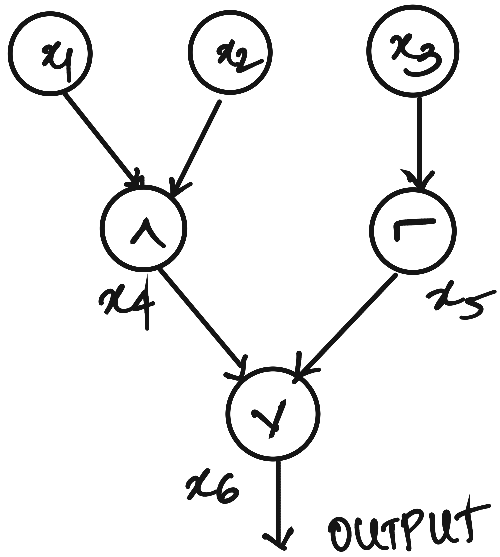
$$(x_1 \vee x_2 \vee x_5) \wedge (x_1 \vee x_2 \vee \bar{x}_5) \wedge (x_1 \vee \bar{x}_2 \vee x_3)$$
$$\wedge (x_2 \vee \bar{x}_4 \vee x_5) \wedge (x_2 \vee \bar{x}_4 \vee \bar{x}_5)$$

LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



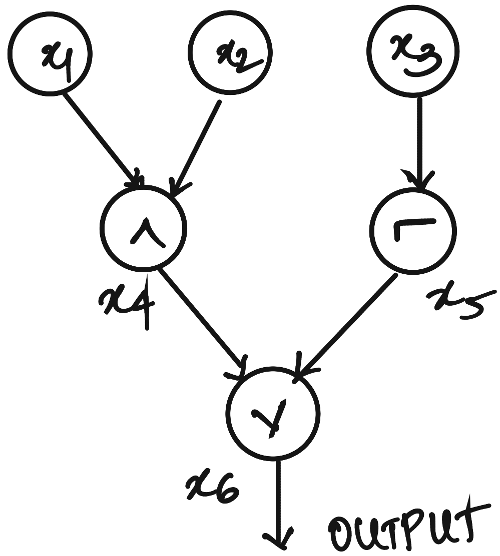
$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

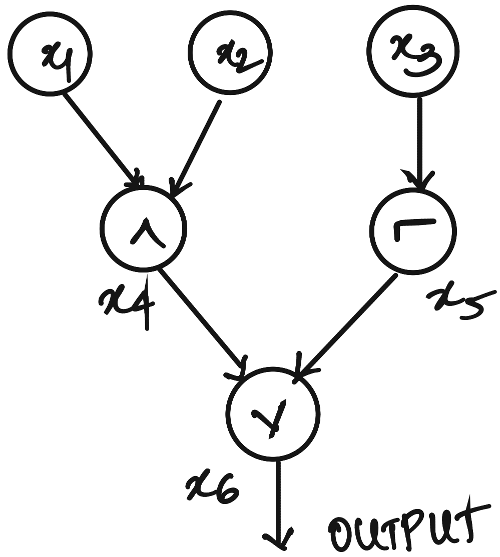


$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$x_5 = \overline{x_3}$

ADD CLAUSES WHICH WILL ENFORCE THIS

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

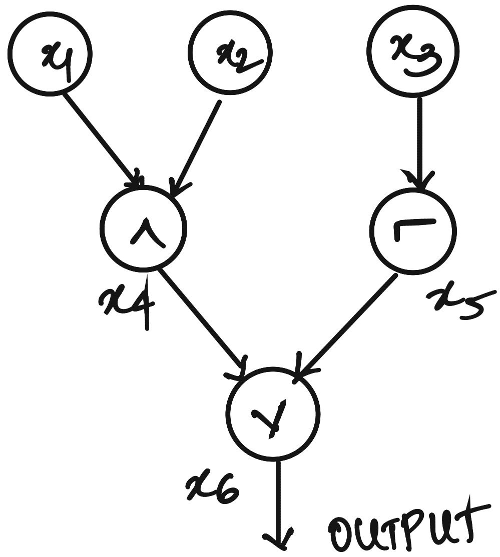
$x_5 = \overline{x_3}$

ADD CLAUSES WHICH WILL ENFORCE THIS

$(x_3 \lor x_5)$, $(\bar{x}_3 \lor \bar{x}_5)$

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$(x_3 \vee x_5), (\overline{x_3} \vee \overline{x_5})$

