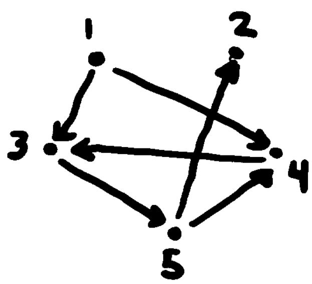
EXAMPLE 2 ANY $L \in P$ IS ALSO IN NP.

LET M BE A POLYTIME TM DECIDING L. THEN A POLYTIME VERIFIER $V(x,y)$ IGNORES y AND ACCEPTS IF AND ONLY IF M ACCEPTS x.

EXAMPLE 3

HAMPATH = {(G, s, t) | G IS A DIRECTED GRAPH WITH A HAMILTONIAN PATH FROM s TO t}

A PATH PASSING THROUGH EACH VERTEX EXACTLY ONCE



$(G,1,2) \in$ HAMPATH

$(G,1,5) \notin$ HAMPATH

VERIFIER: ON $x = (G,s,t)$, y

VIEW y AS A LIST OF NODES/VERTICES BEGINNING WITH s, ENDING WITH t.

IF y IS A LIST OF LENGTH n, EACH VERTEX LISTED EXACTLY ONCE, AND FOR ALL ADJACENT NUMBERS $i, i+1$ ON LIST, $(i, i+1)$ IS AN EDGE IN G, AND s, t ARE FIRST/LAST LIST ELEMENTS, THEN ACCEPT x, y

DEF'N EXPTIME $= \bigcup_k \text{TIME}(2^{n^k})$

THEOREM NP $\subseteq$ EXPTIME

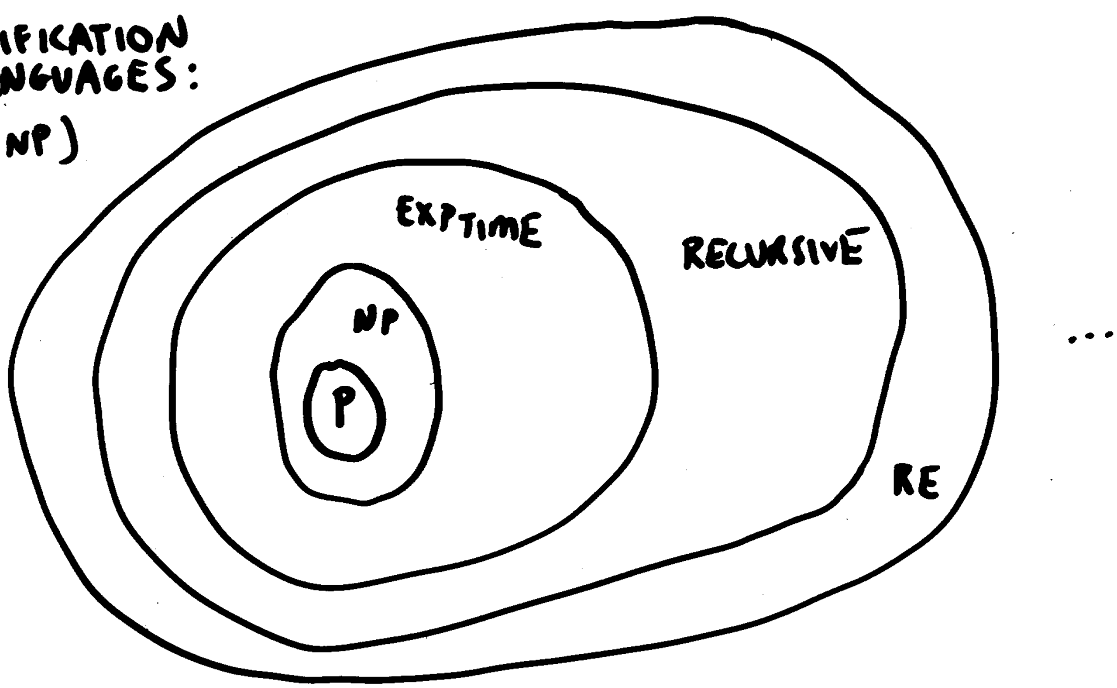
PROOF SKETCH

LET $L \in NP$. THEN THERE IS A POLYTIME VERIFIER V FOR L. ASSUME RUNTIME $V(x,y)$ IS AT MOST n^k FOR ALL x, $|x| = n$.

