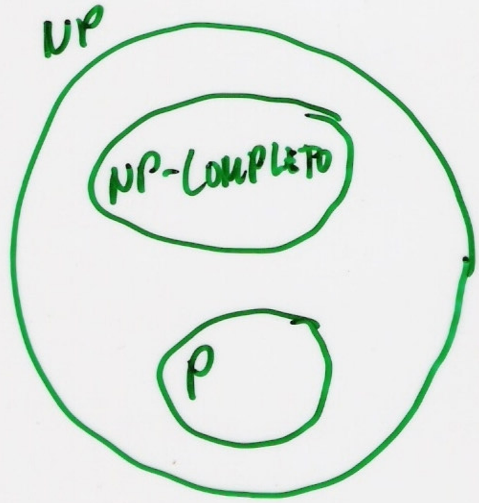
CLASSE P, NP E NP-COMPLETOS



PROVAR NP-COMPLETUDE INDICA QUE NÃO SE CONHECE ALGORITMO DETERMINÍSTICO CAPAZ DE OBTER A RESPOSTA SIM/NÃO CORRETA PARA QUALQUER INSTÂNCIA DO PROBLEMA P. EM TEMPO POLINOMIAL.

- ALGUMAS PROVAS DE NP-COMPLETUDE

SEJA UM PROBLEMA p

O que deve ser provado?

(1) $p \in NP$

APRESENTAR UM CERTIFICADO DA RESPOSTA SIM ($I_p \in Y_p$) QUE PODE SER VERIFICADO EM $O(n^k)$

(2) $\exists\ p' \in$ NP-COMPLETO TAL QUE

$$p' \propto_{POLY} p$$

I.E., APRESENTAR UMA REDUÇÃO DE p' EM p ($\propto_{POLY}$) ONDE POSSA SER VERIFICADO QUE

$$I_{p'} \in Y_{p'} \iff I_p \in Y_p$$

COMO PROVAR NP-COMPLETUDE

$$
\begin{tikzcd}
 & \text{SAT} & & \\
 & \text{3-SAT} \arrow[u] & & \\
\text{3DM} \arrow[ur] & & \text{VC} \arrow[ul] & \\
\text{PARTIÇÃO} \arrow[u] & & \text{HC} \arrow[u] & \text{CLIQUE} \arrow[ul]
\end{tikzcd}
$$

$\mathcal{P}$

(1) $\mathcal{P} \in NP$

(2) APRESENTAR UMA REDUÇÃO DE UM PROBLEMA EM NP-COMPLETO A $\mathcal{P}$ EM TEMPO POLINOMIAL

TEO: 3-SAT É NP-COMPLETO

SAT $\propto_{poly}$ 3-SAT

SAT $X = \{x_1, \dots, x_n\}$ $C = \{C_1, \dots, C_m\}$

3-SAT $Y = \{y_1, \dots, y_t\}$ $\mathcal{C} = \{\mathcal{C}_1, \dots, \mathcal{C}_p\}$ $|\mathcal{C}_i| = 3 \; \forall i$

CLÁUSULAS DE SAT

$|C_i| = 1$ $x_j^{\alpha_j}$ $\rightarrow$ $x_j^{\alpha_j} \vee x_j^{\alpha_j} \vee x_j^{\alpha_j}$

$|C_i| = 2$ $x_i^{\alpha_i} \vee x_j^{\alpha_j}$ $\rightarrow$ $x_i^{\alpha_i} \vee x_j^{\alpha_j} \vee x_j^{\alpha_j}$

$|C_i| = 3$ OK

$|C_i| > 3$

$x_{i_1}^{\alpha_{i_1}} \vee x_{i_2}^{\alpha_{i_2}} \vee \dots \vee x_{i_K}^{\alpha_{i_K}}$ $\rightarrow$