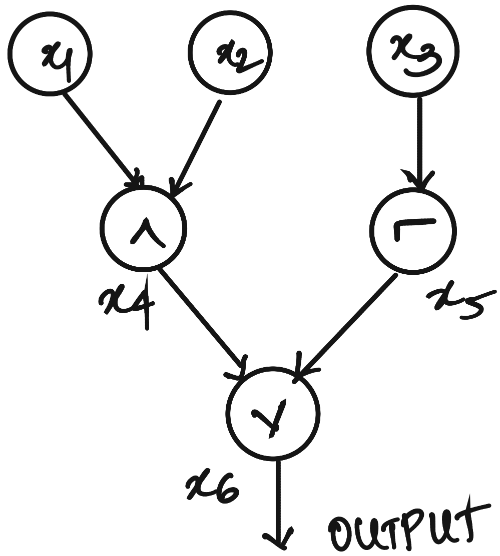


$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$$x_4 = x_1 \wedge x_2$$

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$(x_3 \vee x_5)$, $(\overline{x_3} \vee \overline{x_5})$



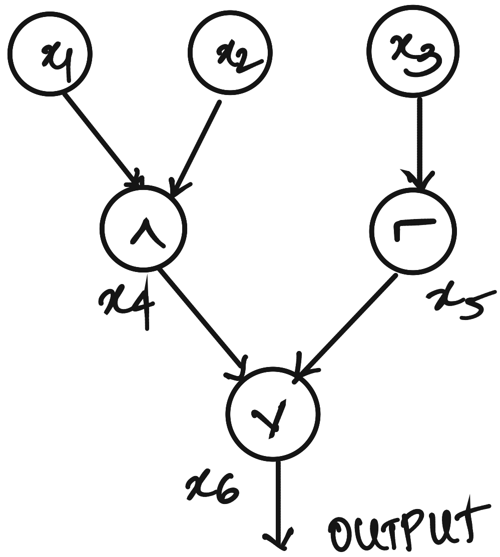
$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$$x_4 = x_1 \wedge x_2$$

x_1	x_2	x_4	
0	0	0	✓
0	0	1	✗
0	1	0	✓
0	1	1	✗
1	0	0	✓
1	0	1	✗
1	1	0	✗
1	1	1	✓

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$(x_3 \vee x_5), (\overline{x_3} \vee \overline{x_5})$



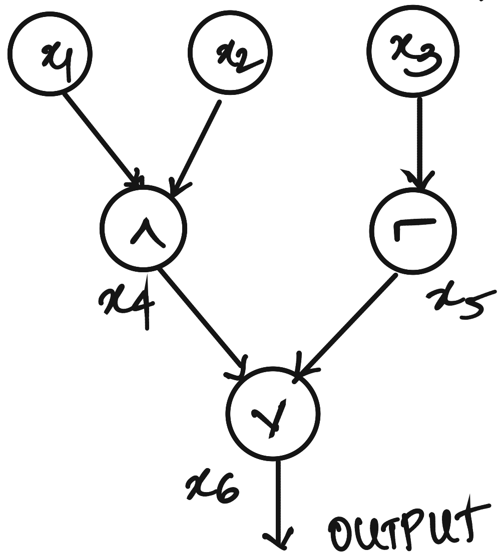
$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$$x_4 = x_1 \wedge x_2$$

x_1	x_2	x_4		
0	0	0	✓	
0	0	1	×	$x_1 \vee x_2 \vee \overline{x_4}$
0	1	0	✓	
0	1	1	×	$x_1 \vee \overline{x_2} \vee \overline{x_4}$
1	0	0	✓	
1	0	1	×	$\overline{x_1} \vee x_2 \vee \overline{x_4}$
1	1	0	×	$\overline{x_1} \vee \overline{x_2} \vee x_4$
1	1	1	✓	

LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$(x_3 \vee x_5)$, $(\bar{x_3} \vee \bar{x_5})$, $(x_1 \vee x_2 \vee \bar{x_4})$, $(x_1 \vee \bar{x_2} \vee x_4)$, $(x_1 \vee x_2 \vee \bar{x_4})$, $(\bar{x_1} \vee \bar{x_2} \vee x_4)$