GIVEN x, SIMULATE $V(x,y)$ FOR ALL y, $|y| \leq |x|^k$
ACCEPT x IF AND ONLY IF V ACCEPTS (x,y) FOR AT LEAST ONE OF THE y's.

$$\text{RUNTIME} = \begin{pmatrix}\text{NUMBER of } y, \\ |y| \leq |x|^k\end{pmatrix} \cdot |x|^k = 2^{O(n^k)}$$

CLASSIFICATION OF LANGUAGES:
(IF P $\neq$ NP)



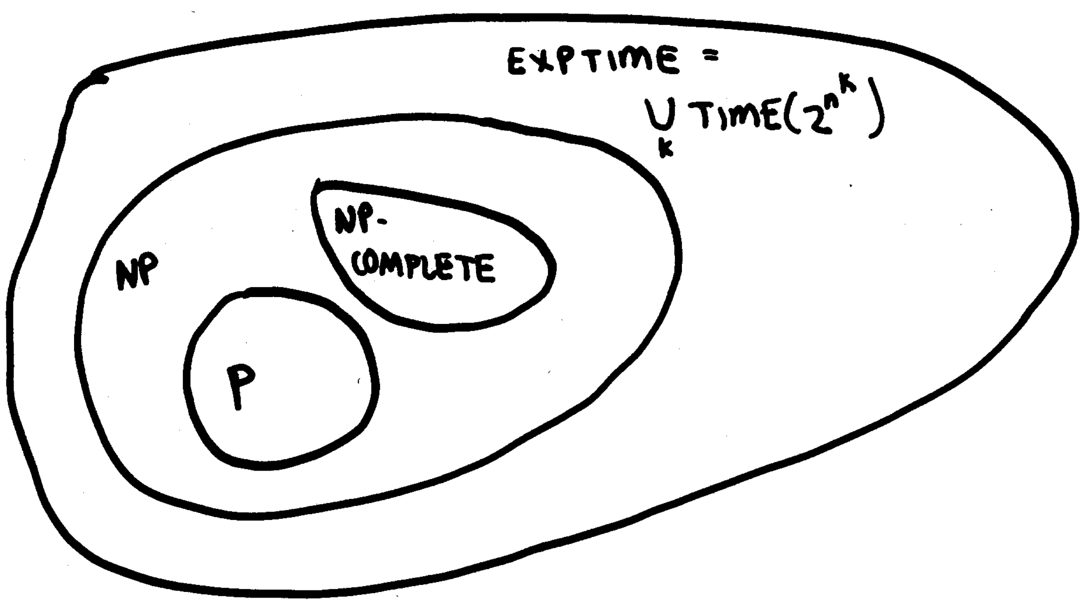
DOES $P = NP$?

- ONE OF THE MOST IMPORTANT MATHEMATICAL PROBLEMS TODAY IS TO DETERMINE IF $P = NP$.
- CLAY INSTITUTE OFFERING 1 MILLION US FOR SOLUTION

$P \approx$ LANGUAGES WHERE MEMBERSHIP CAN BE COMPUTED EFFICIENTLY

$NP \approx$ LANGUAGES WHERE MEMBERSHIP CAN BE VERIFIED EFFICIENTLY.

- IT IS EASY TO SEE THAT $P \subseteq NP$.
  BUT IS THERE A LANGUAGE $L \in NP$ SUCH THAT $L \notin P$?
- MOST PEOPLE CONJECTURE $P \subsetneq NP$, SHOWN BELOW.



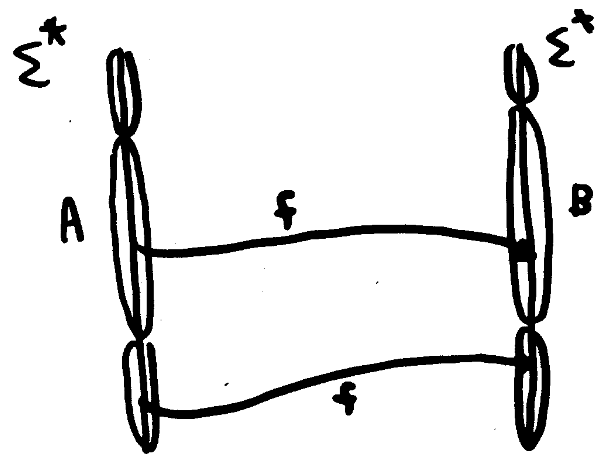
NP COMPLETENESS

COOK AND LEVIN PROVED THAT THERE ARE CERTAIN LANGUAGES IN NP, <u>THE NP-COMPLETE LANGUAGES</u>, SUCH THAT IF L IS NP-COMPLETE, AND $L \in P$, THEN $P = NP$.

