SUBSET SUM

INPUT: $S = \{x_1 \ldots x_k\}, t$ $\quad t, x_1, \ldots, x_k \in \mathbb{N}$

ACCEPT IFF THERE IS A SUBSET $y_1 .. y_s \subseteq S$ SUMMING TO t.

EXAMPLES

$\langle \{1,1,3\}, 4 \rangle$, $\langle \{1,1,3\}, 5 \rangle$ $\in$ SUBSET SUM

$\langle \{1,3\}, 5 \rangle$, $\langle \{4,11,3\}, 5 \rangle$ $\notin$ SUBSET SUM

THEOREM SUBSET-SUM IS NP-COMPLETE

PROOF.

1. SUBSET-SUM $\in$ NP: VERIFIER $V(\langle S,t \rangle, \{y_1 .. y_s\})$ CHECKS IF $\{y_1 .. y_s\} \subseteq S$ AND SUM TO t.

2. SHOW 3SAT $\leq_p$ SUBSET-SUM

GIVEN $\phi = C_1 \wedge .. \wedge C_k$, WE DEFINE S_ϕ, t_ϕ AS FOLLOWS.
S WILL CONSIST OF $2n + 2k$ NUMBERS, WHERE

n = NUMBER OF VARIABLES IN ϕ

k = NUMBER OF CLAUSES IN ϕ

EACH $s_i \in S_\phi$ WILL BE AN $(n+k)$-DIGIT NUMBER, BASE TEN. FURTHER, EACH DIGIT OF s_i WILL BE 1 OR 0.

t WILL BE THE FOLLOWING $(n+k)$-DIGIT NUMBER:

$$\underbrace{111 \cdots 1}_{n}\underbrace{333 \cdots 3}_{k}$$

$$S = \{ S_{x_1}, S_{\bar{x}_1}, S_{x_2}, S_{\bar{x}_2}, \ldots, S_{x_n}, S_{\bar{x}_n}, S_{g_1}, S_{h_1}, \ldots, S_{g_k}, S_{h_k} \}$$

S_{x_i} : The i^{th} digit is 1; the $(n+j)^{th}$ digit is 1 iff $x_i \in C_j$. All other digits are 0.

$S_{\bar{x}_i}$: The i^{th} digit is 1; the $(n+j)^{th}$ digit is 1 iff $\bar{x}_i \in C_j$ all other digits are 0

S_{g_i}, S_{h_i} : The $(n+i)^{th}$ digit is 1. All other digits are 0.

<u>Example</u> $\phi = C_1 \wedge C_2 = (x_1 \vee \bar{x}_2 \vee x_3) \wedge (\bar{x}_2 \vee x_3 \vee x_4)$

	1	2	3	4	C_1	C_2
S_{x_1}	1	0	0	0	1	0
$S_{\bar{x}_1}$	1	0	0	0	0	0
S_{x_2}	0	1	0	0	0	0
$S_{\bar{x}_2}$	0	1	0	0	1	1
S_{x_3}	0	0	1	0	1	1
$S_{\bar{x}_3}$	0	0	1	0	0	0
S_{x_4}	0	0	0	1	0	1
$S_{\bar{x}_4}$	0	0	0	1	0	0
S_{g_1}	0	0	0	0	1	0
S_{h_1}	0	0	0	0	1	0
S_{g_2}	0	0	0	0	0	1
S_{h_2}	0	0	0	0	0	1

t	1	1	1	1	3	3

CLAIM $\phi \in 3SAT$ IFF THERE IS A SUBSET OF S_ϕ SUMMING TO t_ϕ

PROOF

$\Rightarrow$: ASSUME $\phi \in 3SAT$, AND LET α SATISFY ϕ
CONSTRUCT $S'_\phi \subseteq S_\phi$ AS FOLLOWS

- $S_{x_i} \in S'_\phi$ IF $\alpha(x_i)=1$ OTHERWISE $S_{\bar{x}_i} \in S'_\phi$

  THIS MAKES 1^{st} n DIGITS OF S'_ϕ SUM TO $11\cdots1$

- FOR EACH $j \leq k$

  CHOOSE 1, 2, 0 OF S_{gj}, S_{hj} TO BE IN S'_ϕ
  TO MAKE $(n+j)^{th}$ DIGITS OF S'_ϕ SUM TO 3.