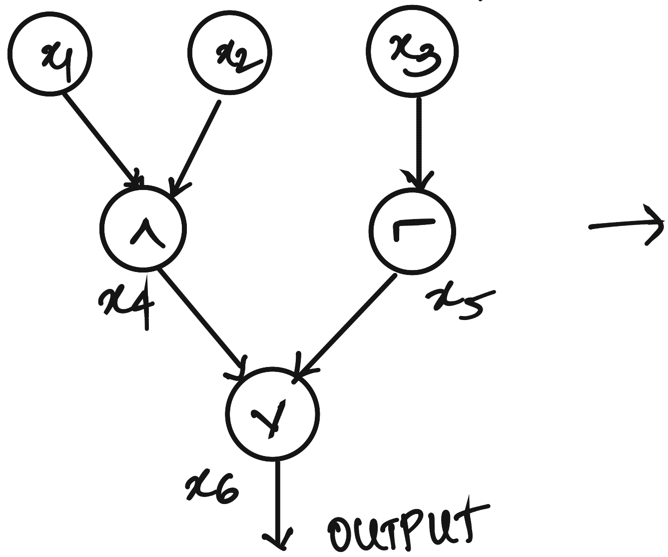


$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$$x_4 = x_1 \wedge x_2$$

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$(x_3 \vee x_5), (\bar{x}_3 \vee \bar{x}_5), (x_1 \vee x_2 \vee \bar{x}_4), (x_1 \vee \bar{x}_2 \vee x_4),$
$(x_1 \vee x_2 \vee \bar{x}_4), (\bar{x}_1 \vee \bar{x}_2 \vee x_4)$

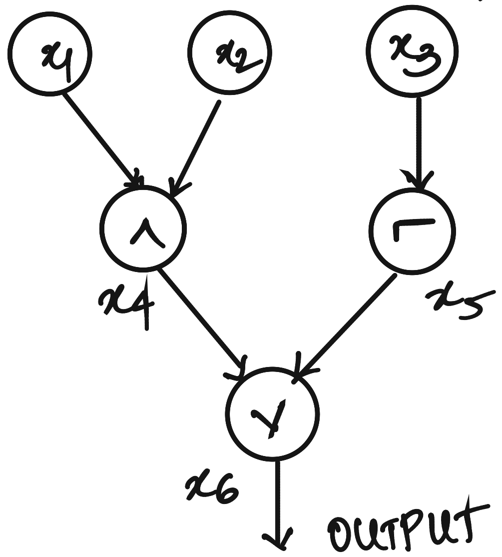


CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$$x_6 = x_4 \vee x_5$$

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$(x_3 \vee x_5)$, $(\bar{x}_3 \vee \bar{x}_5)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(x_1 \vee \bar{x}_2 \vee x_4)$,
$(x_1 \vee x_2 \vee \bar{x}_4)$, $(\bar{x}_1 \vee \bar{x}_2 \vee x_4)$



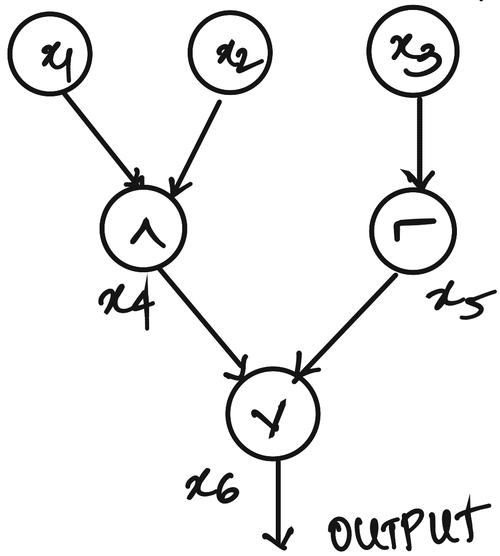
→ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$$x_6 = x_4 \vee x_5$$

x_4	x_5	x_6	
0	0	0	✓
0	0	1	✗
0	1	0	✗
0	1	1	✓
1	0	0	✗
1	0	1	✓
1	1	0	✗
1	1	1	✓

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

$(x_3 \vee x_5)$, $(\overline{x_3} \vee \overline{x_5})$, $(x_1 \vee x_2 \vee \overline{x_4})$, $(x_1 \vee \overline{x_2} \vee x_4)$,
$(x_1 \vee x_2 \vee \overline{x_4})$, $(\overline{x_1} \vee \overline{x_2} \vee x_4)$

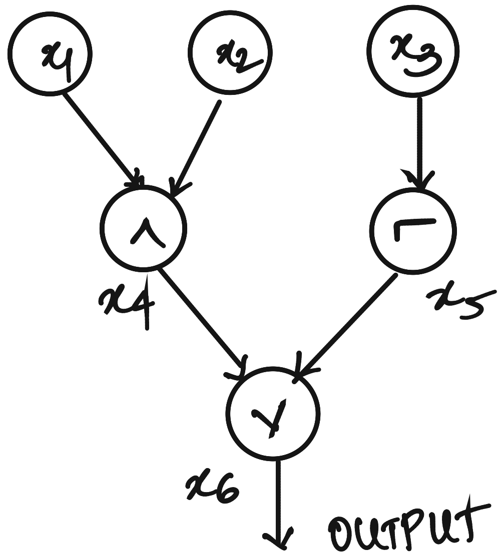


$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$$x_6 = x_4 \vee x_5$$

x_4	x_5	x_6		
0	0	0	✓	
0	0	1	✗	$(x_4 \vee x_5 \vee \overline{x_6})$
0	1	0	✗	$(x_4 \vee \overline{x_5} \vee x_6)$
0	1	1	✓	
1	0	0	✗	$(\overline{x_4} \vee x_5 \vee x_6)$
1	0	1	✓	
1	1	0	✗	$(\overline{x_4} \vee \overline{x_5} \vee x_6)$
1	1	1	✓	