<u>DEF'N</u> $f: \Sigma^* \to \Sigma^*$ IS A POLYTIME (COMPUTABLE) FUNCTION IF SOME POLYTIME TM M COMPUTES f.

<u>DEF'N</u> A LANGUAGE A OVER Σ^* IS POLYTIME (MANY-ONE) REDUCIBLE TO LANGUAGE B, $A \leq_p B$, IF THERE IS A POLYTIME FUNCTION $f: \Sigma^* \to \Sigma^*$ SUCH THAT

$$w \in A \quad \text{IF AND ONLY IF} \quad f(w) \in B$$



<u>THEOREM</u> $A \leq_p B$ AND $B \in P \Rightarrow A \in P$.

<u>PROOF</u> LET M BE A POLYTIME DECIDER FOR B. CONSTRUCT A POLYTIME DECIDER, N, FOR A AS FOLLOWS:

<u>N ON x:</u> COMPUTE $f(x)$
RUN M ON $f(x)$. ACCEPT IFF M ACCEPTS.

★ THESE DEFINITIONS AND THEOREM ARE LIKE TM REDUCIBILITY BUT SCALED DOWN TO POLYTIME COMPUTATION.

DEF'N A LANGUAGE B IS <u>NP-COMPLETE</u> IF

1. $B \in NP$
2. FOR ALL $A \in NP$, $A \leq_p B$.

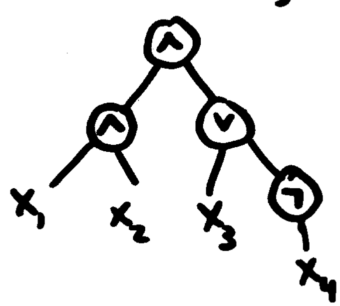
THEOREM IF B IS NP-COMPLETE AND $B \in P$, THEN $P = NP$.

PROOF ASSUME B IS NP-COMPLETE AND $B \in P$. SHOW FOR ANY $A \in NP$, $A \in P$. BY THE PREVIOUS THEOREM AND ABOVE, $A \in P$.

$\boxed{\text{SAT}}$

INPUT: A BOOLEAN FORMULA, WITH N INPUTS

ϕ:



ACCEPT IF THERE IS A 0-1 ASSIGNMENT TO VARIABLES SUCH THAT ϕ EVALUATES TO 1 ON THIS ASSIGNMENT.

ENCODING ϕ AS A STRING OVER $\{0,1\}$, $|\langle\phi\rangle|$ WILL BE AT MOST m^2, m = NUMBER OF LOGICAL CONNECTIVES IN ϕ.

$\boxed{\begin{array}{l}\underline{\text{THEOREM}}\ \text{(COOK, LEVIN)} \\ \qquad \text{SAT IS NP-COMPLETE}\end{array}}$

AS WE SAW WHEN STUDYING UNDECIDABILITY, ONCE WE FOUND ONE UNDECIDABLE LANGUAGE, WE CAN PROVE THAT OTHERS ARE ALSO UNDECIDABLE VIA REDUCTIONS. SIMILARLY ONCE WE HAVE ONE NP-COMPLETE LANGUAGE (SAT), WE CAN PROVE OTHERS ARE NP-COMPLETE VIA REDUCTIONS

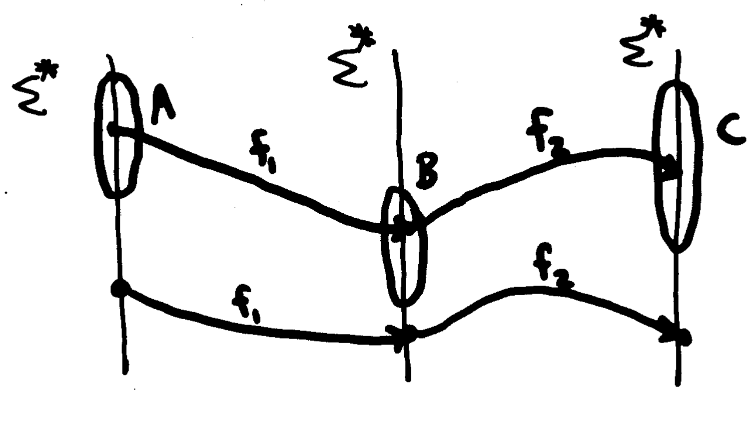
<u>THEOREM</u> IF B IS NP-COMPLETE AND $B \leq_p C$, FOR $C \in NP$, THEN C IS NP-COMPLETE.