$x_{i_1}^{\alpha_{i_1}} \vee x_{i_2}^{\alpha_{i_2}} \vee z_1$

$\bar{z}_1 \vee x_{i_3}^{\alpha_{i_3}} \vee z_2$

$\bar{z}_2 \vee \dots$

$\dots \vee z_{K-3}$

$\bar{z}_{K-3} \vee x_{i_{K-1}}^{\alpha_{i_{K-1}}} \vee x_{i_K}^{\alpha_{i_K}}$

VERTEX COVER (VC)

INSTÂNCIA: UM GRAFO $G=(V,E)$ E UM INTEIRO K, $0 \leq K \leq |V|$

PERGUNTA: $\exists\ S \subseteq V$ t.q. $|S| \leq K$

E $\forall (u,v) \in E$, $u \in S$ ou $v \in S$

TEO: VC É NP-COMPLETO

(i) VC $\in$ NP (EXERCÍCIO)

(ii) 3-SAT $\propto$ VC

3-SAT INSTÂNCIA: $U = \{u_1, \dots, u_n\}$
$C = \{c_1, \dots, c_m\}$

(P0) - $V \leftarrow \emptyset$, $E \leftarrow \emptyset$

(P1) - $\forall u_i \in U$, $V \leftarrow V \cup \{u_i, \bar{u}_i\}$
$E \leftarrow E \cup \{(u_i, \bar{u}_i)\}$

(OBSERVE QUE UM VC TERÁ QUE USAR PELO MENOS UM ENTRE u_i E $\bar{u}_i$ PARA COBRIR $(u_i, \bar{u}_i)$.)

[P2]- $\forall \; c_j = \{a_1^j, a_2^j, a_3^j\} \in C$

$$V \leftarrow V \cup \{a_1^j, a_2^j, a_3^j\}$$

$$E \leftarrow E \cup \{(a_1^j, a_2^j), (a_2^j, a_3^j), (a_1^j, a_3^j)$$

OBSERVE QUE PELO MENOS DOIS VÉRTICES ENTRE a_1^j, a_2^j E a_3^j TEM QUE ESTAR NO VC PARA COBRIR (a_1^j, a_2^j), (a_2^j, a_3^j) E $(a_1^j, a_3$

[P3]- SEJA $c_j = \{x_j, y_j, z_j\} \in C$ ONDE x_j, y_j E z_j SÃO OS LITERAIS DE c_j, u_i OU $\bar{u}_i$