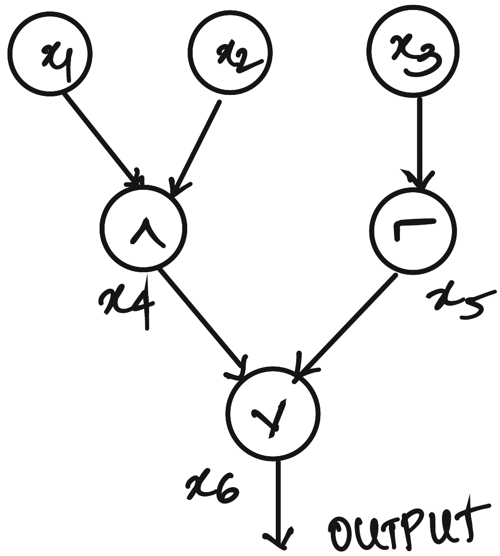
LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$(x_3 \vee x_5)$, $(\bar{x}_3 \vee \bar{x}_5)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(x_1 \vee \bar{x}_2 \vee x_4)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(\bar{x}_1 \vee \bar{x}_2 \vee x_4)$, $(x_4 \vee x_5 \vee \bar{x}_6)$, $(x_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$.

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

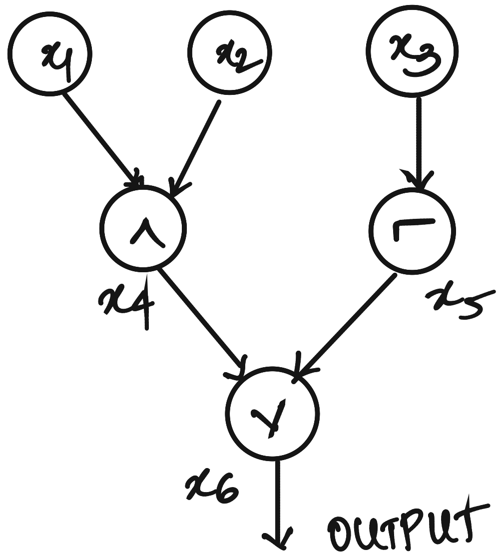


$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$(x_3 \vee x_5)$, $(\bar{x}_3 \vee \bar{x}_5)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(x_1 \vee \bar{x}_2 \vee x_4)$,
$(x_1 \vee x_2 \vee \bar{x}_4)$, $(\bar{x}_1 \vee \bar{x}_2 \vee x_4)$, $(x_4 \vee x_5 \vee \bar{x}_6)$, $(x_4 \vee \bar{x}_5 \vee x_6)$,
$(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, x_6

FORCES $x_6 = 1$ REQUIRES AS WE WANT $x_6 = 1$

LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT

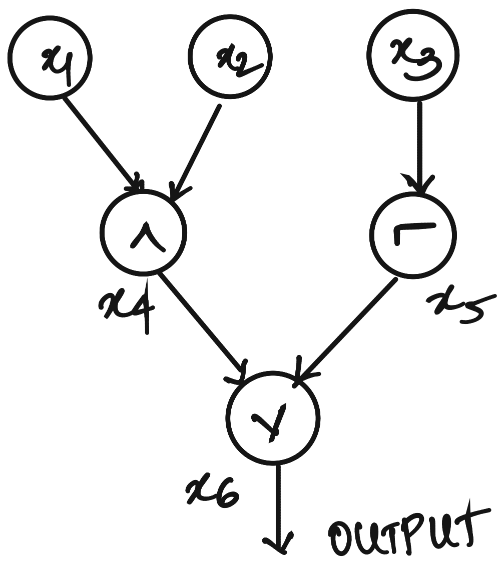


$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$(x_3 \vee x_5)$, $(\bar{x}_3 \vee \bar{x}_5)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(x_1 \vee \bar{x}_2 \vee x_4)$,
$(x_1 \vee x_2 \vee \bar{x}_4)$, $(\bar{x}_1 \vee \bar{x}_2 \vee x_4)$, $(x_4 \vee x_5 \vee \bar{x}_6)$, $(x_4 \vee \bar{x}_5 \vee x_6)$,
$(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, x_6

IS THERE A SATISFYABLE ASSIGNMENT TO THE ABOVE CLAUSES?