<u>PROOF</u> WE KNOW $C \in NP$. TO SHOW THAT C IS NP-COMPLETE WE WANT TO SHOW THAT FOR ANY $A \in NP$, $A \leq_p C$.

WE KNOW: (i) $A \leq_p B$ BY NP-COMPLETENESS OF B

(ii) $B \leq_p C$ BY ASSUMPTION

THUS $A \leq_p C$ BECAUSE POLYTIME REDUCTIONS COMPOSE.
LET f_1 BE A POLYTIME REDUCTION FROM A TO B.
LET f_2 BE A POLYTIME REDUCTION FROM B TO C.
THEN $f_1 \circ f_2$ $[f_1 \circ f_2(x) = f_1(f_2(x))]$ IS A POLYTIME REDUCTION FROM A TO C.



$\boxed{\text{3SAT}}$ INPUT $f = C_1 \wedge C_2 \wedge \cdots \wedge C_m$

EACH C_i IS A CLAUSE CONSISTING OF A DISJUNCTION OF AT MOST 3 LITERALS.

<u>EXAMPLE</u> $f = (x_1 \vee x_2 \vee \bar{x}_3) \wedge (x_1 \vee \bar{x}_4 \vee x_5) \wedge (x_1 \vee x_3) \wedge (x_1 \vee \bar{x}_2 \vee x_2)$

ACCEPT IF THERE IS A 0-1 ASSIGNMENT α TO UNDERLYING VARIABLES SUCH THAT $f(\alpha) = 1$.

<u>THEOREM</u> 3SAT IS NP-COMPLETE.

<u>PROOF.</u>

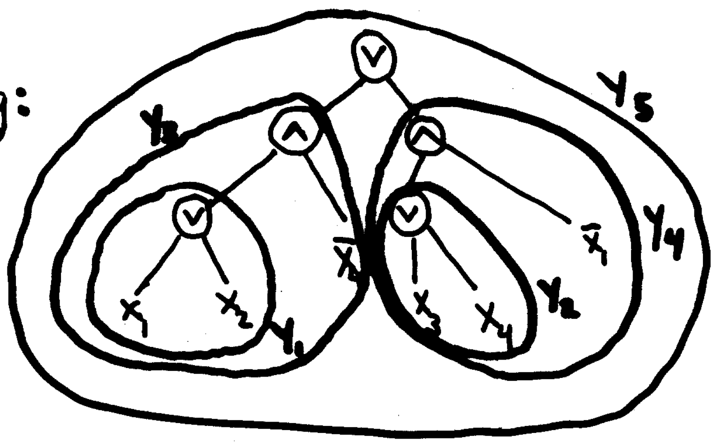
① 3SAT $\in$ NP. VERIFIER $V(f, \alpha)$ CHECKS WHETHER $f(\alpha) = 1$

② SAT $\leq_p$ 3SAT:

LET g BE A FORMULA WITH VARIABLES $x_1, \ldots, x_n$

ASSUME NEGATIONS ONLY AT LEAVES OF g.

g:



<u>Equations defining y's:</u>

$y_1 \leftrightarrow x_1 \vee x_2$

$y_2 \leftrightarrow x_3 \vee x_4$

$y_3 \leftrightarrow y_1 \wedge \bar{x}_4$

$y_4 \leftrightarrow y_2 \wedge \bar{x}_1$

$y_5 \leftrightarrow y_3 \vee y_4$

y_6

$$f_g = \left\{ \begin{array}{l} (\bar{y}_1 \vee x_1 \vee x_2), (\bar{x}_1 \vee y_1), (\bar{x}_2 \vee y_1), \\ (\bar{y}_2 \vee x_3 \vee x_4), (\bar{x}_3 \vee y_2), (\bar{x}_4 \vee y_2), \\ (\bar{y}_3 \vee y_1), (\bar{y}_3 \vee \bar{x}_4), (\bar{y}_1 \vee x_4 \vee y_3), \\ (\bar{y}_4 \vee y_2), (\bar{y}_4 \vee \bar{x}_1), (\bar{y}_2 \vee x_1 \vee y_4), \\ (\bar{y}_5 \vee y_3 \vee y_4), (\bar{y}_3 \vee y_5), (\bar{y}_4 \vee y_5), \\ y_6 \end{array} \right\}$$

CLAIM $g \in SAT$ IFF $f_g \in 3SAT$

PROOF

$\Rightarrow$: LET $g \in SAT$, AND LET α BE A SATISFYING ASSIGNMENT TO $\{x_1 .. x_n\}$. EXTEND α TO $\{y_1 .. y_k\}$ BY THE DEFINING EQUATIONS FOR y's. THE EXTENDED ASSIGNMENT SATISFIES f_g.