  THIS IS POSSIBLE SINCE THE CONTRIBUTION TO
  $(n+j)^{th}$ DIGIT BY S_{x_i}, $S_{\bar{x}_i}$ IS EITHER 1, 2 OR 3.

$\Leftarrow$: ASSUME $S'_\phi \subseteq S_\phi$ SUMS TO t. CONSTRUCT α AS FOLLOWS

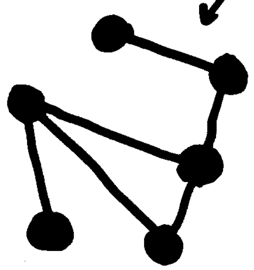
ALL DIGITS IN S_ϕ ARE 0 OR 1 AND EVERY
COLUMN HAS ≤ 5 1's SO THERE ARE NO CARRIES.
THUS S'_ϕ CONTAINS EXACTLY ONE OF S_{x_i}, $S_{\bar{x}_i}$
FOR ALL i.

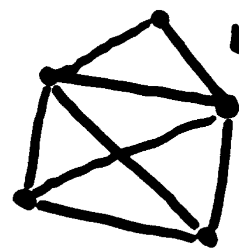
IF $S_{x_i} \in S'_\phi \Rightarrow \alpha(x_i)=1$
IF $S_{\bar{x}_i} \in S'_\phi \Rightarrow \alpha(x_i)=0$

THIS MUST SATISFY ϕ BECAUSE EVERY COLUMN
$(n+j)$, $j \geq 1$, SUMS TO 3 AND AT MOST
2 COMES FROM S_{gj}, S_{hj}, $j \leq k$.

3COL = { G | G IS AN UNDIRECTED GRAPH AND THE NODES OF G CAN BE COLORED B,G,R SUCH THAT NO 2 ADJACENT NODES HAVE SAME COLOR }

EXAMPLES





THEOREM 3COL IS NP COMPLETE.

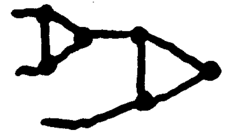
PROOF

1. 3COL $\in$ NP.

2. 3SAT $\leq_p$ 3COL.

GIVEN A 3CNF FORMULA ϕ, WE CONSTRUCT A GRAPH G_ϕ AS FOLLOWS:

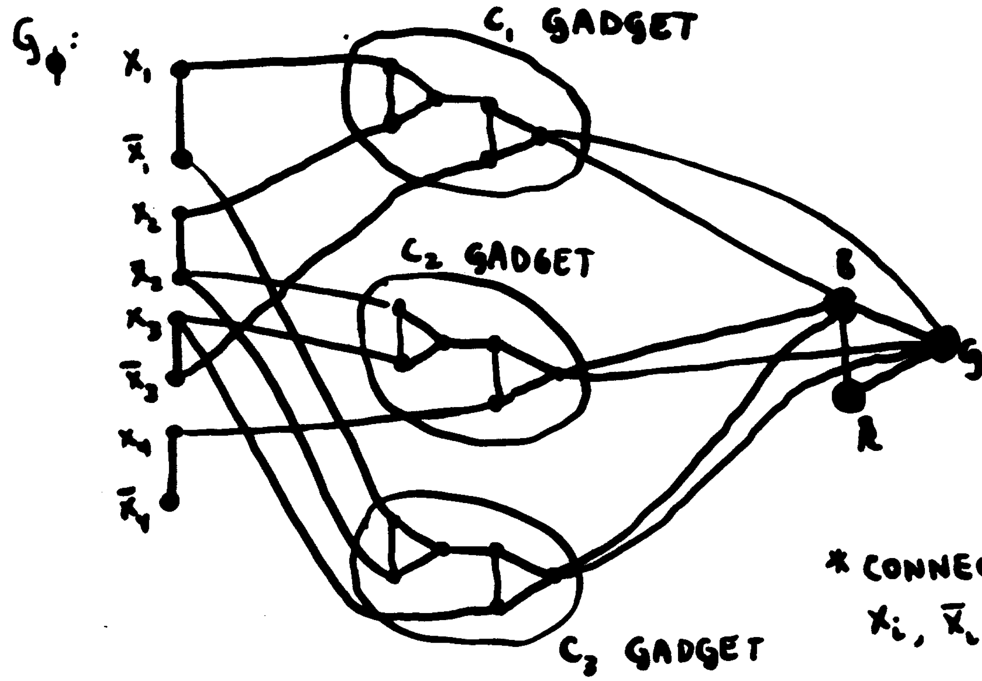
- A VARIABLE GADGET  FOR EACH VAR

- A CLAUSE GADGET  FOR EACH CLAUSE

- ONE TRIANGLE 

EXAMPLE $\phi = \overbrace{(x_1 \vee x_2 \vee \bar{x}_3)}^{C_1} \wedge \overbrace{(\bar{x}_2 \vee x_3 \vee x_4)}^{C_2} \overbrace{(\bar{x}_1 \vee \bar{x}_2 \vee x_3)}^{C_3}$

G_ϕ:



* CONNECT EACH x_i, $\bar{x}_i$ TO G.

- CAN ASSUME WITHOUT LOSS OF GENERALITY THAT NODE R IS COLORED RED, B IS BLUE, G IS GREEN IN ANY LEGAL COLORING. ALSO OUTNODE OF ANY CLAUSE GADGET IS R.

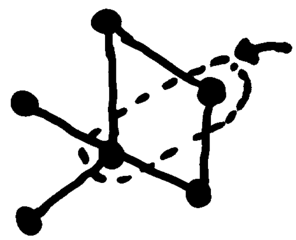
- IN ANY LEGAL COLORING, NODES $x_i / \bar{x}_i$ ARE COLORED EITHER R/B OR B/R.

- GIVEN ANY RED-BLUE COLORING TO INNODES OF A CLAUSE GADGET, THE CLAUSE GADGET IS 3-COLORABLE (WITH OUTNODE COLORED R) IF AND ONLY IF AT LEAST ONE INNODE IS COLORED R.

- BY ABOVE 3 POINTS, ϕ SATISFIABLE IFF G_ϕ HAS A LEGAL 3-COLORING.
  ($\alpha(x_i) = 1 \Rightarrow$ NODE $x_i = R$; $\alpha(x_i) = 0 \Rightarrow$ NODE $x_i = B$)

VERTEX-COVER = $\{(G,k) \mid G$ is an undirected graph with a k-NODE COVER$\}$

EXAMPLE



THEOREM VERTEX COVER IS NP-COMPLETE

PROOF

1. VERTEX COVER IS IN NP. ON $(x=(G,k), y)$ VERIFIER CHECKS WHETHER y DESCRIBES A k-NODE VERTEX COVER

2. WE WILL SHOW $3SAT \leq_p VC$ (VERTEX COVER)

GIVEN ϕ, A 3CNF formula, WE construct (G_ϕ, k_ϕ) AS FOLLOWS:

- EACH CLAUSE GIVES RISE TO A TRIANGLE OF VERTICES (CLAUSE GADGETS)
- EACH UNDERLYING LITERAL GIVES RISE TO A VERTEX (VARIABLE GADGETS)