<u>LEMMA</u> : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

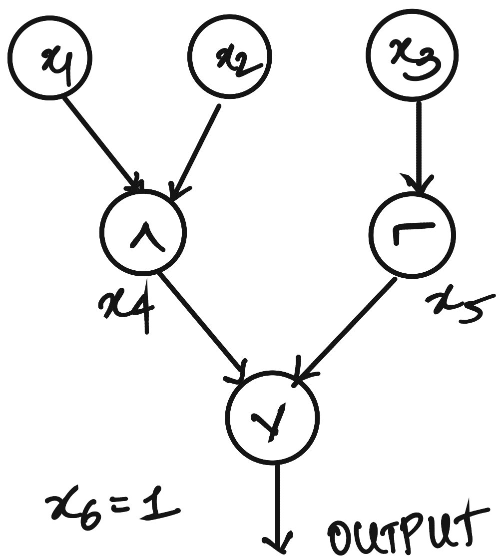
$(x_3 \vee x_5)$, $(\bar{x}_3 \vee \bar{x}_5)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(x_1 \vee \bar{x}_2 \vee x_4)$,
$(x_1 \vee x_2 \vee \bar{x}_4)$, $(\bar{x}_1 \vee \bar{x}_2 \vee x_4)$, $(x_4 \vee x_5 \vee \bar{x}_6)$, $(x_4 \vee \bar{x}_5 \vee x_6)$,
$(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, x_6

IS THERE A SATISFYABLE ASSIGNMENT TO THE ABOVE CLAUSES?

$\Downarrow$ YES

CAN WE SAY ITS A YES INSTANCE OF CIRCUIT SATISFYABILITY.

LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



→ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

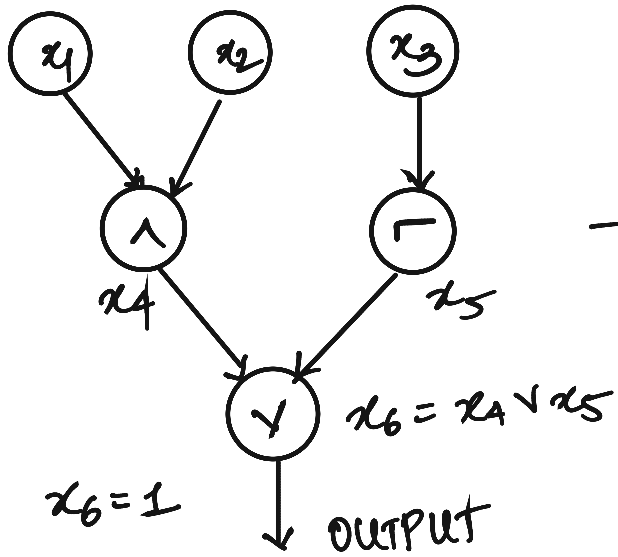
$(x_3 \vee x_5)$, $(\bar{x_3} \vee \bar{x_5})$, $(x_1 \vee x_2 \vee \bar{x_4})$, $(x_1 \vee \bar{x_2} \vee x_4)$, $(x_1 \vee x_2 \vee \bar{x_4})$, $(\bar{x_1} \vee \bar{x_2} \vee x_4)$, $(x_4 \vee x_5 \vee \bar{x_6})$, $(x_4 \vee \bar{x_5} \vee x_6)$, $(\bar{x_4} \vee \bar{x_5} \vee x_6)$, $(\bar{x_4} \vee \bar{x_5} \vee x_6)$, x_6.

IS THERE A SATISFYABLE ASSIGNMENT TO THE ABOVE CLAUSES?

$\Downarrow$ YES

CAN WE SAY ITS A YES INSTANCE OF CIRCUIT SATISFYABILITY.

LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

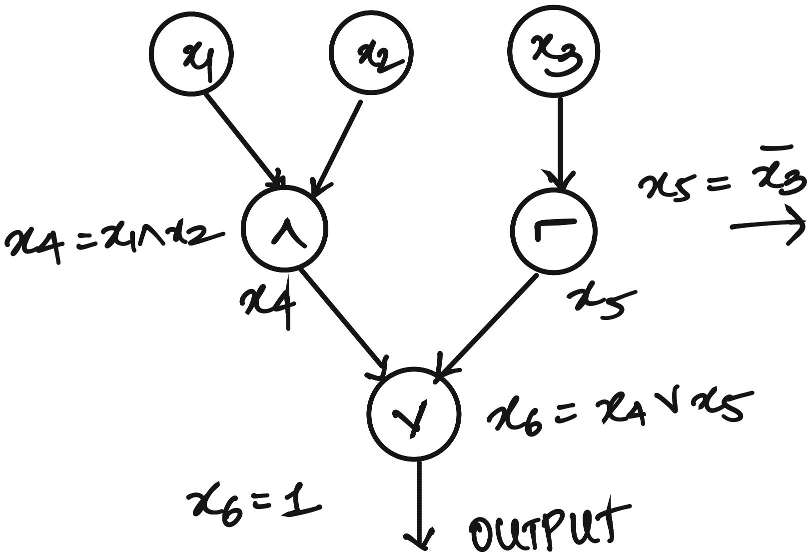
$(x_3 \vee x_5)$, $(\bar{x}_3 \vee \bar{x}_5)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(x_1 \vee \bar{x}_2 \vee x_4)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(\bar{x}_1 \vee \bar{x}_2 \vee x_4)$, $(x_4 \vee x_5 \vee \bar{x}_6)$, $(x_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, x_6