$\Rightarrow$: LET $f_g \in 3SAT$ AND LET α' BE A SATISFYING ASSIGNMENT. THEN THE DEFINING EQUATIONS FOR y's ARE ALL SATISFIABLE, SO VALUE OF $g(\alpha')$ = VALUE OF $y_k = 1$, AND THUS α' SATISFIES g AS WELL.

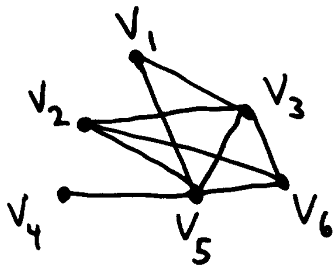
OTHER NP-COMPLETE LANGUAGES

CLIQUE

INPUT: A GRAPH $G=(V,E)$ AND A NUMBER K

ACCEPT IF AND ONLY IF G CONTAINS A CLIQUE OF SIZE K.

EXAMPLE



$\langle G, K=4\rangle \in$ CLIQUE

THEOREM CLIQUE IS NP-COMPLETE.

PROOF

1. CLIQUE $\in$ NP. WE ALREADY SHOWED THIS.

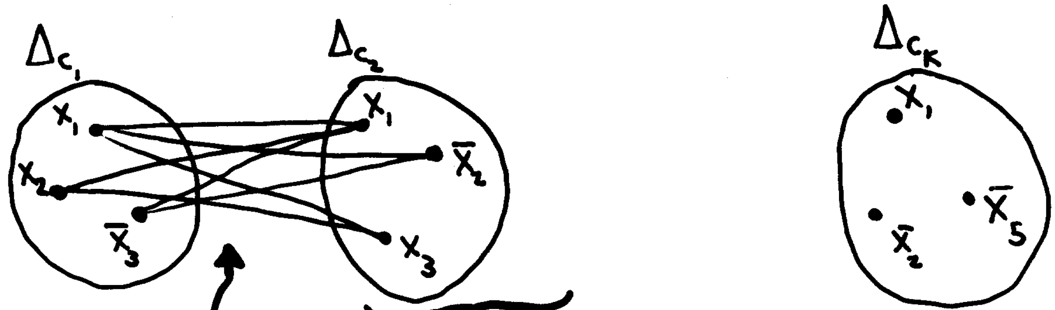
2. 3SAT $\leq_p$ CLIQUE

GIVEN ϕ, PRODUCE A GRAPH AND K, (G_ϕ, K_ϕ) AS FOLLOWS

$$\phi = \overbrace{(x_1 \vee x_2 \vee \bar{x}_3)}^{c_1} \wedge \overbrace{(x_3 \vee x_1 \vee \bar{x}_2)}^{c_2} \wedge \cdots \wedge \overbrace{(x_1 \vee \bar{x}_2 \vee \bar{x}_5)}^{c_K}$$

$G_\phi = (V,E)$, $|V| = 3K$, $K_\phi = K$

G_ϕ:



ALL EDGES EXCEPT BETWEEN x_i, $\bar{x}_i$

NO EDGES WITHIN A CLOUD

CORRECTNESS OF REDUCTION

1. REDUCTION IS IN P
2. SHOW ϕ SATISFIABLE IFF $(G_\phi, k_\phi) \in$ CLIQUE

$\Rightarrow$. ASSUME $\phi \in$ 3SAT. LET $\phi(\alpha) = 1$.
THEN FOR EACH CLAUSE $C_i \in \phi$, SOME LITERAL $l_i^* \in C_i$ IS MADE TRUE BY α.
THE ASSOCIATED SET OF NODES
$(l_1^*$ in $\Delta_{C_1})$, $(l_2^*$ in $\Delta_{C_2})$, ..., $(l_k^*$ in $\Delta_{C_k})$
FORMS A K-CLIQUE IN G_ϕ.

$\Leftarrow$. ASSUME G_ϕ HAS A K-CLIQUE. THEN BECAUSE THERE ARE NO EDGES WITHIN A CLOUD, AND EXACTLY K CLOUDS, THE CLIQUE MUST CONTAIN ONE NODE FROM EACH CLOUD.
ALSO CLIQUE NODES CANNOT CONTAIN ONE LABELLED x AND ANOTHER LABELLED $\bar{x}$, SINCE THERE IS NO EDGE BETWEEN x AND $\bar{x}$.
ASSIGN α ACCORDING TO THE LABELLING OF NODES IN CLIQUE. α SATISFIES ϕ.