# of vertices in $G_\phi = 2n + 3l$

n: NUMBER OF VARIABLES IN ϕ

l: NUMBER OF CLAUSES IN ϕ

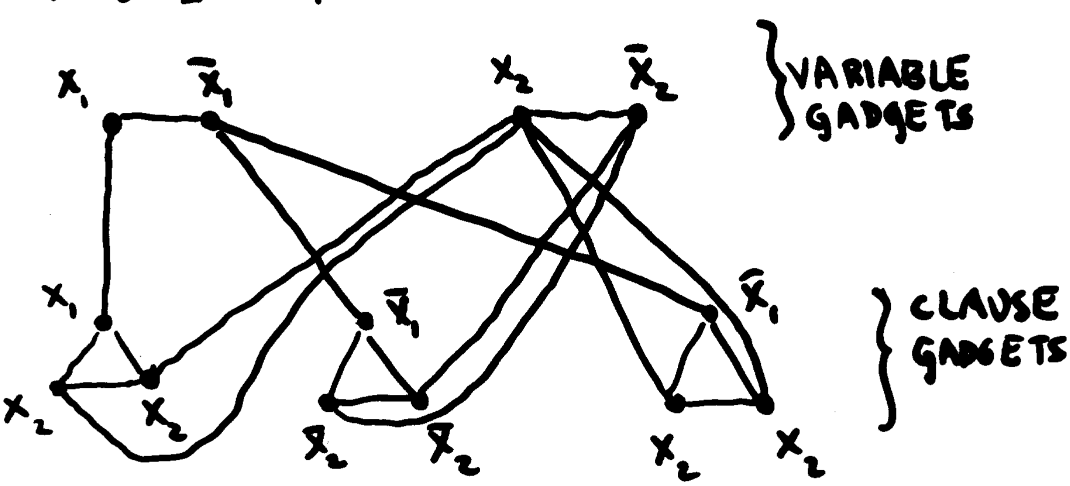
EXAMPLE

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

$$\Downarrow$$

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

G_ϕ:



$K_\phi = n + 2\ell$

$\phi \in 3SAT \Rightarrow (G_\phi, K_\phi) \in VC$: LET α SATISFY ϕ.

SELECT ONE NODE FROM EACH VARIABLE GADGET (THE NODE LABELLED WITH LITERAL SET TO 1 BY α) IN COVER

SELECT ONE NODE FROM EACH CLAUSE GADGET (THE NODE LABELLED WITH THE LITERAL IN THE CLAUSE SET TO 1 BY α) THE <u>OTHER</u> 2 NODES IN COVER

THIS FORMS A SIZE K_ϕ COVER.

$(G_\phi, K_\phi) \in VC \Rightarrow \phi \in 3SAT$:

ANY COVER HAS ONE NODE FROM EACH VAR GADGET AND 2 NODES FROM EACH CLAUSE GADGET.
LET α CORRESPOND TO NODES IN VAR GADGET.
α IS A SATISFYING ASSIGNMENT.

NP AS NONDETERMINISTIC POLYTIME

THERE IS AN ALTERNATIVE CHARACTERIZATION OF NP:

DEF'N

LET N BE A NONDETERMINISTIC TM THAT ALWAYS HALTS. THE RUNNING TIME OF N IS A FUNCTION $t: \mathbb{N} \to \mathbb{N}$ WHERE $t(n)$ IS THE MAXIMUM NUMBER OF STEPS THAT N TAKES ON A BRANCH OF ITS COMPUTATION, OVER ALL x, $|x| = n$.

NTIME$(t(n)) = \{ L \mid L$ IS A LANGUAGE OVER $\{0,1\}^*$ THAT IS DECIDED BY A $O(t(n))$ TIME NONDETERMINISTIC TM (THAT ALWAYS HALTS) $\}$

THEOREM $L \subseteq \{0,1\}^*$ IS IN NP IF AND ONLY IF $L \in \bigcup_k \text{NTIME}(n^k)$.

PROOF IDEA

$\Rightarrow$: LET $A \in$ NP. SHOW THAT A IS DECIDED BY A POLYTIME NTM. LET V BE THE VERIFIER FOR A. ASSUME V RUNS IN TIME n^k. CONSTRUCT N AS FOLLOWS.

N ON W, $|w| = n$:

- NONDETERMINISTICALLY SELECT c, $|c| \leq n^k$.
- RUN V ON (w,c). ACCEPT W IFF V ACCEPTS (w,c).

$\Leftarrow$: ASSUME A IS DECIDED BY NTM, N. CONSTRUCT V AS FOLLOWS

V ON (w,c):

- SIMULATE N ON W, USING C TO SELECT NONDETERMINISTIC CHOICE
- ACCEPT IFF N ACCEPTS ON THIS COMPUTATION PATH