IS THERE A SATISFYABLE ASSIGNMENT TO THE ABOVE CLAUSES?

$\Downarrow$ YES

CAN WE SAY ITS A YES INSTANCE OF CIRCUIT SATISFYABILITY

LEMMA : CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

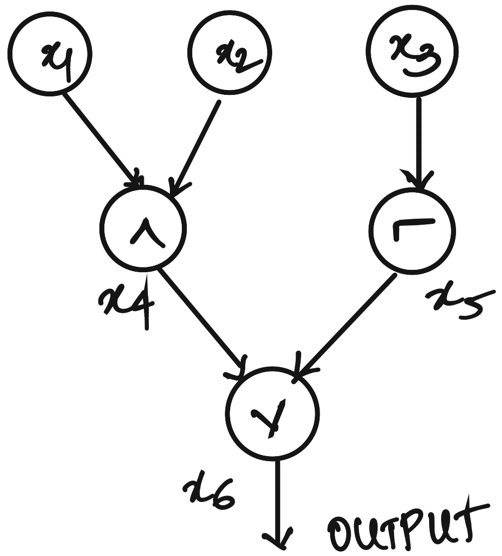
$(x_3 \vee x_5)$, $(\bar{x}_3 \vee \bar{x}_5)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(x_1 \vee \bar{x}_2 \vee x_4)$,
$(x_1 \vee x_2 \vee \bar{x}_4)$, $(\bar{x}_1 \vee \bar{x}_2 \vee x_4)$, $(x_4 \vee x_5 \vee \bar{x}_6)$, $(x_4 \vee \bar{x}_5 \vee x_6)$,
$(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, x_6

IS THERE A SATISFYABLE ASSIGNMENT TO THE ABOVE CLAUSES?

$\Downarrow$ YES

CAN WE SAY ITS A YES INSTANCE OF CIRCUIT SATISFYABILITY

LEMMA: CIRCUIT SATISFYBILITY $\leq_p$ 3-SAT



$\rightarrow$ CONVERT THIS INSTANCE TO A 3-SAT PROBLEM

$(x_3 \vee x_5)$, $(\bar{x}_3 \vee \bar{x}_5)$, $(x_1 \vee x_2 \vee \bar{x}_4)$, $(x_1 \vee \bar{x}_2 \vee x_4)$,
$(x_1 \vee x_2 \vee \bar{x}_4)$, $(\bar{x}_1 \vee \bar{x}_2 \vee x_4)$, $(x_4 \vee x_5 \vee \bar{x}_6)$, $(x_4 \vee \bar{x}_5 \vee x_6)$,
$(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, $(\bar{x}_4 \vee \bar{x}_5 \vee x_6)$, x_6

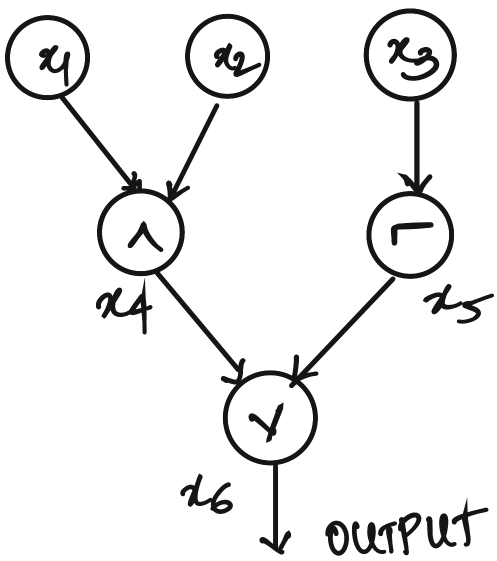
IS THERE A SATISFYABLE ASSIGNMENT TO THE ABOVE CLAUSES?