$\forall \; c_j = \{x_j, y_j, z_j\} \in C$

$$E \leftarrow E \cup \{(a_1^j, x_j), (a_2^j, y_j), (a_3^j, z_j)\}$$

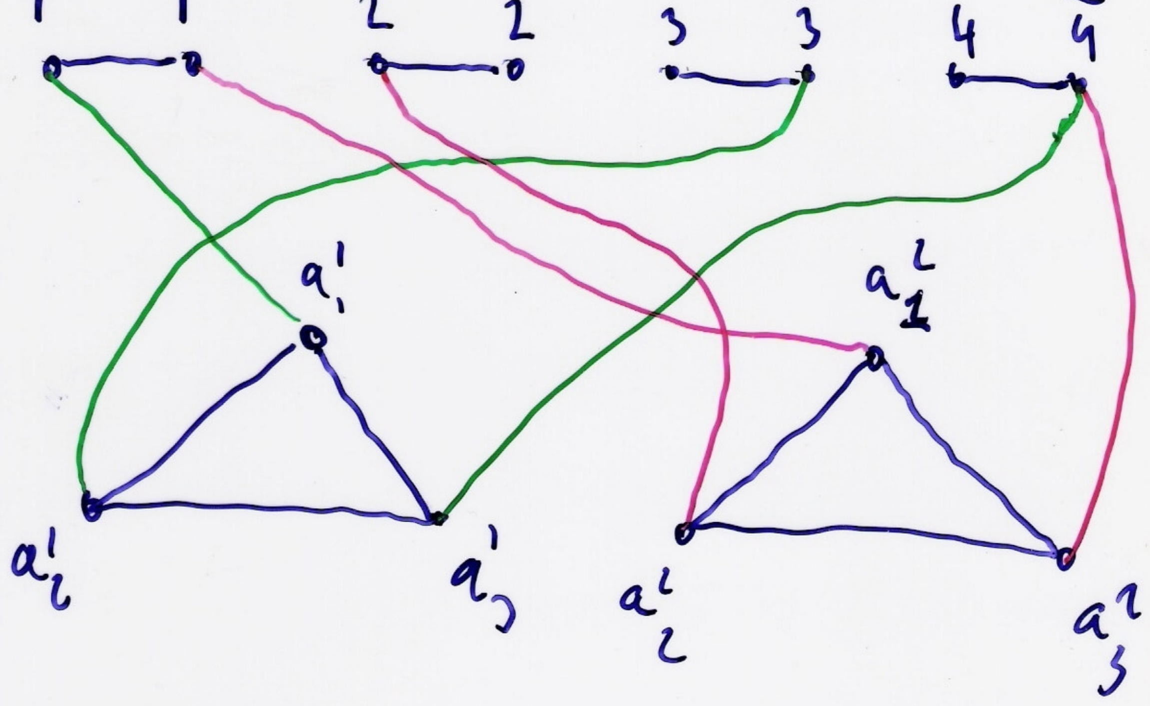
- FINALMENTE

$$K = n + 2m$$

$n + 2m$ É O NÚMERO MÍNIMO DE VÉRTICES NECESSÁRIOS PARA COBRIR AS ARESTAS INCLUÍDAS EM (P_1) E (P_2)

SE COM ESTE Nº DE VÉRTICES FOR POSSÍVEL COBRIR $G = (V, E)$ I.E. VC RESPONDE SIM ENTÃO 3-SAT É SATISFATÍVEL, I.E. RESPONDE SIM E $\boxed{\text{VICE-VERSA}}$

EX: $U = \{u_1, u_2, u_3, u_4\}$



$C = \{\{u_1, \bar{u}_3, \bar{u}_4\}, \{\bar{u}_1, u_2, \bar{u}_4\}\}$

TEO: CONJUNTO INDEPENDENTE EM GRAFOS É NP-COMPLETO

(IS) $G=(V,E)$ V, E, INTEIRO $K>0$

IS $\in$ NP (S' | $|S'| \geq K$ É UM CERTIF.)

3-SAT α_{POLY} IS

$|S| \geq m$

PSPACE

+ PROBLEMAS PSPACE - COMPLETOS

$\boxed{\text{ACEITAÇÃO "IN-PLACE" POR UMA DTM}}$

INSTÂNCIA: UMA DTM M E UMA ENTRADA x.

PERGUNTA: M ACEITA x SEM NUNCA TER SUA "CABEÇA DE L/E" FORA DAS POSIÇÕES 1 a $|x|+1$?