$\Downarrow$ YES

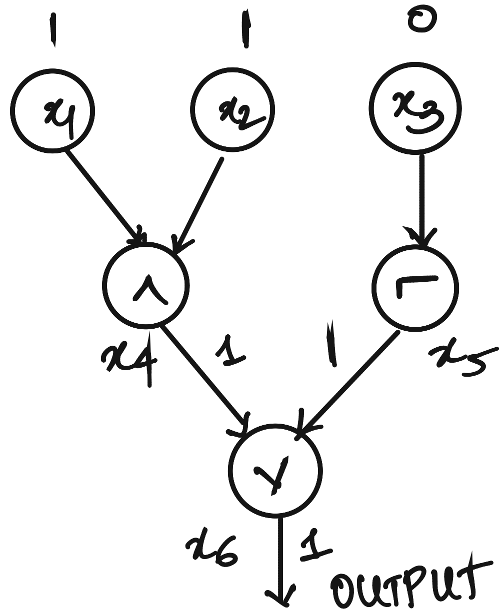
CAN WE SAY ITS A YES INSTANCE OF CIRCUIT SATISFYABILITY

$\Downarrow$ NO

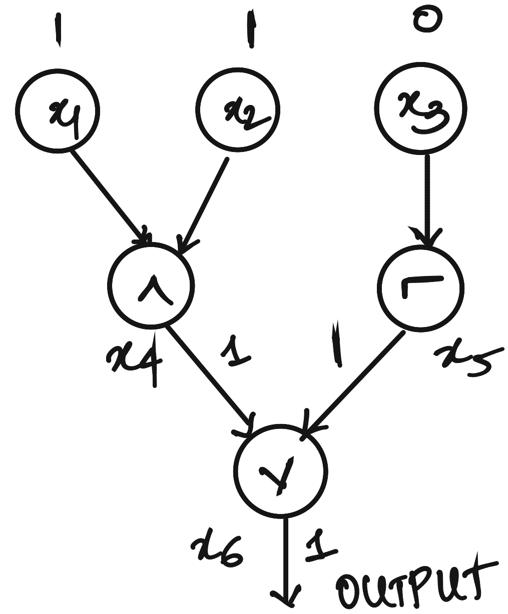
→ IF THE GIVEN INSTANCE IS A YES INSTANCE OF CIRCUIT SATISFYBILITY, THEN THE CORRESPONDING 3-SAT INSTANCE IS SATISFYABLE.



→ IF THE GIVEN INSTANCE IS A YES INSTANCE OF CIRCUIT SATISFYBILITY, THEN THE CORRESPONDING 3-SAT INSTANCE IS SATISFYABLE.



→ IF THE GIVEN INSTANCE IS A YES INSTANCE OF CIRCUIT SATISFYBILITY, THEN THE CORRESPONDING 3-SAT INSTANCE IS SATISFYABLE.



$x_1 = 1$

$x_2 = 1$

$x_3 = 0$ $\Rightarrow$ A SATISFYABLE ASSIGNMENT FOR 3-SAT

$x_4 = 1$

$x_5 = 1$

$x_6 = 1$

SUSPICIOUS USER PROBLEM.

→ YOU ARE OWNER OF IITGN NETWORK.

→ EACH USER OF IITGN ACCESSES ONE WEBSITE PER MINUTE. THIS ACCESS IS LOGGED → e.g.

(gmanoj, 24, www.facebook.com).

SUSPICIOUS USER PROBLEM.

→ YOU ARE OWNER OF IITGN NETWORK.

→ EACH USER OF IITGN ACCESSES ONE WEBSITE PER MINUTE. THIS ACCESS IS LOGGED → e.g.

(gmanoj, 24, www.facebook.com).

→ THERE WAS A CO-ORDINATED ATTACK FROM IITGN WHERE SOME USERS ACCESSED t DISTINCT SITE OVER t MINUTES

(u_1, i_1, s_1)

(u_2, i_2, s_2)

(u_1, i_3, s_3)

$\vdots$

(u_5, i_t, s_t)

→ IS THERE A GROUP OF K-USERS THAT HAVE CARRIED OUT THE ATTACK? OR THERE IS ATLEAST ONE USER IN THIS GROUP THAT ACCESSES s_j AT TIME i_j

$(1 \le j \le t)$

SUSPICIOUS USER PROBLEM.

→ YOU ARE OWNER OF IITGN NETWORK.

→ EACH USER OF IITGN ACCESSES ONE WEBSITE PER MINUTE. THIS ACCESS IS LOGGED → e.g.

(gmanoj, 24, www.facebook.com).

→ THERE WAS A CO-ORDINATED ATTACK FROM IITGN WHERE SOME USERS ACCESSED t DISTINCT SITE OVER t MINUTES

(u_1, i_1, s_1)

(u_2, i_2, s_2)

(u_1, i_3, s_3)

$\vdots$

(u_5, i_t, s_t)

→ IS THERE A GROUP OF K-USERS THAT HAVE CARRIED OUT THE ATTACK? OR THERE IS ATLEAST ONE USER IN THIS GROUP THAT ACCESSES s_j AT TIME i_j $(1 \le j \le t)$

→ SUP IS NP-COMPLETE.

IS $SUP \in NP$?

IS SUP $\in$ NP ?

YES.

REDUCE A KNOWN NP-COMPLETE PROBLEM

TO SUP.

IS SUP $\in$ NP ?

YES.

REDUCE A KNOWN NP-COMPLETE PROBLEM

TO SUP.

VERTEX COVER.

VC $\leq_p$ SUP

VC $\leq_p$ SUP

$\{e_1, e_2, e_3, \ldots, e_m\}$

where $e_j = (u_j, v_j)$

VC $\leq_p$ SUP

$\{e_1, e_2, e_3, \dots, e_m\}$

where $e_j = (u_j, v_j)$

IS THERE A SET OF ATMOST K NODES COVER ALL THE EDGES ?

$\Downarrow$

SUSPICIOUS USER PROBLEM

VC $\leq_p$ SUP

$\{e_1, e_2, e_3, \dots, e_m\}$

where $e_j = (u_j, v_j)$

IS THERE A SET OF ATMOST K NODES COVER ALL THE EDGES ?

$\Downarrow$

SUSPICIOUS USER PROBLEM

Q: MAKE LOGS USING THE ABOVE GRAPH ?

$VC \leq_p SUP$

$\{e_1, e_2, e_3, \ldots, e_m\}$

where $e_j = (u_j, v_j)$

IS THERE A SET OF ATMOST K NODES COVER ALL THE EDGES ?

$\Downarrow$

SUSPICIOUS USER PROBLEM

Q: MAKE LOGS USING THE ABOVE GRAPH ?

AT TIME i_j, SITE s_j WAS ACCESSED BY u_j & v_j AND ALL OTHER NODES ACCESSED NOTHING.

VC $\leq_p$ SUP

$\{e_1, e_2, e_3, \dots, e_m\}$

where $e_j = (u_j, v_j)$

IS THERE A SET OF ATMOST K NODES COVER ALL THE EDGES ?

$\Downarrow$

SUSPICIOUS USER PROBLEM

Q: MAKE LOGS USING THE ABOVE GRAPH ?

AT TIME j, SITE S_j WAS ACCESSED BY u_j & v_j AND ALL OTHER NODES ACCESSED NOTHING.

IS THERE A SET OF K USERS THAT ACCESSED SITES $S_1, S_2, \dots, S_m$ AT TIME $1, 2, \dots, m$ RESPECTIVELY?

$VC \leq_p SUP$

$\{e_1, e_2, e_3, \ldots, e_m\}$
where $e_j = (u_j, v_j)$

IS THERE A SET OF ATMOST K NODES
COVER ALL THE EDGES ?

INSTANCE OF
VC

INSTANCE OF
SUP

AT TIME i_j, SITE S_j
WAS ACCESSED BY u_j & v_j
AND ALL OTHER NODES
ACCESSED NOTHING.

IS THERE A SET OF K USERS
THAT ACCESSED SITES $s_1, s_2, \ldots, s_m$
AT TIME $1, 2, \ldots, m$ RESPECTIVELY?

AT TIME i_j, SITE s_j
WAS ACCESSED BY u_j & v_j
AND ALL OTHER NODES
ACCESSED NOTHING.

IS THERE A SET OF ATMOST K USERS
THAT ACCESSED SITES $s_1, s_2, \ldots, s_m$
AT TIME $1, 2, \ldots, m$ RESPECTIVELY?

$\downarrow$ YES

AT TIME i_j, SITE s_j
WAS ACCESSED BY u_j & v_j
AND ALL OTHER NODES
ACCESSED NOTHING.

IS THERE A SET OF ATMOST K USERS
THAT ACCESSED SITES $s_1, s_2, \dots, s_m$
AT TIME $1, 2, \dots, m$ RESPECTIVELY?

$\downarrow$ YES

A VERTEX COVER OF
SIZE $\leq K$

$\downarrow$ NO

AT TIME i_j, SITE s_j
WAS ACCESSED BY u_j & v_j
AND ALL OTHER NODES
ACCESSED NOTHING.

IS THERE A SET OF ATMOST K USERS
THAT ACCESSED SITES $s_1, s_2, \dots, s_m$
AT TIME $1, 2, \dots, m$ RESPECTIVELY?

$\downarrow$ YES

A VERTEX COVER OF
SIZE $\leq K$

$\downarrow$ NO

LEMMA: If $\exists$ A VERTEX COVER OF SIZE
ATMOST K IN G, THEN THE
CORRESPONDING SUP PROBLEM
IS A YES INSTANCE.