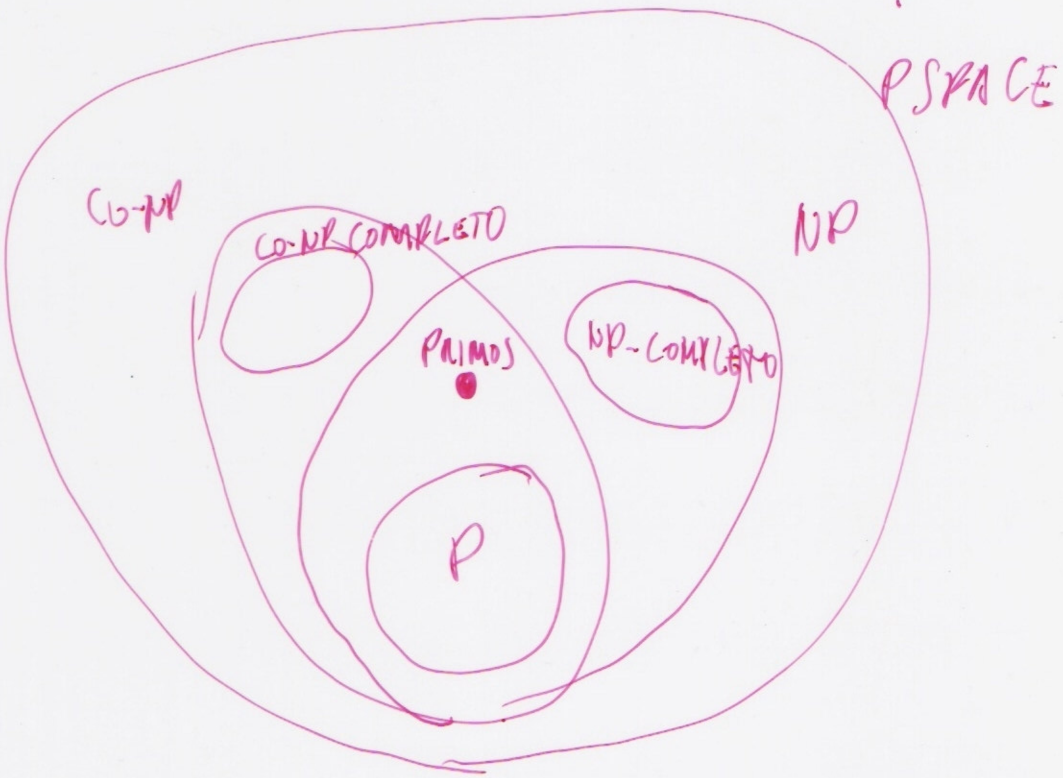
$\boxed{\text{JOGO DE GO}}$

INSTÂNCIA: TABULEIRO $n \times n$
CONFIGURAÇÃO DEPOIS DE $K < n^2$ JOGADAS
VEZ DO PRETO JOGAR (BRANCOS COMEÇAM

PERGUNTA: O PRETO GANHOU?

CO-NP

$$\text{CO-NP} = \{ \Sigma^* - L \mid L \in NP \}$$



PRIMOS:

INSTÂNCIA: UM NÚMERO INTEIRO p ($n = \log p$)

PERGUNTA: p É TAL QUE $\forall q > 1$ INTEIRO

$p \bmod q \neq 0$

PRIMOS $\in$ CO-NP

CERTIFICADO m E n T.Q. $m \cdot n = p$

PRIMOS $\in$ NP CHECAR $\exists\, r$ $1 < r < p$

T.Q. $r^{p-1} \equiv 1 \bmod p$ E $r^{\frac{p-1}{q}} \neq 1 \bmod p$

q UM DIVISOR PRIMO DE $p-1$

NP - DIFÍCIL (NP - HARD)

$\Pi \in$ NP - HARD $\iff \forall\, \Pi' \in NP$

$\Pi' \propto_{POLY} \Pi$

* PROBLEMAS QUE NÃO SE SABE SE ESTÁ EM NP

. CONFIABILIDADE DE REDE

INSTÂNCIA: $G = (V, E)$, $V' \subseteq V$,

PROBABILIDADE DE FALHA

$p(e)$, $0 \leq p(e) \leq 1$, $e \in E$

q RACIONAL $0 \leq q \leq 1$.

PERGUNTA: ASSUMINDO QUE AS PROBABILIDADES DOS LINKS (ARESTAS) SÃO INDEP.

A PROBABILIDADE DE QUE TODO PAR DE VÉRTICES EM V' SEJA LIGADO POR PELO MENOS UM CAMINHO SEM ARESTAS COM FALHA É MAIOR OU IGUAL A q?

NP - HARD OU NP - COMPLETO?

- PROBLEMAS NP-HARD

(PROBLEMAS DE OTIMIZAÇÃO CUJA VERSÃO DECISÃO ESTÁ EM NP-COMPLETO)

TSP VC

SCP ST

→ MINIMIZAÇÃO: SOLUÇÃO ÓTIMA Z^*

* O QUE É UM LIMITE SUPERIOR?

COMO SE OBTÉM A?

* O QUE É UM LIMITE INFERIOR?

O QUE É UMA RELAXAÇÃO?

COMO OBTER?